Hakowanie IoT i OT

Cele kształcenia

Internet przedmiotów (IoT) wyewoluował z konwergencji technologii bezprzewodowej, systemów mikroelektromechanicznych, mikrousług i Internetu. Rozwiązania IoT znajdują zastosowanie w różnych sektorach przemysłu, w tym w służbie zdrowia, zarządzaniu budynkami, rolnictwie, energetyce i transporcie. Wiele organizacji napędza transformację IoT. Urządzenia IoT, takie jak urządzenia ubieralne, urządzenia przemysłowe, połączone urządzenia elektroniczne, inteligentne sieci i inteligentne pojazdy, stają się częścią połączonych sieci. Urządzenia te generują ogromne ilości danych, które są gromadzone, analizowane, rejestrowane i przechowywane w sieciach. IoT wprowadziło szereg nowych technologii wraz z powiązanymi możliwościami do naszego codziennego życia. Ponieważ technologia IoT jest ewoluującą technologią, niedojrzałość technologii i usług dostarczanych przez różnych dostawców będzie miała szeroki wpływ na organizacje, prowadząc do złożonych problemów związanych z bezpieczeństwem. Bezpieczeństwo IoT jest trudne do zapewnienia, ponieważ urządzenia wykorzystują proste procesory i uproszczone systemy operacyjne, które mogą nie obsługiwać wyrafinowanych podejść do bezpieczeństwa. Organizacje używające tych urządzeń jako części swojej sieci muszą chronić zarówno urządzenia, jak i informacje przed atakującymi. Ponieważ przedsiębiorstwa przemysłowe cyfryzują swoje obiekty przemysłowe w celu zwiększenia wydajności operacyjnej poprzez łączność internetową i zdalny dostęp do danych, muszą w coraz większym stopniu koncentrować się na bezpieczeństwie cybernetycznym, aby łagodzić nowe zagrożenia i problemy związane z bezpieczeństwem wynikające z konwergencji technologii operacyjnych i informatycznych (OT-IT). Organizacje muszą zrozumieć krajobraz cyberzagrożeń, infrastruktury przemysłowej i biznesu. Przed wdrożeniem zasad i środków kontroli cyberbezpieczeństwa organizacje muszą zidentyfikować i ustalić priorytety kluczowych ryzyk i zagrożeń, które będą miały największy wpływ na ich działalność. Głównym celem tego modułu jest wyjaśnienie potencjalnych zagrożeń dla platform IoT i OT oraz przedstawienie wskazówek dotyczących zabezpieczania urządzeń IoT i infrastruktury OT przed zmieniającymi się zagrożeniami i atakami.

Koncepcje Internetu Rzeczy

IoT jest ważnym i pojawiającym się tematem w dziedzinie technologii, ekonomii i ogólnie społeczeństwa. Nazywa się to siecią połączonych urządzeń, która jest możliwa dzięki skrzyżowaniu komunikacji między maszynami i analiz dużych zbiorów danych. IoT to przyszłościowy rozwój Internetu i możliwości fizycznych urządzeń, które stopniowo zmniejszają przepaść między światem wirtualnym a fizycznym. Ta sekcja dotyczy niektórych ważnych koncepcji IoT, z którymi należy się zapoznać, aby zrozumieć zaawansowane tematy omówione w dalszej części tego modułu.

Co to jest Internet Rzeczy?

Internet przedmiotów (IoT), znany również jako Internet wszystkiego (IoE), odnosi się do urządzeń komputerowych z dostępem do sieci i możliwością wykrywania, gromadzenia i wysyłania danych za pomocą czujników oraz sprzętu komunikacyjnego i procesorów, które są osadzone w urządzeniu. W IoT „rzecz" odnosi się do urządzenia, które jest wszczepione w obiekt naturalny, stworzony przez człowieka lub maszynę i ma funkcję komunikowania się przez sieć. IoT wykorzystuje istniejącą, rozwijającą się technologię do wykrywania, tworzenia sieci i robotyki, umożliwiając w ten sposób użytkownikowi głębszą analizę, automatyzację i integrację w ramach systemu. Wraz ze wzrostem możliwości sieciowych maszyn i urządzeń codziennego użytku używanych w różnych sektorach, takich jak biura, domy, przemysł, transport, budynki i urządzenia do noszenia, otwierają one świat możliwości poprawy biznesu i zadowolenia klientów. Niektóre z kluczowych cech IoT to łączność, czujniki, sztuczna inteligencja, małe urządzenia i aktywne zaangażowanie.

Jak działa Internet Rzeczy

Technologia IoT obejmuje cztery podstawowe systemy: urządzenia IoT, systemy bramek, systemy przechowywania danych wykorzystujące technologię chmury oraz zdalne sterowanie za pomocą aplikacji mobilnych. Systemy te razem umożliwiają komunikację między dwoma punktami końcowymi. Poniżej omówiono niektóre z ważnych elementów technologii IoT, które odgrywają istotną rolę w funkcjonowaniu urządzenia IoT:

Technologia wykrywania: Czujniki wbudowane w urządzenia wykrywają szeroką gamę informacji z otoczenia, w tym temperaturę, gazy, lokalizację, działanie niektórych maszyn przemysłowych lub dane dotyczące zdrowia pacjenta.

Bramy IoT: Bramy służą do wypełnienia luki między urządzeniem IoT (sieć wewnętrzna) a użytkownikiem końcowym (sieć zewnętrzna), umożliwiając im w ten sposób łączenie się i komunikację między sobą. Dane zebrane przez czujniki w urządzeniu IoT są wysyłane do połączonego użytkownika lub chmury przez bramkę.

Serwer Cloud/Data Storage: Po przejściu przez bramkę zebrane dane docierają do chmury, gdzie są przechowywane i poddawane analizie danych. Przetworzone dane są następnie przekazywane użytkownikowi, który na podstawie otrzymanych informacji może podjąć określone działania.

Zdalne sterowanie za pomocą aplikacji mobilnej: użytkownik końcowy korzysta ze zdalnych elementów sterujących, takich jak telefony komórkowe, tablety, laptopy itp. z zainstalowaną aplikacją mobilną, aby monitorować, kontrolować, pobierać dane i podejmować określone działania na urządzeniach IoT ze zdalnej lokalizacji.

Przykład:

1. Inteligentny system bezpieczeństwa zainstalowany w domu zostanie zintegrowany z bramką, która z kolei pomoże połączyć urządzenie z Internetem i infrastrukturą chmurową.

2. Dane przechowywane w chmurze zawierają informacje o każdym urządzeniu podłączonym do sieci. Informacje te obejmują identyfikator urządzenia oraz aktualny stan urządzenia, a także informacje o tym, kto i ile razy uzyskał dostęp do urządzenia. Zawiera również informacje, takie jak czas wcześniejszego uzyskiwania dostępu do urządzenia.

3. Połączenie z serwerem w chmurze nawiązywane jest za pośrednictwem usług sieciowych.

4. Użytkownik po drugiej stronie, który na swoim telefonie komórkowym posiada wymaganą aplikację umożliwiającą zdalny dostęp do urządzenia, wchodzi z nim w interakcję, co z kolei umożliwia mu interakcję z urządzeniem w domu. Przed uzyskaniem dostępu do urządzenia jest proszony o uwierzytelnienie. Jeśli przesłane przez niego poświadczenia odpowiadają poświadczeniom zapisanym w chmurze, uzyskuje dostęp. W przeciwnym razie jego dostęp jest zabroniony, co zapewnia bezpieczeństwo. Serwer w chmurze identyfikuje identyfikator urządzenia i wysyła żądanie powiązane z tym urządzeniem za pomocą bramek.

5. System bezpieczeństwa, który aktualnie rejestruje materiał w domu, jeśli wykryje jakąkolwiek nietypową aktywność, następnie wysyła alert do chmury przez bramkę, który odpowiada identyfikatorowi urządzenia i powiązanemu z nim użytkownikowi, a na końcu- użytkownik otrzymuje alert.

Architektura IoT

Architektura IoT obejmuje kilka warstw, od warstwy aplikacji na górze do warstwy Edge Technology na dole. Warstwy te są zaprojektowane w taki sposób, aby mogły sprostać wymaganiom różnych sektorów, w tym społeczeństw, przemysłu, przedsiębiorstw, rządów itp. Poniżej przedstawiono funkcje, jakie pełni każda warstwa w architekturze:

Warstwa technologii brzegowej

Ta warstwa składa się ze wszystkich komponentów sprzętowych, w tym czujników, tagów identyfikacji radiowej (RFID), czytników lub innych miękkich czujników oraz samego urządzenia. Podmioty te są podstawową częścią czujników danych, które są rozmieszczone w terenie do monitorowania lub wykrywania różnych zjawisk. Warstwa ta odgrywa ważną rolę w gromadzeniu danych oraz łączeniu urządzeń w sieci i z serwerem.

Dostęp do warstwy bramy

Ta warstwa pomaga wypełnić lukę między dwoma punktami końcowymi, takimi jak urządzenie i klient. W tej warstwie odbywa się również wstępna obsługa danych. W tej warstwie odbywa się kierowanie wiadomości, identyfikacja wiadomości i subskrypcja.

Warstwa internetowa

Jest to kluczowa warstwa, ponieważ służy jako główny element komunikacji między dwoma punktami końcowymi, takimi jak urządzenie-urządzenie, urządzenie-chmura, urządzenie-brama lub udostępnianie danych zaplecza.

Warstwa oprogramowania pośredniego

Jest to jedna z najbardziej krytycznych warstw, która działa w trybie dwukierunkowym. Jak sama nazwa wskazuje, ta warstwa znajduje się pośrodku warstwy aplikacji i warstwy sprzętowej, zachowując się w ten sposób jako interfejs między tymi dwiema warstwami. Odpowiada za ważne funkcje, takie jak zarządzanie danymi, zarządzanie urządzeniami i różne kwestie, takie jak analiza danych, agregacja danych, filtrowanie danych, wykrywanie informacji o urządzeniach i kontrola dostępu.

Warstwa aplikacji

Ta warstwa, umieszczona na szczycie stosu, odpowiada za dostarczanie usług odpowiednim użytkownikom z różnych sektorów, w tym budownictwa, przemysłu, produkcji, motoryzacji, bezpieczeństwa, opieki zdrowotnej itp.

Obszary zastosowań i urządzenia IoT

Urządzenia IoT mają szeroki zakres zastosowań. Są stosowane w prawie każdym sektorze społeczeństwa, pomagając na różne sposoby uprościć rutynową pracę i zadania osobiste, a tym samym poprawić standard życia. Technologia IoT znajduje zastosowanie w inteligentnych domach i budynkach, urządzeniach opieki zdrowotnej, urządzeniach przemysłowych, transporcie, urządzeniach zabezpieczających, sektorze handlu detalicznego itp.

Oto niektóre zastosowania urządzeń IoT:

Inteligentne urządzenia podłączone do Internetu, świadczące różne usługi użytkownikom końcowym, obejmują termostaty, systemy oświetleniowe i systemy bezpieczeństwa oraz kilka innych systemów znajdujących się w budynkach.

W sektorach opieki zdrowotnej i nauk przyrodniczych urządzenia obejmują urządzenia do noszenia, urządzenia do monitorowania stanu zdrowia, takie jak wszczepione rozruszniki serca, EKG, EKG, sprzęt chirurgiczny, telemedycyna itp.

Przemysłowy Internet Rzeczy (IIoT) przyciąga wzrost poprzez trzy podejścia: zwiększenie produkcji w celu zwiększenia przychodów, wykorzystanie inteligentnej technologii, która całkowicie zmienia sposób wytwarzania towarów, oraz tworzenie nowych hybrydowych modeli biznesowych.

Podobnie wykorzystanie technologii IoT w sektorze transportowym jest zgodne z koncepcją komunikacji pojazd-pojazd, pojazd-pobocze i pojazd-pieszy, poprawiając w ten sposób warunki ruchu, systemy nawigacji i schematy parkowania.

LoT w handlu detalicznym jest używany głównie w płatnościach, reklamach oraz śledzeniu lub monitorowaniu produktów w celu ochrony ich przed kradzieżą i utratą, zwiększając w ten sposób przychody.

W informatyce i sieciach urządzenia IoT obejmują głównie różne urządzenia biurowe, takie jak drukarki, faksy i kserokopiarki, a także systemy monitoringu PBX; służą one poprawie komunikacji między punktami końcowymi i zapewniają łatwość przesyłania danych na duże odległości.

Technologie i protokoły IoT

IoT obejmuje szeroki zakres nowych technologii i umiejętności. Wyzwaniem w przestrzeni IoT jest niedojrzałość technologii wraz z powiązanymi usługami oraz niedojrzałość dostawców, którzy je dostarczają. Stanowi to kluczowe wyzwanie dla organizacji wykorzystujących IoT. Aby zapewnić pomyślną komunikację między dwoma punktami końcowymi, IoT implementuje przede wszystkim protokoły standardowe i sieciowe. Główne technologie i protokoły komunikacyjne w odniesieniu do zasięgu między źródłem a miejscem docelowym są następujące:

Komunikacja bezprzewodowa krótkiego zasięgu

Bluetooth Low Energy (BLE): BLE lub Bluetooth Smart to bezprzewodowa sieć osobista. Ta technologia jest przeznaczona do stosowania w różnych sektorach, takich jak opieka zdrowotna, bezpieczeństwo, rozrywka i fitness.

Light-Fidelity (Li-Fi): Li-Fi jest jak Wi-Fi z tylko dwiema różnicami: trybem komunikacji i szybkością. Li-Fi to system komunikacji w świetle widzialnym (VLC), który wykorzystuje zwykłe domowe żarówki do przesyłania danych z bardzo dużą prędkością 224 Gb/s.

Near-Field Communication (NFC): NFC to rodzaj komunikacji krótkiego zasięgu, który wykorzystuje indukcję pola magnetycznego, aby umożliwić komunikację między dwoma urządzeniami elektronicznymi. Stosowany jest przede wszystkim w bezdotykowych płatnościach mobilnych, portalach społecznościowych oraz identyfikacji dokumentów lub innych produktów.

Kody QR i kody kreskowe: Te kody to etykiety do odczytu maszynowego, które zawierają informacje o produkcie lub elemencie, do którego są dołączone. Kod szybkiej odpowiedzi lub kod QR to dwuwymiarowy kod przechowujący informacje o produkcie, który można zeskanować za pomocą smartfonów, podczas gdy kod kreskowy występuje zarówno w formie jednowymiarowej (ID), jak i dwuwymiarowej (2D).

Identyfikacja częstotliwości radiowej (RFID): RFID przechowuje dane w znacznikach, które są odczytywane za pomocą pól elektromagnetycznych. RFID jest używany w wielu sektorach, w tym w przemyśle, biurach, firmach, samochodach, farmaceutykach, zwierzętach gospodarskich i zwierzętach domowych.

Wątek: Wątek to protokół sieciowy oparty na protokole IPv6 dla urządzeń IoT. Jego głównym celem jest automatyka domowa, aby urządzenia mogły komunikować się ze sobą w lokalnych sieciach bezprzewodowych.

Wi-Fi: Wi-Fi to technologia szeroko stosowana w bezprzewodowych sieciach lokalnych (LAN). Obecnie najpopularniejszym standardem Wi-Fi stosowanym w domach lub firmach jest 802.lln, który oferuje maksymalną prędkość 600 Mb/s i zasięg około 50 m.

Wi-Fi Direct: Służy do komunikacji peer-to-peer bez potrzeby korzystania z bezprzewodowego punktu dostępowego. Urządzenia Wi-Fi direct rozpoczynają komunikację dopiero po podjęciu decyzji, które urządzenie będzie pełnić rolę punktu dostępowego.

Z-Wave: Z-Wave to komunikacja o niskim poborze mocy i krótkim zasięgu, przeznaczona głównie do automatyki domowej. Zapewnia prosty i niezawodny sposób bezprzewodowego monitorowania i sterowania urządzeniami domowymi takimi jak FIVAC, termostaty, garaże, kina domowe itp.

Zig-Bee: To kolejny protokół komunikacyjny krótkiego zasięgu oparty na standardzie IEEE 203.15.4. Zig-Bee jest używany w urządzeniach, które rzadko przesyłają dane z małą szybkością na ograniczonym obszarze iw zasięgu 10-100 m.

ANT: Adaptive Network Topology (ANT) to bezprzewodowa technologia sieci czujników multiemisji używana głównie do komunikacji krótkiego zasięgu między urządzeniami związanymi z czujnikami sportowymi i fitness.

Komunikacja bezprzewodowa średniego zasięgu

FlaLow: To kolejny wariant standardu Wi-Fi; zapewnia rozszerzony zasięg, dzięki czemu jest przydatny do komunikacji na obszarach wiejskich. Oferuje niskie szybkości transmisji danych, zmniejszając w ten sposób moc i koszty transmisji.

LTE-Advanced: LTE-Advanced to standard komunikacji mobilnej, który zapewnia udoskonalenie LTE, koncentrując się na zapewnieniu większej przepustowości pod względem szybkości transmisji danych, rozszerzonego zasięgu, wydajności i wydajności.

6L0WPAN: IPv6 over Low-Power Wireless Personal Area Networks (6L0WPAN) to protokół internetowy używany do komunikacji między mniejszymi i energooszczędnymi urządzeniami o ograniczonej zdolności przetwarzania, takimi jak różne urządzenia IoT.

QUIC: Szybkie połączenia internetowe UDP (QUIC) to multipleksowane połączenia między urządzeniami IoT za pośrednictwem protokołu User Datagram Protocol (UDP); zapewniają bezpieczeństwo równoważne z SSL/TLS.

Komunikacja bezprzewodowa dalekiego zasięgu

LPWAN: Low Power Wide Area Networking (LPWAN) to bezprzewodowa sieć telekomunikacyjna zaprojektowana w celu zapewniania komunikacji na duże odległości między dwoma punktami końcowymi. Dostępne protokoły i technologie LPWAN obejmują:

LoRaWAN: Sieć rozległa dalekiego zasięgu (LoRaWAN) jest używana do obsługi aplikacji takich jak mobilna, przemysłowa maszyna-maszyna oraz do bezpiecznej komunikacji dwukierunkowej dla urządzeń IoT, inteligentnych miast i aplikacji związanych z opieką zdrowotną.

Sigfox: jest używany w urządzeniach, które mają krótką żywotność baterii i muszą przesyłać ograniczoną ilość danych.

Neul: jest używany w niewielkiej części widma białej przestrzeni telewizyjnej w celu dostarczania wysokiej jakości, dużej mocy, dużego zasięgu i tanich sieci.

Very Small Aperture Terminal (VSAT): VSAT jest protokołem komunikacyjnym używanym do przesyłania danych za pomocą małych anten talerzowych zarówno dla danych szerokopasmowych, jak i wąskopasmowych.

Komórkowy: Komórkowy to rodzaj protokołu komunikacyjnego, który jest używany do komunikacji na większą odległość. Służy do wysyłania danych wysokiej jakości, ale ma wady związane z wysoką ceną i wysokim zużyciem energii.

MQTT: Message Queuing Telemetry Transport (MQTT) to lekki protokół zgodny ze standardem ISO, używany do przesyłania wiadomości w komunikacji bezprzewodowej dalekiego zasięgu. Pomaga w nawiązywaniu połączeń z odległymi lokalizacjami, na przykład za pośrednictwem łączy satelitarnych.

NB-IoT: Narrowband IoT (NB-IoT) to wariant LoRaWAN i Sigfox, który wykorzystuje udoskonaloną technologię warstwy fizycznej i widmo używane do komunikacji maszyna-maszyna.

Komunikacja przewodowa

Ethernet: Ethernet jest obecnie najczęściej używanym typem protokołu sieciowego. Jest to rodzaj sieci LAN (Local Area Network), która składa się z przewodowego połączenia między komputerami w małym budynku, biurze lub kampusie.

Multimedia over Coax Alliance (MoCA): MoCA to rodzaj protokołu sieciowego, który zapewnia wideo w wysokiej rozdzielczości i powiązane treści do domów za pośrednictwem istniejących kabli koncentrycznych.

Komunikacja Power-Line (PLC): Jest to rodzaj protokołu, który wykorzystuje przewody elektryczne do przesyłania mocy i danych z jednego punktu końcowego do drugiego. PLC jest wymagany do zastosowań w różnych obszarach, takich jak automatyka domowa, urządzenia przemysłowe i szerokopasmowe łącza energetyczne (BPL).

Systemy operacyjne LOT

Urządzenia IoT składają się zarówno z komponentów sprzętowych, jak i programowych. Komponenty sprzętowe obejmują urządzenia końcowe i bramy, podczas gdy komponenty programowe obejmują systemy operacyjne. Ze względu na wzrost produkcji komponentów sprzętowych (bramki, węzły czujnikowe itp.) tradycyjne urządzenia IoT, które wcześniej działały bez systemu operacyjnego, zaczęły przyjmować nowe implementacje systemu operacyjnego zaprogramowane specjalnie dla urządzeń IoT. Te systemy operacyjne zapewniają urządzeniom łączność, użyteczność i interoperacyjność. Poniżej podano niektóre systemy operacyjne używane przez urządzenia IoT:

Windows 10 IoT: To rodzina systemów operacyjnych opracowanych przez firmę Microsoft dla systemów wbudowanych.

Amazon FreeRTOS: Jest to darmowy system operacyjny typu open source używany w mikrokontrolerach IoT, który ułatwia wdrażanie, zabezpieczanie, podłączanie i zarządzanie urządzeniami brzegowymi o niskim poborze mocy, zasilanymi bateryjnie.

Contiki: Jest używany w urządzeniach bezprzewodowych o małej mocy, takich jak oświetlenie uliczne, systemy monitorowania dźwięku itp.

Fuchsia: Jest to system operacyjny typu open source opracowany przez Google dla różnych platform, takich jak systemy wbudowane, smartfony, tablety itp.

RIOT: wymaga mniej zasobów i efektywnie wykorzystuje energię. Ma możliwość działania na systemach wbudowanych, płytach wykonawczych, czujnikach itp.

Ubuntu Core: znany również jako Snappy, jest używany w robotach, dronach, bramkach brzegowych itp.

ARM Mbed OS: jest używany głównie w przypadku urządzeń o niskim poborze mocy, takich jak urządzenia do noszenia.

Zephyr: jest używany w urządzeniach o niskim poborze mocy i ograniczonych zasobach.

Embedded Linux: jest używany ze wszystkimi małymi, średnimi i dużymi systemami wbudowanymi.

NuttX RTOS: Jest to system operacyjny typu open source opracowany głównie do obsługi 8-bitowych i 32-bitowych mikrokontrolerów systemów wbudowanych.

Integrity RTOS: Stosowany głównie w sektorach lotniczym lub obronnym, przemysłowym, motoryzacyjnym i medycznym.

Apache Mynewt: Obsługuje urządzenia działające na protokole BLE.

Protokoły aplikacji IoT

CoAP: Constrained Application Protocol (CoAP) to protokół przesyłania sieciowego używany do przesyłania wiadomości między węzłami z ograniczeniami a sieciami IoT. Ten protokół jest używany głównie w aplikacjach machine-to-machine (M2M), takich jak automatyzacja budynków i inteligentna energia.

Edge: Edge computing pomaga środowisku IoT przenieść przetwarzanie obliczeniowe na brzeg sieci, umożliwiając inteligentnym urządzeniom i bramom wykonywanie zadań i usług z poziomu chmury. Przeniesienie usług obliczeniowych na obrzeża sieci poprawia buforowanie treści, dostarczanie, przechowywanie i zarządzanie IoT.

LWM2M: Lightweight Machine-to-Machine (LWM2M) to protokół komunikacyjny warstwy aplikacji używany do komunikacji na poziomie aplikacji między urządzeniami IoT; służy do zarządzania urządzeniami IoT.

Sieć fizyczna: Sieć fizyczna to technologia umożliwiająca szybszą i bezproblemową interakcję z pobliskimi urządzeniami LoT. Ujawnia listę adresów URL nadawanych przez pobliskie urządzenia z sygnałami nawigacyjnymi BLE.

XMPP: extensible Messaging and Presence Protocol (XMPP) to otwarta technologia komunikacji w czasie rzeczywistym, używana w urządzeniach IoT. Ta technologia jest wykorzystywana do tworzenia interoperacyjnych urządzeń, aplikacji i usług dla środowiska IoT.

Mihini/M3DA: Mihini/M3DA to oprogramowanie służące do komunikacji między serwerem M2M a aplikacjami działającymi na wbudowanej bramie. Pozwala aplikacjom IoT na wymianę danych i poleceń z serwerem M2M.

Modele komunikacji IoT

Technologia IoT wykorzystuje różne techniczne modele komunikacji, z których każdy ma swoje własne cechy. Modele te podkreślają elastyczność, z jaką urządzenia IoT mogą komunikować się ze sobą lub z klientem. Poniżej omówiono cztery modele komunikacji i kluczowe cechy związane z każdym modelem:

Model komunikacji urządzenie-urządzenie

W tego typu komunikacji połączone ze sobą urządzenia komunikują się ze sobą za pośrednictwem Internetu, jednak w przeważającej mierze wykorzystują protokoły takie jak ZigBee, Z-Wave czy Bluetooth. Komunikacja między urządzeniami jest najczęściej stosowana w urządzeniach inteligentnego domu, takich jak termostaty, żarówki, zamki do drzwi, kamery CCTV i lodówki, które przesyłają między sobą małe pakiety danych z niską szybkością transmisji danych. Model ten jest również popularny w komunikacji między urządzeniami ubieralnymi. Na przykład urządzenie EKG/EKG przymocowane do ciała pacjenta zostanie sparowane z jego smartfonem i wyśle mu powiadomienia w sytuacji zagrożenia.

Model komunikacji urządzenie-chmura

W tego rodzaju komunikacji urządzenia komunikują się bezpośrednio z chmurą, zamiast bezpośrednio komunikować się z klientem w celu wysyłania lub odbierania danych lub poleceń. Korzysta z protokołów

komunikacyjnych, takich jak Wi-Fi lub Ethernet, a czasem także z sieci komórkowej. Przykładem komunikacji urządzenie-chmura opartej na Wi-Fi jest kamera CCTV, do której można uzyskać zdalny dostęp na smartfonie. W tym scenariuszu urządzenie (tutaj kamera CCTV) nie może bezpośrednio komunikować się z klientem; raczej najpierw wysyła dane do chmury, a następnie, jeśli klient wprowadzi prawidłowe dane uwierzytelniające, uzyska dostęp do chmury, co z kolei umożliwi mu dostęp do urządzenia w domu.

Model komunikacji urządzenie-brama

W modelu komunikacji device-to-gateway urządzenie IoT komunikuje się z urządzeniem pośredniczącym zwanym bramą, które z kolei komunikuje się z usługą w chmurze. Tym urządzeniem bramowym może być smartfon lub koncentrator działający jako punkt pośredni, który zapewnia również funkcje bezpieczeństwa oraz translację danych lub protokołów. Protokoły powszechnie używane w tym trybie komunikacji to ZigBee i Z-Wave. Jeśli bramą warstwy aplikacji jest smartfon, to może przybrać formę aplikacji, która wchodzi w interakcję z urządzeniem IoT i chmurą. To urządzenie może być inteligentnym telewizorem, który łączy się z usługą w chmurze za pośrednictwem aplikacji na telefon komórkowy.

Model komunikacji udostępniania danych zaplecza

Ten rodzaj modelu komunikacji rozszerza typ komunikacji urządzenie-chmura, tak że dostęp do danych z urządzeń IoT mogą uzyskać upoważnione osoby trzecie. Tutaj urządzenia przesyłają swoje dane do chmury, do której później uzyskują dostęp lub analizują strony trzecie. Przykładem takiego modelu może być analizator rocznego lub miesięcznego zużycia energii w firmie. Później analiza może zostać wykorzystana do zmniejszenia wydatków firmy na energię poprzez przestrzeganie pewnych zasad gromadzenia lub oszczędzania energii.

Wyzwania Internetu Rzeczy

Technologia IoT rozwija się tak szybko, że stała się wszechobecna. Dzięki licznym aplikacjom i funkcjom, ale brakowi podstawowych zasad bezpieczeństwa, urządzenia IoT są obecnie łatwym łupem dla hakerów. Ponadto aktualizacje urządzeń IoT wprowadziły nowe luki w zabezpieczeniach, które mogą być łatwo wykorzystane przez hakerów. Aby przezwyciężyć ten istotny problem, firmy produkcyjne powinny traktować bezpieczeństwo jako najwyższy priorytet, począwszy od planowania i projektowania, a skończywszy na wdrażaniu, wdrażaniu, zarządzaniu i konserwacji. Poniżej omówiono niektóre wyzwania stojące przed urządzeniami IoT, które czynią je podatnymi na zagrożenia:

Brak bezpieczeństwa i prywatności: Większość dzisiejszych urządzeń IoT, takich jak urządzenia gospodarstwa domowego, urządzenia przemysłowe, urządzenia medyczne, samochody itp., jest podłączona do Internetu i zawiera ważne i poufne dane. Urządzenia te nie mają nawet podstawowych zasad bezpieczeństwa i prywatności, a hakerzy mogą to wykorzystać do przeprowadzenia złośliwych działań.

Wrażliwe interfejsy sieciowe: wiele urządzeń IoT jest wyposażonych w technologię wbudowanego serwera sieciowego, co czyni je podatnymi na ataki.

Kwestie prawne, regulacyjne i związane z prawami: Ze względu na wzajemne połączenie urządzeń IoT pojawiają się pewne problemy z bezpieczeństwem, ponieważ nie istnieją przepisy regulujące te kwestie.

Domyślne, słabe i zakodowane na stałe dane uwierzytelniające: Jedną z najczęstszych przyczyn cyberataków na urządzenia IoT są ich systemy uwierzytelniania. Urządzenia te są zwykle dostarczane z domyślnymi i słabymi danymi uwierzytelniającymi, które haker może łatwo wykorzystać w celu uzyskania nieautoryzowanego dostępu do urządzeń.

Protokoły zwykłego tekstu i niepotrzebne otwarte porty: urządzeniom IoT brakuje technik szyfrowania podczas transmisji danych, co czasami powoduje, że używają pewnych protokołów, które oprócz otwartych portów przesyłają dane w postaci zwykłego tekstu.

Błędy kodowania (przepełnienie bufora): Większość dzisiejszych urządzeń IoT ma wbudowane usługi sieciowe, które są narażone na te same luki w zabezpieczeniach, które są powszechnie wykorzystywane na platformach usług sieciowych. W rezultacie aktualizacja takiej funkcjonalności może spowodować problemy, takie jak przepełnienie bufora, wstrzyknięcie kodu SQL itp. w infrastrukturze technologicznej.

Problemy z pamięcią masową: urządzenia IoT zazwyczaj mają mniejszą pojemność do przechowywania danych, ale dane gromadzone i przesyłane przez te urządzenia są nieograniczone. Dlatego powoduje to problemy z przechowywaniem, zarządzaniem i ochroną danych.

Trudne do zaktualizowania oprogramowanie układowe i system operacyjny: Aktualizacja oprogramowania układowego jest niezbędnym krokiem w kierunku przeciwdziałania lukom w zabezpieczeniach urządzenia, ale może pogorszyć funkcjonalność urządzenia. Z tego powodu programiści lub producenci mogą wahać się, a nawet odmówić wsparcia produktu lub wprowadzenia zmian w fazie opracowywania swoich produktów.

Kwestie standardu interoperacyjności: Jedną z największych przeszkód dla urządzeń IoT jest kwestia interoperacyjności, która jest kluczem do rentowności i długoterminowego wzrostu całego ekosystemu IoT. Problemy wynikające z braku interoperacyjności urządzeń IoT to niezdolność producentów do testowania interfejsów programowania aplikacji (API) przy użyciu wspólnych metod i mechanizmów, niemożność zabezpieczenia urządzeń za pomocą oprogramowania stron trzecich oraz niezdolność do zarządzania urządzeniami i monitorowania ich przy użyciu wspólnej warstwy.

Fizyczna kradzież i manipulacja: Fizyczne ataki na urządzenia IoT obejmują manipulowanie urządzeniami w celu wstrzyknięcia złośliwego kodu lub plików, aby urządzenia działały zgodnie z zamierzeniami atakującego, lub dokonywanie modyfikacji sprzętowych urządzeń. Podrabianie urządzeń może również stanowić problem, gdy nie ma odpowiedniej ochrony fizycznej chroniącej urządzenia.

Brak wsparcia dostawcy w celu usunięcia luk w zabezpieczeniach: oprogramowanie układowe urządzeń musi zostać zaktualizowane, aby chronić urządzenia przed pewnymi lukami w zabezpieczeniach, ale dostawcy wahają się lub zwykle odmawiają uzyskania dostępu do swoich urządzeń przez osoby trzecie.

Pojawiające się problemy gospodarcze i rozwojowe: Dzięki szerokim możliwościom urządzeń IoT w każdej dziedzinie, decydenci mają do czynienia z wieloma warstwami złożoności. Nowy krajobraz wprowadzony przez te urządzenia dodaje nowy wymiar decydentom, którzy muszą zaprojektować nowe plany i zasady dla urządzeń IoT.

Obsługa danych nieustrukturyzowanych: wzrost liczby podłączonych urządzeń zwiększy złożoność obsługi danych nieustrukturyzowanych wraz ze wzrostem ich objętości, szybkości i różnorodności. Ważne jest, aby organizacje rozumiały i określały, które dane są wartościowe i możliwe do zastosowania.

Zagrożenie kontra szansa

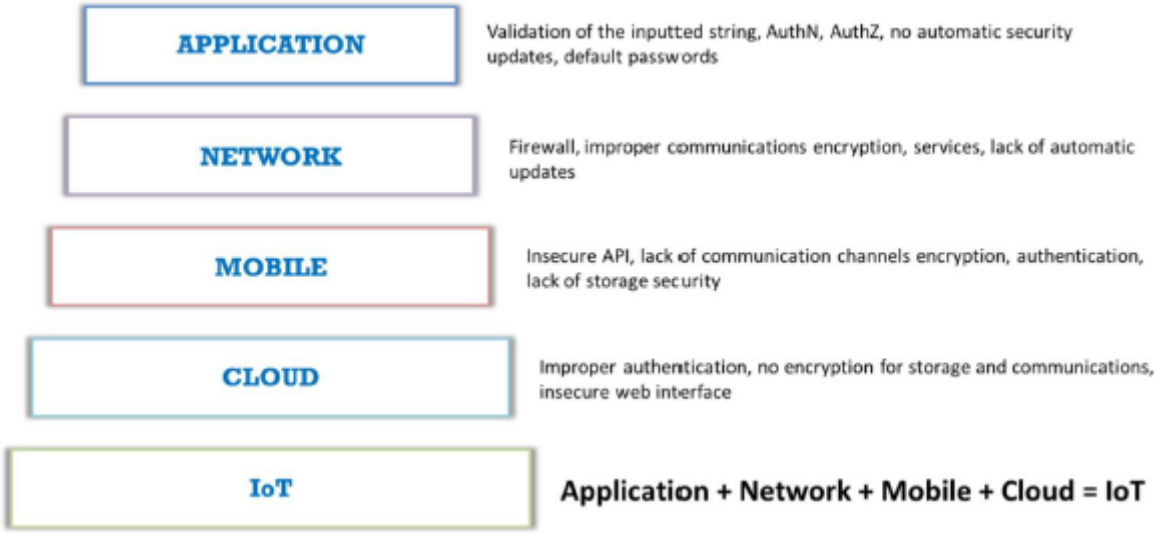
W przypadku NIEWŁAŚCIWEJ KONFIGURACJI i ŹLE POJĘCIA, IoT stwarza bezprecedensowe zagrożenie dla danych osobowych, prywatności i bezpieczeństwa. ZATRZYMANY i CHRONIONY, IoT może zwiększyć transmisję, komunikację, świadczenie usług i standard życia. Zagrożenia dla IoT można podzielić na trzy podstawowe kategorie: Bezpieczeństwo, Prywatność i Bezpieczeństwo. Wszystkie te kategorie są ze sobą powiązane, ponieważ dotyczą tego samego urządzenia i jego łączności. Znaczenie tych kategorii jest oczywiste, ponieważ urządzenia IoT szybko stają się bardziej wszechobecne w naszym życiu niż smartfony i będą miały dostęp do najbardziej poufnych lub wrażliwych informacji osobowych, takich jak dokumentacja medyczna, dokumentacja finansowa czy numery ubezpieczenia społecznego. Na przykład, jeśli chodzi o smartfony lub tablety, istnieje tylko kilka obaw w tych obszarach, podczas gdy jeśli posiadamy jakiekolwiek urządzenie IoT, obawy szybko się mnożą. Dlatego biorąc pod uwagę, do czego IoT może uzyskać dostęp, bezpieczeństwo, prywatność i bezpieczeństwo mają ogromne znaczenie. Jeśli te trzy kategorie zagrożeń zostaną potraktowane priorytetowo i zastosowany

zostanie szereg wymaganych technik w celu przezwyciężenia tych problemów, zaowocuje to ulepszoną i bezpieczną komunikacją między dwoma punktami końcowymi, mniejszą liczbą cyberataków na urządzenia i lepszym doświadczeniem użytkownika; ponadto będzie to również Ataki IoT

Atakujący stosują różne techniki przeprowadzania ataków na docelowe urządzenia lub sieci IoT. W tej sekcji omówiono najważniejsze zagrożenia IoT w odniesieniu do podstawowych typów wektorów i technik ataków IoT, w tym rozproszonych ataków typu „odmowa usługi" (DDoS), ataków na systemy HVAC, ataków typu Rolling Code, ataków BlueBorne i ataków zagłuszających.

Problemy z bezpieczeństwem IoT

Potencjalne luki w systemie IoT mogą spowodować poważne problemy dla organizacji. Większość urządzeń IoT ma problemy z bezpieczeństwem, takie jak brak odpowiedniego mechanizmu uwierzytelniania lub użycie domyślnych danych uwierzytelniających, brak mechanizmu blokady, brak silnego schematu szyfrowania, brak odpowiednich systemów zarządzania kluczami i niewłaściwe zabezpieczenia fizyczne. Poniżej przedstawiono niektóre problemy związane z bezpieczeństwem w każdej warstwie architektury IoT:



OWASP 10 największych zagrożeń IoT

Poniżej wymieniono 10 największych zagrożeń IoT według projektu Open Web Application Security Project (OWASP):

Słabe, łatwe do odgadnięcia lub zakodowane na stałe hasła

Używanie słabych, możliwych do odgadnięcia lub zakodowanych na stałe haseł umożliwia ustalenie publicznie dostępnych lub niezmiennych danych uwierzytelniających za pomocą brutalnego wymuszenia. Obejmuje to również backdoory w oprogramowaniu układowym lub oprogramowaniu klienckim, które prowadzą do nieautoryzowanego dostępu do wdrożonych urządzeń.

Niebezpieczne usługi sieciowe

Niezabezpieczone usługi sieciowe są podatne na różne ataki, takie jak ataki z przepełnieniem bufora, które powodują scenariusz odmowy usługi, pozostawiając urządzenie niedostępne dla użytkownika. Osoba atakująca używa różnych zautomatyzowanych narzędzi, takich jak skanery portów i fuzzery, w celu wykrycia otwartych portów i wykorzystania ich w celu uzyskania nieautoryzowanego dostępu do usług. Te niezabezpieczone usługi

sieciowe, które są dostępne w Internecie, mogą naruszyć poufność, autentyczność, integralność lub dostępność informacji, a także umożliwiają zdalny dostęp do krytycznych informacji.

Niebezpieczne interfejsy ekosystemów

Niezabezpieczone interfejsy ekosystemów, takie jak interfejsy WWW, interfejsy API zaplecza, urządzenia mobilne i interfejsy w chmurze poza urządzeniem, prowadzą do naruszenia bezpieczeństwa urządzenia i jego komponentów. Typowe luki w takich interfejsach obejmują brak uwierzytelniania/autoryzacji, brak szyfrowania lub słabe szyfrowanie oraz brak filtrowania wejścia/wyjścia.

Brak mechanizmów bezpiecznej aktualizacji

Brak bezpiecznych mechanizmów aktualizacji, takich jak brak weryfikacji firmware na urządzeniu, brak bezpiecznego dostarczania, brak mechanizmów anti-rollback czy brak powiadomień o zmianach w zabezpieczeniach, może zostać wykorzystany do przeprowadzenia różnych ataków.

Korzystanie z niezabezpieczonych lub przestarzałych składników

Korzystanie z przestarzałych lub starszych wersji komponentów oprogramowania lub bibliotek, takie jak niezabezpieczone dostosowywanie platform systemu operacyjnego lub korzystanie ze sprzętu lub komponentów oprogramowania innych firm z zagrożonego łańcucha dostaw, może umożliwić narażenie samych urządzeń.

Niewystarczająca ochrona prywatności

Niewystarczająca ochrona prywatności pozwala na naruszenie danych osobowych użytkownika przechowywanych na urządzeniach lub w ekosystemie.

Niebezpieczny transfer i przechowywanie danych

Brak szyfrowania i kontroli dostępu do przesyłanych lub przechowywanych danych może skutkować wyciekiem poufnych informacji do złośliwych użytkowników.

Brak zarządzania urządzeniami

Brak odpowiedniego wsparcia bezpieczeństwa poprzez zarządzanie urządzeniami na urządzeniach wdrożonych w produkcji, w tym zarządzanie zasobami, zarządzanie aktualizacjami, bezpieczne wycofanie z eksploatacji, monitorowanie systemu i możliwości reagowania, może otworzyć drzwi do różnych ataków.

Niebezpieczne ustawienia domyślne

Niepewne lub niewystarczające ustawienia urządzenia uniemożliwiają operatorom modyfikowanie konfiguracji w celu zwiększenia bezpieczeństwa urządzenia.

Brak hartowania fizycznego

Brak fizycznych zabezpieczeń umożliwia potencjalnym atakującym zdobycie poufnych informacji, które pomogą im w przeprowadzeniu zdalnego ataku lub uzyskaniu lokalnej kontroli nad urządzeniem.

Obszary ataków OWASP IoT

Poniżej przedstawiono obszary ataków OWASP IoT:

Powierzchnia ataku: Luki

1.. Ekosystem (ogólnie):

Standardy interoperacyjności

Zarządzanie danymi

Awaria całego systemu

Ryzyka poszczególnych interesariuszy

Niejawne zaufanie między komponentami

Bezpieczeństwo rejestracji

System likwidacji

Utracone procedury dostępu

2. Pamięć urządzenia

Dane wrażliwe

o Nazwy użytkowników w postaci zwykłego tekstu

o Hasła w postaci zwykłego tekstu

o Poświadczenia osób trzecich

o Klucze szyfrujące

3. Fizyczne interfejsy urządzenia

Ekstrakcja oprogramowania układowego

Interfejs wiersza polecenia użytkownika

Interfejs wiersza polecenia administratora

Eskalacja uprawnień

Zresetuj do stanu niezabezpieczonego

Usuwanie nośników pamięci

Odporność na manipulacje

Port debugowania

UART (szeregowy)

JTAG/SWD

Ujawnienie identyfikatora urządzenia/numeru seryjnego

4. Interfejs sieciowy urządzenia

Standardowy zestaw luk w aplikacjach internetowych:

o OWASP Web Top 10

o OWASP ASVS

o Przewodnik testowania OWASP

Luki w zabezpieczeniach zarządzania poświadczeniami:

o Wyliczanie nazwy użytkownika

Słabe hasła

o Blokada konta

o Znane domyślne poświadczenia

o Niepewny mechanizm odzyskiwania hasła

5. Oprogramowanie układowe urządzenia

Ekspozycja danych wrażliwych (patrz OWASP Top 10- A6 Ekspozycja wrażliwych danych):

Konta typu backdoor

o Zakodowane na stałe poświadczenia

Klucze szyfrujące

o Szyfrowanie (symetryczne, asymetryczne)

Informacje wrażliwe

o Ujawnienie wrażliwych adresów URL

Wyświetlanie wersji oprogramowania układowego i/lub daty ostatniej aktualizacji Wrażliwe usługi (internet, SSH, TFTP itp.)

o Zweryfikuj stare wersje oprogramowania i możliwe ataki (Heartbleed, Shellshock, stare wersje PHP itp.)

Ekspozycja interfejsu API funkcji związanych z bezpieczeństwem

Możliwość downgrade'u oprogramowania

6. Usługi sieciowe urządzenia

Ujawnienie informacji

Interfejs wiersza polecenia użytkownika

Interfejs wiersza polecenia administratora

Zastrzyk

Odmowa usługi

Nieszyfrowane usługi

Źle zaimplementowane szyfrowanie

Usługi testowe/rozwojowe

Przepełnienie bufora

UPnP

Wrażliwe usługi UDP

Blok aktualizacji oprogramowania układowego urządzenia OTA

Oprogramowanie układowe załadowane przez niezabezpieczony kanał (bez TLS)

Powtórz atak

Brak weryfikacji ładunku

Brak kontroli integralności wiadomości

Luki w zabezpieczeniach zarządzania poświadczeniami:

o Wyliczanie nazwy użytkownika

Słabe hasła

o Blokada konta

o Znane domyślne poświadczenia

o Niepewny mechanizm odzyskiwania hasła

7. Interfejs administracyjny

Standardowy zestaw luk w aplikacjach internetowych:

o OWASP Web Top 10

o OWASP ASVS

o Przewodnik testowania OWASP

Luki w zabezpieczeniach zarządzania poświadczeniami:

o Wyliczanie nazwy użytkownika

Słabe hasła

o Blokada konta

o Znane domyślne poświadczenia

o Niepewny mechanizm odzyskiwania hasła

* Opcje bezpieczeństwa/szyfrowania

Opcje logowania

Uwierzytelnianie dwuskładnikowe

* Sprawdź, czy nie ma niezabezpieczonych bezpośrednich odniesień do obiektów

Niemożność wyczyszczenia urządzenia

8. Lokalne przechowywanie danych

Nieszyfrowane dane

Dane zaszyfrowane odkrytymi kluczami

Brak kontroli integralności danych

Użycie statycznego tego samego klucza szyfrowania/deszyfrowania

9. Interfejs sieciowy w chmurze

Standardowy zestaw luk w aplikacjach internetowych:

o OWASP Web Top 10

o OWASP ASVS

o Przewodnik testowania OWASP

Luki w zabezpieczeniach zarządzania poświadczeniami

o Wyliczanie nazwy użytkownika

Słabe hasła

o Blokada konta

o Znane domyślne poświadczenia

o Niepewny mechanizm odzyskiwania hasła

Szyfrowanie transportu

Uwierzytelnianie dwuskładnikowe

10. Interfejsy API zaplecza innych firm

Wysłano niezaszyfrowaną PII

Zaszyfrowana PII wysłana

Wyciekły informacje o urządzeniu

Lokalizacja wyciekła

11. Mechanizm aktualizacji

Aktualizacja wysłana bez szyfrowania

Aktualizacje nie podpisane

Możliwość zapisu lokalizacji aktualizacji

Zaktualizuj weryfikację

Zaktualizuj uwierzytelnianie

Złośliwa aktualizacja

Brakujący mechanizm aktualizacji

Brak mechanizmu ręcznej aktualizacji

12. Aplikacja mobilna

Aktualizacja wysłana bez szyfrowania

Aktualizacje nie podpisane

Możliwość zapisu lokalizacji aktualizacji

Zaktualizuj weryfikację

Zaktualizuj uwierzytelnianie

Złośliwa aktualizacja

Brakujący mechanizm aktualizacji

Brak mechanizmu ręcznej aktualizacji

13. Interfejsy API zaplecza dostawcy

Nieodłączne zaufanie chmury lub aplikacji mobilnej

Słabe uwierzytelnianie

Słaba kontrola dostępu

Ataki iniekcyjne

Usługi ukryte

14. Komunikacja ekosystemowa

Badania zdrowia

Bicie serca

Komendy ekosystemu

Wyrejestrowywanie

Wypychanie aktualizacji

15.Ruch sieciowy

LAN

LAN do Internetu

Krótki zasięg

Niestandardowe

Bezprzewodowe (Wi-Fi, Z-wave, XBee, Zigbee, Bluetooth, LoRa)

Fuzzing protokołu

16.Uwierzytelnianie/Autoryzacja

wartości związane z uwierzytelnianiem/autoryzacją (klucz sesyjny,

ujawnienie tokena, pliku cookie itp.).

Ponowne użycie klucza sesji, tokena itp.

Uwierzytelnianie między urządzeniami

Uwierzytelnianie między urządzeniami a aplikacjami mobilnymi

Uwierzytelnianie między urządzeniami a systemem w chmurze

Uwierzytelnianie aplikacji mobilnej do systemu w chmurze

Uwierzytelnianie aplikacji internetowej do systemu w chmurze

Brak dynamicznego uwierzytelniania

17.Prywatność

Ujawnienie danych użytkownika

Ujawnienie lokalizacji użytkownika/urządzenia

Prywatność różnicowa

18. Sprzęt (czujniki)

Wyczuwanie manipulacji środowiskiem

Manipulowanie (fizyczne)

Obrażenia (fizyczne)

Luki w zabezpieczeniach IoT

Poniżej przedstawiono luki w zabezpieczeniach OWASP IoT:

Podatność : Powierzchnia ataku : Opis

1. Wyliczenie nazwy użytkownika: Interfejs administracyjny , Interfejs sieciowy urządzenia , Interfejs chmury , Aplikacja mobilna: Możliwość zebrania zestawu prawidłowych nazw użytkowników poprzez interakcję z mechanizmem uwierzytelniania

2. Słabe hasła: interfejs administracyjny, interfejs sieciowy urządzenia, interfejs chmury, aplikacja mobilna: możliwość ustawienia hasła do konta na przykład „1234” lub „123456”; użycie wstępnie zaprogramowanych haseł domyślnych

3. Blokada konta: interfejs administracyjny, interfejs sieciowy urządzenia, interfejs chmury, aplikacja mobilna: możliwość dalszego wysyłania prób uwierzytelnienia po 3-5 nieudanych próbach logowania

4. Usługi niezaszyfrowane: Usługi sieciowe urządzenia: Usługi sieciowe nie są odpowiednio zaszyfrowane, aby zapobiec podsłuchiwaniu lub manipulowaniu przez atakujących

5. Uwierzytelnianie dwuskładnikowe: administracyjne, interfejs sieciowy w chmurze, aplikacja mobilna: brak mechanizmów uwierzytelniania dwuskładnikowego, takich jak token bezpieczeństwa lub skaner linii papilarnych

6. Źle zaimplementowane szyfrowanie: Usługi sieciowe urządzenia: zaimplementowano szyfrowanie; jest jednak niewłaściwie skonfigurowany lub nie jest odpowiednio aktualizowany, np. przy użyciu protokołu SSL v2

7. Aktualizacja wysłana bez szyfrowania: Mechanizm aktualizacji: Aktualizacje są przesyłane przez sieć bez użycia TLS lub szyfrowania samego pliku aktualizacji

8. Możliwość zapisu lokalizacji aktualizacji: mechanizm aktualizacji: lokalizacja przechowywania plików aktualizacji jest zapisywalna przez wszystkich, co umożliwia modyfikację oprogramowania układowego i dystrybucję do wszystkich użytkowników

9. Odmowa usługi: Usługi sieciowe urządzenia: Usługa może zostać zaatakowana w sposób, który odmówi usługi tej usłudze lub całemu urządzeniu

10. Usuwanie nośników pamięci: Fizyczne interfejsy urządzenia: Możliwość fizycznego usunięcia nośników pamięci z urządzenia

11. Brak mechanizmu aktualizacji ręcznej: Mechanizm aktualizacji: brak możliwości ręcznego wymuszenia sprawdzenia aktualizacji urządzenia

12. Brakujący mechanizm aktualizacji: Mechanizm aktualizacji: brak możliwości aktualizacji urządzenia

13. Wyświetlanie wersji oprogramowania sprzętowego i/lub daty ostatniej aktualizacji: Oprogramowanie układowe urządzenia: Bieżąca wersja oprogramowania układowego nie jest wyświetlana i/lub data ostatniej aktualizacji nie jest wyświetlana

14. Ekstrakcja oprogramowania układowego i pamięci: interfejs JTAG/SWD, zrzucanie In-Situ, przechwytywanie sygnału Over-the-Air (OTA), pobieranie aktualizacji ze strony internetowej producenta, eMMCTapping, rozlutowywanie chipa SPI Flash/eMMC i odczytywanie go w Adapter: oprogramowanie układowe zawiera wiele przydatnych informacji, takich jak kod źródłowy i pliki binarne uruchomionych usług, wstępnie ustawione hasła i klucze SSH

15. Manipulowanie przepływem wykonywania kodu urządzenia: Interfejs JTAG/SWD, ataki typu side-channel, takie jak Glitching: Za pomocą adaptera JTAG i debuggera GNU możemy modyfikować wykonywanie oprogramowania układowego w urządzeniu i ominąć prawie całe oprogramowanie- oparte kontrole bezpieczeństwa; Ataki typu side-channel mogą również modyfikować przebieg wykonywania lub służyć do wycieku interesujących informacji z urządzenia

16. Uzyskanie dostępu do konsoli: interfejsy szeregowe (SPI/UART) : Podłączając się do interfejsu szeregowego możemy uzyskać pełny dostęp konsoli do urządzenia ; Zwykle środki bezpieczeństwa obejmują niestandardowe programy ładujące, które uniemożliwiają atakującemu wejście do pojedynczego użytkownika tryb, ale można to również ominąć

17. Niezabezpieczone komponenty stron trzecich: Oprogramowanie: Nieaktualne wersje BusyBox, OpenSSL, SSH, serwerów WWW itp.

Zagrożenia Internetu Rzeczy

Urządzenia IoT mają bardzo niewiele mechanizmów ochrony przed różnymi pojawiającymi się zagrożeniami. Urządzenia te mogą być zainfekowane złośliwym oprogramowaniem lub złośliwym kodem w alarmującym tempie. Atakujący często wykorzystują te słabo chronione urządzenia w Internecie, aby spowodować fizyczne uszkodzenie sieci, podsłuchiwać komunikację, a także przeprowadzać destrukcyjne ataki, takie jak DDoS. Poniżej wymieniono niektóre rodzaje ataków IoT:

Atak DDoS: osoba atakująca przekształca urządzenia w armię botnetów w celu zaatakowania określonego systemu lub serwera, uniemożliwiając świadczenie usług.

• Atak na systemy HVAC: Luki w systemach HVAC są wykorzystywane przez osoby atakujące do kradzieży poufnych informacji, takich jak dane uwierzytelniające użytkownika, oraz do przeprowadzania dalszych ataków na sieć docelową.

• Atak ze zmiennym kodem: atakujący blokuje i wącha sygnał w celu uzyskania kodu przesłanego do odbiornika pojazdu; atakujący używa go następnie do odblokowania i kradzieży pojazdu.

Atak BlueBorne: Atakujący łączą się z pobliskimi urządzeniami i wykorzystują luki w protokole Bluetooth, aby skompromitować urządzenie.

Jamming Attack: atakujący blokuje sygnał między nadawcą a odbiorcą za pomocą złośliwego ruchu, który uniemożliwia komunikację między dwoma punktami końcowymi.

• Zdalny dostęp za pomocą backdoora: atakujący wykorzystują luki w urządzeniu IoT w celu przekształcenia go w backdoora i uzyskania dostępu do sieci organizacji.

Zdalny dostęp za pomocą usługi Telnet: osoby atakujące wykorzystują otwarty port telnet w celu uzyskania informacji, które są udostępniane między podłączonymi urządzeniami, w tym ich modeli oprogramowania i sprzętu.

Atak Sybil: atakujący wykorzystuje wiele sfałszowanych tożsamości, aby stworzyć silną iluzję przeciążenia ruchu, wpływając na komunikację między sąsiednimi węzłami i sieciami.

Exploit Kits: Złośliwy skrypt jest używany przez osoby atakujące do wykorzystania słabo załatanych luk w urządzeniu IoT.

Man-in-the-Middle Attack: atakujący udaje legalnego nadawcę, który przechwytuje całą komunikację między nadawcą a odbiorcą i przejmuje komunikację.

Atak powtórkowy: Atakujący przechwytują prawidłowe wiadomości z prawidłowej komunikacji i stale wysyłają przechwyconą wiadomość do urządzenia docelowego, aby przeprowadzić atak typu „odmowa usługi" lub spowodować awarię urządzenia docelowego.

Sfałszowane złośliwe urządzenie: atakujący zastępują autentyczne urządzenia IoT złośliwymi urządzeniami, jeśli mają fizyczny dostęp do sieci.

Side-Channel Attack: Atakujący przeprowadzają ataki typu side-channel, wydobywając informacje o kluczach szyfrujących, obserwując emisję sygnałów, tj. „kanałów bocznych" z urządzeń IoT.

Atak ransomware: Ransomware to rodzaj złośliwego oprogramowania, które wykorzystuje szyfrowanie do blokowania dostępu użytkownika do jego/jej urządzenia poprzez blokowanie ekranu lub plików użytkownika.

Podszywanie się pod klienta: osoba atakująca podszywa się pod legalne urządzenie inteligentne/serwer, używając złośliwego urządzenia i podszywając się pod nie, naraża urządzenie klienckie IoT, aby wykonywać nieautoryzowane działania lub uzyskiwać dostęp do poufnych informacji w imieniu legalnego klienta.

Atak SQL Injection: Atakujący przeprowadzają ataki SQL Injection, wykorzystując luki w aplikacjach mobilnych lub internetowych używanych do kontrolowania urządzeń IoT, w celu uzyskania dostępu do urządzeń i przeprowadzania na nie dalszych ataków.

Atak oparty na SDR: Za pomocą opartego na oprogramowaniu systemu komunikacji radiowej osoba atakująca może badać sygnały komunikacyjne przechodzące przez sieć IoT i wysyłać wiadomości spamowe do połączonych urządzeń.

Atak typu Fault Injection: Atak typu Fault Injection ma miejsce, gdy osoba atakująca próbuje wprowadzić błąd w urządzeniu IoT w celu wykorzystania tych błędów do naruszenia bezpieczeństwa tego urządzenia.

Network Pivoting: osoba atakująca używa złośliwego urządzenia inteligentnego do łączenia się i uzyskiwania dostępu do zamkniętego serwera, a następnie wykorzystuje to połączenie do obracania innych urządzeń i połączeń sieciowych z serwerem w celu kradzieży poufnych informacji.

DNS Rebinding Attack: Rebinding DNS to proces uzyskiwania dostępu do routera ofiary za pomocą złośliwego kodu JavaScript wstrzykniętego na stronę internetową.

Hakowanie urządzeń IoT: ogólny scenariusz

IoT obejmuje różne technologie, takie jak wbudowane czujniki, mikroprocesory i urządzenia do zarządzania energią. Kwestie bezpieczeństwa zmieniają się z urządzenia na urządzenie i aplikacji na aplikację. Im większa ilość poufnych danych przesyłanych przez sieć, tym większe ryzyko kradzieży danych, manipulacji danymi, manipulowania danymi oraz ataków na routery i serwery. Niewłaściwa infrastruktura bezpieczeństwa może prowadzić do następujących niepożądanych scenariuszy:

Podsłuchujący przechwytuje komunikację między dwoma punktami końcowymi i odkrywa poufne informacje, które są przesyłane. Może on niewłaściwie wykorzystać te informacje dla własnej korzyści.

Fałszywy serwer może służyć do wysyłania niechcianych poleceń w celu wywołania nieplanowanych zdarzeń.

Na przykład niektóre zasoby fizyczne (woda, węgiel, ropa naftowa, elektryczność) mogą zostać wysłane w nieznane i nieplanowane miejsce docelowe itp.

Fałszywe urządzenie może wstrzyknąć złośliwy skrypt do systemu, aby działał zgodnie z instrukcjami urządzenia. Może to spowodować niewłaściwe i niebezpieczne zachowanie systemu.

Atak DDoS

Rozproszony atak typu „odmowa usługi" (DDoS) to atak, w którym wiele zainfekowanych systemów jest używanych do bombardowania pojedynczego systemu lub usługi online, powodując, że serwer staje się bezużyteczny, powolny lub niedostępny dla uprawnionego użytkownika na krótki okres czasu. Atakujący inicjuje atak, najpierw wykorzystując luki w zabezpieczeniach urządzeń, a następnie instalując złośliwe oprogramowanie w ich systemach operacyjnych. Te liczne zainfekowane urządzenia są określane jako armia botnetów. Gdy atakujący zdecyduje się na swój cel, instruuje botnety lub agentów zombie, aby wysyłali żądania do serwera docelowego, który atakuje. Cel jest atakowany przez dużą liczbę żądań z wielu urządzeń IoT znajdujących się w różnych lokalizacjach. W rezultacie system docelowy jest zalewany większą liczbą żądań, niż może obsłużyć. W związku z tym przechodzi w tryb offline, traci wydajność lub całkowicie się wyłącza.

Poniżej podano kroki, które wykonuje atakujący, aby przeprowadzić atak DDoS na urządzenia IoT:

Atakujący uzyskuje zdalny dostęp do wrażliwych urządzeń

Po uzyskaniu dostępu wprowadza złośliwe oprogramowanie do urządzeń IoT, aby przekształcić je w botnety

Atakujący używa centrum dowodzenia i kontroli do instruowania botnetów i wysyłania wielu żądań do serwera docelowego, co skutkuje atakiem DDoS

Serwer docelowy przechodzi w tryb offline i staje się niedostępny do przetwarzania dalszych żądań

Wykorzystaj HVAC

Wiele organizacji korzysta z podłączonych do Internetu systemów ogrzewania, wentylacji i klimatyzacji (HVAC) bez implementacji mechanizmów bezpieczeństwa, dając atakującym bramę, przez którą mogą włamać się do systemów korporacyjnych. Systemy HVAC mają wiele luk w zabezpieczeniach, które atakujący wykorzystują do kradzieży danych logowania, uzyskania dostępu do systemu HVAC i przeprowadzania dalszych ataków na sieć organizacji. Systemy HVAC są na ogół podłączone do sieci różnych branż, sektorów rządowych, szpitali itp. Systemy te zapewniają prawa dostępu do dostawców HVAC i stronom trzecim w celu wsparcia ich zdalnej administracji, takiej jak zdalne monitorowanie zużycia energii i temperatur w różnych miejscach. Ponadto wiele firm HVAC udostępnia wspólne nazwy logowania i hasła różnym organizacjom. Atakujący wykorzystują to, aby uzyskać zdalny dostęp do sieci korporacyjnych i wykraść poufne informacje z organizacji.

Kroki podejmowane przez atakującego w celu wykorzystania systemów HVAC:

• Atakujący używa Shodan (https://www.shodan.io) i wyszukuje podatne na ataki przemysłowe systemy sterowania (ICS)

• Na podstawie znalezionych wrażliwych systemów ICS atakujący wyszukuje następnie domyślne dane uwierzytelniające użytkownika za pomocą narzędzi online, takich jak https://www.defpass.com

• Atakujący używa domyślnych poświadczeń użytkownika, aby uzyskać dostęp do ICS

• Po uzyskaniu dostępu do ICS atakujący próbuje uzyskać zdalny dostęp do systemu HVAC za pośrednictwem ICS

• Po uzyskaniu dostępu do systemu HVAC, atakujący może sterować temperaturą z HVAC lub przeprowadzić inne ataki na sieć lokalną

Atak Rolling Code

Większość inteligentnych pojazdów korzysta z inteligentnych systemów blokowania, które obejmują sygnał radiowy przesyłany w postaci kodu z nowoczesnego breloka do kluczyków w celu zablokowania lub odblokowania pojazdu. Tutaj kod wysłany do pojazdu jest używany tylko raz i jest inny dla każdego innego użycia, co oznacza, że jeśli pojazd ponownie otrzyma ten sam kod, odrzuca go. Kod, który blokuje lub odblokowuje samochód lub garaż, nazywany jest kodem zmiennym lub kodem zmiennym. Jest używany w systemie dostępu bezkluczykowego, aby zapobiec atakom powtórkowym. Podsłuchujący może przechwycić przesyłany kod, a następnie użyć go do odblokowania garażu lub pojazdu. Aby uzyskać kod zmienny, atakujący udaremnia transmisję sygnału z pilota do odbiornika w pojeździe. Atak ten jest wykonywany za pomocą urządzenia zakłócającego, które jednocześnie blokuje sygnał i wącha kod, a następnie atakujący używa tego kodu do odblokowania pojazdu lub bramy garażowej. Na przykład poniżej podano kroki, które wykonuje osoba atakująca, aby przeprowadzić atak typu „rolling code”:

Ofiara naciska przycisk pilota samochodu i próbuje odblokować samochód

Atakujący używa zakłócacza, który blokuje odbiór przez samochód kodu zmiennego wysłanego przez ofiarę i jednocześnie wącha pierwszy kod

Samochód nie odblokowuje się; ofiara próbuje ponownie, wysyłając drugi kod

Atakujący sniffuje drugi kod

Przy drugiej próbie ofiary atakujący przekazuje pierwszy kod, który odblokowuje samochód

Nagrany drugi kod jest później używany przez atakującego do odblokowania i kradzieży pojazdu

Atakujący mogą skorzystać z narzędzi takich jak rfcat-rolljam i RFCrack, aby przeprowadzić ten atak.

Atak BlueBorne'a

Atak BlueBorne jest wykonywany na połączeniach Bluetooth w celu uzyskania dostępu do urządzenia docelowego i przejęcia nad nim pełnej kontroli. Atakujący łączą się z pobliskimi urządzeniami i wykorzystują luki w protokole Bluetooth, aby skompromitować urządzenia. BlueBorne to zbiór różnych technik opartych na znanych lukach protokołu Bluetooth. Atak ten może zostać przeprowadzony na wielu urządzeniach IoT, w tym na tych z systemami operacyjnymi, takimi jak Android, Linux, Windows i starsze wersje iOS. We wszystkich systemach operacyjnych proces Bluetooth ma wysokie uprawnienia. Po uzyskaniu dostępu do jednego urządzenia atakujący może przeniknąć do dowolnej sieci korporacyjnej za pomocą tego urządzenia, aby ukraść krytyczne informacje z organizacji i rozesłać złośliwe oprogramowanie na pobliskie urządzenia. BlueBorne jest kompatybilny ze wszystkimi wersjami oprogramowania i nie wymaga żadnej interakcji użytkownika, warunków wstępnych ani konfiguracji, z wyjątkiem aktywnego Bluetooth. Ten atak ustanawia połączenie z docelowym urządzeniem obsługującym technologię Bluetooth, nawet bez parowania z urządzeniem. Korzystając z tego ataku, osoba atakująca może wykryć urządzenia obsługujące technologię Bluetooth, nawet jeśli nie są one w aktywnym trybie wykrywania. Gdy atakujący zidentyfikuje dowolne urządzenie znajdujące się w pobliżu, próbuje wydobyć adres MAC i informacje o systemie operacyjnym, aby przeprowadzić dalsze wykorzystanie docelowego systemu operacyjnego. W oparciu o luki obecne w protokole Bluetooth osoby atakujące mogą nawet działać zdalne wykonanie kodu i ataki typu man-in-the-middle na urządzenie docelowe. Atak ten może zostać przeprowadzony na różne urządzenia IoT, takie jak inteligentne telewizory, telefony, zegarki, samochodowe systemy audio, drukarki itp.

Kroki do wykonania ataku BlueBorne:

Atakujący odkrywa wokół siebie aktywne urządzenia obsługujące technologię Bluetooth; wszystkie urządzenia z obsługą Bluetooth można zlokalizować, nawet jeśli nie są w trybie wykrywalnym

Po zlokalizowaniu dowolnego urządzenia w pobliżu atakujący uzyskuje adres MAC urządzenia

Teraz atakujący wysyła ciągłe sondy do urządzenia docelowego w celu określenia systemu operacyjnego

Po zidentyfikowaniu systemu operacyjnego atakujący wykorzystuje luki w protokole Bluetooth, aby uzyskać dostęp do urządzenia docelowego

Teraz atakujący może wykonać zdalne wykonanie kodu lub atak typu man-in-the-middle i przejąć pełną kontrolę nad urządzeniem

Zagłuszający atak

Zagłuszanie to rodzaj ataku, w którym komunikacja między bezprzewodowymi urządzeniami IoT jest zakłócana w celu ich skompromitowania. Podczas tego ataku wysyłana jest przytłaczająca ilość złośliwego ruchu, co skutkuje atakiem DoS na autoryzowanych użytkowników, blokując w ten sposób legalny ruch i uniemożliwiając komunikację między punktami końcowymi. Każde urządzenie bezprzewodowe i sieć bezprzewodowa są podatne na ten atak. Atakujący wykorzystują specjalne rodzaje sprzętu i losowo przesyłają sygnały radiowe z częstotliwością, z jaką komunikuje się docelowe urządzenie. Sygnały lub ruch generowany przez

urządzenia zakłócającego pojawiają się jako szum w urządzeniach bezprzewodowych, co powoduje, że wstrzymują one transmisję do czasu ustąpienia szumu. Powoduje to atak DoS, który blokuje sieć, a urządzenia nie mogą wysyłać ani odbierać żadnych danych.

Hakowanie inteligentnych sieci/urządzeń przemysłowych: zdalny dostęp za pomocą backdoora

Atakujący zbierają podstawowe informacje o docelowej organizacji za pomocą różnych technik socjotechnicznych. Po uzyskaniu informacji, takich jak identyfikatory e-mail pracowników, osoba atakująca wysyła e-maile phishingowe do pracowników ze złośliwym załącznikiem (np. dokumentem programu Word). Kiedy pracownik docelowej organizacji otwiera wiadomość e-mail i klika załącznik, w docelowym systemie automatycznie instalowany jest backdoor. Za pomocą backdoora atakujący uzyskuje dostęp do prywatnej sieci organizacji. Weźmy na przykład atak na sieć energetyczną. W takim ataku, po uzyskaniu dostępu do sieci prywatnej, atakujący może uzyskać dostęp do sieci SCADA, która kontroluje sieć. Po uzyskaniu dostępu do sieci SCADA, atakujący podmienia legalny firmware na złośliwy firmware w celu przetworzenia poleceń wysyłanych przez atakującego. Wreszcie atakujący może wyłączyć zasilanie w dowolnym miejscu, wysyłając złośliwe polecenia do systemów sterowania stacją z sieci SCADA.

Ataki oparte na SDR na IoT

Radio definiowane programowo (SDR) to metoda generowania komunikacji radiowej i wdrażania przetwarzania sygnału za pomocą oprogramowania (lub oprogramowania układowego) zamiast zwykłej metody używania sprzętu. Korzystając z tego opartego na oprogramowaniu systemu komunikacji radiowej (stworzone przez siebie SDR), osoba atakująca może badać sygnały komunikacyjne w sieciach IoT i wysyłać spam lub wiadomości tekstowe do połączonych urządzeń. System SDR może również zmieniać transmisję i odbiór sygnałów pomiędzy urządzeniami, w zależności od ich implementacji programowej. Atak można przeprowadzić zarówno w trybie transmisji full-duplex (komunikacja dwukierunkowa), jak i half-duplex (komunikacja jednokierunkowa). Rodzaje ataków opartych na SDR przeprowadzanych przez osoby atakujące w celu włamania się do środowiska IoT:

Replay atak

Jest to główny atak opisany w zagrożeniach IoT, w którym osoby atakujące mogą przechwycić sekwencję poleceń z podłączonych urządzeń i wykorzystać ją do późniejszej retransmisji. Atakujący może wykonać poniższe kroki, aby przeprowadzić atak powtórkowy:

o Atakujący atakuje określoną częstotliwość, która jest wymagana do udostępniania informacji między urządzeniami

o Po uzyskaniu częstotliwości atakujący może przechwycić oryginalne dane, gdy polecenia są inicjowane przez podłączone urządzenia

o Po zebraniu oryginalnych danych atakujący używa bezpłatnych narzędzi, takich jak URH (Universal Radio Hacker), aby oddzielić sekwencję poleceń

o Następnie atakujący wstrzykuje oddzielną sekwencję poleceń na tej samej częstotliwości do sieci IoT, która odtwarza polecenia lub przechwycone sygnały urządzeń

Atak kryptoanalizy

Atak kryptoanalityczny to kolejny rodzaj poważnego ataku na urządzenia IoT. W tym ataku procedura zastosowana przez atakującego jest taka sama jak w przypadku ataku powtórkowego, z wyjątkiem jednego dodatkowego kroku, tj. inżynierii wstecznej protokołu w celu uzyskania oryginalnego sygnału. Aby wykonać to zadanie, atakujący musi być biegły w kryptografii, teorii komunikacji i schemacie modulacji (w celu usunięcia

szumów z sygnału). Atak ten praktycznie nie jest tak łatwy do przeprowadzenia jak atak powtórkowy, jednak osoba atakująca może próbować złamać zabezpieczenia za pomocą różnych narzędzi i procedur.

Atak rozpoznawczy

Zakłócenia zasilania/zegara/resetowania

Tego typu ataki mają miejsce, gdy do zasilacza wprowadzane są usterki lub usterki, które można wykorzystać do zdalnego wykonania, powodując również pomijanie kluczowych instrukcji. Błędy mogą być również wstrzykiwane do sieci zegarowej używanej do dostarczania zsynchronizowanego sygnału przez układ.

Manipulowanie częstotliwością/napięciem

w tych atakach atakujący próbują manipulować warunkami pracy chipa, a także mogą modyfikować poziom zasilania i zmieniać częstotliwość zegara chipa. Intencją atakujących jest wprowadzenie błędu do układu, aby zagrozić bezpieczeństwu urządzenia.

Ataki temperaturowe

Atakujący zmieniają temperaturę pracy chipa, zmieniając w ten sposób całe środowisko operacyjne. Atak ten można przeprowadzić w warunkach nienominalnych.

Po wprowadzeniu błędów przy użyciu różnych technik, osoby atakujące mogą teraz wykorzystać wadliwe zachowanie urządzenia do przeprowadzenia różnych ataków w celu kradzieży poufnych informacji lub przerwania normalnego działania urządzenia.

Inne ataki IoT

Atak Sybilli

Komunikacja samochodowa odgrywa ważną rolę w bezpiecznym transporcie, wymieniając ważne komunikaty dotyczące bezpieczeństwa i aktualizacje ruchu, ale nawet samochodowe sieci ad-hoc (VANET) nie są bezpieczne przed zasięgiem atakujących. Osoba atakująca wykorzystuje wiele sfałszowanych tożsamości, aby stworzyć silną iluzję przeciążenia ruchu, wpływając na komunikację między sąsiednimi węzłami i sieciami. Za najpoważniejsze ataki uważa się ataki Sybil w sieciach VANET, które mają ogromny wpływ na wydajność sieci. Ten rodzaj ataku osłabia potencjalne aplikacje w sieciach VANET, tworząc silną iluzję

natężenie ruchu. Aby przeprowadzić ten rodzaj ataku, deklaruje się obecność pojazdu w różnych miejscach w tym samym czasie. Na przykład, niech węzeł, który podszywa się pod inne węzły i rozpoczyna atak, będzie nazywany węzłem Sybil „X". Powstaje poprzez utworzenie nowej tożsamości lub kradzież istniejącej tożsamości prawnej. W prawidłowej komunikacji pozostałe węzły „A" i „B" powinny komunikować się tylko ze sobą. Flowever w tym scenariuszu węzeł „X" interweniuje jako znany węzeł wewnętrzny i atakuje sieć. Węzeł „X" próbuje komunikować się z normalnymi sąsiednimi węzłami („A" i „B") przy użyciu wielu sfałszowanych tożsamości. W ten sposób powoduje znaczny chaos i zagrożenia bezpieczeństwa w sieci.

Zestawy eksploitów

Zestaw exploitów to złośliwy skrypt używany przez atakujących do wykorzystywania słabo załatanych luk w zabezpieczeniach urządzenia IoT. Zestawy te są zaprojektowane w taki sposób, że w przypadku pojawienia się nowych luk, nowe sposoby wykorzystania i dodatkowe funkcje zostaną automatycznie dodane do urządzenia. Po wykryciu luk w zabezpieczeniach zestawy te wysyłają dokładnego exploita w celu zainstalowania złośliwego oprogramowania, które może uruchomić i uszkodzić urządzenie. Te zestawy exploitów stanowią niebezpieczne zagrożenie, ponieważ pozostają niewykryte w środowiskach IoT, wpływając na urządzenia i infrastrukturę IoT, zmuszając je do nieoczekiwanego zachowania.

Atak typu Man-in-the-Middle

W ataku typu man-in-the-middle atakujący udaje legalnego nadawcę, przechwytuje całą komunikację między nadawcą a odbiorcą i przejmuje komunikację. Urządzenia IoT są zwykle podłączone do sieci i działają jako brama do wszystkich poufnych i osobistych informacji. W związku z tym każdy złośliwy użytkownik może udawać legalnego nadawcę i wysyłać złośliwe żądania do urządzenia w celu przejęcia nad nim kontroli. Urządzenia IoT, takie jak kamery IP, routery, modemy i bramy internetowe, mają luki kryptograficzne, które prowadzą do ataków typu man-in-the-middle.

Atak z powtórzeniem

W ataku z powtórzeniem atakujący przechwytują prawidłowe wiadomości z prawidłowej komunikacji i stale wysyłają przechwyconą wiadomość do urządzenia docelowego w celu przeprowadzenia ataku DoS lub opóźnienia go w celu manipulowania wiadomością lub awarii urządzenia docelowego. Rozważmy na przykład atak polegający na powtórce, który regeneruje sygnał używany do sterowania urządzeniami IoT jak drzwi wejściowe. Drzwi wejściowe wykorzystują zamek, który otwiera się za pomocą prostych sygnałów podczerwieni. Zasadniczo atakujący rejestruje wzór modulacji podczerwieni, odtwarza sygnał i przeprowadza atak powtórkowy na drzwi, aby je odblokować.

Sfałszowane złośliwe urządzenie

Atakujący podmieniają autentyczne urządzenia IoT na złośliwe urządzenia, jeśli mają fizyczny dostęp do sieci. Wykrycie takich ataków jest bardzo trudne, ponieważ sfałszowane urządzenie przypomina to legalne. Sfałszowane urządzenia zawierają backdoory, które są wykorzystywane przez osoby atakujące do wykonywania różnych złośliwych działań w sieci.

Atak bocznym kanałem

Atakujący przeprowadzają atak typu side-channel, wydobywając informacje o kluczach szyfrujących, obserwując emisję sygnałów, czyli tzw. „kanałów bocznych" z urządzeń IoT. Wszystkie urządzenia emitują te sygnały, które dostarczają informacji o wewnętrznym procesie obliczeniowym, poprzez zużycie energii lub emanacje elektromagnetyczne. Atakujący uważnie obserwują emisje z kanału bocznego, aby zdobyć całą możliwą wiedzę o zmiennym zużyciu energii, aby móc uzyskać dostęp do klucza szyfrującego i powielić go w sposób nieunikniony.

Główną zaletą tego ataku jest to, że dostęp do kluczy szyfrujących jest łatwy i wymaga mniej czasu, a informacje wyciekające z podatnych na ataki urządzeń pomagają atakującym wykorzystać inne techniki kanału bocznego, takie jak przeprowadzanie ataków pochłaniających energię i ataków opartych na czasie.

Atak ransomware

Ransomware to rodzaj złośliwego oprogramowania, które wykorzystuje szyfrowanie w celu zablokowania dostępu użytkownika do jego urządzenia poprzez zablokowanie ekranu lub plików użytkownika i pozostaje zablokowane do momentu zapłacenia okupu umożliwiającego użytkownikowi odzyskanie dostępu do jego/ jej urządzenie.

Użytkownik może napotkać ten problem na wiele sposobów, może zostać omyłkowo pobrany wraz z innym złośliwym oprogramowaniem, oprogramowaniem lub plikami, a czasem poprzez złośliwe reklamy (malvertisements).

Poniżej omówiono fazy ransomware:

Faza 1: Ofiara otrzymuje wiadomość e-mail od atakującego, która wydaje się pochodzić od legalnego nadawcy. Ten e-mail zawiera załącznik w postaci złośliwego pliku.

Faza 2:

• Użytkownik otwiera wiadomość i klika szkodliwy plik. Malware jest pobierane i uruchamia legalne procesy potomne, takie jak PowerShell, mechanizm szyfrowania Vssadmin lub cmd.exe. W rezultacie urządzenie zostaje połączone z serwerem dowodzenia i kontroli atakującego (C&C).

• Pliki osobiste na urządzeniu ofiary są szyfrowane.

Faza 3: Na urządzenie ofiary dostarczane jest powiadomienie o oprogramowaniu ransomware, a ofiara jest proszona o zapłacenie okupu w postaci pieniędzy lub bitcoinów w celu uzyskania dostępu do swoich plików.

Ataki IoT w różnych sektorach

Technologia IoT robi postępy w każdym sektorze społeczeństwa, w tym w przemyśle, służbie zdrowia, rolnictwie, inteligentnych miastach, bezpieczeństwie, transporcie itp. Jednak ze względu na wdrożenie zdecentralizowanego podejścia w technologii IoT organizacje w mniejszym stopniu skupiają się na bezpieczeństwie urządzeń . Dlatego zamiast dzielić technologię IoT na różne części, dostawcy koncentrują się bardziej na wykrywaniu słabych punktów i wykorzystywaniu ich. Te luki obecne w urządzeniach IoT mogą być wykorzystywane przez osoby atakujące do przeprowadzania różnego rodzaju ataków, takich jak ataki DoS, ataki zagłuszające, ataki MITM i ataki Sybil, oraz do gromadzenia danych, co skutkuje utratą prywatności i poufności.

Studium przypadku: Enemybot

Enemybot to złośliwe oprogramowanie typu botnet oparte na Mirai, wykryte na początku 2022 r. Złośliwe oprogramowanie typu botnet rozprzestrzenia się, wykorzystując słabości Internetu rzeczy (IoT) i innych urządzeń trasujących na całym świecie. Po zidentyfikowaniu i zainfekowaniu słabo skonfigurowanego urządzenia Enemybot dodaje to zainfekowane urządzenie IoT do swojej floty botnetów. Szkodliwe oprogramowanie przejmuje zasoby obliczeniowe urządzeń IoT i wykorzystuje je do rozproszonych ataków typu „odmowa usługi" (DDoS) lub wydobywania kryptowalut. Enemybot wykorzystuje wyrafinowane metody zaciemniania ciągów znaków, aby ominąć rozwiązania/analizy bezpieczeństwa i utrzymuje trwałe połączenie z serwerem dowodzenia i kontroli (C2) znajdującym się w sieci Tor.

Scenariusz ataku Enemybota:

Krok 1: Tworzenie exploitów

Enemybot pożycza niektóre moduły, takie jak skaner i zabójca botów, z kodu źródłowego Mirai i modyfikuje go w celu zidentyfikowania wrażliwych urządzeń lub procesów w celu rozprzestrzeniania infekcji. Przykładowy kod zmodyfikowanego modułu skanera pokazano na zrzucie ekranu:

Krok 2: Wyłączanie innego złośliwego oprogramowania w miejscu docelowym

Enemybot atakuje wiele architektur, aby rozprzestrzeniać swoją infekcję. Oprócz urządzeń IoT, złośliwe oprogramowanie może również infekować architektury komputerów stacjonarnych, takie jak i586, arm, arm5, arm64, arm7, Darwin, bsd, i686, m68k, mips, mpsl, ppc-440fp, sh4, spc, ppc, x64 i x86 .

Korzystając z modułu bot killer, złośliwe oprogramowanie wykrywa aktywne procesy uruchamiane z określonych ścieżek lub pamięci urządzenia i natychmiast je zabija. Enemybot ulepsza kod źródłowy Mirai za pomocą dodatkowych słów kluczowych, aby wykrywać i usuwać wszelkie konkurencyjne złośliwe oprogramowanie aktywne na tym samym urządzeniu.

Krok 3: Uzyskanie dostępu

Po zaktualizowaniu kodu źródłowego Mirai o odpowiednie funkcje, Enemybot inicjuje atak bruteforce poprzez listę zakodowanych na stałe kombinacji nazwy użytkownika i hasła, aby uzyskać dostęp do urządzeń skonfigurowanych ze słabymi lub domyślnymi danymi uwierzytelniającymi. Złośliwe oprogramowanie może również infekować słabo skonfigurowane urządzenia z Androidem działające na porcie Android Debug Bridge (5555) za pomocą poleceń powłoki. Ponadto złośliwe oprogramowanie może wykorzystywać kilka innych luk wymienionych w tabeli.

CVE-2020-17456 CVE-2021-41773/CVE-2021-42013

CVE-2018-10823 CVE-2018-20062

CVE-2022-27226 CVE-2017-18368

CVE-2022-25075 do 25084 CVE-2016-6277

CVE-2021-44228/2021-45046 CVE-2015-2051

CVE-2014-9118 Exploit NETGEAR DGN1000

Krok 4: Rozpoczęcie ataku

Wykorzystując powyższe luki, grupa zagrożeń może przeprowadzać ataki wykraczające poza DDoS, takie jak ataki polegające na wydobywaniu kryptowalut. Gdy eksploatacja się powiedzie, na urządzeniu wykonywane jest polecenie powłoki w celu pobrania kolejnego kodu powłoki z adresu URL, który jest dynamicznie aktualizowany przez zdalny serwer (C2) za pomocą polecenia LDSERVER. To polecenie może również pomóc grupie zagrożeń w aktualizowaniu adresu URL, nawet jeśli serwer pobierania jest niedostępny. Następnie skrypt powłoki update.sh pobiera i wykonuje pliki binarne rzeczywistego złośliwego oprogramowania (Enemybot) na docelowej architekturze.

Gdy szkodliwy bot zostanie zainstalowany na urządzeniu docelowym, czeka na polecenia z serwera C2, aby rozpocząć ataki na cel; większość otrzymywanych poleceń jest ukierunkowana na atak DDoS. W poniższej tabeli wymieniono niektóre polecenia DDoS, z których może korzystać zainstalowany bot.

Opis polecenia

ADNS Rozpoczyna atak wzmacniający DNS

Rozpoczyna atak na serwery poświęcone grze „ARK:

Ewolucja przetrwania” ARK

Zalewa cel komunikatem ICMP Destination Port Unreachable

wiadomości BLACKNURSE

DNS Zalewa serwery DNS zakodowanymi na stałe zapytaniami DNS UDP

Zalewa cel połączeniami TCP i zatrzymuje je przez ok

określony czas HOLD

HTTP Zalewa cel żądaniami FITTP

JUNK Zalewa cel losowymi, niezerowymi pakietami UDP

LDSERVER Aktualizuje serwer pobierania dla ładunku

OVH Zalewa docelowe hostowane serwery OVFI niestandardowymi pakietami UDP

Rozprzestrzenia infekcję na inne urządzenia poprzez brutalne wymuszanie SSFI/Telnet

i wykorzystuje SCANNER

SH Wykonuje polecenie powłoki

STD Zalewa cel pakietami UDP o losowych bajtach

STOP Zatrzymuje równoczesne ataki DoS

TCP Zalewa cel pakietami TCP ze sfałszowanymi nagłówkami źródłowymi

TCPON/TCPOFF Włącza lub wyłącza proces podsłuchiwania

TLS Uruchamia atak SSL/TLS

Zalewa cel pakietami UDP ze sfałszowanym źródłem

nagłówki UDP

OVERTCP Przeprowadza atak TCP z losowymi interwałami dostarczania pakietów

Krok 5: Wytrwałość

Szkodliwe oprogramowanie może zaciemniać swoje ciągi znaków za pomocą kilku technik, takich jak kodowanie XOR za pomocą kilkubajtowych kluczy, jednobajtowa operacja XOR za pomocą 0x22, szyfrowanie poleceń za pomocą szyfrów podstawieniowych oraz kodowanie ciągów znaków przez dodanie wartości trzy do każdego znaku. Korzystając z tych metod zaciemniania, Enemybot może ukryć swoją obecność przed analitykami i innym złośliwym oprogramowaniem działającym na tym samym urządzeniu.

Metodologia hakowania IoT

Korzystając z metodologii hakowania IoT, osoba atakująca uzyskuje informacje za pomocą technik, takich jak zbieranie informacji, identyfikacja obszaru ataku i skanowanie luk w zabezpieczeniach, a następnie wykorzystuje je do zhakowania docelowego urządzenia i sieci. Ta sekcja skupi się na narzędziach i technikach wykorzystywanych przez osoby atakujące do osiągnięcia celu, jakim jest zhakowanie docelowego urządzenia IoT.

Co to jest hakowanie urządzeń IoT?

Dzięki znacznemu rozwojowi paradygmatu IoT każdego dnia coraz więcej urządzeń wkracza w nasze życie. Od automatyzacji domów po zastosowania w opiece zdrowotnej, Internet Rzeczy jest wszędzie. Jednak pomimo zdolności urządzeń IoT do uczynienia naszego życia łatwiejszym i wygodniejszym, nie możemy lekceważyć ryzyka cyberataków. Urządzenia IoT nie posiadają podstawowych zabezpieczeń, przez co są podatne na różnego rodzaju cyberataki. Celem hakera wykorzystującego urządzenia IoT jest uzyskanie nieautoryzowanego dostępu do urządzenia i danych użytkownika. Haker może wykorzystać zainfekowane urządzenia IoT do zbudowania armii botnetów, które z kolei są wykorzystywane do przeprowadzania ataku DDoS.

Jak haker czerpie zyski z IoT, gdy zostanie pomyślnie naruszony

Obecnie wszystkie Twoje dane, lokalizacja, konta e-mail, informacje finansowe i zdjęcia znajdują się na Twoich inteligentnych urządzeniach lub urządzeniach IoT, które są skarbnicą danych dla hakerów. Wraz ze wzrostem

sprzedaży i kupna urządzeń IoT na rynku ich liczba przewyższa obecnie liczbę ludzi. Oczekuje się, że liczba urządzeń IoT osiągnie 75 miliardów w 2025 roku. Ze względu na brak zasad bezpieczeństwa, inteligentne urządzenia stają się łatwym celem dla hakerów, którzy mogą je narazić na szpiegowanie działań użytkowników, niewłaściwe wykorzystanie poufnych informacji (takich jak karta zdrowia pacjenta), instalować oprogramowanie ransomware w celu zablokowania dostępu do urządzenia docelowego, monitorować działania ofiary za pomocą kamer CCTV, dokonywać oszustw związanych z kartami kredytowymi, uzyskiwać dostęp do domu użytkownika lub dodawać urządzenie do armii botnetów przeprowadzających ataki DDoS.

Metodologia hakowania IoT

Poniżej przedstawiono różne fazy hakowania urządzenia IoT:

Zbieranie informacji

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Uruchom ataki

Uzyskaj zdalny dostęp

Zachowaj dostęp

Zbieranie informacji

Pierwszym i najważniejszym krokiem hakowania urządzeń IoT jest wydobycie informacji, takich jak adres IP, używane protokoły (Zigbee, BLE, 5G, IPv6LoWPAN itp.), otwarte porty, typ urządzenia, geolokalizacja urządzenia, numer produkcyjny i numer produkcyjny firmy urządzenia, na tym etapie atakujący identyfikuje również projekt sprzętu, jego infrastrukturę oraz główne komponenty osadzone w urządzeniu docelowym, które jest obecne online. Atakujący wykorzystują narzędzia takie jak Shodan, Censys i Thingful do zbierania informacji lub rekonesansu na docelowym urządzeniu. Urządzenia, które są niedostępne w sieci, ale znajdują się w obszarze komunikacji, można również wykryć za pomocą snifferów, takich jak Foren6, Suphacap, CloudShark i Wireshark.

Zbieranie informacji za pomocą Shodan

Shodan to wyszukiwarka, która dostarcza informacji o wszystkich urządzeniach podłączonych do Internetu, takich jak routery, sygnalizacja świetlna, kamery CCTV, serwery, urządzenia inteligentnego domu i urządzenia przemysłowe. Atakujący mogą wykorzystać to narzędzie do zebrania informacji, takich jak adres IP, nazwa hosta, dostawca usług internetowych, lokalizacja urządzenia i baner docelowego urządzenia IoT. Atakujący mogą zbierać informacje o urządzeniu docelowym, korzystając z poniższych filtrów:

Wyszukiwanie kamer internetowych za pomocą geolokalizacja kraju

webcamxp: „us” (pobiera wszystkie kamery internetowe webcamxp obecne w USA).

Szukaj według miasta

webcamxp city: „streetsboro” (Pobiera istniejące kamery internetowe webcamxp w Streetsboro.)

Znajdź kamery internetowe na podstawie długości i szerokości geograficznej

webcamxp geo:" -50.81.201.80" (Uzyskuje określoną kamerę internetową obecną w geolokalizacji "-50.81.201.80" w mieście Boston i kraju USA.)

Dodatkowe filtry używane przez atakujących w celu uzyskania informacji o celu:

Sieć: Wyszukiwanie na podstawie adresu IP lub CIDR

System operacyjny: Wyszukiwanie na podstawie systemu operacyjnego używanego przez urządzenia

Port: Znajdź wszystkie otwarte porty

Przed/po: Zapewnia wynik w określonych ramach czasowych

Zbieranie informacji za pomocą MultiPing

Atakujący może użyć narzędzia MultiPing, aby znaleźć adres IP dowolnego urządzenia IoT w sieci docelowej. Po uzyskaniu adresu IP urządzenia IoT atakujący może przeprowadzić dalsze skanowanie w celu zidentyfikowania luk w zabezpieczeniach tego urządzenia.

Kroki, aby przeprowadzić skanowanie w celu zidentyfikowania adresu IP dowolnego urządzenia IoT:

Otwórz aplikację MultiPing i wybierz Plik -> Dodaj zakres adresów

W wyskakującym oknie Dodaj zakres adresów:

o Wybierz adres IP bramy routera z rozwijanego pola Adres początkowy do dodania

o Ustaw Liczbę adresów na „255”

o Kliknij OK

MultiPing przejdzie przez każdy możliwy adres IP z wybranego zakresu i rozpocznie testowanie każdego adresu IP, który odpowiada na jego polecenie ping

Każdy wiersz w oknie MultiPing to urządzenie w sieci; z listy atakujący może zidentyfikować adres IP docelowego urządzenia IoT

Aby szybciej znaleźć urządzenie docelowe, ustaw interwał ping na 1 sekundę

Zbieranie informacji przy użyciu FCC ID Search

Wyszukiwarka FCC ID pomaga w znalezieniu szczegółów urządzeń i przyznanych im certyfikatów. Strona wyszukiwania zawiera kilka pól, które umożliwiają dostęp do informacji o urządzeniach. Wszystkie urządzenia są oznaczone unikalnymi identyfikatorami FCC. Identyfikatory FCC składają się z dwóch elementów, znanych jako identyfikator beneficjenta (początkowe trzy lub pięć znaków) i identyfikator produktu (pozostałe znaki). Korzystając z identyfikatora FCC, można zebrać szczegółowe informacje o urządzeniu docelowym, wykonując poniższe czynności:

Otwórz urządzenie i sprawdź dołączoną etykietę

Etykieta zawiera FCC ID urządzenia

Teraz przejdź do formularza wyszukiwania FCC ID na oficjalnej stronie https://www.fcc.gov/oet/ea/fccid

Wprowadź w polach kod stypendysty i identyfikator produktu

Po wpisaniu danych kliknij "szukaj" -wyświetlą się szczegóły i podsumowanie urządzenia z różnymi częstotliwościami

Podstawowe informacje o urządzeniu można uzyskać, klikając link „Podsumowanie”, jak pokazano na poniższym zrzucie ekranu:

Exhibit Type	File Type	File Size	Description	Submission Date	Permanent Confidential	Short-Term Confidential	Date Available
Block Diagram	Adobe Acrobat PDF	16234	Block Diagram	01/26/2019	Yes	No	
Cover Letter(s)	Adobe Acrobat PDF	72964	Cover letter	01/26/2019	No	No	01/27/2019
Cover Letter(s)	Adobe Acrobat PDF	89962	Cover letter	01/26/2019	No	No	01/27/2019
External Photos	Adobe Acrobat PDF	1059770	External photos	01/26/2019	No	No	01/27/2019
ID Label/Location Info	Adobe Acrobat PDF	114618	Label	01/26/2019	No	No	01/27/2019
Internal Photos	Adobe Acrobat PDF	2895206	Internal photos	01/26/2019	No	No	01/27/2019
Operational Description	Adobe Acrobat PDF	206948	Operational Description	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	49567	Tune up	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	29959	Parts list	01/26/2019	Yes	No	
Schematics	Adobe Acrobat PDF	643217	Schematics	01/26/2019	Yes	No	
Test Report	Adobe Acrobat PDF	3507723	Test report	01/26/2019	No	No	01/27/2019
Test Setup Photos	Adobe Acrobat PDF	388298	Test setup	01/26/2019	No	No	01/27/2019
Users Manual	Adobe Acrobat PDF	1049119	User manual	01/26/2019	No	No	01/27/2019

Dalsze szczegóły urządzenia można znaleźć, klikając łącze „Szczegóły”, takie jak List przewodni, Zdjęcia zewnętrzne, Zdjęcia wewnętrzne, Raport z testów, Instrukcja obsługi itp.

Po uzyskaniu wymaganych informacji atakujący może znaleźć ukryte luki w urządzeniu docelowym i przeprowadzić dalsze ataki.

Wykrywanie urządzeń IoT z domyślnymi poświadczeniami za pomocą IoTSeeker

Atakujący używają narzędzi, takich jak IoTSeeker, do wykrywania urządzeń IoT, które używają domyślnych poświadczeń i są podatne na różne ataki polegające na przejmowaniu kontroli. IoTSeeker przeskanuje sieć w poszukiwaniu określonych typów urządzeń IoT, aby wykryć, czy używają one domyślnych, fabrycznych poświadczeń. Niedawna awaria Internetu została przypisana używaniu urządzeń IoT (kamer CCTV, rejestratorów DVR i innych) z domyślnymi danymi uwierzytelniającymi. To narzędzie pomaga organizacjom skanować ich sieci w celu wykrycia tego typu urządzeń IoT oraz określenia, czy poświadczenia zostały zmienione lub czy urządzenie nadal korzysta z ustawień fabrycznych. IoTSeeker koncentruje się na usługach HTTP/HTTPS. Na przykład osoby atakujące uruchamiają następujące polecenie, aby znaleźć urządzenia z domyślnymi poświadczeniami:

perl iotScanner.pl 1.1.1.1-1.1.4.254,2.1.1.1-2.2.3.254

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Gdy osoby atakujące zbiorą informacje o urządzeniu docelowym, wyszukują powierzchnie ataku urządzenia (zidentyfikują luki), które mogą zaatakować. Skanowanie pod kątem luk w zabezpieczeniach umożliwia atakującemu znalezienie łącznej liczby luk w oprogramowaniu układowym, infrastrukturze i komponentach systemowych urządzenia IoT, które są dostępne. Po zidentyfikowaniu obszaru powierzchni ataku atakujący skanuje luki w tym obszarze, aby zidentyfikować wektor ataku i przeprowadzić dalsze wykorzystanie urządzenia. Skanowanie pod kątem luk w zabezpieczeniach pomaga atakującemu zidentyfikować urządzenia IoT ze słabymi konfiguracjami, takimi jak ukryte exploity, błędy oprogramowania układowego, słabe ustawienia i hasła oraz słabo zaszyfrowana komunikacja. W przeciwieństwie do tego, pomaga również specjalistom ds. Bezpieczeństwa w zabezpieczaniu urządzeń IoT w sieci poprzez określanie luk w zabezpieczeniach lub słabych punktów w obecnych mechanizmach bezpieczeństwa, zanim atakujący będą mogli je wykorzystać.

Skanowanie luk w zabezpieczeniach za pomocą Nmap

Atakujący używają narzędzi do skanowania luk w zabezpieczeniach, takich jak Nmap, do identyfikowania urządzeń IoT podłączonych do sieci wraz z ich otwartymi portami i usługami. Nmap generuje surowe pakiety IP na różne sposoby, aby zidentyfikować działające hosty lub urządzenia w sieci, oferowane przez nie usługi, ich

systemy operacyjne, rodzaj używanych filtrów pakietów itp. Atakujący używają następującego polecenia Nmap do skanowania określonego adresu IP:

nmap -n -Pn -sS -pT:0-65535 -v -A -oX <NazwaXIP>

Aby wykonać pełne skanowanie urządzenia loT, które sprawdza usługi i porty TCP i UDP:

nmap -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <NazwaXIP>

Aby zidentyfikować możliwości IPv6 urządzenia:

nmap -6 -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <NazwaXIP>

Skanowanie luk w zabezpieczeniach za pomocą skanera Retina IoT (RIoT).

Skaner Retina IoT (RIoT) identyfikuje zagrożone urządzenia IoT, takie jak kamery IP, rejestratory DVR, drukarki i routery. To narzędzie daje atakującemu widok wszystkich urządzeń IoT i związanych z nimi luk w zabezpieczeniach. Wykorzystując dokładne informacje, takie jak baner serwera i dane nagłówka, RIoT określi markę i model konkretnego urządzenia IoT. Wykonuje również testy, aby sprawdzić, czy to urządzenie używa domyślnych lub zakodowanych na stałe poświadczeń do uwierzytelniania telnet, SSH lub podstawowego HTTP, które są preferowanymi wektorami ataku, które botnety początkowo wykorzystują do włamania do systemu. Za pomocą tego narzędzia osoba atakująca może określić docelowy adres IP lub zakres adresów IP w celu zidentyfikowania luk w zabezpieczeniach. Skaner luk w zabezpieczeniach RIoT umożliwia atakującym identyfikację wrażliwych urządzeń IoT, sprawdzanie domyślnych lub zakodowanych na stałe haseł oraz wykonywanie zewnętrznych skanów w celu zidentyfikowania luk w zabezpieczeniach IoT.

Sniffowanie za pomocą Foren6

Atakujący wykorzystują narzędzia takie jak Foren6 do wąchania ruchu urządzeń loT. Foren6 to nieinwazyjne narzędzie do analizy sieci 6L0WPAN. Wykorzystuje pasywne urządzenia sniffer do rekonstrukcji wizualnej i tekstowej reprezentacji informacji sieciowych w celu obsługi rzeczywistych aplikacji loT. Foren6 używa snifferów do przechwytywania ruchu 6L0WPAN i renderuje stan sieci w graficznym interfejsie użytkownika (GUI). Wykrywa problemy z routingiem. Protokół routingu dla sieci 6L0WPAN, RPL, to nowy standard IETF. Foren6 przechwytuje wszystkie informacje związane z RPL i identyfikuje nieprawidłowe zachowania. Łączy w sobie wiele snifferów i przechwytuje pakiety na żywo z wdrożonych sieci w nieinwazyjny sposób. Na przykład podstawowe kroki analizy rzeczywistej sieci 6L0WPAN przy użyciu modułu sniffer opartego na Contiki są następujące:

Otwórz Foren6 po instalacji

Teraz otwórz okno dialogowe „Zarządzaj źródłami", klikając przycisk Zarządzaj źródłami na pasku narzędzi lub z menu „Plik"

W tym oknie dialogowym usuń wszystkie istniejące wpisy w górnej części, wybierając każdy element i naciskając przycisk „Usuń".

Następnie dodaj nowe źródło, określając trzy pola, jak pokazano poniżej:

o Cel: Wpisz ścieżkę do urządzenia USB (przykład: /dev/ttyUSBO)

o Channel: Wartość całkowita kanału, który chcesz obwąchać (1 do 26)

o Typ: Wybierz wąchanie

Kliknij przycisk Dodaj po wprowadzeniu powyższych informacji

Jeśli urządzenie zostanie znalezione przez aplikację, pojawi się na liście dostępnych urządzeń. Jeśli twoje urządzenie istnieje, ale w tym momencie pojawia się błąd, prawdopodobnie użytkownik uruchamiający Foren6 nie ma uprawnień dostępu do tego urządzenia szeregowego. Następnie uruchom aplikację Foren6 jako root.

Przesuń przycisk Zamknij, aby powrócić do głównego okna

Kliknij przycisk Start (który będzie teraz włączony), aby uruchomić przechwytywanie pakietów

Sniffowanie za pomocą Wireshark

Wiele urządzeń LoT, takich jak kamery bezpieczeństwa, udostępnia stronę internetową do sterowania lub konfigurowania kamer ze zdalnej lokalizacji. Witryny te w większości implementują niezabezpieczony protokół HTTP zamiast HTTPS i są podatne na różne ataki. Jeśli kamery używają domyślnych poświadczeń fabrycznych, osoba atakująca może łatwo przechwycić cały ruch przepływający między kamerą a aplikacją internetową i uzyskać dostęp do samej kamery. Atakujący mogą użyć narzędzi takich jak Wireshark, aby przechwycić taki ruch i odszyfrować klucz Wi-Fi docelowej sieci. Czynności stosowane przez atakujących do wąchania ruchu bezprzewodowego z kamery internetowej:

Uruchom Nmap, aby zidentyfikować urządzenia loT używające niezabezpieczonych portów HTTP do przesyłania danych:

nmap -p 80,81,8080,8081 <Docelowy zakres adresów IP>

Teraz skonfiguruj kartę bezprzewodową w trybie monitorowania i zidentyfikuj kanał używany przez docelowy router do nadawania. W tym celu uruchom ifconfig, aby zidentyfikować swoją kartę bezprzewodową, tutaj:

wlan0

Uruchom Airmon-ng, aby przełączyć kartę bezprzewodową w tryb monitorowania:

airmon-ng start wlan0

Następnie uruchom Airodump-ng, aby przeskanować wszystkie pobliskie sieci bezprzewodowe:

airodump-ng start wlanOmon

Teraz odkryj docelową sieć bezprzewodową i zanotuj odpowiedni kanał, aby wykryć ruch za pomocą Wireshark

Następnie skonfiguruj kartę bezprzewodową, aby nasłuchiwała ruchu na tym samym kanale. Na przykład, jeśli kanał sieci docelowej to 11, uruchom Airmon-ng, aby ustawić słuchanie karty bezprzewodowej na kanale 11:

airmon-ng start wlanOmon 11

Uruchom Wireshark i kliknij dwukrotnie interfejs, który był utrzymywany w trybie monitorowania, tutaj wlanOmon, i zacznij przechwytywać ruch

Po przechwyceniu ruchu atakujący mogą odszyfrować klucze WEP i WPA za pomocą programu Wireshark oraz zhakować docelowe urządzenie loT w celu kradzieży poufnych informacji.

Analiza widma i ruchu IoT

Analiza widma za pomocą Gqrx

Gqrx to SDR zaimplementowany za pomocą narzędzia GNU Radio i Qt GUI. Atakujący używają urządzeń sprzętowych, takich jak klucze sprzętowe FunCube, Airspy, HackRF i RTL-SDR wraz z Gqrx SDR, do analizy widma.

Atakujący używają Gqrx do obserwacji pasm częstotliwości czujników temperatury/wilgotności, włączników światła, kluczyków samochodowych, nadajników M-bus itp. Gqrx może również umożliwić atakującemu słuchanie lub podsłuchiwanie częstotliwości radiowych FM lub dowolnych rozmów radiowych.

Kroki analizy widma za pomocą Gqrx:

Pakiet Gqrx i GNU Radio zawiera wszystkie narzędzia Gqrx. Aby zainstalować ten pakiet, użyj polecenia podanego poniżej:

apt-get install gnuradio gqrx

Atakujący używają narzędzi sprzętowych, takich jak FunCube Dongle Pro+, podłączając go do portu USB-2 komputera w celu analizy różnych pasm częstotliwości

Uruchom Gqrx za pomocą następującego polecenia:

gqrx

Polecenie to otwiera okno konfiguracji wejść/wyjść

* Kliknij przycisk Start/Stop, aby aktywować/dezaktywować Gqrx

* Po aktywacji Gqrx w centralnym oknie wyświetlane są częstotliwości, a ich odgłosy można usłyszeć przez słuchawki lub głośnik

Zmieniając ustawienia FFT (znajdujące się w prawym dolnym rogu), możesz przechwytywać i analizować różne częstotliwości w pobliżu.

Analiza ruchu IoT za pomocą IoT Inspector

Atakujący używają narzędzi takich jak LoT Inspector do wykrywania docelowych urządzeń IoT i analizowania ich ruchu sieciowego w celu identyfikacji luk w zabezpieczeniach. LoT Inspector pomaga atakującemu w naruszeniu prywatności i mechanizmy bezpieczeństwa. To narzędzie wyświetla luki w zabezpieczeniach w postaci tabel i wykresów. To umożliwia również atakującemu nagrywanie i odtwarzanie wszystkich informacji z komunikujących się urządzeń zbierać poufne informacje. LoT Inspector automatycznie skanuje i wyświetla dostępne urządzenia w sieci. Wybieranie urządzenie docelowe może wyświetlać działania sieciowe i punkty końcowe komunikacji urządzenie. Po kliknięciu „aktywności w sieci" wyświetla się na żywo wykres ruchu na urządzeniu dostępnym, a punkty końcowe komunikacji wyświetlą usługi, które posiada urządzenie IoT

Uruchom ataki

W fazie skanowania pod kątem luk atakujący próbują określić luki obecne w urządzeniu docelowym. Wykryte luki są następnie wykorzystywane do przeprowadzania różnych ataków, takich jak ataki DDoS, ataki z wykorzystaniem kodu zmiennego, ataki z zagłuszaniem sygnału, ataki Sybil, ataki MUM oraz ataki związane z kradzieżą danych i tożsamości. Na przykład osoba atakująca może użyć narzędzia RFCrack do przeprowadzenia ataku typu „rolling code", „replay" i „jamming" na urządzeniu. Podobnie osoba atakująca może również użyć narzędzi takich jak KillerBee do zaatakowania sieci ZigBee i IEEE 802.15.4.

Atak Rolling Code przy użyciu RFCrack

Atakujący wykorzystują narzędzie RFCrack, aby uzyskać kod zmienny wysłany przez ofiarę w celu odblokowania pojazdu, a następnie użyć tego samego kodu do odblokowania i kradzieży pojazdu. RFCrack służy do testowania

komunikacji RF między urządzeniami fizycznymi, które komunikują się na częstotliwościach sub-GFIz. Jest używany wraz z kombinacją sprzętu, takiego jak mierniki, do zagłuszania, odtwarzania i wąchania sygnału pochodzącego od nadawcy. Atakujący wykonują następujące ataki za pomocą RFCrack:

Wykonaj powtarzające się ataki (-i -F)

Wyślij zapisane ładunki (-s -u)

Wykonuj ataki z obejściem kodu zmiennego (-r -F -M)

Wykonaj zagłuszanie (-j -F)

Skanuj przyrostowo przez częstotliwości (-b -v -F)

Skanuj wspólne częstotliwości (-k)

Komendy używane przez atakującego do przeprowadzenia ataku typu Rolling-Code podano poniżej:

Powtórka na żywo:

python RFCrack.py -i

Kod kroczący:

python RFCrack.py -r -M MOD_2FSK -F 314350000

Dostosuj zakres RSSI:

python RFCrack.py -r -U "-75" -L "-5" -M MOD_2FSK -F 314350000

Zagłuszanie:

python RFCrack.py -j -F 314000000

Skanuj wspólne częstotliwości:

python RFCrack.py -k

Skanuj swoją listą:

python RFCrack.py -k -f 433000000 314000000 390000000

Skanowanie przyrostowe:

python RFCrack.py

Wyślij zapisany ładunek:

python RFCrack.py

MOD ZAPYTAJ OK

-b -v 5000000

-s -u ./files/test.cap -F 315000000 –M

Hakowanie urządzeń Zigbee za pomocą Attify Zigbee Framework

Większość urządzeń IoT wykorzystuje protokół ZigBee do komunikacji bezprzewodowej krótkiego zasięgu. Atakujący znajdują luki w zabezpieczeniach IoT i inteligentnych urządzeń opartych na ZigBee i wykorzystują je za pomocą narzędzi takich jak Attify ZigBee Framework. Atakujący wykorzystują luki w zabezpieczeniach tych urządzeń, aby wąchać poufne informacje podczas przesyłania, aw niektórych przypadkach przejąć kontrolę nad samym urządzeniem. Attify ZigBee Framework składa się z zestawu narzędzi służących do przeprowadzania testów penetracyjnych ZigBee. Protokół ZigBee wykorzystuje 16 różnych kanałów do całej komunikacji. Atakujący wykorzystują zbstumbler z platformy Attify Zigbee do identyfikacji kanału używanego przez urządzenie docelowe. Gdy atakujący to zidentyfikuje, zaczyna przechwytywać pakiety przesyłane z i/lub do urządzenia. Na tym etapie osoba atakująca może po prostu przeprowadzić atak z powtórzeniem, przechwytując i odtwarzając te same pakiety, aby obserwować zachowanie urządzenia. Następnie osoba atakująca może dokonać dalszej eksploatacji urządzenia.

Atak BlueBorne przy użyciu HackRF One

Urządzenia IoT wykorzystują komunikację bezprzewodową za pomocą RF, ZigBee lub LoRa. Atakujący używają HackRF One do wykonywania ataków, takich jak ataki BlueBorne lub AirBorne, w tym powtarzanie, fuzzowanie i zagłuszanie. HackRF One to zaawansowane radio definiowane sprzętowo i programowo o zakresie od 1 MHz do 6 GHz. Wysyła i odbiera fale radiowe w trybie half-duplex, dzięki czemu atakujący mogą łatwo przeprowadzać ataki przy użyciu tego urządzenia. Może wąchać szeroką gamę protokołów bezprzewodowych, od GSM po Z-wave.

Powtórz atak za pomocą HackRF One

Atakujący przeprowadzają ataki powtórkowe na docelowe urządzenia IoT za pomocą narzędzi takich jak HackRF One. Aby przeprowadzić ten atak, atakujący muszą odkryć częstotliwość radiową docelowego urządzenia. Atakujący wykorzystują zasoby online, takie jak baza danych FCC, w celu określenia częstotliwości docelowego urządzenia. Alternatywnie, atakujący używają również narzędzi, takich jak RTL-SDR, do określenia częstotliwości docelowego urządzenia w pobliżu. Po uzyskaniu częstotliwości atakujący używają narzędzi takich jak HackRF One do przeprowadzenia ataku powtórkowego. Kroki, aby przeprowadzić atak powtórkowy na docelowe urządzenie IoT:

Krok 1: Nagraj sygnał urządzenia za pomocą następującego polecenia:

hackrf_transfer -r złącze.raw -f [częstotliwość urządzenia]

Tutaj -r -> służy do nagrywania sygnału, -f -> częstotliwość urządzenia

Krok 2: Odtwórz sygnał do celu za pomocą następującego polecenia:

hackrf_transfer -t złącze.raw -f [częstotliwość urządzenia]

Tutaj -t -> służy do odtwarzania sygnału

Po pomyślnym przeprowadzeniu ataku atakujący może wydawać polecenia i kontrolować docelowe urządzenie IoT w celu przeprowadzenia dalszych ataków.

Ataki oparte na SDR przy użyciu RTL-SDR i GNU Radio

Atak sprzętowy

Atakujący używają narzędzi sprzętowych, takich jak RTL-SDR, do przeprowadzania ataków opartych na SDR na urządzeniu IoT.

RTL-SDR

Sprzęt RTL-STR jest dostępny w postaci klucza sprzętowego USB, który można wykorzystać do przechwytywania aktywnych sygnałów radiowych w pobliżu (połączenie z Internetem nie jest wymagane). Jest dostępny w różnych modelach, takich jak DVB-T SDR, RTL2832, klucz sprzętowy RTL lub klucz sprzętowy DVB-T. Narzędzie RTL-STR może przechwytywać częstotliwości w zakresie od 500 kHz do 1,75 GHz w oparciu o wybrane modele SDR.

Atakujący wykorzystują skaner radiowy RTL-SDR do wykonywania następujących czynności:

• Odbieranie i dekodowanie sygnałów GPS

• Analiza widma

• Słuchanie audycji radiowych DAB

• Słuchanie i dekodowanie radia HD

• Wąchanie sygnałów GSM

• Słuchanie radia amatorskiego VHF

• Skanowanie trankingowych rozmów radiowych

• Skanowanie w poszukiwaniu telefonów bezprzewodowych

Atak oparty na oprogramowaniu

Oprócz narzędzi sprzętowych atakujący mogą również atakować urządzenia loT oparte na SDR za pomocą różnych narzędzi programowych, takich jak GNU Radio.

GNU Radio

Narzędzie GNU Radio wykorzystuje zewnętrzny sprzęt RF do generowania SDR. Oferuje ramy i wymagane narzędzia do generowania programowych sygnałów radiowych. Oferuje również jednostki przetwarzające sygnały do realizacji radiotelefonów programowych. Atakujący używają GNU Radio do przeprowadzania różnych ataków opartych na SDR na docelowe urządzenia loT. Przed atakiem na urządzenie docelowe atakujący muszą zbudować i skonfigurować GNU Radio. Po udanej instalacji GNU Radio osoby atakujące wykorzystują poniższe narzędzia do dalszych ataków.

GNU Radio składa się z wielu predefiniowanych programów i narzędzi, które mogą być używane do różnych zadań, jeśli jest instalowane z Pythona, pliki źródłowe można znaleźć w gr-utils/src/python i gr-uhd/ aplikacje.

• uhd_ft Analizator widma, który można podłączyć do urządzenia UHD w celu znalezienia widma na danej częstotliwości

• uhd_rx_cfile -> Przechowuje próbki fal za pomocą urządzenia UHD; próbki można przechowywać w pliku i analizować później za pomocą GNU Radio lub podobnych narzędzi, takich jak Matlab lub Octave

• uhd_rx_nogui Służy do uzyskiwania i słuchania sygnałów przychodzących na urządzeniu audio

• uhd_siggen_gui Służy do tworzenia prostych sygnałów, takich jak sinus, kwadrat lub szum

• gr_plot Służy do prezentacji wcześniej nagranych sampli zapisanych w pliku

Atak kanałami bocznymi przy użyciu ChipWhisperer

ChipWhisperer to łańcuch narzędzi typu open source, używany głównie do badań bezpieczeństwa sprzętu wbudowanego oraz do przeprowadzania analizy mocy kanału bocznego i ataków powodujących usterki. Ataki te

służą głównie do wydobywania kluczy kryptograficznych z systemu. Atak typu side-channel to atak kryptograficzny, który wykorzystuje implementację systemu fizycznego w celu uzyskania informacji, takich jak informacje dotyczące zużycia energii, czasu, dźwięku i wycieków elektromagnetycznych, zamiast wykorzystywać luki w kodzie. Aby przeprowadzić atak typu side-channel, sprzęt ChipWhisperer potrzebuje następujących dwóch rzeczy:

• Karta przechwytywania: zawiera specjalny sprzęt używany do przechwytywania bardzo małych sygnałów z dokładnie zsynchronizowanym zegarem

Płytka docelowa: Jest to procesor, który można zaprogramować do wykonywania bezpiecznej operacji. Atakujący wykorzystują ChipWhisperer do złamania implementacji złożonych algorytmów, takich jak AES i potrójny DES, za pomocą techniki zwanej atakiem analizy mocy, która jest formą ataku bocznego. W tej metodzie atakujący przejmuje kontrolę nad danymi wejściowymi i zużyciem energii. Następnie znane dane wejściowe są poddawane operacji XOR z nieznanymi danymi wejściowymi w celu uzyskania nieznanych danych wyjściowych, a odgadnięty tajny klucz jest porównywany z rzeczywistymi pomiarami w celu uzyskania oryginalnego tajnego klucza. Niektóre z klas ataków typu side-channel używanych do uzyskiwania informacji o tajemnicach w systemie to ataki na pamięć podręczną, ataki czasowe, ataki z monitorowaniem zasilania, ataki elektromagnetyczne, kryptoanaliza akustyczna, analiza błędów, remanencja danych i ataki optyczne. ChipWhisperer jest również używany do wprowadzania usterek do dowolnego wbudowanego sprzętu z zamiarem ujawnienia informacji. W tym ataku atakujący może manipulować kodem, uzyskując dostęp do zegara lub mocy wejściowej urządzenia.

Identyfikacja magistral i interfejsów komunikacyjnych IoT

Atakujący identyfikują różne interfejsy szeregowe i równoległe, takie jak UART, Serial Peripheral Interface (SPI), Joint Test Action Group (JTAG) i Inter-

Układ scalony (I2C), aby uzyskać dostęp do powłoki, wyodrębnić oprogramowanie układowe i tak dalej. Atakujący używają takich narzędzi, jak BUS Auditor, Damn Insecure and Vulnerable Application (DIVA), płytka drukowana (PCB) oraz framework EXPLIoT do identyfikacji interfejsów. BUS Auditor składa się z 16 niezależnych kanałów (CHO do CH15). Najpierw należy połączyć styki uziemienia BUS Auditor i płyty DIVA IoT.

UART

Poniżej wymieniono kroki związane z identyfikacją UART na płytce drukowanej bez danych mikrokontrolerów:

1. Podłącz dwa kanały CHO i CHI BUS Auditor do nagłówka UART.

2. Podłącz do komputera zarówno kartę DIVA IoT, jak i BUS Auditor.

3. Uruchom następującą komendę w środowisku EXPLIOT:

uruchom busauditor.generic.uartscan -v 3.3 -p /dev/ttyACMO -s 0 -e 1

-v -> napięcie

-p -> port dev/tty*

-s -> kanał początkowy

-e -> kanał końcowy

JTAG

Joint Test Action Group (JTAG) dostosowana do IEEE 1149.1 składa się z czterech styków — wyboru trybu testowego (TMS), zegara testowego (TCK), wejścia danych testowych (TDI) i wyjścia danych testowych (TDO) — oraz jednego dodatkowego opcjonalnego styku , Reset testowy (TRST). Poniżej wymieniono kroki związane z identyfikacją JTAG:

1. Podłącz kanały CHO do CH8 BUS Auditor do nagłówka JTAG.

2. Podłącz do komputera zarówno kartę DIVA, jak i BUS Auditor.

3. Uruchom następującą komendę w środowisku EXPLIOT:

run busauditor.generic.jtagscan -v 3.3 -p /dev/ttyACMO -s 0 -e 10

I2C

Inter-Integrated Circuit (I2C) wykorzystuje dane szeregowe (SDA) do wysyłania i odbierania danych oraz zegar szeregowy (SCL).

Poniżej wymieniono kroki związane z identyfikacją I2C:

1. Podłącz kanały CHO do CH8 BUS Auditor do nagłówka.

2. Podłącz do komputera zarówno kartę DIVA, jak i BUS Auditor.

3. Uruchom następującą komendę w środowisku EXPLIOT:

run busauditor.generic.i2scan -v 3.3 -p /dev/ttyACMO -s 0 -e 10

SPI

Atakujący przeprowadzają wyszukiwanie w Google, aby zidentyfikować szeregowy interfejs peryferyjny (SPI) i jego pinouty za pomocą numerów chipów.

Poniżej wymieniono niektóre dodatkowe narzędzia do identyfikacji interfejsu:

JTAGulator (http://www.grandideastudio.com)

Attify Badge (https://www.attify-store.com)

Saleae Logic Analyzer (https://www.saleae.com)

NAND Glitching

Atakujący często skupiają się na uzyskaniu uprzywilejowanego dostępu do urządzeń lub routerów IoT, wykorzystując ich luki w zabezpieczeniach podczas uruchamiania za pomocą technik takich jak glitchowanie. Usterka NAND to proces uzyskiwania uprzywilejowanego dostępu do konta root podczas uruchamiania urządzenia, co można wykonać, wykonując połączenie uziemiające z stykiem szeregowego wejścia/wyjścia układu pamięci flash. Atakujący wykorzystują następującą lukę w zabezpieczeniach urządzenia wbudowanego: proces tworzenia kopii zapasowej załadowany do lokalnego układu pamięci flash w celu przyznania uprzywilejowanego dostępu pojedynczemu użytkownikowi podczas awarii uruchamiania. Odpowiednio zsynchronizowana usterka może trwać nawet 1 ms, co skutkuje uprzywilejowanym dostępem administratora do urządzenia docelowego.

Kroki wdrażania procesu NAND Glitching

Wykonaj następujące polecenie, aby zainicjować proces rekonesansu za pomocą przetwornika UART-USB

minicom -D /dev/ttyUSBO -w -C D-link_startup.txt

Powyższe polecenie zwraca dzienniki rozruchowe, które są przekazywane podczas uruchamiania urządzenia, co pomaga atakującemu w uzyskaniu rzeczywistego układu pamięci załadowanego z oprogramowaniem rozruchowym.

Glitching

Następnym krokiem jest zwarcie styku wejścia/wyjścia szeregowego układu pamięci flash do masy w celu przerwania trwającego procesu uruchamiania, co skutkuje załadowaniem zapasowego kodu programu ładującego.

Uruchom komendę printenv, aby wyświetlić bootargi załadowane podczas tego procesu, co zwróci następujące informacje:

bootargs=noinitrd ubi.mtd=5 root=ubi0:rootfs rw gpmi badupdater

console=ttyAM0,115200 rootfstype=ubifs

Uruchom następujące polecenie, aby załadować zmienne środowiskowe do urządzenia:

setenv bootargs 'noinitrd console=ttyAM0,115200 rootfstype=ubifs ubi.mtd=5 root=ubi0:rootfs rw gpmi init=/bin/sh';

Uruchom następujące polecenie w konsoli UART, aby uzyskać dostęp do konta root:

nand odczyt ${loadaddr} app-kernel 0x00400000 && bootm ${loadaddr}

W tym przypadku polecenie bootm pomaga w ładowaniu kopii zapasowej uprzywilejowanego obrazu rozruchowego

pamięć flash.

Uzyskaj zdalny dostęp

Luki zidentyfikowane w fazie skanowania luk w zabezpieczeniach umożliwiają atakującemu zdalne uzyskanie dostępu oraz kierowanie atakiem i kontrolowanie go, jednocześnie unikając wykrycia przez różne produkty zabezpieczające. W oparciu o luki w urządzeniu IoT, atakujący może zamienić urządzenie w backdoora, aby uzyskać dostęp do sieci organizacji bez infekowania jakiegokolwiek systemu końcowego chronionego przez IDS/IPS, firewall, oprogramowanie antywirusowe itp. Po uzyskaniu zdalnego dostępu, osoby atakujące wykorzystują te urządzenia jako platformę do przeprowadzania ataków na inne urządzenia w sieci.

Uzyskanie dostępu zdalnego za pomocą usługi Telnet

Atakujący przeprowadzają skanowanie portów, aby dowiedzieć się o otwartych portach i usługach na docelowym urządzeniu IoT. Jeśli atakujący zidentyfikuje, że port telnet jest otwarty, wykorzystuje tę lukę w celu uzyskania zdalnego dostępu do urządzenia. Wiele wbudowanych aplikacji systemowych w urządzeniach IoT, takich jak przemysłowe systemy sterowania, routery, telefony VoIP i telewizory, implementuje funkcje zdalnego dostępu za pomocą telnetu. Aplikacje te obejmują serwer telnet do zdalnego dostępu. Gdy atakujący zidentyfikuje otwarty port telnet, może dowiedzieć się, jakie informacje są udostępniane między podłączonymi urządzeniami, w tym ich oprogramowanie i modele sprzętu. Następnie atakujący przeprowadza dalsze ataki, wykorzystując swoje specyficzne podatności. Najpierw atakujący określa, czy wymagane jest uwierzytelnienie, czy nie. Jeśli nie, uzyskuje bezpośrednio nieautoryzowany dostęp w celu przeglądania danych przechowywanych na urządzeniu, jeśli wymagane jest uwierzytelnienie, atakujący próbuje wszystkich domyślnych poświadczeń, takich jak

root/root i system/system, lub przeprowadza atak brute-force w celu uzyskania hasła do kont administratora lub zwykłych użytkowników. Na przykład osoba atakująca może użyć narzędzi takich jak Shodan i Censys, aby uzyskać zdalny dostęp do urządzenia docelowego.

Zachowaj dostęp

Gdy osoba atakująca uzyska dostęp do urządzenia, stosuje różne techniki w celu utrzymania dostępu i dalszej eksploatacji. Atakujący pozostają niewykryci, czyszcząc dzienniki, aktualizując oprogramowanie układowe i używając złośliwych programów, takich jak backdoor, trojany itp., Aby zachować dostęp. Atakujący używają narzędzi, takich jak Firmware Mod Kit, Firmwalker, Firmalyzer Enterprise i Firmware Analysis Toolkit, aby wykorzystać oprogramowanie układowe.

Zachowaj dostęp, wykorzystując oprogramowanie sprzętowe

Zestaw Firmware Mod Kit umożliwia łatwą dekonstrukcję i rekonstrukcję obrazów oprogramowania układowego dla różnych urządzeń wbudowanych. Chociaż jest skierowany głównie do routerów opartych na systemie Linux, jest kompatybilny z większością oprogramowania układowego, które wykorzystuje popularne formaty oprogramowania układowego i systemy plików, takie jak TRX/ulmage i SquashFS/CramFS. Firmware Mod Kit to zbiór narzędzi, narzędzi i skryptów powłoki. Narzędzia mogą być używane bezpośrednio lub skrypty powłoki mogą być używane do automatyzacji i łączenia wspólnego oprogramowania układowego operacji (np. wyodrębnianie i odbudowywanie). Korzystając z zestawu Firmware Mod Kit, osoby atakujące mogą wykonać następujące czynności:

Wyodrębnij obraz oprogramowania układowego do jego części składowych

Użytkownik dokonuje żądanej modyfikacji w systemie plików oprogramowania układowego lub web Ul (webif)

Odbuduj oprogramowanie układowe

Sflashuj zmodyfikowane oprogramowanie układowe na urządzenie i zablokuj je

Poniżej wymieniono podstawowe skrypty ułatwiające obsługę oprogramowania układowego.

Skrypty podstawowe: Skrypty dodatkowe

extract-firmware.sh -> Wyodrębnianie oprogramowania układowego

scenariusz

ddwrt-gui-extract.sh -> Wyodrębnia pliki Web GUI

z wyodrębnionego oprogramowania DD-WRT

build-firmware.sh -> Przebudowa oprogramowania układowego

scenariusz

ddwrt-gui-rebuild.sh -> Przywraca zmodyfikowane

Pliki Web GUI do wyodrębnionego oprogramowania układowego DD-WRT

Analiza oprogramowania układowego i inżynieria wsteczna

Firmware działa jako centralny punkt w sterowaniu różnymi urządzeniami loT. Atakujący analizują oprogramowanie układowe docelowych urządzeń loT, aby odkryć leżące u jego podstaw luki i luki w

zabezpieczeniach. Atakujący przeprowadzają analizę oprogramowania układowego w celu zidentyfikowania haseł, tokenów API i punktów końcowych, uruchomionych usług podatnych na ataki, kont typu backdoor, używanych plików konfiguracyjnych, kluczy prywatnych, przechowywanych danych itp. Kroki stosowane przez osoby atakujące w celu przeprowadzenia analizy oprogramowania układowego i inżynierii wstecznej:

Uzyskaj oprogramowanie układowe

Po uzyskaniu dostępu do docelowego urządzenia IoT, rozpakuj firmware z urządzenia

Analiza oprogramowania układowego

Uruchom następujące polecenia, aby przeanalizować oprogramowanie układowe:

Uruchom komendę „file" na pliku „*.bin".

Sprawdź podpis MD5

Uruchom komendę „cat" na pliku *.md5

Uruchom komendę „md5sum" na pliku *.bin

Uruchom „strings" w pliku *.bin

Na przykład,

strings -n 10 xyz.bin > strings.out

less strings.out

Uruchom „hexdump" dla pliku *.bin

Na przykład,

hexdump -C -n 512 xyz.bin > hexdump.out

cat hexdump.out

Uruchomienie zrzutu szesnastkowego może pomóc zidentyfikować typ kompilacji oprogramowania układowego

Wypakuj system plików

Uruchom binwalk w celu analizy, inżynierii wstecznej i wyodrębnienia danych z obraz oprogramowania układowego

Na przykład,

binwalk xyz.bin

binwalk zidentyfikuje typ używanego systemu plików

Wyodrębnij system plików za pomocą „dd"

Na przykład,

dd if=xyz.bin bs=l pomiń=922460 liczba=2522318

of=xyz.squashfs

Zamontuj system plików

Utwórz katalog montowania

Na przykład mkdir rootfs

sudo mount -t ext2 {nazwa pliku} rootfs

Przeanalizuj zawartość systemu plików

Sprawdź następujące pliki i foldery po zamontowaniu systemu plików:

etc/passwd, etc/shadow, etc/ssl

grep -rnw ' /ścieżka/do/gdzieś/ ' -e "wzorzec" taki jak hasło,

admin i root.

znajdować . -nazwa „*.conf” i inne typy plików, takie jak *.pern, *.crt, *.cfg,

.sh i .bin.

Możesz także uruchomić skrypt Firmwalker, aby wyszukać te elementy w wyodrębnionym pliku system plików

Emuluj oprogramowanie sprzętowe do testów dynamicznych

Przeprowadź dynamiczne testy interfejsu sieciowego urządzenia za pomocą oprogramowania do emulacji, takiego jak QEMU lub Firmware Analysis Toolkit.

Identyfikacja architektury procesora: Użyj poleceń, takich jak file lub readelf, aby określić architekturę procesora.

Emulacja trybu użytkownika: Poniżej wymieniono polecenia emulacji trybu użytkownika:

qemu-mipsel -L <przedrostek> <binarny>

qemu-arm -L <przedrostek> <binarny>

qemu-<arch> -L <przedrostek> <binarny>

Inną opcją użycia QEMU jest wykonanie chroota między architekturami. Przenieś plik qemu-<arch>-static binary do głównego folderu systemu plików oprogramowania sprzętowego /usr/bin/ za pomocą następującego polecenia:

chroot ~/<nazwa pliku> /bin/

Narzędzia hakerskie IoT

Atakujący używają narzędzi hakerskich IoT do zbierania informacji o urządzeniach podłączonych do sieci, ich otwartych portach i usługach, obszarze ataku i powiązanych lukach w zabezpieczeniach w celu dalszej eksploatacji urządzenia i sieci organizacji. Ta sekcja dotyczy różnych narzędzi hakerskich IoT.

Narzędzia do zbierania informacji

Atakujący używają narzędzi do zbierania informacji, takich jak Shodan i Censys, w celu zebrania podstawowych informacji o docelowym urządzeniu i sieci. Za pomocą tych narzędzi atakujący uzyskują informacje, takie jak aktywne urządzenia podłączone do sieci, ich marka, otwarte porty i usługi, ich fizyczna lokalizacja itp.

Censys

Censys to publiczna wyszukiwarka i narzędzie do przetwarzania danych, wspierane przez dane zebrane z trwających skanów całego Internetu. Censys obsługuje wyszukiwanie pełnotekstowe na banerach protokołów i wysyła zapytania do szerokiego zakresu pól pochodnych. Może identyfikować określone podatne na ataki urządzenia i sieci oraz generować raporty statystyczne dotyczące ogólnych wzorców i trendów użytkowania. Censys stale monitoruje każdy osiągalny serwer i urządzenie w Internecie, dzięki czemu można je wyszukiwać i analizować w czasie rzeczywistym. Pozwala pentesterowi zrozumieć powierzchnię ataku sieciowego, odkryć nowe zagrożenia i ocenić ich globalny wpływ. Censys zbiera dane o hostach i witrynach internetowych poprzez codzienne skanowanie przestrzeni adresowej IPv4 przez ZMap i ZGrab, z kolei utrzymując bazę danych konfiguracji hostów i witryn.

Thingful

Thingful to wyszukiwarka służąca do wyszukiwania i wykorzystywania otwartych danych IoT z całego świata. Pomaga organizacjom podejmować lepsze decyzje dzięki zewnętrznym danym IoT. Gromadzi dane IoT w czasie rzeczywistym z dziesiątek branż, w tym pogody, środowiska, inteligentnych miast, energii i transportu. Potoki danych Thingful sprawiają, że znalezienie i wykorzystanie danych IoT jest szybkie i łatwe.

Narzędzia do sniffowania

Administratorzy systemów używają zautomatyzowanych narzędzi do monitorowania swojej sieci i urządzeń podłączonych do sieci, ale osoby atakujące niewłaściwie wykorzystują te narzędzia do wąchania danych sieciowych. Poniżej wymieniono niektóre narzędzia, których osoba atakująca może użyć do wąchania ruchu generowanego przez urządzenia IoT.

Suphacap

Suphacap, sniffer Z-Wave, to narzędzie sprzętowe służące do wąchania ruchu generowanego przez inteligentne urządzenia podłączone do sieci. Umożliwia atakującym monitorowanie w czasie rzeczywistym i przechwytywanie pakietów ze wszystkich sieci Z-Wave. Działa ze wszystkimi kontrolerami Z-Wave, w tym Fibaro, Homeseer, Tridium Niagara, Z-Way, SmartThings i Vera.

Poniżej wymieniono niektóre z dodatkowych narzędzi używanych do wąchania ruchu generowanego przez urządzenia IoT:

CloudShark (https://www.qocofe.com)

Ubiqua Protocol Analyzer (https://www.ubilogix.com)

Perytons Protocol Analyzers (http://www.perytons.com)

tcpdump (https://www.tcpdump.org)

Open Sniffer (https://www.sewio.net)

Narzędzia do skanowania luk w zabezpieczeniach

Skanowanie pod kątem luk w zabezpieczeniach pozwala atakującemu zidentyfikować luki w zabezpieczeniach urządzeń IoT i ich sieci oraz określić, w jaki sposób można je wykorzystać. Narzędzia te pomagają specjalistom ds. bezpieczeństwa sieci w przezwyciężaniu zidentyfikowanych słabych punktów w urządzeniu i sieci, sugerując różne techniki naprawcze w celu ochrony sieci organizacji.

beSTORM

beSTORM to inteligentny fuzzer, który wykrywa luki w zabezpieczeniach związane z przepełnieniem bufora, automatyzując i dokumentując proces dostarczania uszkodzonych danych wejściowych i obserwując nieoczekiwaną odpowiedź z aplikacji. Stosując zautomatyzowane techniki fuzzingu oparte na protokołach, beSTORM działa jako zautomatyzowane narzędzie do audytu czarnej skrzynki. Inteligentnie wypróbowuje praktycznie każdą kombinację ataków, zaczynając od najbardziej prawdopodobnych scenariuszy, i wykrywa anomalie aplikacji, które wskazują na udany atak. Odkrywa słabe punkty kodu i poświadcza siłę bezpieczeństwa dowolnego produktu bez dostępu do źródła kodu. Testuje dowolny protokół lub sprzęt, nawet te używane w IoT, kontroli procesów, motoryzacji i lotnictwie.

Poniżej wymieniono niektóre dodatkowe skanery luk w zabezpieczeniach dla urządzeń loT:

Metasploit Pro (https://www.ropid7.com)

IoTsploit (https://iotsploit.co)

loTSeeker (https://informotion.ropid7.com)

Bitdefender Home Scanner (https://www.bitdefender.com)

Inspektor loT (https://www.iot-inspector.com)

Narzędzia do przeprowadzania ataków opartych na SDR

Atakujący używają różnych narzędzi, takich jak RTL-SDR, GNU Radio i Universal Radio Hacker, do przeprowadzania różnych rodzajów ataków, takich jak ataki zwiadowcze, ataki powtórkowe i ataki kryptoanalizy, na urządzenia oparte na SDR.

Universal Radio Hacker

Universal Radio Hacker (URH) to oprogramowanie do badania nieznanych protokołów bezprzewodowych używanych przez różne urządzenia IoT. To narzędzie umożliwia atakującym wykonanie następujących czynności:

o Zidentyfikować interfejsy sprzętowe dla typowych SDR

o Wykonaj demodulację sygnałów

o Przypisz uczestników do przeglądu danych

o Złam nawet skomplikowane kodowanie, takie jak wybielanie danych CC1101

o Przypisz etykiety, aby ujawnić logikę protokołu

o Wykonaj automatyczną inżynierię wsteczną pól protokołów

o Wykonaj fuzzing, aby znaleźć luki w zabezpieczeniach

o Wykonaj modulację, aby wprowadzić dane z powrotem do systemu

Poniżej wymieniono niektóre z dodatkowych narzędzi do przeprowadzania ataków opartych na SDR:

BladeRF (https://www.nuond.com)

Rfcat (https://code.google.com)

HackRF (https://greotscottgodgets.com)

FunCube Dongle (http://www.funcubedongle.com)

Gqrx (https://gqrx.dk)

Narzędzia hakerskie IoT

Poniżej wymieniono niektóre narzędzia hakerskie IoT wykorzystywane przez osoby atakujące do wykorzystywania docelowych urządzeń i sieci IoT do przeprowadzania różnych ataków, takich jak DDoS, zagłuszanie i ataki BlueBorne.

IoTVAS

IoTVAS umożliwia dostawcom urządzeń i specjalistom ds. bezpieczeństwa przeprowadzanie automatycznej oceny bezpieczeństwa oprogramowania, które zasila urządzenia IoT (oprogramowanie sprzętowe) w celu zidentyfikowania luk w konfiguracji i aplikacjach. To narzędzie powiadamia użytkowników o wykrytych lukach w zabezpieczeniach i pomaga w ich łagodzeniu w odpowiednim czasie.

Poniżej wymieniono kilka dodatkowych narzędzi do hakowania IoT:

Firmwalker (https://github.com)

rfcat-rolljam (https://github.com)

KillerBee (https://github.com)

GATTack.io (http://www.gottock.io)

JTAGULATOR® (http://www.grondideostudio.com)

Środki zaradcze na ataki IoT

W tej sekcji omówiono różne środki bezpieczeństwa IoT, zarządzanie urządzeniami i narzędzia bezpieczeństwa, których można użyć do zapobiegania, ochrony i odzyskiwania danych po różnego rodzaju atakach na urządzenia IoT i ich sieci. Stosując te środki zaradcze, organizacje mogą wdrożyć odpowiednie mechanizmy bezpieczeństwa w celu ochrony poufnych informacji przesyłanych między urządzeniami a siecią korporacyjną.

Jak bronić się przed hakowaniem IoT

Wyłącz konta użytkowników „gość” i „demo”, jeśli są włączone.

Użyj funkcji „Zablokuj”, aby zablokować konta w przypadku nadmiernej liczby nieudanych prób logowania.

Zaimplementuj silny mechanizm uwierzytelniania.

Lokalizowanie sieci i urządzeń systemu sterowania za zaporami sieciowymi i izolowanie ich od sieci firmowej.

Implementacja IPS i IDS w sieci.

Wdrażaj kompleksowe szyfrowanie i korzystaj z infrastruktury klucza publicznego (PKI).

Użyj architektury VPN do bezpiecznej komunikacji.

Wdróż zabezpieczenia jako ujednolicony, zintegrowany system.

Zezwalaj tylko zaufanym adresom IP na dostęp do urządzenia z Internetu.

Wyłącz telnet (port 23).

Wyłącz port UPnP na routerach.

Chroń urządzenia przed fizycznymi manipulacjami.

Regularnie łataj luki w zabezpieczeniach i aktualizuj oprogramowanie urządzenia.

Monitoruj ruch na porcie 48101, ponieważ zainfekowane urządzenia próbują rozprzestrzeniać szkodliwy plik za pomocą portu 48101.

Pozycja węzłów mobilnych powinna być weryfikowana w celu odniesienia jednego węzła fizycznego tylko do jednego identyfikatora pojazdu, co oznacza, że jeden pojazd nie może mieć dwóch lub więcej identyfikatorów.

Należy wdrożyć ochronę danych; dlatego konto lub tożsamość użytkownika powinny być chronione i ukryte przed innymi użytkownikami.

Należy przeprowadzić uwierzytelnianie danych w celu potwierdzenia tożsamości pierwotnego węzła źródłowego.

Zachowaj poufność danych dzięki szyfrowaniu z kluczem symetrycznym.

Wdrażaj zasady silnych haseł, które wymagają hasła o długości co najmniej 8-10 znaków z kombinacją liter, cyfr i znaków specjalnych.

Używaj metod CAPTCHA i zasad blokowania konta, aby uniknąć ataków typu brute-force .

Korzystaj z urządzeń wyprodukowanych przez producentów, którzy mają doświadczenie w zakresie świadomości bezpieczeństwa.

Izoluj urządzenia IoT w chronionych sieciach.

Zaimplementuj opcję bezpiecznego rozruchu, która wykorzystuje techniki podpisywania kodu kryptograficznego, i upewnij się, że urządzenie wykonuje kod wygenerowany przez producenta oryginalnego sprzętu (OEM).

Zaimplementuj uwierzytelnianie dwukierunkowe za pomocą algorytmu kryptograficznego, który może używać zarówno kluczy symetrycznych przy użyciu SHA z HMAC, jak i kluczy asymetrycznych przy użyciu ECDSA.

Utwórz inwentaryzację zasobów w celu mapowania sieci i wykrywania wszystkich ścieżek wejścia i wyjścia, aby określić, czy sieć IoT ma własną bramę internetową, która nie jest zgodna z zasadami bezpieczeństwa lub obowiązującymi przepisami, regulacjami i umowami.

Zastosuj kontrolę dostępu między urządzeniami IoT a zasobami IT, korzystając z korporacyjnych zapór ogniowych, IDS/IPS, UBA, 1AM itp.

Zawsze czytaj politykę prywatności aplikacji przed instalacją, aby sprawdzić, do jakich informacji może uzyskać dostęp.

Użyj zaufanego środowiska wykonawczego (TEE) lub elementu bezpieczeństwa (SE), TrustZone dla ARM, aby zabezpieczyć poufne informacje.

Zaimplementuj aktywne maskowanie lub ekranowanie, aby chronić urządzenia przed atakami typu side-channel.

Sprawdź poprawność kodu bezpośrednio przed jego użyciem, aby zmniejszyć ryzyko ataków typu time-of-check to time-ofuse (TOCTOU).

Zabezpiecz klucze szyfrowania i poświadczenia, przechowując je w module Secure Access Module (SAM), Trusted Platform Module (TPM), Hardware Security Module (HSM) lub innym zaufanym magazynie kluczy.

Zapobiegaj ujawnianiu adresów IP, wyłączając WebRTC w przeglądarce.

Używaj blokad reklam i rozszerzeń niemożliwych do śledzenia dostępnych w przeglądarce, aby zapobiegać atakom internetowym na urządzenia IoT.

Filtruj prywatne adresy IP z odpowiedzi DNS za pomocą dnswall, aby zapobiec atakom polegającym na ponownym powiązaniu DNS.

Użyj opartego na chmurze rozwiązania anty-DDoS do filtrowania lub przekierowania złośliwego ruchu DDoS.

Wykorzystaj sieci dystrybucji treści (CDN) i usługi inteligentnego rozpoznawania DNS, aby zapewnić dodatkową warstwę infrastruktury sieciowej.

Zmień domyślne ustawienia routera, w tym nazwę routera i hasło.

Nie używaj publicznych sieci Wi-Fi do zarządzania urządzeniami IoT.

Wyłącz niechciane funkcje urządzeń IoT, gdy nie są używane.

Wdrażaj rozwiązania oparte na chmurze, które zapewniają większe bezpieczeństwo urządzeniom brzegowym IoT.

Utrzymuj odpowiednią politykę ujawniania luk w celu poprawy bezpieczeństwa. Należy okresowo dbać o te luki w zabezpieczeniach i sprawdzać ich poprawność.

Zastosuj zasady dostępu z ograniczonymi uprawnieniami zarówno do sprzętu, jak i oprogramowania sprzętowego IoT (tj. nieużywane porty, uprzywilejowany dostęp do danych, dostęp administracyjny itp.).

Jak zapobiegać atakom opartym na SDR

Ataki na urządzenia IoT można przeprowadzać z dowolnego kierunku przy wytrwałych wysiłkach i posiadaniu wiedzy na temat niektórych dostępnych narzędzi. Należy jednak działać proaktywnie, aby zapobiegać takim atakom, zanim urządzenia zostaną naruszone. Następujące metody mogą pomóc w ochronie urządzeń IoT przed atakami opartymi na SDR:

Zabezpieczenie sygnału

Jednym z najważniejszych środków zapobiegawczych pozwalających uniknąć ataków radiowych opartych na oprogramowaniu jest zabezpieczenie sygnałów za pomocą standardowych metod szyfrowania.

Unikanie powtarzania poleceń przy użyciu techniki toczenia

Częste używanie tych samych poleceń może pozwolić na powtarzające się ataki. Polecenia powinny być inicjowane w oparciu o schemat ruchomego okna; oznacza to, że polecenie użyte wcześniej nie powinno być inicjowane ponownie. Luki w tej implementacji mogą pozwolić na ataki typu brute-force.

Przyjęcie synchronizacji i półbajtów preambuły

Oddziel sekwencję poleceń za pomocą preambuły i półbajtów synchronizacji, w przeciwnym razie protokoły można brutalnie wymusić przy użyciu metody redukcji, takiej jak sekwencja de Bruijna. Może to nakładać się na wspólne bity negocjujące liczbę bitów potrzebnych do odtworzenia wielu sekwencji poleceń.

Ogólne wytyczne dla producentów urządzeń IoT

Producenci urządzeń IoT powinni zapewnić wdrożenie następujących podstawowych środków bezpieczeństwa:

SSL/TLS powinien być używany do celów komunikacyjnych.

Powinna istnieć wzajemna kontrola certyfikatów SSL i listy unieważnionych certyfikatów.

Należy zachęcać do używania silnych haseł.

Upewnij się, że poświadczenia nie są zakodowane na stałe; muszą być przechowywane oddzielnie w bezpiecznym zaufanym magazynie.

Proces aktualizacji urządzenia powinien być prosty, zabezpieczony łańcuchem zaufania.

Zaimplementuj mechanizmy blokady konta po pewnych niepoprawnych próbach logowania, aby zapobiec atakom siłowym.

Blokuj urządzenia zawsze i wszędzie, gdzie to możliwe, aby zapobiec atakom.

Okresowo sprawdzaj urządzenie pod kątem nieużywanych narzędzi i korzystaj z białej listy, aby zezwalać na uruchamianie tylko zaufanych narzędzi lub aplikacji.

Użyj bezpiecznego łańcucha rozruchowego, aby zweryfikować całe oprogramowanie uruchamiane na urządzeniu.

Analizuj nowe funkcje produktu pod kątem luk w zabezpieczeniach, zanim zostaną wydane.

Używaj bezpiecznych funkcji, takich jak (gets()->fgets()), aby zmniejszyć ryzyko przepełnienia bufora, ponieważ większość programów IoT jest napisana w C lub C++.

Włącz zabezpieczenia do cyklu życia oprogramowania IoT.

Zapewnienia bezpieczeństwa danych osobowych użytkowników poprzez udzielanie szczegółowych informacji dotyczących udostępniania informacji i przekazywania danych.

Zapewnij konsumentom odpowiednie wytyczne dotyczące bezpieczeństwa urządzenia i ustawień konfiguracyjnych.

Zaimplementuj zewnętrzne ostrzeżenie o sabotażu sprzętu, aby zapewnić fizyczne bezpieczeństwo urządzenia IoT dla użytkownika końcowego.

OWASP 10 najlepszych rozwiązań luk w zabezpieczeniach IoT

Technologia IoT rozwijała się szybko, nie poświęcając należytej uwagi bezpieczeństwu urządzeń. Ze względu na luki bezpieczeństwa obecne w urządzeniach IoT, ryzyko związane z potencjalnymi cyberatakami, kradzieżą poufnych informacji, naruszeniem prywatności itp. szybko rośnie. Konieczne jest, aby programiści lub specjaliści ds. bezpieczeństwa przetestowali urządzenia pod kątem różnych luk w zabezpieczeniach przed zintegrowaniem systemu IoT i produktów z infrastrukturą. Poniżej podano 10 największych luk w zabezpieczeniach OWASP oraz rozwiązania związane z każdą luką:

Luki w zabezpieczeniach: Rozwiązania

1. Słabe, łatwe do odgadnięcia lub zakodowane na stałe hasła:

* Użyj automatycznego zarządzania hasłami (APM)

* Używaj silnych i złożonych haseł

* Unikaj używania zakodowanych na stałe haseł

2. Niebezpieczne usługi sieciowe:

* Zamknij otwarte porty sieciowe

* Wyłącz UPnP

* Szyfruj dane przed komunikacją TLS

3. Niebezpieczne interfejsy ekosystemów:

* Włącz mechanizm blokady konta

* Przeprowadzaj okresową ocenę interfejsów

* Wykonaj sprawdzanie poprawności i filtrowanie danych wyjściowych

* Używaj silnego hasła i uwierzytelniania dwuskładnikowego

4. Brak mechanizmu bezpiecznej aktualizacji:

* Sprawdź źródło i integralność aktualizacji

* Szyfruj komunikację między punktami końcowymi

* Powiadamiaj użytkowników końcowych o aktualizacjach zabezpieczeń

5. Używanie niezabezpieczonych lub przestarzałych komponentów:

* Regularnie monitoruj nieobsługiwane komponenty

* Usuń nieużywane zależności i niepotrzebne funkcje

* Unikaj oprogramowania innych firm z zagrożonego łańcucha dostaw

6. Niewystarczająca ochrona prywatności:

* Zminimalizuj gromadzenie danych

* Anonimizuj zebrane dane

* Zapewnij użytkownikom końcowym możliwość decydowania, jakie dane są gromadzone

7. Niebezpieczny transfer i przechowywanie danych:

* Szyfruj komunikację między punktami końcowymi

* Utrzymanie implementacji SSL/TLS

* Unikaj używania odpowiednich rozwiązań szyfrujących

8. Brak zarządzania urządzeniami:

* Czarna lista złośliwych urządzeń z podejrzanych źródeł

* Sprawdź wszystkie atrybuty aktywów

* Bezpieczna likwidacja urządzeń

9. Niezabezpieczone ustawienia domyślne:

* Zmień domyślne nazwy użytkownika i hasła

* Niestandardowa modyfikacja ustawień prywatności i bezpieczeństwa

* Wyłącz zdalny dostęp do urządzeń IoT, gdy nie są używane

10. Brak hartowania fizycznego:

* Ustaw unikalne hasło dla BIOS/firmware

* Skonfiguruj kolejność uruchamiania urządzeń, aby zapobiec nieautoryzowanemu uruchamianiu

* Zminimalizuj porty zewnętrzne, takie jak porty USB

Hartowanie

Zagadnienia dotyczące bezpieczeństwa platformy IoT

Aby zaprojektować bezpieczne i chronione urządzenia IoT, należy odpowiednio rozważyć kwestie bezpieczeństwa. Jedną z najważniejszych kwestii jest opracowanie bezpiecznego środowiska IoT do budowy urządzenia. W idealnej sytuacji framework powinien być zaprojektowany w sposób zapewniający domyślne zabezpieczenia, aby programiści nie musieli go później rozważać. Kryteria oceny bezpieczeństwa dla ram IoT są podzielone na cztery części. Każda część ma swoje własne problemy związane z bezpieczeństwem, które są omówione w kryteriach oceny dla każdej części. Poniżej omówiono kryteria oceny bezpieczeństwa urządzeń IoT:

Krawędź

Edge to główne urządzenie fizyczne w ekosystemie IoT, które wchodzi w interakcję z otoczeniem i zawiera różne komponenty, takie jak czujniki, siłowniki, systemy operacyjne, sprzęt i sieć oraz możliwości komunikacyjne. Jest heterogeniczny i można go wdrożyć w dowolnym miejscu iw każdych warunkach. W związku z tym idealna platforma dla krawędzi byłaby taka, która zapewniałaby komponenty międzyplatformowe, dzięki czemu można ją wdrożyć i działać w każdych możliwych warunkach fizycznych. Inne kwestie ramowe dotyczące krawędzi to

odpowiednia komunikacja i szyfrowanie pamięci masowej, brak domyślnych poświadczeń, silne hasła, korzystanie z najnowszych, aktualnych komponentów itp.

Wejście

Brama stanowi pierwszy krok do wejścia na krawędź świata Internetu, ponieważ łączy inteligentne urządzenia z komponentami chmury. Nazywany jest agregatorem komunikacji, który umożliwia komunikację z bezpieczną i zaufaną siecią lokalną oraz bezpieczne połączenie z niezaufaną siecią publiczną. Zapewnia również warstwę bezpieczeństwa wszystkim podłączonym do niej urządzeniom. Brama służy jako punkt agregacji dla krawędzi; dlatego pełni kluczową rolę w zakresie bezpieczeństwa w ekosystemie. Idealna struktura bramy powinna obejmować silne techniki szyfrowania w celu zapewnienia bezpiecznej komunikacji między punktami końcowymi. Ponadto mechanizm uwierzytelniania dla komponentów brzegowych powinien być tak silny, jak każdy inny komponent w ramach. Tam, gdzie to możliwe, brama powinna być zaprojektowana w taki sposób, aby uwierzytelniała się wielokierunkowo w celu przeprowadzenia zaufanej komunikacji między brzegiem a chmurą. Należy również zapewnić automatyczne aktualizacje urządzenia w celu przeciwdziałania lukom w zabezpieczeniach.

Platforma chmurowa

W ekosystemie IoT komponent chmurowy nazywany jest centralnym punktem agregacji i zarządzania danymi. Dostęp do chmury musi być ograniczony. Komponent chmury jest zwykle bardziej zagrożony, ponieważ jest centralnym punktem agregacji danych dla większości danych w ekosystemie. Obejmuje również komponent dowodzenia i kontroli (C2), który jest scentralizowanym komputerem, który wydaje różne polecenia w celu dystrybucji rozszerzeń i aktualizacji. Bezpieczna struktura komponentu chmurowego powinna obejmować szyfrowaną komunikację, silne uwierzytelnianie, bezpieczny interfejs sieciowy, szyfrowaną pamięć masową, automatyczne aktualizacje itp.

Mobilne

W ekosystemie IoT interfejs mobilny odgrywa ważną rolę, szczególnie tam, gdzie dane muszą być gromadzone i zarządzane. Korzystając z interfejsów mobilnych, użytkownicy mogą uzyskiwać dostęp do krawędzi i wchodzić z nią w interakcje w domu lub miejscu pracy z odległości wielu kilometrów. Niektóre aplikacje mobilne dostarczają użytkownikom tylko ograniczone dane z określonych urządzeń brzegowych, podczas gdy inne pozwalają na pełną manipulację komponentami brzegowymi. Należy zwrócić szczególną uwagę na interfejs mobilny, ponieważ jest on podatny na różne cyberataki.

Idealny framework dla interfejsu mobilnego powinien zawierać odpowiedni mechanizm uwierzytelniania użytkownika, mechanizm blokady konta po określonej liczbie nieudanych prób, bezpieczeństwo lokalnego przechowywania danych, szyfrowane kanały komunikacji oraz bezpieczeństwo danych przesyłanych tym kanałem.

Najlepsze praktyki w zakresie bezpieczeństwa sprzętu IoT

Zabezpieczenie sprzętu IoT odgrywa ważną rolę w zapobieganiu najbardziej uporczywym atakom na poziomie początkowym. Istnieje jednak kilka różnic w produkcji, rozwoju i wdrażaniu sprzętu IoT różnych producentów. Organizacje mogą zastosować następujące środki zaradcze w celu zabezpieczenia swojego sprzętu IoT przed najbardziej uporczywymi atakami powszechnymi we współczesnym cyfrowym świecie:

Ogranicz punkty wejścia

Ogranicz zakres wejść dla atakujących, unikając wdrażania dodatkowych punktów wejścia, takich jak porty USB, do sprzętu IoT. Pomaga to uniknąć wtargnięcia atakujących przez otwarte lub nieużywane porty. Zablokuj najmniej używane lub otwarte punkty wejścia, aby uniknąć bezpośredniego wtargnięcia do urządzenia.

Zastosuj sprzętowy mechanizm ochrony przed manipulacją

Zaimplementuj mechanizm wykrywania ingerencji w sprzęt, aby wykrywać bezpośrednie uszkodzenia fizyczne lub wtargnięcie na poziom płyty głównej sprzętu IoT. Pomaga to w wykrywaniu podnoszenia urządzenia, modyfikacji, zdejmowania pokrywy, dostępu na poziomie układu scalonego itp. na jednostce sprzętowej. Instalacja odpowiedniego urządzenia GPS pomaga również w śledzeniu zgubionego urządzenia.

Monitoruj bezpieczne uruchamianie

Monitoruj źródło rozruchu, aby uniemożliwić atakującym modyfikację lub usterkę jednostki sprzętowej w celu przeprowadzenia ataków na poziomie rozruchu, co zapewnia atakującym uprzywilejowany dostęp. W zależności od wartości aktywów wdrażaj bezpieczne mechanizmy przechowywania danych, takie jak układy Trusted Platform Module (TPM).

Wdrażaj poprawki bezpieczeństwa

Aktualizuj oprogramowanie układowe w odpowiednim czasie iw bezpieczny sposób, ponieważ sprzęt IoT staje się podatny na poważne zagrożenia podczas procesów aktualizacji przed i po aktualizacji.

Utrzymuj odpowiedni system zarządzania interfejsem

Prawidłowo zintegruj sprzęt IoT z bezpiecznymi interfejsami na etapie opracowywania, aby uniknąć wykradania API i bibliotek z urządzenia. Interfejsy API stwarzają luki w zabezpieczeniach sprzętu, ponieważ dostarczają rzeczywistych danych dotyczących działań i funkcjonalności urządzenia w lokalizacji użytkownika końcowego.

Unikaj otwartego dostępu do jednostki sprzętowej

Zaimplementuj odpowiednią ochronę fizyczną jednostki sprzętowej, ponieważ większość wdrożeń sprzętu IoT odbywa się w otwartych miejscach publicznych i trudnych warunkach. Aby uniknąć poważnych uszkodzeń jednostki sprzętowej, zamknij wszystkie otwarte porty lub punkty wejścia za pomocą atrap, aby uniknąć niepożądanej ingerencji lub fizycznego uszkodzenia jednostki.

Bezpieczne klucze uwierzytelniające

Bezpiecznie zabezpiecz klucze używane do uwierzytelniania każdego urządzenia powiązanego z unikalnym identyfikatorem urządzenia utworzonym przez odpowiednią usługę w chmurze. Zaimplementuj odpowiedni mechanizm bezpieczeństwa, aby zabezpieczyć wszystkie te klucze, ponieważ naruszenie bezpieczeństwa tych list kluczy umożliwia atakującym kontrolę nad jednostkami sprzętowymi.

Utrzymuj prawidłowy mechanizm rejestrowania zdarzeń

Wdrażaj terminowe audyty bezpieczeństwa, aby utrzymywać mechanizm ciągłego rejestrowania i monitorowania zdarzeń w celu poprawy obsługi incydentów i reagowania na nie. Utrzymuj odpowiednie dzienniki dla wszystkich naruszeń bezpieczeństwa, aby zapobiec powtarzającym się atakom na jednostki sprzętowe.

Utrzymuj odpowiedni system ochrony przed złośliwym oprogramowaniem

Zainstaluj zaufane oprogramowanie antywirusowe/przeciw złośliwemu oprogramowaniu innych firm, aby wykrywać i unikać naruszeń bezpieczeństwa w punktach wejścia jednostki sprzętowej.

Włącz domyślny mechanizm rejestrowania na poziomie podstawowym

Okresowo monitoruj dzienniki wpisów, włączając funkcję ciągłego rejestrowania zapewnianą przez większość systemów operacyjnych (OS). Mechanizm monitorowania logów pomaga uniknąć poważnych naruszeń bezpieczeństwa na poziomie wejścia.

Chroń poświadczenia dostępu do urządzenia

Zabezpiecz dane uwierzytelniające dostęp do urządzenia, utrzymując kilka mechanizmów bezpieczeństwa, takich jak implementacja liczb magicznych, szyfrowanie i uwierzytelnianie dwuskładnikowe.

Odizoluj urządzenia od regularnych jednostek zasilających

Zabezpiecz urządzenie przed elektryfikacją i atakami kolcami, takimi jak ataki młotem wioślarskim, które powodują nagły wzrost impulsów elektrycznych i powodują uszkodzenie układów scalonych i rdzenia pamięci RAM.

Wdrożenie mechanizmu Root-on-Trust

Zapewnij bezpieczny system punktu wejścia dla dostępu na poziomie administratora, wdrażając mechanizm „root-on-trust", który umożliwia dostęp tylko zaufanym lub autoryzowanym użytkownikom.

Bezpieczne starsze jednostki obsługujące nowoczesne funkcje zabezpieczeń bramek

Wdrażaj nowoczesne bramki w sieciach IoT zawierających starsze jednostki, aby stosować mechanizmy bezpieczeństwa bez żadnych zmian lub aktualizacji urządzenia.

Poniżej przedstawiono środki zaradcze dotyczące szyfrowania danych komunikacyjnych i modułów TPM jednostek sprzętowych IoT:

Korzystaj z oprogramowania uwierzytelniającego innych firm, takiego jak szyfrowanie dysków Bitlocker, aby uwierzytelniać dane importowane z zewnętrznej lokalizacji pamięci masowej poza granicami modułu TPM.

Zastosuj narzędzia programowe, takie jak Nuvoton, dla jednostek sprzętowych IoT, korzystając z interfejsów komunikacyjnych, takich jak I2C i SPI w urządzeniach TPM.

Powiąż dane, które mają zostać przesłane, za pomocą klucza powiązania TPM, który jest specjalnym kluczem szyfrowania opartym na standardzie szyfrowania RSA.

Wdrażaj koncepcję pieczętowania i otwierania uwierzytelniania sprzętowego podczas głównych aktualizacji obliczeniowych jednostek sprzętowych IoT, takich jak aktualizacje oprogramowania układowego i poprawki zabezpieczeń.

Zastosuj mechanizm bezpiecznej komunikacji danych oparty na kluczu HMAC między urządzeniem IoT opartym na module TPM a użytkownikiem końcowym.

Zaimplementuj szyfrowanie oparte na kluczu symetrycznym dla aplikacji o niskiej transmisji danych, w których dane są przechowywane poza granicami modułu TPM, aby zapewnić autentyczność i integralność importowanych danych.

Zweryfikuj uwierzytelnienie nadawcy przed odszyfrowaniem otrzymanych danych, korzystając z procedury weryfikacji HMAC obsługiwanej przez urządzenia TPM przy użyciu algorytmów szyfrowania w trybie blokowym, takich jak łańcuch bloków szyfrowania (CBC) i sprzężenie zwrotne tekstu zaszyfrowanego (CFB).

Korzystaj z szyfrowania opartego na RSA, aby zapewnić integralność danych za pomocą podpisu cyfrowego.

Moduły TPM ułatwiają przechowywanie kluczy w nieulotnej pamięci o dostępie swobodnym (NVRAM), aby włączyć opcję R/W podczas niepożądanych incydentów, takich jak utrata danych z powodu stresu środowiskowego lub złośliwych ataków.

Wykorzystaj kanoniczny tryb przesyłania danych, który pomaga zoptymalizować przesyłanie danych, eliminując niechciane bajty z aplikacji do komunikacji z przedłużonym strumieniem danych przy użyciu urządzeń IoT opartych na TPM.

Wykorzystaj modele root-of-trust (RT), takie jak RT do pomiarów (RTM) i RT do weryfikacji (RTV), dostarczane przez urządzenia TPM, do bezpiecznego uruchamiania i transmisji danych w jednostkach sprzętowych IoT.

Zarządzanie urządzeniami IoT

Zarządzanie urządzeniami IoT pomaga specjalistom ds. bezpieczeństwa śledzić, monitorować i zarządzać fizycznymi urządzeniami IoT ze zdalnej lokalizacji. Specjaliści ds. bezpieczeństwa mogą korzystać z rozwiązań takich jak Azure IoT Central, Oracle Fusion Cloud Internet of Things (IoT) i Predix do zarządzania urządzeniami IoT. Rozwiązania te umożliwiają specjalistom ds. bezpieczeństwa zdalną aktualizację oprogramowania układowego. Ponadto zarządzanie urządzeniami IoT pomaga w udzielaniu uprawnień i zwiększaniu możliwości bezpieczeństwa w celu zapewnienia ochrony przed różnymi lukami w zabezpieczeniach. Zarządzanie urządzeniami IoT może bardzo pomóc w zapobieganiu atakom IoT, ponieważ zapewnia:

Właściwe uwierzytelnianie, ponieważ rejestrowane są tylko zaufane i bezpieczne urządzenia z odpowiednimi danymi uwierzytelniającymi

Dokładna konfiguracja, sterowanie urządzeniami w celu zapewnienia właściwej funkcjonalności i lepszej wydajności. Może również przywrócić ustawienia fabryczne podczas likwidacji urządzenia.

Właściwe monitorowanie w celu wykrywania wad i diagnozowania problemów operacyjnych i błędów oprogramowania za pomocą dzienników programu

Bezpieczna konserwacja urządzeń zdalnych i częste aktualizacje urządzeń dzięki najnowszym poprawkom bezpieczeństwa

Rozwiązania do zarządzania urządzeniami IoT

Rozwiązania do zarządzania urządzeniami IoT są używane przez specjalistów ds. bezpieczeństwa, administratorów IT lub IoT administratorów do wdrażania, organizowania, monitorowania i zarządzania urządzeniami IoT omówione poniżej przedstawiono niektóre rozwiązania do zarządzania urządzeniami IoT:

Azure IoT Central

Azure IoT Central to hostowana, rozszerzalna platforma oprogramowania jako usługi (SaaS), która upraszcza konfigurację rozwiązań IoT. Pomaga łatwo łączyć się, monitorować i zarządzać zasobami IoT na dużą skalę. Azure IoT Central może uprościć początkową konfigurację rozwiązania IoT i zmniejszyć obciążenie związane z zarządzaniem, koszty operacyjne i koszty ogólne typowego projektu IoT.

Poniżej wymieniono niektóre z dodatkowych rozwiązań do zarządzania urządzeniami IoT:

Oracle Fusion Cloud Internet rzeczy (IoT) (https://www.orocle.com)

Predix (https://www.ge.com)

Cloud IoT Core (https://cloud.google.com)

Platforma IBM Watson IoT (https://www.ibm.com)

BalenaCloud (https://www.boleno.io)

Narzędzia bezpieczeństwa IoT

IoT to nie jedyna gama urządzeń podłączonych do Internetu, ale także bardzo złożona, szybko rozwijająca się technologia. Aby zrozumieć i przeanalizować różne czynniki ryzyka, należy zastosować odpowiednie rozwiązania zabezpieczające w celu ochrony urządzeń IoT. Korzystanie z narzędzi bezpieczeństwa IoT pomaga organizacjom znacznie ograniczyć luki w zabezpieczeniach, chroniąc w ten sposób urządzenia i sieci IoT przed różnymi rodzajami ataków.

SeaCat.io

SeaCat.io to bezpieczna technologia SaaS do obsługi produktów IoT w niezawodny, skalowalny i bezpieczny sposób. Zapewnia ochronę użytkownikom końcowym, firmom i danym. Specjaliści ds. bezpieczeństwa używają SeaCat.io do zarządzania połączonymi produktami z centralnego miejsca, uzyskiwania dostępu do zdalnych urządzeń za pomocą różnych narzędzi, monitorowania podłączonych urządzeń i automatyzacji aktualizacji w celu naprawiania błędów, ochrony użytkowników za pomocą autoryzowanej kryptografii i przestrzegania przepisów, zapewnienia, że urządzenia są wolne od złośliwego oprogramowania i zapobiegania hakerzy przed kontrolowaniem ich i uczynieniem ich częścią botnetu itp.

Menedżer urządzeń DigiCert IoT

DigiCert IoT Device Manager wykorzystuje nowoczesną infrastrukturę klucza publicznego (PKI), aby zapewnić cyfrowe zaufanie, które spełnia potrzeby nawet najbardziej wymagających wdrożeń IoT. Rozwiązanie centralnie zarządza wykrywaniem, raportowaniem, tworzeniem i unieważnianiem certyfikatów oraz dostępem i uprawnieniami użytkowników. Umożliwia łatwą współpracę zabezpieczeń przedsiębiorstwa z dowolną liczbą systemów korzystających z interfejsu programowania aplikacji REST (API), protokołu Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) i protokołu zarządzania certyfikatami w wersji 2 (CMPv2).

Poniżej wymieniono niektóre z dodatkowych narzędzi i rozwiązań bezpieczeństwa IoT:

FortiNAC (https://www.fortinet.com)

Darktrace Antigena (https://www.darktrace.com)

Symantec Critical System Protection (https://www.symantec.com)

Cisco Industrial Threat Defense (https://www.cisco.com)

AWS IoT Device Defender (https://aws.amazon.com)

Bayshore Industrial Cyber Protection Platform (https://www.bayshorenetworks.com)

NSFOCUS ADS (https://nsfocusglobal.com)

Norton Core (https://us.norton.com)

zvelo IoT Security Solution (https://zvelo.com)

Barbara (https://barbaraiot.com)

Sternum (https://www.sternumiot.com)

Pulse Secure (https://www.pulsesecure.net)

ByteSweep (https://gitlab.com)

Fortify Static Code Analyzer (https://www.microfocus.com)

IOT ASSET DISCOVERY (https://securolytics.io)

Hakowanie OT

Koncepcje ST

Technologia operacyjna (OT) odgrywa ważną rolę w dzisiejszym nowoczesnym społeczeństwie, ponieważ steruje zbiorem urządzeń zaprojektowanych do współpracy jako zintegrowany lub jednorodny system. Na przykład OT w telekomunikacji służy do przesyłania informacji z sieci elektrycznej za pośrednictwem energii kołowej. Ta sama telekomunikacja jest również wykorzystywana do transakcji finansowych między producentami a konsumentami energii elektrycznej. OT to połączenie sprzętu i oprogramowania, które służy do monitorowania, uruchamiania i sterowania zasobami procesów przemysłowych. Zanim nauczysz się hakować OT, ważne jest, aby zrozumieć jego podstawowe pojęcia. W tej sekcji omówiono różne ważne koncepcje związane z OT.

Co to jest OT?

OT to połączenie oprogramowania i sprzętu przeznaczone do wykrywania lub powodowania zmian w operacjach przemysłowych poprzez bezpośrednie monitorowanie i/lub sterowanie fizycznymi urządzeniami przemysłowymi. Urządzenia te obejmują przełączniki, pompy, światła, czujniki, kamery monitorujące, windy, roboty, zawory oraz systemy chłodzenia i ogrzewania. Każdy system, który analizuje i przetwarza dane operacyjne (takie jak komponenty techniczne, elektronika, telekomunikacja, systemy komputerowe) może być częścią OT. Systemy OT są wykorzystywane w sektorach wytwórczym, wydobywczym, medycznym, budowlanym, transportowym, naftowym i gazowym, obronnym i użyteczności publicznej, a także w wielu innych gałęziach przemysłu w celu zapewnienia bezpieczeństwa urządzeń fizycznych i ich działania w sieciach. Technologia ta składa się z przemysłowych systemów sterowania (ICS), które obejmują kontrolę nadzorczą i pozyskiwanie danych (SCADA), zdalne terminale (RTU), programowalne sterowniki logiczne (PLC), rozproszone systemy sterowania (DCS) i wiele innych dedykowanych systemów sieciowych, które pomoc w monitorowaniu i kontrolowaniu operacji przemysłowych. Systemy OT wykorzystują różne podejścia do projektowania sprzętu i protokołów, które nie są znane IT. Obsługa starszych wersji oprogramowania i sprzętu sprawia, że systemy OT są bardziej podatne na cyberataki, ponieważ opracowywanie poprawek lub poprawek dla nich jest bardzo trudne.

Podstawowa terminologia

Poniżej omówiono niektóre z najważniejszych i najczęściej używanych terminów związanych z systemami OT:

Aktywa

Różne składniki OT są ogólnie określane jako aktywa. Większość systemów OT, takich jak ICS, obejmuje zasoby fizyczne, takie jak czujniki i siłowniki, serwery, stacje robocze, urządzenia sieciowe, sterowniki PLC itp. Systemy ICS obejmują również zasoby logiczne reprezentujące działanie i przechowywanie zasobów fizycznych, takie jak grafika przedstawiająca przebieg procesu , logikę programu, bazę danych, oprogramowanie układowe lub reguły zapory.

Strefy i kanały

Strefy i kanały to technika segregacji sieci używana do izolowania sieci i zasobów w celu narzucenia i utrzymania silnych mechanizmów kontroli dostępu.

Sieć przemysłowa i sieć biznesowa

OT ogólnie obejmuje zbiór zautomatyzowanych systemów sterowania. Systemy te są połączone w sieć, aby osiągnąć cel biznesowy. Sieć obejmująca te systemy jest znana jako sieć przemysłowa. Sieć korporacyjna lub biznesowa obejmuje sieć systemów, które oferują biznesowi infrastrukturę informacyjną. Firmy często muszą ustanowić komunikację między sieciami biznesowymi a sieciami przemysłowymi.

Protokoły przemysłowe

Większość systemów OT wykorzystuje zastrzeżone protokoły (S7, CDA, SRTP itp.) lub niezastrzeżone protokoły (Modbus, OPC, DNP3, CIP itp.). Protokoły te są zwykle używane do komunikacji szeregowej i mogą być również używane do komunikacji przez standardową sieć Ethernet przy użyciu protokołu internetowego (IP) wraz z protokołami warstwy transportowej TCP lub UDP. Ponieważ protokoły te działają w warstwie aplikacji, nazywane są aplikacjami.

Obwód sieci/obwód bezpieczeństwa elektronicznego

Obwód sieci to najbardziej zewnętrzna granica strefy sieci, tj. zamknięta grupa aktywów. Pełni funkcję punktu oddzielającego strefę wewnętrzną i zewnętrzną. Zasadniczo kontrole bezpieczeństwa cybernetycznego są wdrażane na obrzeżach sieci. Elektroniczny obwód bezpieczeństwa odnosi się do granicy między bezpiecznymi i niezabezpieczonymi strefami.

Infrastruktura krytyczna

Infrastruktura krytyczna odnosi się do zbioru fizycznych lub logicznych systemów i aktywów, których awaria lub zniszczenie poważnie wpłynie na bezpieczeństwo, gospodarkę lub zdrowie publiczne.

Konwergencja IT/OT (HOT)

Konwergencja IT/OT to integracja systemów obliczeniowych IT (informatycznych) i systemów monitorowania operacji OT. Wypełnienie luki między IT a OT może poprawić ogólną działalność biznesową, generując szybsze i skuteczniejsze wyniki. Konwergencja IT/OT to nie tylko łączenie technologii, ale także zespołów i operacji. Zespoły IT i OT są tradycyjnie rozdzielone i znajdują się w swoich odpowiednich domenach. Na przykład zespoły IT monitorują procesy wewnętrzne, takie jak programowanie, aktualizowanie systemów i zabezpieczanie sieci przed cyberatakami, podczas gdy zespoły OT zapewniają ogólną konserwację i zarządzanie, w tym pracowników i sprzętu przemysłowego.

Zespoły IT/OT są zobowiązane do wzajemnego zrozumienia swoich operacji i struktury pracy. To nie oznacza zamiany inżynierów IT na inżynierów terenowych/zakładowych i odwrotnie; to jest budowanie pomostu między nimi, aby współpracować ze sobą w celu poprawy bezpieczeństwa, wydajności, jakości i produktywności.

Korzyści z połączenia OT z IT

Konwergencja IT/OT może umożliwić inteligentną produkcję znaną jako przemysł 4.0, w której IoT aplikacje są wykorzystywane w operacjach przemysłowych. Wykorzystywanie IoT do operacji przemysłowych, takich jak monitorowanie systemów łańcucha dostaw, produkcji i zarządzania jest określane jako Przemysłowy Internet Rzeczy (IIoT). Oto niektóre z korzyści płynących z konwergencji IT/OT:

Usprawnianie podejmowania decyzji: Podejmowanie decyzji można usprawnić, integrując dane OT w rozwiązania Business Intelligence.

Ulepszona automatyzacja: przepływy biznesowe i operacje kontroli przemysłowej można zoptymalizować poprzez połączenie OT/IT; razem mogą poprawić automatyzację.

Przyspieszenie wyników biznesowych: konwergencja IT/OT może organizować lub usprawniać projekty rozwojowe w celu przyspieszenia wyników biznesowych.

Minimalizacja wydatków: Zmniejsza koszty ogólne i technologiczne.

Ograniczanie ryzyka: Połączenie tych dwóch dziedzin może poprawić ogólną produktywność, bezpieczeństwo i niezawodność, a także zapewnić skalowalność.

Model Purdue'a

Model Purdue wywodzi się z modelu Purdue Enterprise Reference Architecture (PERA), który jest szeroko stosowanym modelem koncepcyjnym opisującym wewnętrzne połączenia i zależności ważnych komponentów w sieciach ICS. Model Purdue jest również znany jako model referencyjny systemu automatyki przemysłowej i sterowania. Model Purdue składa się z trzech stref: produkcyjnej (OT) i korporacyjnej (IT), oddzielonych strefą zdemilitaryzowaną (DMZ), która służy do ograniczenia bezpośredniej komunikacji między systemami OT i IT. Intencją dodania tej dodatkowej warstwy jest ograniczenie sieci lub kompromisów systemowych w tej warstwie i zapewnienie nieprzerwanej produkcji. Trzy strefy są dodatkowo podzielone na kilka poziomów operacyjnych. Każda strefa wraz z powiązanymi poziomami została opisana poniżej:

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Strefa Enterprise (Systemy IT)

Strefa bezpieczeństwa przedsiębiorstwa to część IT, w której zarządzanie łańcuchem dostaw i harmonogramowanie odbywa się za pomocą systemów biznesowych, takich jak SAP i ERP. Lokalizuje również centra danych, użytkowników i dostęp do chmury. Strefa Enterprise składa się z dwóch poziomów.

o Poziom 5 (sieć korporacyjna)

Jest to sieć na poziomie korporacyjnym, w której realizowane są operacje biznesowe, takie jak usługi B2B (business-to-business) i B2C (business-to-customer). Łączność z Internetem i zarządzanie nim mogą być obsługiwane na tym poziomie. Systemy sieciowe przedsiębiorstwa gromadzą również dane ze wszystkich podsystemów zlokalizowanych w poszczególnych zakładach w celu raportowania stanu inwentaryzacji i ogólnego stanu produkcji.

o Poziom 4 (systemy logistyki biznesowej)

Na tym poziomie leżą wszystkie systemy informatyczne wspierające proces produkcyjny w zakładzie. Zarządzanie harmonogramami, planowanie i inna logistyka operacji produkcyjnych są wykonywane tutaj. Systemy poziomu 4 obejmują serwery aplikacji, serwery plików, serwery baz danych, systemy nadzorujące, klientów poczty e-mail itp.

Strefa Produkcyjna (Systemy OT)

Wszystkie urządzenia, sieci, systemy sterowania i monitoringu znajdują się w tej strefie. Strefa produkcyjna składa się z czterech poziomów.

o Poziom 3 (systemy operacyjne/operacje w witrynie)

Na tym poziomie definiuje się zarządzanie produkcją, monitorowanie poszczególnych instalacji i funkcje kontrolne. Na tym poziomie zapewnione są przepływy pracy produkcji i produkcja pożądanego produktu. Zarządzanie produkcją obejmuje systemy zarządzania wydajnością zakładu, planowanie produkcji, zarządzanie partiami, zapewnianie jakości, historię danych, wykonywanie produkcji/zarządzanie operacjami systemów (MES/MOMS), laboratoriów i optymalizacji procesów. Tutaj gromadzone są szczegóły produkcji z niższych poziomów, które następnie mogą być przenoszone na wyższe poziomy lub mogą być instruowane przez systemy wyższego poziomu.

o Poziom 2 (Systemy sterowania/Kontrole nadzoru obszaru)

Na tym poziomie odbywa się nadzorowanie, monitorowanie i sterowanie procesem fizycznym. Systemami sterowania mogą być systemy DCS, oprogramowanie SCADA, interfejsy człowiek-maszyna (HMI), oprogramowanie czasu rzeczywistego i inne nadzorcze systemy sterowania, takie jak prace inżynieryjne i sterowanie linią PLC.

o Poziom 1 (podstawowe sterowanie/inteligentne urządzenia)

Na tym poziomie można przeprowadzić analizę i modyfikację procesu fizycznego. Operacje w zakresie sterowania podstawowego obejmują „uruchamianie silników", „otwieranie zaworów", „ruch siłowników" itp. Systemy poziomu 1 obejmują analizatory, czujniki procesowe i inne systemy oprzyrządowania, takie jak inteligentne urządzenia elektroniczne (IED), sterowniki PLC, jednostki RTU, układy proporcjonalno-całkujące Regulatory pochodne (PID), urządzenia pod kontrolą (EUC) i zmienne napędy częstotliwości (VFD). PLC był używany na poziomie 2 z funkcją nadzorczą, ale jest używany jako funkcja kontrolna na poziomie 1.

o Poziom 0 (proces fizyczny)

Na tym poziomie definiowany jest rzeczywisty proces fizyczny i wytwarzany jest produkt. Wyższe poziomy kontrolują i monitorują operacje na tym poziomie; dlatego ta warstwa jest również określana jako sprzęt pod kontrolą (EUC). Systemy poziomu 0 obejmują urządzenia, czujniki (np. prędkość, temperaturę, ciśnienie), siłowniki lub inne urządzenia przemysłowe wykorzystywane do wykonywania operacji produkcyjnych lub przemysłowych. Drobny błąd w którymkolwiek z urządzeń na tym poziomie może wpłynąć na ogólne działanie.

Przemysłowa strefa zdemilitaryzowana (IDMZ)

Strefa zdemilitaryzowana stanowi barierę między strefą produkcyjną (systemy OT) a strefą korporacyjną (systemy IT), która umożliwia bezpieczne połączenie sieciowe między tymi dwoma systemami. Strefa jest tworzona w celu sprawdzenia ogólnej architektury. Jeśli jakiekolwiek błędy lub włamania zagrażają działającym systemom, IDMZ zatrzymuje błąd i umożliwia kontynuowanie produkcji bez przerwy. Systemy IDMZ obejmują kontrolery domen firmy Microsoft, serwery replikacji baz danych i serwery proxy.

Wyzwania OT

OT odgrywa kluczową rolę w kilku sektorach infrastruktury krytycznej, takich jak elektrownie, wodociągi i opieka zdrowotna. To absurdalne, że większość systemów OT działa na starych wersjach oprogramowania i korzysta z przestarzałego sprzętu, co czyni je podatnymi na złośliwe exploity, takie jak phishing, szpiegostwo, ataki ransomware itp. Tego typu ataki mogą mieć katastrofalne skutki dla produktów i usług. Aby ograniczyć te luki, system OT musi przeprowadzić krytyczną analizę kluczowych obszarów podatności na ataki, korzystając z różnych narzędzi i taktyk bezpieczeństwa. Poniżej omówiono niektóre wyzwania i zagrożenia dla OT, które czynią go podatnym na wiele zagrożeń:

Brak widoczności: Szerszy wgląd w cyberbezpieczeństwo w sieci OT zapewnia większe bezpieczeństwo, dzięki czemu można szybko reagować na wszelkie potencjalne zagrożenia. Jednak większość organizacji nie ma wyraźnego wglądu w cyberbezpieczeństwo, co utrudnia zespołom ds. bezpieczeństwa wykrywanie nietypowych zachowań i sygnatur.

Hasła w postaci zwykłego tekstu: większość sieci zakładów przemysłowych używa haseł słabych lub w postaci zwykłego tekstu. Hasła w postaci zwykłego tekstu prowadzą do słabego uwierzytelnienia, co z kolei naraża systemy na różne ataki zwiadu cybernetycznego.

Złożoność sieci: większość środowisk sieciowych OT jest złożona, ponieważ obejmuje wiele urządzeń, z których każde ma inne potrzeby i wymagania w zakresie bezpieczeństwa.

Starsza technologia: systemy OT na ogół wykorzystują starsze technologie bez odpowiednich środków bezpieczeństwa, takich jak szyfrowanie i ochrona hasłem, przez co są podatne na różne ataki. Wyzwaniem jest również stosowanie nowoczesnych praktyk bezpieczeństwa.

Brak ochrony antywirusowej: Branże korzystające ze starszych technologii i przestarzałych systemów nie są wyposażone w żadną ochronę antywirusową, która może automatycznie aktualizować sygnatury, co naraża tchem na infekcje złośliwym oprogramowaniem.

Brak wykwalifikowanych specjalistów ds. bezpieczeństwa: Luka w umiejętnościach związanych z cyberbezpieczeństwem stanowi ogromne zagrożenie dla organizacji, ponieważ brakuje wykwalifikowanych specjalistów ds.

Szybkie tempo zmian: Utrzymanie tempa zmian jest największym wyzwaniem w dziedzinie bezpieczeństwa, a powolna transformacja cyfrowa może również zagrozić systemom OT.

Przestarzałe systemy: większość urządzeń OT, takich jak sterowniki PLC, korzysta z przestarzałego oprogramowania układowego, co czyni je podatnymi na wiele współczesnych cyberataków.

Przypadkowa modernizacja: Ponieważ zapotrzebowanie na OT rośnie, musi być na bieżąco z najnowszymi technologiami. Jednak ze względu na wykorzystanie starszych komponentów w aktualizacji i łataniu systemu OT, aktualizacja systemu może zająć kilka lat, co może niekorzystnie wpłynąć na kilka operacji.

Niepewne połączenia: systemy OT komunikują się przez publiczne Wi-Fi i niezaszyfrowane połączenia Wi-Fi w sieci IT w celu przesyłania danych kontrolnych, co czyni je podatnymi na ataki typu man-in-the-middle.

Wykorzystanie nieuczciwych urządzeń: Wiele zakładów przemysłowych ma podłączone do swoich sieci nieznane lub nieuczciwe urządzenia, które są podatne na różne ataki.

Konwergencja z IT: OT łączy się głównie z siecią korporacyjną; w rezultacie jest podatny na różne ataki złośliwego oprogramowania i złośliwych wtajemniczonych. Ponadto systemy OT obsługują technologię IT, a zespół ds. bezpieczeństwa IT nie ma dużego doświadczenia z systemami i protokołami OT.

Wyzwania organizacyjne: wiele organizacji wdraża i utrzymuje różne architektury bezpieczeństwa, które spełniają potrzeby zarówno IT, jak i OT. Może to spowodować pewne luki w zarządzaniu bezpieczeństwem, pozostawiając atakującym łatwe możliwości wtargnięcia do systemów.

Unikalne sieci produkcyjne/własne oprogramowanie: branże stosują unikalne konfiguracje sprzętu i oprogramowania, które są zależne od standardów branżowych i wyraźnych wymagań operacyjnych. Korzystanie z zastrzeżonego oprogramowania utrudnia aktualizację i poprawianie oprogramowania układowego, ponieważ kontroluje je wielu dostawców.

Wrażliwe protokoły komunikacyjne: OT wykorzystuje protokoły komunikacyjne, takie jak Modbus i Profinet, do nadzorowania, sterowania i łączenia różnych mechanizmów, takich jak sterowniki, siłowniki i czujniki. Protokoły te nie mają wbudowanych funkcji bezpieczeństwa, takich jak uwierzytelnianie, wykrywanie wad lub wykrywanie nieprawidłowego zachowania, co czyni je podatnymi na różne ataki.

Protokoły zdalnego zarządzania: zakłady przemysłowe używają protokołów zdalnego zarządzania, takich jak RDP, VNC i SSH. Gdy atakujący skompromituje się i uzyska dostęp do sieci OT, może przeprowadzić dalsze działania, aby zrozumieć i manipulować konfiguracją i działaniem sprzętu.

Wprowadzenie do ICS

Przemysłowy system sterowania (ICS) jest istotną częścią każdego procesu przemysłowego i krytycznej infrastruktury w przemyśle. Typowy ICS reprezentuje system informacyjny, który kontroluje i obsługuje wszystkie rodzaje procesów przemysłowych, takich jak produkcja, wytwarzanie, obsługa produktów, dystrybucja itp. ICS często odnosi się do zbioru różnych typów systemów sterowania i związanego z nimi sprzętu, takiego jak systemy, urządzenia, sieci i kontrole używane do obsługi i automatyzacji kilku procesów przemysłowych. ICS obejmuje kilka rodzajów systemów sterowania, takich jak systemy SCADA, DCS, podstawowe systemy sterowania procesami (BPCS), systemy oprzyrządowania bezpieczeństwa (SIS), HMI, PLC, RTU i diody LED. Technologia ta składa się z różnych komponentów, takich jak czujniki, sterowniki i siłowniki (mechaniczne, elektryczne, hydrauliczne, pneumatyczne itp.), które wspólnie działają w celu osiągnięcia przemysłowego celu. Proces jest częścią systemu ICS, która jest głównie odpowiedzialna za wytwarzanie danych wyjściowych. Sterowanie jest częścią systemu ICS, która zawiera instrukcje potrzebne do uzyskania pożądanego efektu wyjścia. Ta część kontrolna jest albo w pełni zautomatyzowana, albo może wymagać interwencji człowieka w pętli procesu. Działanie systemów ICS można skonfigurować w trzech trybach, a mianowicie w pętli otwartej, pętli zamkniętej i trybie pętli ręcznej.

Otwarta pętla: Wyjście systemu zależy od wstępnie skonfigurowanych ustawień.

Zamknięta pętla: Wyjście zawsze ma wpływ na wejście w celu osiągnięcia pożądanego celu.

Pętla ręczna: System jest całkowicie kontrolowany przez ludzi.

Kontroler (kontrola) systemu ICS odpowiada przede wszystkim za utrzymanie zgodności z pożądaną specyfikacją. Zasadniczo systemy ICS obejmują wiele pętli sterowania, interfejsy HMI i narzędzia używane do zdalnej konserwacji i diagnostyki. Narzędzia do zdalnego zarządzania i diagnostyki są zbudowane przy użyciu różnych protokołów sieciowych. Systemy ICS są szeroko stosowane w branżach takich jak produkcja i dystrybucja energii elektrycznej, zaopatrzenie w wodę i oczyszczanie ścieków, dostawy ropy naftowej i gazu ziemnego, produkcja chemiczna i farmaceutyczna, celuloza i papier oraz żywność i napoje. W niektórych branżach systemy ICS są nawet fizycznie rozmieszczone w wielu lokalizacjach, a ich procesy mogą być od siebie zależne. W takich przypadkach protokoły komunikacyjne są szeroko stosowane do wydajnej komunikacji między rozproszonymi systemami ICS.

Składniki ICS

ICS to szeroka klasa sieci i systemów dowodzenia i kontroli, które są wymagane do sterowania i monitorowania każdego procesu przemysłowego. Każdy typ ICS działa i funkcjonuje inaczej w zależności od funkcjonalności i złożoności akcji kontrolnej. ICS można podzielić na następujące typy najczęściej i najszerzej stosowanych systemów sterowania:

Rozproszony system sterowania (DCS)

DCS służy do sterowania systemami produkcyjnymi rozmieszczonymi w tej samej lokalizacji geograficznej. Takie systemy są używane głównie w dużych, złożonych i rozproszonych procesach, które są przeprowadzane w branżach takich jak produkcja chemiczna i elektrownie jądrowe, rafinerie ropy naftowej, oczyszczalnie wody i ścieków, elektrownie oraz produkcja samochodów i farmaceutyków. DCS to ogólnie zaawansowany technologicznie system sterowania na dużą skalę, który jest często używany do wykonywania zadań specyficznych dla branży. Zawiera scentralizowaną nadrzędną jednostkę sterującą używaną do sterowania wieloma lokalnymi sterownikami, tysiącami punktów wejścia/wyjścia (I/O) i różnymi innymi urządzeniami obiektowymi, które są częścią całego procesu produkcyjnego. Aby uzyskać kontrolę procesu, DCS wykorzystuje różne pętle sprzężenia zwrotnego i sprzężenia zwrotnego wraz z kluczowymi warunkami produktu, które są ustalane zgodnie z docelowymi wartościami zadanymi. Działa przy użyciu scentralizowanej pętli sterowania nadzorczego, takiej jak SCADA i MTU, która łączy grupę zlokalizowanych sterowników, takich jak RTU/PLC, w celu wykonywania ogólnych zadań wymaganych do działania całego procesu produkcyjnego. Na każdym poziomie zapewniony jest wysoki poziom redundancji, począwszy od wejść/wyjść sterowników, a skończywszy na poziomie sieci. Ta nadmiarowość pomaga innym procesom płynnie działać w przypadku awarii pojedynczego procesora. Głównym powodem wyboru systemów DCS w przemyśle są możliwości dostosowania i elastyczność, jakie zapewniają one w sterowaniu rozproszonymi dyskretnymi urządzeniami polowymi i ich stacjami operacyjnymi. Co więcej, system DCS jest skalowalny, a zatem można go ustawić w szyku podczas początkowej instalacji jako duży zintegrowany system lub jako system modułowy, który można zintegrować zgodnie z wymaganiami. Systemy DCS są w stanie ciągłego rozwoju, ponieważ nowe technologie, takie jak systemy i protokoły bezprzewodowe, zdalna transmisja, logowanie i archiwizacja danych oraz wbudowane serwery sieciowe są z czasem dołączane.

Kontrola Nadzorcza i Pozyskiwanie Danych (SCADA)

SCADA to scentralizowany system nadzoru i kontroli, który służy do sterowania i monitorowania obiektów i infrastruktury przemysłowej. Wiele organizacji wykorzystuje systemy SCADA do automatyzacji złożonych procesów przemysłowych, mierzenia trendów w czasie rzeczywistym oraz wykrywania i korygowania problemów. Ogólnie rzecz biorąc, systemy SCADA są rozmieszczone na dużym obszarze geograficznym; w rezultacie różne gałęzie przemysłu polegają na systemach SCADA w transporcie ropy i gazu, oczyszczaniu ścieków i zarządzaniu nimi, eksploatacji rurociągów, telekomunikacji, sieciach energetycznych, automatyce budynków, systemy transportowe itp. System SCADA jest systemem scentralizowanym, który zapewnia kontrolę nadzorczą, a także umożliwia pozyskiwanie w czasie rzeczywistym danych z rozproszonych zasobów wykorzystywanych w procesach przemysłowych. Składa się z komponentów sprzętowych i programowych, które zbierają i wysyłają dane w celu zarządzania i sterowania procesami zarówno lokalnie, jak iw zdalnych lokalizacjach. Zebrane dane są przechowywane w urządzeniach do długotrwałego przechowywania, takich jak rejestrator danych, aby pomóc operatorom w interpretacji danych i umożliwić różne nastawy. Te wartości zadane pomagają systemowi skutecznie reagować na nietypowe działania, wysyłając same polecenia lub wysyłając alerty do operatora. Systemy SCADA zapewniają scentralizowane sterowanie i monitorowanie wielu wejść i wyjść procesowych poprzez integrację systemu akwizycji danych z systemem transmisji danych oraz oprogramowaniem HMI. Systemy SCADA zbierają informacje z urządzeń polowych i przesyłają je do centralnego systemu komputerowego. Ta informacja jest wyświetlana operatorowi w formacie graficznym lub tekstowym, umożliwiający operatorowi kontrolę i monitorowanie całości Systemu SCADA z centralnej lokalizacji w czasie rzeczywistym. Architektura SCADA składa się ze sprzętu, takiego jak serwer sterujący (SCADA-MTU) i urządzeń komunikacyjnych (kable sieciowe, urządzenia radiowe, linie telefoniczne, kable itp.) itp., które służą do monitorowania i sterowania pracą

urządzeń przemysłowych.Informacje z RTU są kontrolowane i przetwarzane przez serwer sterujący, a urządzenia polowe są sterowane i monitorowane przez RTU lub PLC. Oprogramowanie SCADA jest zaprogramowane tak, aby informować cały system o tym, co ma być monitorowane, kiedy powinno być monitorowane i jakie są dopuszczalne zakresy parametrów, a także informować system o reakcji, jaka ma zostać zainicjowana, gdy wartości parametrów przekroczą ustawić zakresy. Urządzenie IED może zbierać dane i przesyłać je bezpośrednio do serwera sterującego lub lokalny RTU może poinstruować urządzenie IED, aby zebrało dane i wysłało je do serwera sterującego. Urządzenie IED zawiera interfejs komunikacyjny do monitorowania i sterowania różnymi czujnikami i sprzętem. Diody LED są albo bezpośrednio kontrolowane przez serwer sterujący, albo obejmują lokalne programowanie, które umożliwia im niezależne działanie bez interwencji serwera sterującego. Systemy SCADA są systemami odpornymi na błędy z systemami redundantnymi. Ta nadmiarowość może nie być wystarczająca do ochrony systemów SCADA przed złośliwymi atakami.

Programowalny sterownik logiczny (PLC)

PLC to cyfrowy komputer czasu rzeczywistego używany w automatyce przemysłowej. Sterowniki PLC są uważane za coś więcej niż tylko komputery cyfrowe w różnych przemysłowych systemach sterowania ze względu na ich niezwykłe cechy, takie jak solidna konstrukcja, łatwość programowania, sterowanie sekwencyjne, łatwość obsługi sprzętu, timery i liczniki oraz niezawodne możliwości sterowania. Zasadniczo są one zbudowane tak, aby przetrwać w trudnych warunkach przemysłowych. Branże, w których stosowane są sterowniki PLC, obejmują przemysł stalowy, samochodowy, energetyczny, chemiczny, szklarski, papierniczy, cementowy. PLC to mały półprzewodnikowy komputer sterujący, dla którego można dostosować instrukcje do wykonania określonego zadania. Instrukcje przechowywane w sterownikach PLC mogą być wykorzystywane do wykonywania określonych funkcji, takich jak logika, synchronizacja, zliczanie, sterowanie wejściami/wyjściami, komunikacja, arytmetyka oraz przetwarzanie plików i danych. Zastosowanie sterowników PLC w przemyśle w dużej mierze zastąpiło sekwencery bębnowe, przekaźniki przewodowe i timery. Sterowniki PLC wykonują ciągłe monitorowanie wartości wejściowych wytwarzanych przez czujniki oraz generują wyjścia potrzebne do działania elementów wykonawczych. System PLC składa się z trzech modułów:

1. Moduł CPU: Moduł CPU składa się z centralnego procesora i jego komponentu pamięci. Procesor jest odpowiedzialny za wykonanie wymaganych obliczeń i przetwarzania danych poprzez odbieranie danych wejściowych i wytwarzanie odpowiednich danych wyjściowych. Część pamięci składa się zarówno z pamięci RAM, jak i pamięci ROM. Pamięć RAM przechowuje programy napisane przez użytkownika, podczas gdy pamięć ROM przechowuje systemy operacyjne, sterowniki i aplikacje. Sterowniki PLC zawierają również pamięć retencyjną, która służy do przechowywania programów użytkownika i danych w przypadku przerwy w zasilaniu. Ta pamięć podtrzymująca pomaga w wznowieniu wykonywania programu użytkownika po przywróceniu zasilania. Z tego powodu sterowniki PLC na ogół nie używają monitora ani klawiatury do przeprogramowania procesora w przypadku awarii zasilania.

2. Moduł zasilacza: Moduł zasilacza zapewnia niezbędne zasilanie wymagane dla procesora i modułów we/wy poprzez konwersję prądu przemiennego na prąd stały. Ten moduł jest zasadniczo odpowiedzialny za działanie systemu. Wyjście 5 V DC z modułu zasilacza służy do zasilania obwodów komputera PLC, podczas gdy w niektórych PLC wyjście 24 V DC z modułu zasilacza jest wykorzystywane do uruchamiania czujników i elementów wykonawczych.

3. Moduły I/O: Moduły wejściowe i wyjściowe systemu PLC służą do łączenia czujników i elementów wykonawczych z systemem w celu wykrywania i kontrolowania wartości w czasie rzeczywistym, takich jak ciśnienie, temperatura i przepływ. Istnieją różne typy modułów I/O. Niektóre z najważniejszych omówiono poniżej:

Cyfrowy moduł we/wy: Używany do podłączania czujników i elementów wykonawczych o charakterze cyfrowym (tylko do włączania i wyłączania). Moduły te współpracują z wieloma wejściami i wyjściami cyfrowymi i obsługują zarówno napięcia AC, jak i DC.

Moduł wejść/wyjść analogowych: Służy do podłączania czujników i elementów wykonawczych dostarczających analogowe sygnały elektryczne. Moduł ten zawiera przetwornik analogowo-cyfrowy do konwersji danych analogowych na dane cyfrowe. Moduł CPU przetwarza te dane cyfrowe.

Komunikacyjny moduł we/wy: używany do wymiany informacji między siecią komunikacyjną a oddalonym od siebie procesorem. Głównym celem PLC jest automatyczne działanie maszyn i systemów bez interwencji człowieka. Dlatego PLC jest bardzo ważny, ponieważ jest odpowiedzialny za cały wzrost, produkcję, produkcję itp.

Podstawowy system sterowania procesem (BPCS)

BPCS jest odpowiedzialny za wykonywanie kontroli i monitoringu procesów dla infrastruktury przemysłowej. Jest to system, który reaguje na sygnały wejściowe z procesów i związanych z nimi urządzeń w celu generowania sygnałów wyjściowych, które umożliwiają działanie procesu i związanych z nim urządzeń w oparciu o zatwierdzoną strategię kontroli projektu. Systemy BPCS mają charakter dynamiczny i można je w dużym stopniu dostosować do zmieniających się warunków procesowych. Można je stosować we wszelkiego rodzaju pętlach sterowania, w tym w pętlach sterowania temperaturą, wsadem, ciśnieniem, przepływem, sprzężeniem zwrotnym i sprzężeniem zwrotnym, stosowanych w branżach takich jak przemysł chemiczny, naftowy i gazowy oraz spożywczy i napoje. Stosowanie BPCS ma kluczowe znaczenie w przemyśle, ponieważ działają one jako pierwsza warstwa ochrony przed wszelkimi niebezpiecznymi warunkami dla sprzętu. Systemy BPCS są często używane do przesuwania granic wydajności w celu osiągnięcia pożądanej wydajności. BPCS różnią się od systemów sterowania bezpieczeństwem pod względem bezpieczeństwa, ponieważ brakuje im procedur diagnostycznych, które identyfikowałyby wszelkie wady systemu. Mogą jednak sprostać wielu wyzwaniom przemysłowym związanym z obsługą systemu, a monitoring biznesowy może skorzystać z dobrze zaprojektowanego systemu sterowania. Poniżej wymieniono niektóre z ważnych funkcji oferowanych przez BPCS:

o Oferuje funkcje rejestrowania trendów i alarmów/zdarzeń

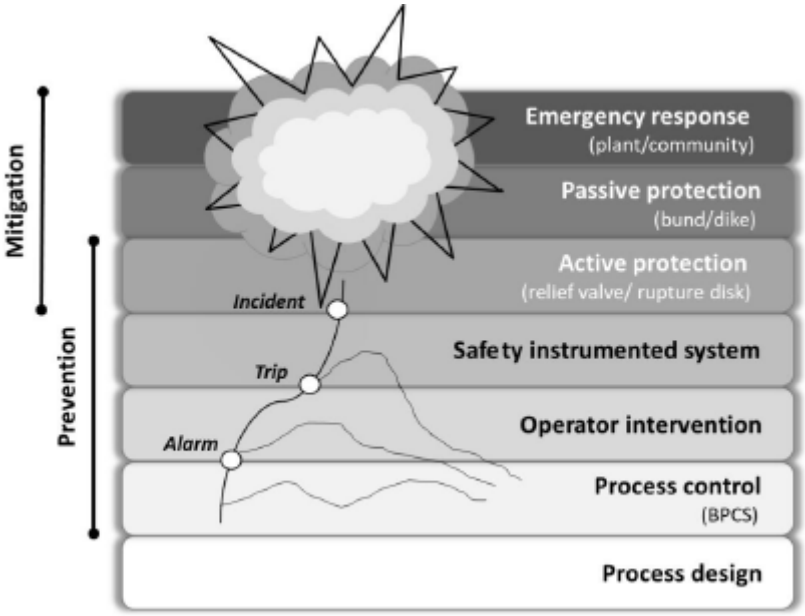
o Zapewnia interfejs, z którego operator może monitorować i sterować systemem za pomocą konsoli operatora (HMI)

o Kontroluje procesy, które z kolei optymalizują działanie zakładu w celu poprawy jakości produktu

Instrumentalne systemy bezpieczeństwa (SIS)

Przyrządowe systemy bezpieczeństwa (SIS) to zautomatyzowany system sterowania zaprojektowany w celu ochrony środowiska produkcyjnego w przypadku jakiegokolwiek niebezpiecznego zdarzenia w przemyśle. Monitorują i wykonują „specyficzne funkcje kontrolne" w celu zamknięcia monitorowanego systemu lub wprowadzenia go do wcześniej określonego stanu bezpiecznego w celu zmniejszenia negatywnych skutków incydentu. Funkcjonują one jako istotny składnik strategii zarządzania ryzykiem, która wykorzystuje warstwy ochrony, aby zapobiec osiągnięciu przez granice operacyjne krytycznego stanu niebezpiecznych warunków operacyjnych. Typowymi przykładami systemów SIS są systemy przeciwpożarowe i gazowe, systemy blokad bezpieczeństwa, systemy wyłączania bezpieczeństwa itp. W przemyśle SIS zastępuje BPCS pod względem operacyjnym i działa, gdy BPCS nie obsługuje procesu w ramach normalnych parametrów operacyjnych. W danych warunkach, jeśli BPCS zacznie działać poza normalnymi granicami operacyjnymi, SIS zapewnia zautomatyzowane środowisko kontrolne do wykrywania i reagowania na krytyczny proces. SIS albo zachowuje stan, albo zmienia go na stan bezpieczny, tj. wyłączenie sprzętu lub procesu. Wreszcie, ostatnia warstwa ochrony jest stosowana tam, gdzie stosowane są urządzenia takie jak zawory nadmiarowe, płytki bezpieczeństwa,

systemy pochodni itp., zanim proces wejdzie w niebezpieczne granice operacyjne. Generowane zdarzenia i akcje wykonywane przez system SIS ilustruje schemat:



Wymagania funkcjonalne pracy wykonywanej przez SIS oraz jej skuteczność można określić na podstawie badań zagrożeń i operacyjności (HAZOP), analizy warstw ochrony (LOPA), wykresów ryzyka itp. System SIS działa niezależnie od innych kontroli systemy. Składa się z czujników, solwerów logicznych i końcowych elementów sterujących, które zapewniają bezpieczną pracę procesu, realizując następujące funkcje:

Czujniki terenowe zbierają informacje w celu określenia i pomiaru parametrów procesu, takich jak temperatura, ciśnienie, przepływ itp., aby przewidzieć, czy sprzęt działa w bezpiecznym stanie, czy nie. Dostępne są różne rodzaje czujników, takie jak przełączniki pneumatyczne, elektryczne, inteligentne nadajniki itp.

Solvery logiczne są pomocne w podjęciu decyzji o niezbędnych działaniach, które należy podjąć na podstawie zebranych informacji. Zapewniają działania zarówno w sytuacjach odpornych na awarie, jak i odpornych na uszkodzenia. Działają jak kontrolery, które przechwytują sygnały z czujników i wykonują zaprogramowane działania, aby uniknąć ryzyka, dostarczając dane wyjściowe do końcowych elementów sterujących.

Końcowe elementy kontrolne realizują działania określone przez sterownik logiczny w celu doprowadzenia systemu do stanu bezpiecznego. Elementy te obejmują na ogół uruchamiane pneumatycznie zawory włączające i wyłączające, sterowane przez zawory elektromagnetyczne.

Ponieważ żaden element systemu nie może być całkowicie odporny na awarie, ważne jest, aby przemysł stale testował systemy SIS. Ważne jest również przeprowadzenie oceny jego podstawowego środowiska cyberbezpieczeństwa, aby zapewnić sprawne działanie SIS. Głównym celem oceny warunków pracy systemu SIS jest zagwarantowanie bezpieczeństwa i utrzymania SIS na poziomie projektowym.

Technologie i protokoły OT

Protokoły sieci przemysłowych zapewniają łączność w czasie rzeczywistym i wymianę informacji między systemami i strefami przemysłowymi. Te protokoły sieciowe są wdrażane w całej sieci ICS w dowolnej branży. Aby zrozumieć jakąkolwiek sieć przemysłową, inżynier ds. bezpieczeństwa musi zrozumieć protokoły istniejące

w tych sieciach. Kluczowe technologie komunikacyjne i protokoły sieci OT w modelu Purdue zdefiniowanym przez ISA-95 są następujące:

Protokoły używane na poziomie 4 i 5

DCOM: DCOM (Distributed Component Object Model) to zastrzeżone oprogramowanie firmy Microsoft, które umożliwia niezawodną i bezpieczną komunikację składników oprogramowania bezpośrednio przez sieć.

DDE: DDE (Dynamic Data Exchange) jest używany do IPC (Inter-Process Communication).

FTP/SFTP: FTP nawiązuje połączenie z określonym serwerem lub komputerem, a także służy do pobierania lub przesyłania plików. SFTP weryfikuje tożsamość klienta, a po nawiązaniu bezpiecznego połączenia następuje wymiana informacji.

GE-SRTP: GE-SRTP (Service Request Transport Protocol), opracowany przez GE Intelligent Platforms, służy do przesyłania danych ze sterowników PLC i działa na wybranej liczbie sterowników PLC GE, które przekształcają polecenia cyfrowe w działania fizyczne.

IPv4/IPv6: IPv4 to protokół bezpołączeniowy używany w sieciach z komutacją pakietów. Protokół IPv6 jest używany do pracy w sieci z komutacją pakietów, która zapewnia transmisję datagramów typu end-to-end w wielu sieciach IP.

OPC: OPC (Open Platform Communications) to zestaw protokołów klient/serwer zaprojektowanych do komunikacji danych w czasie rzeczywistym między urządzeniami do zbierania danych, takimi jak sterowniki PLC, a urządzeniami interfejsowymi, takimi jak interfejsy HMI.

TCP/IP: TCP/IP to zestaw protokołów komunikacyjnych używanych do łączenia urządzeń sieciowych przez Internet.

Wi-Fi: Wi-Fi to technologia szeroko stosowana w bezprzewodowych sieciach lokalnych lub LAN. Najpopularniejszym standardem Wi-Fi stosowanym w domach lub firmach jest 802.lln, który oferuje maksymalną prędkość 600 Mb/s i zasięg około 50 m.

Protokoły używane na poziomie 3

CC-Link: CC-Link (Control and Communications Link) to otwarta sieć przemysłowa, która umożliwia komunikację urządzeniom różnych producentów. Znajduje zastosowanie w sterowaniu maszynami, procesami i automatyką budynkową.

HSCP: Hybrid SCP (Secure Copy Protocol) został opracowany do przesyłania plików o większych rozmiarach z dużą prędkością w infrastrukturze dalekosiężnej i szerokopasmowej.

ICCP (IEC 60870-6): ICCP (Inter-Control Center Communications Protocol) (IEC 60870-6) zapewnia zestaw standardów i protokołów obejmujących komunikację ICS lub SCADA w automatyce systemów elektroenergetycznych.

IEC 61850: IEC 61850 to powszechny protokół, który umożliwia interoperacyjność i komunikację między diodami LED w podstacjach elektrycznych.

ISA/IEC 62443: ISA/IEC 62443 zapewnia elastyczne ramy do adresowania i łagodzenia obecnych i przyszłych luk w zabezpieczeniach systemów automatyki przemysłowej i sterowania.

Modbus: Modbus to protokół komunikacji szeregowej używany ze sterownikami PLC i umożliwiający komunikację między wieloma urządzeniami podłączonymi do tej samej sieci.

NTP: NTP (Network Time Protocol) to protokół sieciowy używany do synchronizacji zegarów między systemami komputerowymi w sieciach danych z przełączaniem pakietów i zmiennym opóźnieniem.

Profinet: Profinet to protokół komunikacyjny używany do wymiany danych między sterownikami, takimi jak PLC, a urządzeniami, takimi jak czytniki RFID.

SuiteLink: Protokół SuiteLink jest oparty na protokole TCP/IP i działa jako usługa w systemach operacyjnych Windows. Jest używany głównie w zastosowaniach przemysłowych, w których ceni się czas, jakość i wysoką przepustowość.

Tase-2: Tase-2, określany również jako IEC 60870-6, to otwarty protokół komunikacyjny, który umożliwia wymianę krytycznych czasowo informacji między systemami sterowania za pośrednictwem sieci WAN i LAN.

Protokoły używane na poziomie 2

6L0WPAN: IPv6 over Low Power Personal Area Networks (6L0WPAN) to protokół internetowy używany do komunikacji między mniejszymi i energooszczędnymi urządzeniami o ograniczonej mocy obliczeniowej; jest używany głównie do automatyki domowej i budynkowej.

DNP3: DNP3 (Distributed Network Protocol 3) to protokół komunikacyjny używany do łączenia komponentów w systemach automatyzacji procesów.

DNS/DNSSEC: rozszerzenia zabezpieczeń systemu nazw domen (DNSSEC) zapewniają sposób uwierzytelniania danych odpowiedzi DNS i mogą zabezpieczać informacje dostarczane przez DNS.

FTE: Fault Tolerant Ethernet (FTE) został zaprojektowany w celu zapewnienia szybkiej redundancji sieci, a każdy węzeł jest podłączony dwukrotnie do jednej sieci LAN za pośrednictwem podwójnych interfejsów sieciowych.

FIART-IP: Protokół FIART-IP służy do ścisłej i wydajnej integracji bramek WirelessFIART i multiplekserów HART w celu wysyłania i odbierania informacji cyfrowych.

IEC 60870-5-101/104: Jest to rozszerzenie protokołu IEC 101 z pewnymi modyfikacjami w transporcie, sieci, łączach i usługach warstwy fizycznej. Umożliwia komunikację pomiędzy stacją sterowniczą a podstacją poprzez standardową sieć TCP/IP.

SOAP: SOAP (Simple Object Access Protocol) to protokół przesyłania wiadomości zawierający surowy zestaw reguł, które mogą zarządzać przesyłaniem danych między klientem a serwerem przy użyciu formatu wiadomości XML.

Protokoły używane na poziomie 0 i 1

BACnet: BACnet (Building Automation and Control network) to protokół transmisji danych przeznaczony do sieci automatyki budynkowej i sterowania, który wdraża standardy takie jak ASHRAE, ANSI i ISO 16484-5.

EtherCAT: Ethernet for Control Automation Technology (EtherCAT) to system magistrali polowej oparty na sieci Ethernet, który jest odpowiedni zarówno dla twardych, jak i miękkich potrzeb obliczeniowych w czasie rzeczywistym w technologii automatyzacji.

CANopen: CANopen to protokół komunikacyjny wysokiego poziomu oparty na protokole CAN (Controller Area Network). Jest używany we wbudowanych aplikacjach sieciowych, takich jak sieci samochodowe.

Crimson: Crimson to wspólna platforma programistyczna używana w różnych produktach Red Lion, takich jak interfejsy HMI z serii G3 i G3 Kadet, Data Station Plus, Modular Controller i Productivity Station.

DeviceNet: DeviceNet to kolejny wariant wspólnego protokołu przemysłowego (CIP), który jest używany w branży automatyki do łączenia urządzeń sterujących w celu wymiany danych.

Zigbee: Zigbee to protokół komunikacyjny krótkiego zasięgu oparty na standardzie IEEE 203.15.4. Zigbee jest używany w urządzeniach, które przesyłają dane w sposób przerywany z niską szybkością transmisji danych na ograniczonym obszarze i w zasięgu 10-100 m.

ISA SP100: ISA SP100 to komitet mający na celu ustanowienie przemysłowego standardu bezprzewodowego ISA100. ISA100 jest używany w przemysłowym środowisku produkcyjnym i przemyśle automatyzacji procesów.

MELSEC-Q: MELSEC-Q zapewnia otwarte i bezproblemowe środowisko sieciowe integrujące różne poziomy automatyzacji sieci, takie jak CC-Link IE, szybkie i zintegrowane otwarte sieci Ethernet o dużej pojemności.

Niagara Fox: Protokół Niagara Fox to protokół automatyki budynkowej używany między systemami oprogramowania Niagara opracowanymi przez firmę Tridium.

Omron Fins: Omron Fins jest używany przez programy PLC do przesyłania danych i wykonywania innych usług ze zdalnym PLC podłączonym do sieci Ethernet. Może być również używany przez zdalne urządzenia, takie jak FieldServer do przesyłania danych.

PCWorx: PCWorx jest używany w wielu komponentach ICS i tworzy serię wbudowanych kontrolerów (ILC). Te kontrolery umożliwiają korzystanie z różnych protokołów ICS i niektórych popularnych protokołów TCP/IP.

Profibus: Profibus jest bardziej złożony niż Modbus i został zaprojektowany i opracowany w celu rozwiązania problemów związanych z interoperacyjnością. Jest stosowany w automatyzacji procesów i automatyzacji fabryk.

Sercos II: Szeregowy system komunikacji w czasie rzeczywistym (Sercos II) zawiera cyfrowy interfejs napędu odpowiedni do stosowania w maszynach przemysłowych. Jest używany w złożonych aplikacjach sterowania ruchem z projektami o wysokich parametrach.

Komunikacja S7: Komunikacja S7 jest zastrzeżonym protokołem firmy Siemens, który działa między programowalnymi sterownikami logicznymi (PLC) z rodziny Siemens S7-300/400 i jest używany w programowaniu sterowników PLC oraz do uzyskiwania dostępu do danych PLC z systemu SCADA.

WiMax: Worldwide Interoperability for Microwave Access (WiMax) jest oparty na standardzie IEEE 802.16 i jest przeznaczony dla bezprzewodowych sieci miejskich. WiMax działa na częstotliwościach od 2,5 GHz do 5,8 GHz z szybkością transferu 40 Mb/s.

Ataki OT

Wraz ze zmieniającymi się zagrożeniami bezpieczeństwa i postawą bezpieczeństwa organizacji korzystających z OT, organizacje muszą przywiązywać najwyższą wagę do bezpieczeństwa OT i przyjąć odpowiednie strategie w celu rozwiązania problemów związanych z bezpieczeństwem w związku z konwergencją OT/IT. W tej sekcji omówiono różne zagrożenia i ataki OT, takie jak hakowanie sieci przemysłowych, ataki HMI, ataki typu side-channel, hakowanie sterowników PLC, hakowanie maszyn przemysłowych za pomocą zdalnych kontrolerów RF itp.

Luki w zabezpieczeniach OT

Systemy OT są w coraz większym stopniu powiązane z sieciami informatycznymi. Wraz ze wzrostem integracji i konwergencji OT/IT zwiększyły się również obszary ataków systemów OT. Sieci i systemy IT są często narażone na ataki cybernetyczne; w związku z tym systemy i sieci OT mogą zostać naruszone przez sieci IT. Luki istniejące w sieciach IT mogą być wykorzystywane przez osoby atakujące do inicjowania różnych ataków na sieci OT. Poniżej omówiono niektóre typowe luki w zabezpieczeniach OT:

Luka w zabezpieczeniach: Opis

1. Publicznie dostępne systemy OT:

* Systemy OT są bezpośrednio podłączone do Internetu, dzięki czemu dostawcy zewnętrzni mogą zdalnie przeprowadzać konserwację i diagnostykę

* Systemy OT nie są chronione przy użyciu nowoczesnych środków bezpieczeństwa

* Możliwość przeprowadzania brutalnego wymuszania hasła lub sondowania systemów OT

wyłączyć lub zakłócić ich działanie

2. Niebezpieczne połączenia zdalne:

* Sieci korporacyjne używają jump boxów do ustanawiania zdalnej łączności z siecią OT

* Możliwość wykorzystania luk w skrzynkach przesiadkowych w celu uzyskania zdalnego dostępu

do systemów OT

3. Brakujące aktualizacje zabezpieczeń:

* Nieaktualne wersje oprogramowania prowadzą do zwiększonego ryzyka i torują drogę atakującym do zhakowania systemów OT

4. Słabe hasła:

* Operatorzy i administratorzy używają domyślnych nazw użytkowników i haseł do systemów OT, które są łatwe do odgadnięcia

* Możliwość uzyskania dostępu do systemów OT, jeśli są domyślne poświadczenia dostawcy urządzeń wbudowanych i interfejsów zarządzania

nie zmieniony

5. Niebezpieczna konfiguracja zapory:

* Błędnie skonfigurowane reguły dostępu umożliwiają niepotrzebny dostęp między korporacyjnymi sieciami IT i OT

* Zespoły wsparcia zezwalają na nadmierne uprawnienia dostępu do interfejsów zarządzania na zaporach

* Niezabezpieczone zapory rozprzestrzeniają zagrożenia bezpieczeństwa w sieci OT, co czyni je podatnymi na ataki

6. Systemy OT umieszczone w ramach Korporacyjnej Sieci Informatycznej:

* Systemy korporacyjne są połączone z siecią OT w celu uzyskiwania dostępu do danych operacyjnych lub eksportowania danych do systemów zarządzania innych firm

* Systemy OT, takie jak stacje kontrolne i serwery raportujące, są umieszczane w sieci IT

* Możliwość wykorzystania skompromitowanego systemu IT w celu uzyskania dostępu do sieci OT

7. Niewystarczające bezpieczeństwo korporacyjnej sieci IT ze strony systemów OT:

* Ataki również pochodzą z systemów OT, ponieważ wykorzystują one przestarzałe starsze oprogramowanie i są dostępne ze zdalnych lokalizacji

* Możliwość uzyskania nieautoryzowanego dostępu do korporacyjnych systemów IT za pośrednictwem niezabezpieczonych urządzeń OT

8. Brak segmentacji w sieciach OT:

* Kilka sieci OT ma płaską i niesegmentowaną konfigurację, w której zakłada się, że wszystkie systemy mają jednakowe znaczenie i funkcje

* Awaria pojedynczego urządzenia może narazić całą sieć OT

9. Brak szyfrowania i uwierzytelniania w bezprzewodowych sieciach OT:

* Sprzęt bezprzewodowy w sieciach OT wykorzystuje niepewne i przestarzałe protokoły bezpieczeństwa

* Zdolność do przeprowadzania ataków z obejściem wąchania i uwierzytelniania

10. Nieograniczony wychodzący dostęp do Internetu z sieci OT:

* Sieci OT umożliwiają bezpośrednie wychodzące połączenia sieciowe w celu obsługi poprawek i działań konserwacyjnych ze zdalnej lokalizacji

* Bezpośrednia wychodząca łączność internetowa do niezabezpieczonych i niezałatanych

Urządzenia OT zwiększają ryzyko ataków złośliwego oprogramowania

* Podatność na złośliwe oprogramowanie i ataki typu „dowódź i kontroluj”.

MITER ATT&CK dla ICS

MITRE ATT&CK for ICS może służyć jako baza wiedzy przez zespoły ds. bezpieczeństwa ICS lub dostawców, aby zrozumieć działania atakującego przeciwko systemom OT i opracować system obrony, aby im zapobiegać. Pomaga także zespołom ds. bezpieczeństwa zilustrować i scharakteryzować zachowanie osoby atakującej po jakimkolwiek kompromitacji.

MITRE ATT&CK dla ICS oferuje różne taktyki, które omówiono poniżej.

Wstępny dostęp

Odnosi się do metod lub technik, które osoba atakująca może zastosować w celu uzyskania wstępnego dostępu w docelowym środowisku ICS. Osoba atakująca może naruszyć różne zasoby OT, strony internetowe, zasoby IT i inne usługi zewnętrzne, aby uzyskać dostęp do środowiska ICS. Poniżej wymieniono niektóre techniki stosowane przez osobę atakującą w celu uzyskania wstępnego dostępu:

o Kompromitacja typu drive-by: osoba atakująca może uzyskać dostęp do systemu OT, wykorzystując przeglądarkę internetową docelowego użytkownika i nakłaniając go do odwiedzenia zaatakowanej witryny podczas normalnej sesji przeglądania.

o Wykorzystanie aplikacji dostępnej publicznie: osoba atakująca wykorzystuje znane luki aplikacji dostępnej w Internecie, aby uzyskać dostęp do sieci OT. Takie aplikacje mogą służyć do zdalnego monitorowania i zarządzania.

o Wykorzystywanie usług zdalnych: osoba atakująca może manipulować znanymi lukami w zabezpieczeniach aplikacji, wykorzystując komunikaty o błędach generowane przez system operacyjny, program lub jądro, aby przeprowadzać dalsze ataki na usługi zdalne.

Poniżej wymieniono niektóre dodatkowe techniki wykorzystywane przez osoby atakujące w celu uzyskania wstępnego dostępu do środowiska ICS:

o Zewnętrzne usługi zdalne

o Urządzenia z dostępem do Internetu

o Usługi zdalne

o Replikacja na nośnikach wymiennych

o Nieuczciwy mistrz

Załącznik spear-phishing

Kompromis w łańcuchu dostaw

Przejściowe zasoby cybernetyczne

Bezprzewodowy kompromis

Wykonanie

Wykonanie odnosi się do próby wykonania złośliwego kodu przez osobę atakującą, manipulowania danymi lub wykonania innych funkcji systemowych za pomocą nielegalnych metod. Atakujący używają różnych technik do uruchamiania złośliwego kodu w urządzeniu lub zasobie w środowisku ICT. Niektóre techniki związane z tym etapem są następujące:

o Zmiana trybu działania: atakujący uzyskuje dodatkowy dostęp do różnych funkcjonalności OT poprzez manipulowanie trybami działania kontrolera w infrastrukturze, np. pobieranie programu.

o Interfejs wiersza poleceń (CLI): osoba atakująca używa interfejsu CLI do uruchamiania różnych złośliwych poleceń i komunikowania się z systemem OT. Pozwala im instalować i uruchamiać różne złośliwe programy oraz wykonywać złośliwe operacje bez wykrycia.

o Wykonywanie za pośrednictwem interfejsów API: osoby atakujące wstrzykują kod do interfejsów API w celu wykonania określonej funkcji w systemie po wywołaniu przez powiązane oprogramowanie.

Poniżej wymieniono niektóre z dodatkowych technik wykorzystywanych przez osoby atakujące na etapie wykonywania:

o Graficzny interfejs użytkownika (GUI)

o Zahaczanie

o Zmodyfikuj zadania kontrolera

Trwałość

Atakujący wykorzystują procedury trwałości, aby zachować dostęp w środowisku ICS, nawet jeśli zaatakowane urządzenie zostanie ponownie uruchomione lub komunikacja zostanie przerwana. Poniżej przedstawiono niektóre techniki, które atakujący może zastosować na tym etapie.

o Modyfikowanie programu: osoba atakująca nadużywa kontrolera w systemie OT, zmieniając lub dołączając do niego program. Pozwala zmienić sposób, w jaki kontroler komunikuje się z innymi urządzeniami lub procesami w tym środowisku.

o Oprogramowanie układowe modułu: atakujący może umieścić złośliwe oprogramowanie układowe w urządzeniach sprzętowych w celu utrzymania dostępności na innych urządzeniach lub systemach oraz przechowywania śladów na potrzeby długoterminowych ataków.

o Infekcja pliku projektu: osoby atakujące wykorzystują złośliwy kod do infekowania zależności plików, takich jak obiekty lub zmienne wymagane do działania programowalnych sterowników logicznych (PLC). Atakujący często próbują nadużywać domyślnych funkcji PLC.

Poniżej wymieniono kilka dodatkowych technik wykorzystywanych przez osoby atakujące w celu utrzymania uporczywości:

o Oprogramowanie systemowe

o Ważne konta

Eskalacja uprawnień

Eskalacja uprawnień umożliwia atakującemu uzyskanie wyższego poziomu dostępu i autoryzacji do wykonywania dalszych złośliwych działań w systemie ICS lub sieci. Poniżej przedstawiono niektóre techniki, których osoba atakująca może użyć w celu eskalacji uprawnień.

o Wykorzystywanie oprogramowania: osoby atakujące mogą wykorzystać znane luki w oprogramowaniu, wykorzystując wszelkie błędy programistyczne w celu podniesienia uprawnień.

o Przechwytywanie: umożliwia atakującym przechwytywanie interfejsów API różnych procesów w celu przekierowania i wywołania ich w celu podniesienia uprawnień.

o Natywne API

o Skrypty

o Wykonanie użytkownika

Uchylanie się

Atakujący wykorzystują tę taktykę, aby uniknąć konwencjonalnych mechanizmów obronnych podczas swoich operacji. Oto niektóre techniki stosowane w celu uniknięcia wykrycia.

o Usuwanie wskaźników: wskaźniki potencjalnego ataku są usuwane z hosta, aby uniknąć wykrycia i zakryć ślady ataku.

o Rootkity: Osoba atakująca może zainstalować rootkity, aby uniknąć wykrycia, ukrywając różne usługi, połączenia i inne sterowniki systemowe.

o Zmiana trybu operatora: osoby atakujące mogą modyfikować tryb działania kontrolera, aby uzyskać dostęp do różnych funkcji systemu i kontrolować je.

Poniżej wymieniono niektóre dodatkowe techniki unikania:

o Wykorzystanie luk w oprogramowaniu

o Maskarada

o Sfałszowane wiadomości raportowania

Wykrywanie

Wykrywanie to proces uzyskiwania informacji o środowisku ICS w celu oceny i identyfikacji zasobów docelowych. Poniżej przedstawiono niektóre techniki, których można użyć do uzyskania informacji o środowisku ICS.

o Wyliczanie połączenia sieciowego: osoby atakujące mogą uzyskać informacje o wzorcach komunikacji różnych urządzeń sieciowych.

o Podsłuchiwanie sieci: osoba atakująca może przechwycić lub monitorować informacje o sieci, takie jak używany protokół, adres docelowy i źródłowy oraz inne ważne informacje.

o Identyfikowanie systemów zdalnych: osoba atakująca znajduje szczegółowe informacje o innych systemach w sieci poprzez ich nazwy hostów, adresy IP lub inne szczegóły w celu wykonania złośliwych działań.

Poniżej wymieniono niektóre dodatkowe techniki, których atakujący może użyć w celu wykrycia:

o Zdalne wykrywanie informacji o systemie

o Bezprzewodowe wąchanie

Ruch boczny

Atakujący próbują wykonać dodatkowe ruchy w docelowym środowisku ICS, wykorzystując istniejący dostęp. Niektóre techniki stosowane przez napastników do ruchu bocznego są następujące.

o Domyślne poświadczenia: osoba atakująca może wykorzystać wbudowane poświadczenia systemów kontroli do wykonywania zadań administracyjnych.

o Pobieranie programu: osoba atakująca może przesłać program użytkownika w kontrolerze, wykonując pobieranie programu.

o Usługi zdalne: osoba atakująca może nadużywać usług zdalnych w celu wykonywania ruchów poprzecznych w obrębie zasobów i komponentów sieciowych.

Niektóre z dodatkowych technik ruchu bocznego są wymienione poniżej:

o Korzystanie z usług zdalnych

o Boczny transfer narzędzi

o Ważne konta

Kolekcja

Gromadzenie odnosi się do różnych metod wykorzystywanych przez osobę atakującą do gromadzenia informacji i zdobywania wiedzy dotyczącej danych i domen infrastruktury ICS. Osoba atakująca może użyć następujących technik w celu zebrania informacji.

o Zautomatyzowane gromadzenie: osoba atakująca może użyć różnych narzędzi lub skryptów do automatycznego gromadzenia informacji o środowisku ICS.

o Repozytoria informacji: osoby atakujące mogą uzyskać poufne informacje, takie jak układy systemu sterowania i specyfikacje, atakując repozytoria informacji.

o Obraz wejścia/wyjścia: osoby atakujące mogą uzyskać dostęp do pamięci, uzyskując obraz wejścia/wyjścia sterownika PLC w celu wykonania dalszych złośliwych działań.

Poniżej wymieniono niektóre dodatkowe techniki gromadzenia danych:

o Wykrywanie trybu pracy

o Atak typu man-in-the-middle

o Monitorowanie stanu procesu

o Identyfikacja punktów i znaczników

o Ładowanie programu

Przechwytywanie ekranu

o Bezprzewodowe wąchanie

Dowodzenie i kontrola

Osoba atakująca próbuje dezaktywować, kontrolować lub wykorzystywać procesy kontroli fizycznej w docelowym środowisku ICS za pomocą poleceń i kontroli. Niektóre z technik używanych do dowodzenia i kontroli są następujące.

o Często używane porty: Osoba atakująca może używać popularnych portów, takich jak 80 i 443, do komunikowania się i unikania konwencjonalnych mechanizmów wykrywania.

o Serwer proxy połączenia: osoby atakujące mogą kontrolować ruch sieci docelowej w środowisku ICS za pomocą serwera proxy połączenia.

o Standardowy protokół warstwy aplikacji: osoby atakujące mogą używać różnych protokołów warstwy aplikacji, takich jak HTTPS, Telnet i protokół RDP (Remote Desktop Protocol), aby ukryć swoje działania i przejąć kontrolę nad systemami.

Funkcja wstrzymania odpowiedzi

Hamowanie funkcji odpowiedzi odnosi się do różnych sposobów, w jakie atakujący próbuje udaremnić reakcje na dowolne zdarzenie związane z bezpieczeństwem, takie jak zagrożenie lub awaria. Niektóre techniki związane z tą taktyką są następujące.

o Aktywuj tryb aktualizacji oprogramowania układowego: osoba atakująca może aktywować tryb aktualizacji oprogramowania układowego i udaremnić normalne funkcje odpowiedzi podczas zdarzenia związanego z bezpieczeństwem.

o Blokuj komunikaty z poleceniami: osoba atakująca może blokować różne polecenia lub komunikaty z instrukcjami, zanim dotrą one do systemów sterowania.

o Blokowanie komunikatów raportowania: osoba atakująca może zatrzymać lub zakłócić przesyłanie komunikatów raportowania z systemów przemysłowych i uniemożliwić im dotarcie do celu, umożliwiając atakującemu ukrycie swoich działań.

Poniżej wymieniono niektóre dodatkowe techniki hamowania funkcji odpowiedzi:

o Steruj obrazem we/wy

o Zmiana ustawień alarmu

o rootkit

o Przerwa serwisowa

o Oprogramowanie systemowe

o Tłumienie alarmu

o Blokowanie szeregowego COM

Niszczenie danych

o Odmowa usługi (DoS)

o Ponowne uruchomienie/wyłączenie urządzenia

Zakłócić kontrolę procesu

Atakujący wykorzystują tę taktykę do wyłączania, wykorzystywania lub kontrolowania procesów kontroli fizycznej w docelowym środowisku. Niektóre techniki stosowane w tej taktyce są następujące.

o Brutalne wymuszanie wejścia/wyjścia: Atakujący mogą brutalnie wymusić adresy wejścia/wyjścia w celu kontrolowania funkcjonalności procesu bez atakowania konkretnego interfejsu.

o Zmień parametry: osoba atakująca może manipulować systemami sterowania, zmieniając ich parametry instrukcji za pomocą odpowiedniego oprogramowania.

o Oprogramowanie układowe modułu: osoba atakująca może przeprogramować urządzenie poprzez wstrzyknięcie do niego złośliwego oprogramowania układowego iw ten sposób przygotować je do wykonania innych złośliwych zadań.

Poniżej wymieniono niektóre dodatkowe techniki związane z upośledzeniem kontroli procesu:

o Sfałszowane wiadomości raportowania

o Nieautoryzowane komunikaty poleceń

Uderzenie

Wpływ odnosi się do technik stosowanych przez osobę atakującą w celu uszkodzenia, zakłócenia lub przejęcia kontroli nad danymi i systemami docelowego środowiska ICS i jego otoczenia. Niektóre techniki stosowane w tej taktyce są następujące.

o Uszkodzenie mienia: atakujący może spowodować poważne uszkodzenia mienia i otaczającego go środowiska, przeprowadzając różne ataki na ICS.

o Utrata dostępności: osoby atakujące mogą zakłócić lub utrudnić procesy przemysłowe, powodując, że przestaną one reagować na powiązane połączenia.

o Odmowa kontroli: osoba atakująca może manipulować kontrolkami, aby zakłócić komunikację między operatorami a kontrolkami procesu.

Poniżej wymieniono niektóre dodatkowe techniki, których mogą użyć osoby atakujące:

o Utrata wzroku

o Manipulowanie kontrolą

o Manipulacja widokiem

o Kradzież informacji operacyjnych

o Odmowa widzenia

Utrata kontroli

o Utrata produktywności i przychodów

o Utrata ochrony

o Utrata bezpieczeństwa

Zagrożenia OT

Wraz z konwergencją OT i IT systemy OT są wykorzystywane do celów, do których służą a nie były pierwotnie projektowane. Systemy OT są integrowane i łączone z sieciami informatycznymi oraz udostępniane w Internecie, który ma zasięg globalny. Większość systemów OT korzysta ze starszego i przestarzałego oprogramowania bez żadnych zabezpieczeń, co pozostawia potencjalnym cyberprzestępcom furtkę umożliwiającą uzyskanie dostępu do korporacyjnych sieci IT i infrastruktury OT. Ponadto sieci OT łączą wszystkie maszyny i infrastrukturę produkcyjną, prowadząc do złożonych i wyrafinowanych cyberataków, które powodują nawet szkody fizyczne. Poniżej omówiono niektóre z ważnych zagrożeń, przed którymi stoją sieci OT:

Utrzymanie i Zagrożenie Administracyjne

Atakujący wykorzystują luki dnia zerowego w celu utrzymania i administrowania siecią OT. Wykorzystując te luki, atakujący wstrzykują i rozpowszechniają złośliwe oprogramowanie w systemach IT oraz atakują połączone przemysłowe systemy sterowania, takie jak SCADA i PLC.

Wyciek danych

Atakujący mogą wykorzystać systemy IT podłączone do sieci OT, aby uzyskać dostęp do bramy IT/OT i wykraść dane o znaczeniu operacyjnym, takie jak pliki konfiguracyjne.

Nadużycie protokołu

Ze względu na problemy ze zgodnością wiele systemów OT wykorzystuje przestarzałe protokoły i interfejsy, takie jak Modbus i CAN. Atakujący wykorzystują te protokoły i interfejsy do przeprowadzania różnych ataków na systemy OT. Na przykład osoby atakujące mogą nadużywać funkcji zatrzymania awaryjnego (e-stop), która jest mechanizmem bezpieczeństwa używanym do wyłączania maszyn w sytuacjach awaryjnych w celu przeprowadzania ataków jednopakietowych.

Potencjalne zniszczenie zasobów ICS

Atakujący wykorzystują luki w systemach OT, aby zakłócić lub obniżyć funkcjonalność infrastruktury OT, co prowadzi do problemów o krytycznym znaczeniu dla życia i bezpieczeństwa.

Ataki rozpoznawcze

Systemy OT umożliwiają zdalną komunikację przy minimalnych lub zerowych mechanizmach szyfrowania lub uwierzytelniania. Atakujący mogą przeprowadzić wstępny rekonesans i skanowanie docelowej infrastruktury OT w celu zebrania informacji niezbędnych do dalszych etapów ataku.

Ataki typu „odmowa usługi".

Atakujący wykorzystują protokoły komunikacyjne, takie jak Common Industrial Protocol (CIP), do przeprowadzania ataków DoS na docelowe systemy OT. Na przykład osoba atakująca może wysłać złośliwe żądanie połączenia CIP do urządzenia docelowego; po nawiązaniu połączenia może wysłać do urządzenia fałszywą konfigurację IP; jeśli urządzenie zaakceptuje konfigurację, może dojść do utraty komunikacji między urządzeniem a innymi podłączonymi systemami.

Ataki oparte na HMI

Interfejsy człowiek-maszyna (HMI) są często nazywane interfejsami haker-maszyna. Nawet przy postępie i automatyzacji OT interakcja człowieka i kontrola nad procesem operacyjnym pozostają wyzwaniem ze względu na leżące u jego podstaw słabe punkty. Brak światowych standardów tworzenia oprogramowania HMI bez środków bezpieczeństwa zapewniających dogłębną obronę prowadzi do wielu problemów związanych z bezpieczeństwem. Atakujący wykorzystują te luki do przeprowadzania różnych ataków, takich jak uszkodzenie pamięci, wstrzyknięcie kodu, eskalacja uprawnień itp. na docelowe systemy OT.

Wykorzystanie systemów i narzędzi specyficznych dla przedsiębiorstwa

Atakujący mogą atakować urządzenia ICS, takie jak Safety Instrumented Systems (SIS), aby wstrzykiwać złośliwe oprogramowanie, wykorzystując podstawowe protokoły do wykrywania sprzętu i systemów używanych w komunikacji oraz dalszego zakłócania lub uszkodzenia ich usług.

Wyłudzanie informacji

Atakujący wysyłają do ofiary fałszywe wiadomości e-mail zawierające złośliwe łącza lub załączniki, które pozornie pochodzą z legalnych lub dobrze znanych źródeł. Kiedy ofiara klika łącze lub pobiera załącznik, wprowadza złośliwe oprogramowanie, zaczyna uszkadzać zasoby i rozprzestrzenia się na inne systemy. Na przykład osoba atakująca wysyła oszukańczą wiadomość e-mail ze złośliwym załącznikiem do systemu ofiary, który utrzymuje oprogramowanie sprzedażowe działającego zakładu. Gdy ofiara pobiera załącznik, plik

złośliwe oprogramowanie jest wstrzykiwane do oprogramowania sprzedażowego, rozprzestrzenia się na inne systemy sieciowe i ostatecznie uszkadza elementy automatyki przemysłowej.

Ataki złośliwego oprogramowania

Atakujący ponownie wykorzystują starsze pakiety złośliwego oprogramowania, które były wcześniej wykorzystywane do wykorzystywania systemów IT do wykorzystywania systemów OT. Przeprowadzają ataki rozpoznawcze w celu zidentyfikowania luk w nowo podłączonych systemach OT. Po wykryciu luk ponownie wykorzystują starsze wersje złośliwego oprogramowania do przeprowadzania różnych ataków na systemy OT. W niektórych scenariuszach osoby atakujące opracowują również złośliwe oprogramowanie atakujące systemy OT, takie jak ICS/SCADA.

Wykorzystywanie niezałatanych luk w zabezpieczeniach

Atakujący wykorzystują niezałatane luki w produktach ICS, oprogramowaniu układowym i innym oprogramowaniu używanym w sieciach OT. Dostawcy systemów ICS opracowują produkty, które są niezawodne i zapewniają wysoką szybkość działania w czasie rzeczywistym bez wbudowanych funkcji zabezpieczeń. Ponadto dostawcy ci nie mogą opracowywać poprawek dla zidentyfikowanych luk z taką samą szybkością jak dostawcy IT. Z tych powodów napastnicy celują w luki w zabezpieczeniach ICS i wykorzystują je do przeprowadzania różnych ataków na sieci OT.

Ataki kanałami bocznymi

Atakujący przeprowadzają ataki typu side-channel w celu pobrania krytycznych informacji z systemu OT poprzez obserwację jego fizycznej implementacji. Atakujący używają różnych technik, takich jak analiza czasu i analiza mocy, do przeprowadzania ataków typu side-channel.

Atak przepełnienia bufora

Atakujący wykorzystuje różne luki w zabezpieczeniach związane z przepełnieniem bufora, które istnieją w oprogramowaniu ICS, takim jak interfejs sieciowy HMI, klient sieciowy ICS, interfejsy komunikacyjne itp., aby wstrzyknąć złośliwe dane i polecenia w celu zmodyfikowania normalnego zachowania i działania systemów.

Wykorzystywanie pilotów zdalnego sterowania RF

Sieci OT wykorzystują technologię RF do zdalnego sterowania różnymi operacjami przemysłowymi. Protokoły komunikacji radiowej nie mają wbudowanych zabezpieczeń komunikacji zdalnej. Luki w tych protokołach mogą zostać wykorzystane przez osoby atakujące do przeprowadzenia różnych ataków na maszyny przemysłowe, które prowadzą do sabotażu produkcji, kontroli systemu i nieautoryzowanego dostępu.

Ataki oparte na interfejsie HMI

Atakujący często próbują włamać się do systemu HMI, ponieważ jest to główny węzeł sterujący infrastrukturą krytyczną. Jeśli atakujący uzyskają dostęp przez systemy HMI, mogą spowodować fizyczne uszkodzenie urządzeń SCADA lub zebrać poufne informacje związane z architekturą krytyczną, które mogą być później wykorzystane do przeprowadzenia złośliwych działań. Korzystając z tych informacji, osoby atakujące mogą wyłączyć powiadomienia o zagrożeniach przychodzących do systemów SCADA. Poniżej omówiono różne luki SCADA wykorzystywane przez osoby atakujące do przeprowadzania ataków opartych na interfejsie HMI na przemysłowe systemy sterowania:

Uszkodzenie pamięci

Luki w tej kategorii to problemy z bezpieczeństwem kodu, które obejmują luki w zabezpieczeniach związane z odczytem/zapisem oraz przepełnienie bufora sterty i stosu. W interfejsie HMI uszkodzenia pamięci mają miejsce,

gdy zawartość pamięci jest zmieniana z powodu błędów znajdujących się w kodzie. Gdy używana jest ta zmieniona zawartość pamięci, program ulega awarii lub wykonuje niezamierzone wykonania. Atakujący mogą wykonać zadania związane z uszkodzeniem pamięci, po prostu nadpisując kod, aby spowodować przepełnienie bufora. Czasami nieopróżniony stos może również pozwolić atakującym na użycie manipulacji łańcuchami w celu nadużycia programu.

Zarządzanie poświadczeniami

Luki w tej kategorii obejmują użycie zakodowanych na stałe haseł, zapisywanie poświadczeń w prostych formatach, takich jak zwykły tekst, oraz nieodpowiednią ochronę poświadczeń. Luki te mogą zostać wykorzystane przez osoby atakujące w celu uzyskania dostępu administratora do systemów i zmiany baz danych systemu lub innych ustawień.

Brak autoryzacji/uwierzytelniania i niebezpieczne ustawienia domyślne

Luki w zabezpieczeniach z tej kategorii obejmują przesyłanie poufnych informacji w postaci zwykłego tekstu, niezabezpieczone ustawienia domyślne, brak szyfrowania i niezabezpieczone formanty ActiveX używane do tworzenia skryptów. Autentyczny administrator rozwiązania SCADA może przeglądać i uzyskiwać dostęp do haseł innych użytkowników. Atakujący mogą wykorzystać te luki w celu uzyskania nielegalnego dostępu do docelowego systemu i dalszego rejestrowania lub manipulowania przesyłanymi lub przechowywanymi informacjami.

Wstrzykiwanie kodu

Luki w tej kategorii obejmują typowe wstrzyknięcia kodu, takie jak SQL, system operacyjny, komendy i niektóre wstrzyknięcia specyficzne dla domeny. Gamma jest jednym z czołowych języków specyficznych dla domeny dla interfejsów człowiek-maszyna (HMI), który jest podatny na ataki polegające na wstrzykiwaniu kodu. Ten skrypt jest przeznaczony do tworzenia szybkich faz Ul i aplikacji kontrolnych. Luka oceny, kompilacji i wykonania kodu w czasie wykonywania (EvalExpression) w Gamma może zostać wykorzystana przez atakujących do wysyłania i wykonywania kontrolowanych arbitralnych skryptów lub polecenia w docelowym systemie kontroli nadzorczej i akwizycji danych (SCADA).

Ataki kanałami bocznymi

Atakujący przeprowadzają atak typu side-channel, monitorując jego fizyczną implementację w celu uzyskania krytycznych informacji z systemu docelowego. Atakujący stosują dwie techniki, a mianowicie analizę czasu i analizę mocy w celu przeprowadzania ataków typu side-channel na docelowe systemy OT. Atak analizy czasowej opiera się na ilości czasu potrzebnego urządzeniu do wykonania różnych obliczeń. Atak analizy mocy opiera się na zmianie zużycia energii podczas operacji kryptograficznych. Systemy ICS są często podatne na te dwa ataki typu side-channel.

Analiza czasu

Hasła są często przesyłane kanałem szeregowym. Atakujący stosują strategię pętli, aby odzyskać te hasła. Używają jednego znaku na raz, aby sprawdzić, czy pierwszy wprowadzony znak jest poprawny; jeśli tak, pętla jest kontynuowana dla kolejnych znaków. Jeśli nie, pętla się kończy. Atakujący sprawdzają, ile czasu zajmuje urządzeniu ukończenie jednego pełnego procesu uwierzytelnienia hasła, dzięki któremu mogą określić, ile wprowadzonych znaków jest poprawnych. Ataki oparte na synchronizacji można łatwo wykryć i zablokować.

Analiza mocy

Ataki oparte na analizie mocy są trudne do wykrycia; zaatakowane urządzenie może działać nawet po zainfekowaniu. Dlatego osoby atakujące często wolą przeprowadzić atak oparty na analizie mocy niż atak oparty na synchronizacji w celu odzyskania poufnych informacji. Atak ten przeprowadza się obserwując zmianę poboru

mocy przez półprzewodniki podczas cykli zegara. Oscyloskop obserwuje szczelinę czasową między dwoma impulsami za pomocą sondy. Profil mocy utworzony przez sygnały może pozostawić wskazówkę, w jaki sposób dane są przetwarzane.

Na przykład, obserwując profil mocy, można odzyskać jeden znak hasła, porównując właściwy wprowadzony znak z niewłaściwym znakiem. Klucz kryptograficzny można również uzyskać tą samą metodą. Atakujący mogą uzyskać fizyczny dostęp przez niechronione lub nienadzorowane urządzenie. Następnie używają oscyloskopu i specjalnego urządzenia sprzętowego, które działa na oprogramowaniu do analizy, aby odzyskać klucze kryptograficzne.

Atakujący mogą wykorzystać odzyskane klucze do wprowadzania zmian w konfiguracji analizowanych urządzeń. Ponieważ systemy te są najczęściej wykorzystywane do ochrony sieci elektroenergetycznych, zmiany konfiguracji mogą mieć katastrofalne skutki. Dzięki tym zmianom atakujący mogą utrudnić działanie systemu lub wykorzystać go do przekazania operatorowi nieprawidłowych danych. Urządzenia te są często dystrybuowane i obsługiwane przez scentralizowany system. Nieprawidłowe dane z jednego urządzenia mogą mieć wpływ na główne części sieci OT.

Hakowanie programowalnego sterownika logicznego (PLC)

Sterowniki PLC są podatne na cyberataki, ponieważ służą do kontrolowania fizycznych procesów infrastruktury krytycznej. Atakujący identyfikują sterowniki PLC wystawione na działanie Internetu za pomocą narzędzi online, takich jak Shodan. Zaatakowane sterowniki PLC mogą stanowić poważne zagrożenie dla bezpieczeństwa organizacji. Atakujący mogą ingerować w integralność i dostępność systemów PLC, wykorzystując operacje kontroli pinów i mogą przeprowadzać ataki, takie jak sabotaż ładunku i rootkity PLC.

Kroki użyte do przeprowadzenia ataku typu rootkit PLC:

• Krok 1: atakujący uzyskuje autoryzowany dostęp do urządzenia PLC poprzez wstrzyknięcie rootkita. Następnie przeprowadza atak kontrolny na środowisko wykonawcze PLC, aby odgadnąć domyślne hasło i uzyskać dostęp do sterownika PLC na poziomie administratora.

• Krok 2: Teraz osoba atakująca mapuje moduły wejściowe i wyjściowe wraz z ich lokalizacją w pamięci, aby nadpisać parametry wejściowe i wyjściowe sterownika PLC.

•Krok 3: Po zapoznaniu się z pinami I/O i mapowaniem logiki PLC, atakujący manipuluje sekwencją inicjalizacji I/O, przejmując w ten sposób pełną kontrolę nad operacjami PLC.

Rootkit PLC może wykorzystać wady architektury mikroprocesorów i ominąć nowoczesne mechanizmy wykrywania. Wykorzystując ten atak, osoba atakująca może uzyskać pełną kontrolę nad przetwarzaniem danych wejściowych i wyjściowych PLC poprzez manipulowanie inicjalizacją we/wy. Atak typu rootkit PLC jest również określany jako atak ducha PLC. Aby przeprowadzić ten atak, osoby atakujące muszą mieć dogłębną wiedzę na temat architektury PLC. Jednostka centralna PLC działa w dwóch trybach, tj. trybie programowania i trybie pracy. W trybie programowania PLC może zdalnie pobrać kod z dowolnego komputera, a tryb pracy służy do wykonania właściwego kodu. Po uzyskaniu dostępu do sterownika PLC osoby atakujące mogą pobrać kod złośliwego oprogramowania do sterownika PLC, który jest przechowywany w procesorze. Ten złośliwy kod jest wykonywany w miejsce oryginalnego kodu. Teraz atakujący manipuluje danymi wejściowymi i wyjściowymi, aby uzyskać pełną kontrolę nad urządzeniami mechanicznymi i dodatkowo uszkodzić lub zniszczyć ich działanie.

Hakowanie systemów przemysłowych za pomocą zdalnych kontrolerów RF

Większość maszyn przemysłowych jest obsługiwana za pomocą zdalnych sterowników. Te zdalne kontrolery są wykorzystywane w różnych branżach, takich jak produkcja, logistyka, górnictwo i budownictwo, do automatyzacji lub sterowania maszynami. Urządzenia w sieci używają nadajnika (TX) i odbiornika (RX) do komunikowania się ze

sobą. Podczas gdy nadajnik (TX) przekazuje polecenia radiowe (za pomocą przycisków), odbiornik (TX) reaguje na odpowiednie polecenia. Niewłaściwe implementacje zabezpieczeń w urządzeniach obsługiwanych za pomocą zdalnych sterowników mogą stanowić poważne zagrożenie bezpieczeństwa dla systemów przemysłowych. Atakujący mogą znajdować się w promieniu docelowego systemu i korzystać ze specjalnie zaprojektowanego urządzenia typu nadajnik-odbiornik radiowy. Urządzenie pomaga atakującym projektować własne pakiety i wysyłać je w sieci w celu uzyskania dostępu przez system przemysłowy i wykonywania różnych złośliwych działań. Poniżej wymieniono zagrożenia, z którymi systemy przemysłowe często spotykają się za pośrednictwem zdalnych sterowników RF:

Atak powtórzeniowy

Atakujący rejestrują polecenia (pakiety RF) przesyłane przez operatora i odtwarzają je w systemie docelowym, aby uzyskać podstawową kontrolę nad systemem.

Wstrzyknięcie polecenia

Znając protokoły RF, osoby atakujące mogą zmieniać pakiety RF lub wstrzykiwać własne pakiety, wykorzystując techniki inżynierii wstecznej, aby uzyskać pełny dostęp do maszyny. Atakujący przechwytują i rejestrują polecenia, przeprowadzają inżynierię wsteczną w celu uzyskania innych poleceń używanych do sterowania urządzeniem docelowym i wprowadzają te polecenia w celu manipulowania normalnym działaniem urządzenia docelowego.

Nadużywanie wyłącznika awaryjnego

Korzystając z powyższych informacji, atakujący może wysłać wiele poleceń e-stop (zatrzymania awaryjnego) do urządzenia docelowego, aby wywołać DoS.

Ponowne parowanie ze złośliwym kontrolerem RF

Atakujący może przejąć kontrolę nad oryginalnym pilotem i sparować go z maszyną za pomocą złośliwego kontrolera RF, udającego legalny. Atakujący wysyłają złośliwe żądania sparowania z docelowymi kontrolerami RF, przechwycenia sekwencji poleceń, przejęcia legalnego kontrolera i wykorzystania złośliwego kontrolera do przeprowadzenia różnych ataków na urządzenie docelowe.

Złośliwy atak przeprogramowujący

Atakujący mogą wstrzykiwać złośliwe oprogramowanie do oprogramowania układowego działającego na zdalnych kontrolerach, aby utrzymać stały i pełny zdalny dostęp do docelowego systemu przemysłowego.

Złośliwe oprogramowanie

Atakujący opracowują złośliwe oprogramowanie atakujące systemy przemysłowe. Złośliwe oprogramowanie OT, takie jak Havex i Industroyer, spowodowało poważne zakłócenia procesów biznesowych w sieciach przemysłowych. Może to spowodować potencjalne uszkodzenie oprogramowania i sprzętu używanego do obsługi infrastruktury krytycznej. W niektórych scenariuszach złośliwe oprogramowanie OT może również rozprzestrzeniać infekcję i uniemożliwiać działanie urządzeń podłączonych do sieci. Przemysłowe systemy sterowania są bardziej podatne na ataki złośliwego oprogramowania, ponieważ są podłączone do szerszej sieci. Ponadto rozwiązania OT są często podatne na ataki złośliwego oprogramowania, ponieważ wykorzystują zastrzeżone systemy i starsze technologie, które nie są regularnie aktualizowane i łatane. Ransomware OT, po zainfekowaniu systemu przemysłowego, może destrukcyjnie zablokować i zaszyfrować pliki na dysku twardym, czyniąc system niedostępnym i bezużytecznym. Poniżej omówiono kilka popularnych przykładów złośliwego oprogramowania OT:

PIPEDREAM

PIPEDREAM to struktura ataku zaprojektowana z zestawem narzędzi skierowanych na urządzenia ICS/SCADA. Atakujący używają tego zestawu narzędzi do skanowania, naruszania bezpieczeństwa i kontrolowania urządzeń sieci OT. PIPEDREAM zawiera pięć komponentów: EvilScholar, BadOmen, DustTunnel, MouseHole i LazyCargo. Złośliwe oprogramowanie umożliwia atakującym wykonywanie ruchów poprzecznych, zwiększanie uprawnień i zakłócanie krytycznych funkcji. Ponadto osoby atakujące mogą wykorzystać to złośliwe oprogramowanie do naruszenia bezpieczeństwa urządzeń z systemem Windows, wykorzystując luki w sterowniku płyty głównej ASRock. Za pomocą DustTunnel i LazyCargo osoby atakujące próbują penetrować systemy IT i przestawiać sieci OT w celu wykonywania złośliwych działań; na przykład mogą przesyłać

Poniżej wymieniono kilka dodatkowych przykładów złośliwego oprogramowania OT:

CaddyWiper

EKANS

MegaCortex

Disruptionware

LockerGoga

Triton

Olympic Destroyer

OT Analiza złośliwego oprogramowania: INDUSTROYER.V2

INDUSTROYER.V2 to ponownie załadowany wariant złośliwego oprogramowania ICS Industroyer, który został wykryty pod koniec 2016 r., kiedy to złośliwe oprogramowanie było wykorzystywane do powodowania przerw w dostawie prądu na Ukrainie. INDUSTROYER.V2 został wykryty w 2022 roku wraz z kilkoma dodatkowymi niestandardowymi fragmentami kodu, których celem były sieci energetyczne oparte na OT w określonych regionach Ukrainy. Dzięki niezależnym plikom wykonywalnym i plikom konfiguracyjnym złośliwe oprogramowanie implementuje protokół komunikacyjny IEC-104 w sieci docelowej w celu manipulowania zdalnymi jednostkami terminali (RTU) za pośrednictwem połączeń TCP. INDUSTROYER.V2 umożliwia atakującym zintegrowanie niestandardowej konfiguracji, która może zmienić zachowanie złośliwego oprogramowania zgodnie z funkcjonalnością urządzenia docelowego. Przekaźniki zabezpieczające i jednostki łączące są głównymi celami do osiągnięcia celu.

Etap 1: Wykorzystanie zasobów początkowych

INDUSTROYER.V2 zawiera payloadI04 .dll, który jest podobny do tego używanego przez jego wcześniejszy wariant, Industroyer, do atakowania sieci ICS. Szkodliwe oprogramowanie jest wyposażone w wysoce konfigurowalne programy do atakowania docelowej sieci OT. Konfiguracja ładunku jest zapisywana w formacie łańcuchowym i wstrzykiwana przez protokół IEC-104. Poniższa tabela przedstawia strukturę konfiguracyjną szkodliwego oprogramowania.

Opcje Konfiguracja Opis

1 Adres IP stacji

2 Port stacji

3 Wartość indeksu wpisu

4 Włącz zakodowane telegramy o określonym zakresie

5 Włącz opcje konfiguracji 6-14

5b Jeśli wpis 4 jest włączony, zakres początkowy telegramu

6 Włącz zakończenie procesu

6b Jeśli wpis 4 jest włączony, telegram kończy zakres

7 Nazwa procesu do zakończenia

8 Włącz Zmień nazwę pliku

9 Ścieżka katalogu dla zmiany nazwy pliku

10 Uśpienie przed funkcjonalnością IEC-104

11 Wartość początkowa czasu snu

12 Kontrola wykonania

13 Wartość początkowa czasu snu

14 nieużywane

15 Stan polecenia — WŁ./WYŁ

16 Zmień opcję - wyślij odwrócone polecenia włączania/wyłączania

17 Liczba wpisów danych ASDU

18 Pierwsze wprowadzenie danych ASDU

Te pliki konfiguracyjne są przechowywane niezależnie w pliku .INI, który jest prawdopodobnie przekompilowaną wersją dostępną na publicznych platformach online. Poniższy zrzut ekranu przedstawia przykładową konfigurację złośliwego oprogramowania.

Wpis konfiguracji z powyższego przykładu może wyglądać następująco:

```
192.168.XXX.XXX 2404 2 0 1 1 Example StoppedProcess.exe 1 "Example PATH" 0 1 0 0 1
0 0 8 1104 0 0 0 1 1 1105 0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0 1 5
1101 0 0 0 1 6 1102 0 0 0 1 7 1103 0 0 0 1 8
```

Etap 2: Komunikacja z docelową elektrownią

Jeśli opcja 4 jest włączona we wpisie konfiguracji, złośliwe oprogramowanie wysyła określone polecenia, aby zmienić stan adresów obiektów informacyjnych (IOA) stacji docelowej na wyłączony. Zakres IOA jest określany przez opcje konfiguracyjne #5 i #6. Wpisy konfiguracyjne złośliwego oprogramowania zawierają kilka domyślnie włączonych opcji, w tym zmianę nazwy pliku, zakończenie procesu i wpisy jednostki danych usługi aplikacji (ASDU). Wpisy ASDU są wykorzystywane do tworzenia odpowiednich telegramów ASDU do komunikacji ze stacją zdalną. Strukturę wpisów ASDU przedstawia poniższa tabela.

Opcje Opis ASDU

1 Adres obiektu informacyjnego stacji (IOA)

2 Ustaw typ wiadomości — Pojedyncze lub Podwójne polecenie

3 Ustaw typ polecenia — wybierz lub wykonaj

4 Odwróć domyślny stan WŁ./WYŁ

5 Kontrola wykonania

6 Indeks wpisów ASDU

Po przeanalizowaniu wpisu konfiguracji złośliwe oprogramowanie skanuje wszystkie aktywne procesy w celu wykrycia i zabicia każdego aktywnego procesu zakodowanego na stałe. Wkrótce po zakończeniu zakodowanego procesu złośliwe oprogramowanie ponownie skanuje aktywne procesy i zabija te, które zostały uwzględnione przez operatora w konfiguracji. Szkodliwe oprogramowanie może zmienić nazwę procesu, dodając rozszerzenie .MZ do nazwy pliku, co może uniemożliwić automatyczne odrodzenie docelowego procesu po ponownym uruchomieniu systemu. Dla każdego ustawienia konfigurującego protokół IEC-104 z systemem ICS generowany jest nowy wątek. Protokół wykorzystuje specyfikacje jednostek danych protokołu aplikacji (APDU). Ramka APDU może zawierać tylko ramkę informacji o sterowaniu protokołem aplikacji (APCI) o stałej długości i ramkę ASDU wraz z nagłówkiem APCI o zmiennej długości.

Etap 3: Rozpoczęcie rzeczywistego ataku

Złośliwe oprogramowanie początkowo przesyła komunikaty związane z funkcjami kontrolnymi w ramce APCI. Pierwszy komunikat TESTFR ACT z ramki testowej jest przesyłany do stacji zdalnej w celu sprawdzenia ustanowionego połączenia. Jeśli połączenie jest prawidłowe, stacja odpowiada komunikatem TESTFR CON. Następnie INDUSTROYER.V2 tworzy kanał przesyłania danych w kierunku stacji zdalnej za pomocą rozpoczęcia przesyłania danych (STARTDT). Bezpośredni transfer danych między zdalnym a stacją kontrolną nie jest możliwy, chociaż nawiązane jest aktywne połączenie. W ten sposób INDUSTROYER.V2 przekazuje komunikat STARTDT ACT w celu otwarcia kanału przesyłania danych, a stacja zdalna odpowiada potwierdzeniem STARTDT CON.

Po uruchomieniu transmisji danych INDUSTROYER.V2 wykorzystuje ramkę ASDU do inicjowania poleceń do stacji zdalnej. Telegramy ASDU zawierają zestaw funkcji, które mogą włączać i wyłączać adresy obiektów informacyjnych (IOA) stacji docelowej. Takie polecenia są tworzone na podstawie opcji konfiguracyjnych lub wpisów ASDU określonych powyżej. Na przykład, pierwszym wpisem ASDU dla powyższej konfiguracji może być 1104 0 0 0 1 1. Biorąc pod uwagę wpisy konfiguracji 15 i 16, INDUSTROYER.V2 generuje pakiet ASDU o następującej charakterystyce.

Information Object Address: 1104

ASDU message type: C-DC_NA_1 (Double Command)

ASDU command type: Execute

Set state value: OFF

Wygenerowany telegram ASDU może wyglądać tak, jak pokazano na poniższym zrzucie ekranu:

```
▷ Frame 242: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
  Raw packet data
▷ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▷ Transmission Control Protocol, Src Port: 2140, Dst Port: 2404, Seq: 41, Ack: 41, Len: 16
◢ IEC 60870-5-104-Apci: <- I (1,1)
    START
    ApduLen: 14
    .... ...0 = Type: I (0x00)
    Tx: 1
    Rx: 1
◢ IEC 60870-5-104-Asdu: ASDU=2 C_DC_NA_1 Act     IOA=1104 'double command'
    TypeId: C_DC_NA_1 (46)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 0110 = CauseTx: Act (6)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 2
  ◢ IOA: 1104
      IOA: 1104
    ◢ DCO: 0x05
        .... ..01 = ON/OFF: OFF (1)
        .000 01.. = QU: Short Pulse (1)
        0... .... = S/E: Execute
```

Złośliwe oprogramowanie tworzy odpowiednie telegramy dla każdej docelowej stacji zdalnej i odpowiednio je wysyła. Ustawienia konfiguracyjne złośliwego oprogramowania mogą generować dodatkowe telegramy ASDU w celu włączenia lub wyłączenia IOA stacji zdalnej. Sekwencja komunikacji komunikatów ASDU jest opisana poniżej:

Inicjuje komunikat ramki testowej w celu sprawdzenia poprawności połączenia

Inicjuje komunikat Start Data Transfer, aby włączyć kanał do przesyłania danych

Inicjuje ogólne polecenie dochodzenia w celu określenia stanu stacji zdalnej

Przekazuje spreparowane telegramy lub komunikaty za pomocą polecenia zmiany stanu adaptera IOA aby włączyć lub wyłączyć

Poniższy zrzut ekranu przedstawia sekwencję komunikacji między docelową stacją zdalną a złośliwym oprogramowaniem za pośrednictwem protokołu IEC-104. Sekwencja komunikatów zawiera wszystkie wyżej wymienione polecenia, takie jak TESTFR i STARTDT, jak również inne komunikaty generowane przez ASDU, które mogą być kierowane do IOA docelowej stacji zdalnej.

Metodologia hakowania OT

Systemy OT, takie jak ICS/SCADA i DCS, są często wykorzystywane do monitorowania i sterowania fizycznymi procesami przemysłowymi. Systemy te są wykorzystywane głównie do pozyskiwania danych z procesów, takich jak temperatury, ciśnienia, pozycje zaworów, operatorzy itp. oraz do sterowania siłownikami elektrycznymi, hydraulicznymi, mechanicznymi i pneumatycznymi. W przeszłości te systemy i sieci OT były całkowicie odizolowane od Internetu, ale interoperacyjność i potrzeby biznesowe wymagały konwergencji sieci OT/IT. Luki istniejące w sieciach IT umożliwiają cyberprzestępcom przeprowadzanie destrukcyjnych ataków na systemy OT. W tej sekcji omówiono metodologię hakowania OT oraz sposób przeprowadzania hakowania OT przy użyciu różnych zautomatyzowanych narzędzi.

Co to jest hakowanie OT?

W dzisiejszych czasach systemy przemysłowe są bardziej niż kiedykolwiek połączone z Internetem, przez co są coraz bardziej narażone na luki w zabezpieczeniach i cyberataki. Atakujący przeprowadzają bardziej wyrafinowane i ukierunkowane ataki cybernetyczne, które powodują fizyczne zniszczenie systemów przemysłowych. W niektórych scenariuszach organizacje używają urządzeń ze starszym oprogramowaniem, aby spełnić wymagania dotyczące zgodności i udostępniać poufne informacje stronom trzecim w celu zdalnej konserwacji sprzętu. Czynniki te stwarzają poważne zagrożenia dla bezpieczeństwa organizacji. Celem hakowania OT jest uszkodzenie lub zakłócenie procesów biznesowych poprzez przemysłowe systemy kontroli w różnych zakładach produkcyjnych. Ze względu na wzajemne powiązania IT z OT, OT była narażona na wiele zagrożeń ze strony zdalnych czujników, kontrolerów obsługujących Wi-Fi, urządzeń USB używanych do aktualizacji oprogramowania/oprogramowania układowego, usług w chmurze (na przykład SCADA-as-a-service), itp. Ze względu na tę ekspozycję systemy OT stają się atrakcyjnym celem hakerów. Flow czy haker może czerpać korzyści z OT, gdy zostanie pomyślnie przejęty?

Przejmij pełną kontrolę nad systemami, niszcz systemy lub kradnij krytyczne dane biznesowe lub operacyjne

Całkowicie zamknij fabrykę lub zablokuj produkcję, aby przeprowadzić ataki DoS i spowodować szkody finansowe lub reputacyjne

Przeprogramuj proces montażu, aby pominąć etapy produkcji, co skutkuje wytwarzaniem wadliwych produktów

Narażać maszyny przemysłowe, aby potencjalnie zranić pracowników poprzez przegrzanie, wyłączenia awaryjne itp.

Instaluj złośliwe oprogramowanie, aby zakłócić działanie infrastruktury krytycznej

Zainstaluj oprogramowanie ransomware, aby zablokować dostęp do systemów OT i poprosić o okup

Metodologia hakowania OT

Poniżej przedstawiono różne fazy hakowania sieci OT:

Zbieranie informacji

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Uruchom ataki

Uzyskaj zdalny dostęp

Zachowaj dostęp

Zbieranie informacji

Pierwszym krokiem w hakowaniu sieci OT jest zebranie informacji o docelowej sieci i systemach OT za pomocą różnych technik śledzenia i rozpoznania. Techniki te pozwalają atakującym wyliczyć sieć, zidentyfikować urządzenia podłączone do sieci OT, zidentyfikować geolokalizację urządzeń, zebrać domyślne hasła podłączonych urządzeń, wykryć otwarte porty i uruchomione usługi itp. Atakujący wykorzystują narzędzia takie jak Shodan, CRITIFENCE Default Password Baza danych i Nmap. aby zebrać informacje o docelowej sieci OT.

Identyfikacja systemów ICS/SCADA za pomocą Shodan

Wyszukiwarka Shodan pomaga atakującym zebrać informacje o urządzeniach OT podłączonych do Internetu. To narzędzie online może służyć do uzyskiwania szczegółowych informacji na temat systemów SCADA stosowanych w stacjach uzdatniania wody, elektrowniach jądrowych, systemach HVAC, elektrycznych systemach przesyłowych, domowych systemach grzewczych itp.

Identyfikacja systemów SCADA za pomocą numerów portów

Systemy ICS/SCADA wykorzystują wiele protokołów, które są unikalne dla producentów sterowników PLC. Niektóre z ważnych protokołów SCADA obejmują port Modbus 502, port Fieldbus 1089-91, port DNP 19999, port Ethernet/IP 2222, port DNP3 20000, port PROFINET 34962-64 i port EtherCAT 34980. Wykrywanie portów, na których działają te systemy umożliwia atakującemu zidentyfikowanie wrażliwych systemów SCADA podłączonych do Internetu.

Wyszukiwanie systemów ICS/SCADA z obsługą Modbus:

port:502 (Pobiera wszystkie systemy ICS/SCADA z włączonym portem Modbus 502)

Wykrywanie systemów SCADA po nazwie PLC

Atakujący mogą również wykrywać systemy SCADA na podstawie numerów wersji, nazw sterowników PLC lub nazw producentów. Korzystając z Shodan, osoba atakująca może wyszukać baner systemowy, który wyświetla informacje, takie jak nazwa PLC, producent i wersje. Na przykład Schneider Electric to firma, która wdraża różne protokoły Modbus związane z systemami ICS. Atakujący może wykryć wszystkie systemy z nazwami firm na swoim banerze za pomocą Shodan.

Wyszukiwanie systemów SCADA po nazwie PLC:

Na przykład ciąg wyszukiwania „Schneider Electric” wyświetla wszystkie systemy, w których wdrażane są produkty Schneider Electric.

Wyszukiwanie systemów SCADA na podstawie geolokalizacji

Wyszukiwanie systemów SCADA za pomocą geolokalizacji:

SCADA country:nusM (wyświetla wszystkie systemy SCADA obecne w USA)

Zbieranie domyślnych haseł za pomocą CRITIFENCE

CRITIFENCE to internetowa baza danych przechowująca domyślne hasła infrastruktury krytycznej, SCADA, ICS i IIoT. Atakujący mogą użyć tego narzędzia online, aby odkryć domyślne dane uwierzytelniające urządzenia lub produktu, po prostu wprowadzając nazwę urządzenia lub nazwę producenta. Baza danych zawiera informacje, takie jak kod produktu, dostawca, typ urządzenia oraz jego domyślna nazwa użytkownika i hasło.

Atakujący mogą również korzystać z narzędzi takich jak SCADAPASS (http://www.scodo.sl), które składają się z domyślnych danych logowania różnych produktów, takich jak bramy bezprzewodowe, moduły sieciowe, serwery, sterowniki PLC i routery branżowe, wraz z nazwami dostawców.

Skanowanie systemów ICS/SCADA za pomocą Nmap

Atakujący używają narzędzi skanujących, takich jak Nmap, do identyfikowania otwartych portów i uruchomionych usług w systemach podłączonych do sieci OT. Poniżej omówiono różne polecenia Nmap używane przez atakujących do wyliczania otwartych portów i usług systemów ICS/SCADA:

Identyfikowanie otwartych portów i usług

nmap -Pn -sT --scan-delay Is --max-równoległość 1 -p 80, 102, 443,

502, 530, 593, 789, 1089-1091, 1911, 1962, 2222, 2404, 4000,

4840, 4843, 4911, 9600, 19999, 20000, 20547, 34962-34964, 34980,

44818, 46823, 46824, 55000-55003 CDocelowy adres IP>

Atakujący używają powyższego polecenia Nmap do przeprowadzenia wstępnego rekonesansu w celu zidentyfikowania aktywnych protokołów ICS/SCADA. Numery portów wymienione w poleceniu są dobrze znanymi numerami portów używanymi przez protokoły ICS/SCADA.

Identyfikacja systemów HMI

nmap -Pn -sT -p 46824 CDocelowy adres IP>

Niektórzy dostawcy dostarczają interfejsy HMI, które działają na portach innych niż porty ICS/SCADA. Weźmy na przykład oprogramowanie HMI Sielco Sistemi Winlog, które wykorzystuje port TCP 46824.

Skanowanie sterowników PLC Siemens SIMATIC S7

nmap -Pn -sT -p 102 --script s7-info <docelowy adres IP>

Atakujący używają powyższego polecenia do wykrywania urządzeń PLC z otwartym portem 102. Urządzenia PLC Siemens SIMATIC S7 używają portu 102 do komunikacji S7, używanej do wymiany informacji między urządzeniami PLC a systemami SCADA.

Skanowanie urządzeń Modbus

nmap -Pn -sT -p 502 --script modbus-discover <docelowy adres IP>

nmap -sT -Pn -p 502 --script modbus-discover --scriptargs='

modbus-discover.aggressive=true 1 <Docelowy adres IP>

Atakujący używają powyższego polecenia do identyfikacji urządzeń obsługujących protokół Modbus wraz z ich identyfikatorami Slave.

Skanowanie urządzeń BACnet

nmap -Pn -sU -p 47808 --script bacnet-info <docelowy adres IP>

Atakujący wyliczają urządzenia BACnet używane do łączenia i sterowania systemami budynkowymi i automatyki, systemami HVAC itp. Powyższe polecenie pomaga atakującym uzyskać informacje, takie jak nazwa producenta, nazwa urządzenia, numer seryjny i wersja oprogramowania układowego. Pomaga także atakującym wykrywać urządzenia do zarządzania transmisją BACnet (BBMD) za pomocą skryptu NSE BACnet-discover-enumerate.nse.

Skanowanie urządzeń Ethernet/IP

nmap -Pn -sU -p 44818 --script enip-info <docelowy adres IP>

Ethernet/IP to popularny protokół zaimplementowany w wielu sieciach przemysłowych. Ethernet/IP wykorzystuje Ethernet jako protokół warstwy transportowej, a CIP służy do świadczenia usług dla zastosowań przemysłowych. Protokół ten działa na porcie UDP o numerze 44818. Korzystając z powyższego polecenia, osoby atakujące mogą zbierać informacje, takie jak nazwa dostawcy, kod i nazwa produktu, nazwa urządzenia, adres IP itp.

Skanowanie urządzeń Niagara Fox

nmap -Pn -sT -p 1911,4911 --script fox-info <docelowy adres IP>

Niagara Fox to protokół używany do komunikacji między urządzeniami w systemach zarządzania budynkiem (BMS). Ten protokół działa na portach TCP 1911 i 4911. Powyższe polecenie umożliwia atakującym zebranie informacji, takich jak nazwa aplikacji, wersja Java, system operacyjny hosta, strefa czasowa, lokalny adres IP i wersje oprogramowania.

Skanowanie urządzeń ProConOS

nmap -Pn -sT -p 20547 --script proconos-info <docelowy adres IP>

ProConOS to wysokowydajny silnik wykonawczy dla urządzeń PLC przeznaczony do sterowania wbudowanymi i opartymi na komputerach PC aplikacjami sterującymi. Atakujący mogą użyć powyższego polecenia do wyliczenia informacji, takich jak typ PLC, nazwa projektu, nazwa kodu źródłowego projektu i informacje o czasie wykonywania logiki drabinkowej.

Skanowanie urządzeń PLC firmy Omron

nmap -Pn -sT -p 9600 --script omron-info <docelowy adres IP>

nmap -Pn -sU -p 9600 --script omron-info CTarget IP>

Factory Interface Network Service (FINS) to protokół firmy Omron używany przez programy PLC do przesyłania danych programu i wykonywania innych usług za pomocą zdalnego urządzenia PLC. FINS używa portu TCP lub UDP 9600 do świadczenia usług.

Skanowanie urządzeń PCWorx

nmap -Pn -sT -p 1962 --script pcworx-info <docelowy adres IP>

PCWorx to zautomatyzowane rozwiązania oparte na komputerach PC dla sieci przemysłowych. Systemy te przetwarzają nieuwierzytelnione wiadomości z systemów zdalnych. Atakujący używają powyższego polecenia do zbierania informacji, takich jak typ sterownika PLC, numer modelu i wersja oprogramowania układowego.

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Gdy atakujący zbiorą informacje o docelowej sieci i systemach OT, przeprowadzają skanowanie pod kątem luk w celu zidentyfikowania dostępnych exploitów i luk w infrastrukturze krytycznej i OT. Atakujący używają narzędzi, takich jak SCADA Family for Nessus i Skybox Vulnerability Control, do wykrywania luk w zabezpieczeniach urządzeń OT i IT, protokołów i aplikacji, w tym ICS/SCADA, PLC, RTU, interfejsów HMI, bramek, komputerów stacjonarnych i innych systemów sieciowych. Atakujący używają również narzędzi, takich jak Wireshark, do identyfikowania luk w zabezpieczeniach poprzez monitorowanie i analizę ruchu w sieci przemysłowej.

Skanowanie luk w zabezpieczeniach za pomocą Nessusa

Nessus to narzędzie do oceny podatności, które umożliwia atakującym znalezienie luk w systemach ICS i SCADA. To narzędzie zapewnia również atakującym szybki podgląd luk w zabezpieczeniach związanych z domyślnymi zasadami i szablonami, a następnie umożliwia im tworzenie własnych zasad. Atakujący używają Nessusa do wykrywania i grupowania wszystkich luk w celu przeprowadzania różnych ataków na docelowe sieci OT. Nessus zawiera kilka wtyczek SCADA, za pomocą których osoby atakujące mogą przeprowadzać skanowanie pod kątem luk w zabezpieczeniach docelowych urządzeń ICS/SCADA. Luki są uzyskiwane na podstawie sygnatur wtyczek.

Kroki przeprowadzania skanowania w poszukiwaniu luk w systemach ICS/SCADA za pomocą Nessusa

Krok 1: Zaloguj się do klienta internetowego Nessus za pomocą poświadczeń podanych podczas procesu instalacji. Kliknij kartę Zasady i wybierz opcję Utwórz nową politykę. Następnie wybierz szablon Podstawowe skanowanie sieciowe.

Krok 2: Zmodyfikuj ustawienia w węźle DISCOVERY dla skanowania portów. Podaj port z zakresu 0-1000.

Krok 3: Sprawdź, czy w zakładce Wtyczki istnieją wtyczki SCADA. Jeśli nie, wyniki pojawią się tylko dla portów innych niż SCADA.

Krok 4: Zapisz politykę. Następnie otwórz folder Moje skany i wybierz Nowy skan. Kliknij sekcję Zasady zdefiniowane przez użytkownika i wybierz politykę utworzoną w kroku 1.

Krok 5: Wybierz politykę i wprowadź wymagane informacje w odpowiednich polach wraz z docelowym adresem IP. Następnie kliknij Uruchom.

Po zakończeniu skanowania wynik wyświetla wykryte luki; na poniższym zrzucie ekranu Nessus zidentyfikował dwie luki w zabezpieczeniach SCADA, które są zaznaczone na żółto.

Po uzyskaniu powiązanych luk w systemie atakujący stosuje różne techniki w celu ich wykorzystania i przeprowadzenia dalszych ataków na docelowe systemy OT.

Skanowanie luk w zabezpieczeniach za pomocą Skybox Vulnerability Control

Skybox przeprowadza szczegółową analizę ścieżek w połączonych sieciach OT i IT oraz zapewnia wgląd w powiązane luki w zabezpieczeniach i powiązane wektory ataków. Skybox może łączyć dane SCADA i ICS z informacjami zebranymi z analizy wektorów ataków, danych wywiadowczych Skybox, SIEM, danych

analitycznych o zagrożeniach itp. To narzędzie może nadać priorytet milionom luk w sieciach OT/IT w oparciu o związane z nimi zagrożenia. Atakujący mogą analizować i grupować wszystkie luki w sieciach za pomocą Skybox, aby przeprowadzać różne ataki na środowisko IT/OT.

Fuzzing protokołów ICS

Fuzzing protokołów ICS, takich jak Modbus, BACnet i Internet Printing Protocol (IPP), ma kluczowe znaczenie dla gromadzenia informacji i identyfikowania krytycznych działań sieciowych. Atakujący używają narzędzi takich jak Fuzzowski do testowania sieci przemysłowych pod kątem potencjalnych błędów i luk, które można wykorzystać.

Fuzzowski

Fuzzowski to fuzzer protokołów sieciowych, który pomaga atakującym przeprowadzać testy fuzz na protokołach ICS. Pomaga atakującym w całym procesie fuzowania protokołu sieciowego, a także konfigurowania komunikacji. Atakujący muszą najpierw dogłębnie zrozumieć protokół, który chcą zakłócić.

Poniżej omówiono przykłady fuzzujących protokołów ICS, takich jak BACnet, Modbus i IPP.

Fuzzowanie protokołu BACnet:

python -m fuzzowski 127.0.0.1 47808 -p udp -f bacnet -rt 0.5 -m

BACnetMon

Fuzzing Modbus:

python -m fuzzowski 127.0.0.1 502 -p tcp -f modbus -rt 1

modbuspon

-M

Rozmyty IPP:

python -m fuzzowski printerl 631 -f ipp -r get_printer_attribs --

Sniffowanie za pomocą NetworkMiner

NetworkMiner pomaga atakującym przeprowadzać pasywne podsłuchiwanie sieci i przechwytywanie pakietów w celu wykrycia otwartych portów, nazw hostów, systemów operacyjnych, sesji itp. bez generowania ruchu w sieci. Atakujący wykorzystują również NetworkMiner do analizowania i analizowania plików PCAP oraz ponownego składania/odtwarzania przesyłanych plików lub certyfikatów z plików PCAP. Korzystając z NetworkMiner, atakujący mogą uzyskać dostęp do plików PCAP, których można użyć do analizy przechwyconego wcześniej ruchu sieciowego z sieci ICS.

Analiza ruchu Modbus/TCP za pomocą Wireshark

Wireshark to narzędzie do analizy protokołów sieciowych o otwartym kodzie źródłowym, którego można używać do przechwytywania i analizowania ruchu sieciowego. Atakujący używają tego narzędzia do przechwytywania i analizowania ruchu Modbus/TCP w sieciach przemysłowych. Atakujący manipulują przechwyconymi pakietami i wysyłają szkodliwy ładunek do urządzenia Modbus. Protokół Modbus/TCP nie ma wbudowanego szyfrowania ani zabezpieczeń, więc osoby atakujące mogą łatwo zbierać informacje z pakietów danych przesyłanych między siecią a portem Modbus w urządzeniu.

Odkrywanie topologii sieci ICS/SCADA za pomocą GRASSMARLIN

GRASSMARLIN to narzędzie typu open source, które pasywnie mapuje i wizualnie wyświetla topologię sieci ICS/SCADA, jednocześnie bezpiecznie przeprowadzając wykrywanie urządzeń, rozliczanie i raportowanie tych krytycznych systemów cyberfizycznych. Umożliwia atakującym wykrywanie i katalogowanie hostów ICS/SCADA w sieciach opartych na protokole IP. To narzędzie wykorzystuje różne źródła do generowania tych danych, w tym pliki PCAP, pliki konfiguracyjne routerów i przełączników, tabele CAM i przechwytywanie sieci na żywo. Atakujący używają tego narzędzia do określania dostępnych sieci, generowania topologii sieci i dalszej wizualizacji komunikacji między zidentyfikowanymi hostami.

Uruchom ataki

W fazie skanowania podatności osoby atakujące próbują znaleźć luki obecne w docelowej sieci przemysłowej i systemach. Wykryte luki są następnie wykorzystywane do przeprowadzania różnych ataków, takich jak ataki oparte na interfejsie HMI, ataki typu side-channel, wykorzystujące sterowniki PLC, ataki typu „replay", ataki polegające na wstrzykiwaniu poleceń itp. Atakujący wykorzystują narzędzia, takie jak Metasploit i modbus-cli, do włamywania się do urządzeń PLC poprzez protokół Modbus.

Hakowanie sprzętu ICS

Atakujący wykorzystują publicznie dostępne źródła online, aby zebrać szczegółowe informacje na temat chipa sprzętowego używanego w określonym urządzeniu ICS. Te szczegóły obejmują połączenia lub liczbę pinów osadzonych w chipie oraz akceptowalny typ wejścia/wyjścia. Atakujący mogą również analizować zintegrowane oprogramowanie wewnątrz chipa w celu uzyskania informacji, takich jak certyfikaty, algorytmy generowania kluczy, funkcje szyfrowania itp. Korzystając z tych informacji, atakujący mogą kontrolować analogowe i cyfrowe wejścia/wyjścia oraz dalej modyfikować normalne działanie urządzenia, a także resetować i ponownie uruchomić proces. Przeprowadzając analizę statyczną i dynamiczną funkcji uruchomionych w chipie, atakujący mogą wykryć użyte argumenty oraz obecność i brak walidacji wejść/wyjść. Korzystając z tej analizy, osoby atakujące mogą dalej znajdować luki w zabezpieczeniach, takie jak przepełnienie bufora i kilka innych podstawowych luk, które są często ignorowane przez producentów. Atakujący mogą zhakować sprzęt ICS, wykorzystując te luki w zabezpieczeniach za pomocą różnych narzędzi programowych i sprzętowych. Poniżej wymieniono niektóre popularne narzędzia programowe/sprzętowe, które osoby atakujące mogą wykorzystać do przeprowadzania ataków na sprzęt ICS:

Narzędzia sprzętowe:

Analizator sygnału: atakujący używają tego narzędzia do rozpoczęcia testu z flagami, aby zrozumieć działanie binarne poszczególnych pinów chipa.

Multimetr: osoby atakujące używają multimetrów lub mierników napięcia do przeprowadzania pewnych testów podobnych do analizatora.

Mikrokontrolery i programator pamięci: atakujący mogą używać tych narzędzi do zrozumienia i programowania różnych typów układów scalonych, pamięci flash, EPROM itp.

Oscyloskop: atakujący używają tego narzędzia do dokładnej interpretacji sygnałów analogowych lub cyfrowych.

Sprzęt do lutowania: osoby atakujące używają narzędzi do lutowania w celu podłączania i odłączania elementów sprzętowych, takich jak układy scalone i pamięci, w celu zbadania ich w odizolowanym środowisku iw określonych warunkach.

Mikroskop cyfrowy lub szkło powiększające: osoby atakujące mogą używać tych narzędzi do zwiększania precyzji lutowania komponentów. Może również pomóc w odczytaniu niektórych informacji zapisanych małą czcionką lub wizualizacji drobnych elementów urządzenia.

Interfejs komunikacyjny (taki jak JTAG): osoby atakujące mogą go używać do łączenia się i komunikowania z urządzeniami ICS.

Wkrętaki i wkrętaki precyzyjne: Atakujący używają tego sprzętu do otwierania lub demontażu urządzeń w celu analizy części wewnętrznych.

Precyzyjne pęsety do połączeń i konwerterów: Atakujący mogą używać pęset do połączeń, konwerterów UART/portów szeregowych do USB itp., aby przechwycić informacje bezpośrednio z magistrali komunikacyjnej.

Narzędzia programowe:

GDB

GDB to narzędzie do debugowania dla systemu Linux, które umożliwia atakującym zrozumienie procesu wykonania na chipie.

OpenOCD

OpenOCD umożliwia atakującym podłączenie ich systemu i układu, który chcą zbadać. Komunikacja może być dozwolona za pomocą GDB w porcie 333/ lub za pomocą interfejsu telnet przez port 4444/TCP.

Binwalk

Binwalk pomaga atakującym skanować i badać pliki binarne i obrazy oprogramowania układowego; natychmiast wyświetla różne typy szyfrowania, rozmiary, partycje, zaangażowane systemy plików itp.

Fritzing

Narzędzie Fritzing pomaga atakującym w projektowaniu schematów i obwodów elektronicznych.

Radare2

Radare2 to przenośna platforma, która pomaga atakującym w przeprowadzaniu inżynierii wstecznej i różnych czynnościach, takich jak analiza plików binarnych.

OllyDbg

OllyDbg to narzędzie do deasemblacji kodu, które umożliwia atakującym badanie plików binarnych w systemach Windows.

IDA Pro

IDA Pro to narzędzie do dysemblera, które wykonuje tę samą operację, co OllyDbg.

Hakowanie urządzeń Modbus Slave za pomocą Metasploit

Modbus Master i Slaves komunikują się w postaci zwykłego tekstu bez uwierzytelniania. Atakujący mogą wykorzystać tę lukę do generowania i wysyłania podobnych pakietów zapytań do urządzeń podrzędnych Modbus w celu uzyskania dostępu do rejestrów i cewek urządzenia podrzędnego oraz manipulowania nimi. Atakujący mogą przeprowadzić ten atak tylko wtedy, gdy maszyna atakującego może wysyłać pakiety do Modbus Slave, a

wysyłane pakiety wykorzystują format protokołu Modbus. Atakujący używają narzędzi hakerskich, takich jak Metasploit, do przeprowadzania różnych ataków na Modbus Slaves.

Skanowanie Slave Modbus

Atakujący używają modułu pomocniczego/scanner/scada/modbus_findunitid Metasploit do skanowania i wykrywania modułów Slave Modbus podłączonych do docelowej sieci LAN lub wewnątrz bramki Modbus.

Manipulowanie danymi Modbus Slave

Atakujący wykorzystują moduł Metasploit pomocniczy/skaner/scada/modbusclient do odczytu lub zapisu rejestrów i cewek na docelowym urządzeniu Modbus Slave.

Hakowanie PLC za pomocą modbus-cli

Sterowniki PLC są używane do sterowania infrastrukturą przemysłową, taką jak zakłady produkcyjne, oczyszczalnie ścieków, sieci elektryczne i rafinerie ropy naftowej. Atakujący atakują urządzenia PLC, takie jak Schneider Electric TM221, które są używane do automatyzacji procesów w wielu branżach produkcyjnych. Urządzenia te wykorzystują protokół Modbus/TCP do komunikacji z innymi urządzeniami przemysłowymi. Atakujący używają narzędzi takich jak modbus-cli do wykorzystywania urządzeń PLC za pośrednictwem protokołu Modbus.

Kroki, aby zhakować PLC za pomocą modbus-cli:

Krok 1: Zidentyfikuj sterowniki PLC podłączone do Internetu

Możesz użyć narzędzi takich jak Shodan, Nmap itp., aby znaleźć obiekty przemysłowe wyeksponowane w Internecie. Aby wykryć sterowniki PLC Schneider Electric TM221 podłączone do Internetu, wpisz TM221ME16R w pasku wyszukiwania Shodan. Shodan pobiera wszystkie sterowniki Schneider Electric TM221PLC podłączone do Internetu, gdzie wiele z tych systemów jest podatnych na ataki.

Krok 2: Zainstaluj modbus-cli

Po zidentyfikowaniu wrażliwych urządzeń PLC za pomocą Shodan, zainstaluj teraz modbus-cli za pomocą następującego polecenia:

gem install modbus-cli

Krok 3: Zrozum typy danych

Przed eksploatacją przy użyciu modbus-cli musisz zrozumieć typy danych używane do odczytywania wartości. Te typy danych wykorzystują dwa typy adresów, a mianowicie adresy Schneider i Modicon. Adres Schneidera zaczyna się od %M przed adresem.

Typ danych : Rozmiar danych : Adres Schneidera : Parametr adresu : Modicona

word (domyślnie, bez znaku) : 16 bitów : %MW100 : 400101 : --word

integer (ze znakiem) : 16 bitów : %MW100 : 400101 : --int

floating point : 32 bity : %MF100 : 400101 : --float

double word : 32 bity : %MD100 : 400101 : --dword

Boolean : 1 bit : %M100 : 101 : N/D

Krok 4: Odczytaj wartości rejestru

Aby odczytać wartości rejestrów z urządzeń zidentyfikowanych w kroku 1, użyj następującego polecenia:

Używając adresu Schneider: modbus read <Target IP> %MW100 10

Używając adresu Modicon: modbus read <Target IP> 400101 10

Powyższe polecenie pobiera dziesięć słów z rejestrów.

Krok 5: Manipuluj wartościami rejestrów

Teraz możesz manipulować wartościami rejestru za pomocą następujących poleceń:

modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2

modbus write <Target IP> 400101 2 2 2 2 2 2 2 2

Po uruchomieniu powyższego polecenia pierwsze osiem wartości rejestrów jest zastępowanych przez 2.

Krok 6: Odczytaj wartości cewki

Teraz spróbuj pobrać wartości cewek. Te wartości wykorzystują typy danych Boolean do przechowywania wartości WŁ./WYŁ. (1/0). Uruchom następujące polecenia, aby pobrać wartości cewek:

modbus read <Target IP> 101 10

modbus read <Target IP> %M100 10

Krok 7: Manipuluj wartościami cewek

Możesz użyć modbus-cli do manipulowania wartościami cewek. Użyj następujących poleceń, aby włączyć wszystkie cewki:

modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1

modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1

Po uruchomieniu powyższego polecenia, jeśli sprawdzisz wartości cewek, zobaczysz wszystkie cewki o wartości 1:

Krok 8: Przechwyć dane do pliku wyjściowego

Teraz możesz przechwytywać dane z urządzeń SCADA do przyszłych analiz i testów. Użyj następującego polecenia, aby przechwycić wartości rejestru do pliku wyjściowego:

modbus read --output SCADAregisters.txt <Target IP> 400101 200

modbus read --output SCADAregisters.txt <Target IP> %MW100 200

Użyj następującego polecenia, aby przechwycić wartości cewek do pliku wyjściowego:

modbus read --output SCADAcoils.txt <IP> 101 100

modbus read --output SCADAcoils.txt <IP> %M100 100

Uzyskaj i utrzymuj zdalny dostęp

Fazy zbierania informacji i skanowania luk w zabezpieczeniach umożliwiają atakującym badanie środowiska OT i identyfikowanie luk, które pomagają im uzyskać zdalny dostęp do przemysłowych systemów sterowania. Na przykład osoby atakujące mogą wykorzystać luki w zabezpieczeniach protokołów przemysłowych lub wstrzyknąć złośliwe oprogramowanie w celu przeprowadzenia ukierunkowanych ataków i uzyskania dostępu do przemysłowych systemów kontroli. Gdy osoby atakujące uzyskają dostęp do systemów przemysłowych, manipulują i zmieniają operacje i funkcje kontroli przemysłowych, powodując szkody fizyczne i finansowe organizacji. Po uzyskaniu zdalnego dostępu osoby atakujące wykorzystują te urządzenia jako platformę do przeprowadzania ataków na inne urządzenia podłączone do sieci. Po uzyskaniu dostępu do urządzenia atakujący stosuje różne techniki w celu utrzymania dostępu i dalszej eksploatacji. Atakujący pozostają niewykryci, czyszcząc dzienniki, aktualizując oprogramowanie układowe i wprowadzając rootkity, aby zachować dalszy dostęp do urządzenia docelowego. Po uzyskaniu dostępu do urządzenia docelowego atakujący może zmodyfikować oprogramowanie układowe na urządzeniach takich jak sterowniki PLC, aby przeprowadzić ataki na oprogramowanie układowe w celu monitorowania i kontrolowania różnych operacji na urządzeniu docelowym.

Uzyskanie dostępu zdalnego za pomocą DNP3

Internetowe systemy sterowania można spotkać w różnych gałęziach przemysłu, w tym w elektrowniach, przemyśle wytwórczym, budownictwie itp. Te systemy sterowania mają na celu umożliwienie monitorowania lub sterowania systemami z odległych lokalizacji. Ta zdalna komunikacja jest często konfigurowana z bezpośrednim dostępem do Internetu, ignorując implementacje zapory lub dostęp przy użyciu domyślnych poświadczeń. Atakujący mogą wykorzystać te źle skonfigurowane sieci lub słabe/domyślne poświadczenia hasła, aby uzyskać nieautoryzowany dostęp do systemów przemysłowych. Te domyślne dane uwierzytelniające są publicznie dostępne w Internecie, a słabe hasła można łatwo wymusić brutalnie. Atakujący mogą używać narzędzi online, takich jak Shodan, do skanowania otwartych portów lub usług na docelowych urządzeniach ICS. Gdy atakujący znajdą otwarty port, mogą wykorzystać istniejące luki w celu uzyskania zdalnego dostępu do systemów przemysłowych. Na przykład osoby atakujące atakujące określone protokoły ICS, takie jak DNP3 — port 20000, przeprowadzają skanowanie portów za pomocą narzędzia Shodan, które wyświetla otwarte porty i powiązane luki w zabezpieczeniach. Klikając na otwarty port, atakujący są przekierowywani na stronę logowania docelowego systemu. Z tego miejsca osoby atakujące mogą uzyskać zdalny dostęp do sieci lub systemów ICS, wprowadzając domyślne hasła lub brutalnie wymuszając poświadczenia.

Narzędzia hakerskie OT

Atakujący używają narzędzi hakerskich OT do identyfikowania przemysłowych systemów sterowania podłączonych do docelowej sieci, starszego oprogramowania zainstalowanego na tych urządzeniach, wrażliwych portów i usług, używanych niezabezpieczonych i niezaszyfrowanych protokołów komunikacyjnych itp. W celu przeprowadzenia różnego rodzaju ataków na docelowe systemy i sieć. W tej sekcji omówiono różne narzędzia hakerskie OT.

Narzędzia do zbierania informacji

Poniżej omówiono różne narzędzia do gromadzenia informacji OT:

SearchDiggity

Źródło: https://bishopfox.com

SearchDiggity to główne narzędzie ataku Google Hacking Diggity Project. Składa się z zestawu narzędzi, w tym GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch i NotInMyBackYard Diggity. Shodan Diggity zapewnia łatwy w użyciu interfejs skanowania do popularnej wyszukiwarki hakerskiej Shodan; ponadto jest wyposażony w wygodną listę 167 zapytań gotowych w gotowym pliku słownika znanym jako Shodan

Hacking Database (SHDB). Shodan to wyszukiwarka, która pozwala znaleźć określone typy komputerów (routery, serwery itp.) przy użyciu różnych filtrów. Atakujący wykorzystują Shodan Diggity do wykrywania systemów SCADA podłączonych do Internetu wraz z ich szczegółami, takimi jak adres IP, geolokalizacja itp.

Poniżej wymieniono kilka dodatkowych narzędzi do zbierania informacji OT:

Kamerka-GUI (https://github.com)

Redpoint (https://github.com)

s7scan (https://github.com)

SCADAPASS (http://www.scodo.sl)

plcscan (https://code.google.com)

Narzędzia do wykrywania i wykrywania luk w zabezpieczeniach

Narzędzie do sniffowania: Sniffer pakietów SmartRF

SmartRF Packet Sniffer zawiera oprogramowanie i oprogramowanie sprzętowe do przechwytywania i wyświetlania pakietów drogą radiową. Urządzenie przechwytujące jest podłączone do komputera przez USB. SmartRF Packet Sniffer obsługuje urządzenia z rodziny CC13xx i CC26xx jako urządzenie przechwytujące; ponadto używa Wireshark do wyświetlania i filtrowania pakietów. Obsługuje protokoły takie jak ZigBee, EasyLink i BLE.

Narzędzie do wykrywania luk w zabezpieczeniach: Microsoft Defender dla IoT

Platforma Microsoft Defender for IoT przeprowadza ocenę podatności na zagrożenia w środowisku IoT i ICS i zwraca obiektywną ocenę ryzyka. Identyfikuje wszystkie zasoby IoT i ICS podłączone do sieci docelowej. Wylicza luki w zabezpieczeniach na poziomie urządzenia, takie jak brakujące poprawki, słabe hasła, nieużywane otwarte porty, porty zdalnego dostępu itp. Generuje raporty dotyczące luk w zabezpieczeniach na poziomie sieci, takich jak nieautoryzowane połączenia internetowe, słabe reguły zapory ogniowej, nieuczciwe połączenia podsieci między IT, IoT, i ICS, nieautoryzowane punkty dostępu bezprzewodowego (WAP) oraz nielegalne urządzenia.

Narzędzia hakerskie OT

Poniżej omówiono różne narzędzia wykorzystywane przez osoby atakujące do hakowania systemów i sieci OT:

Ramy eksploatacji ICS (ISF)

ICS Exploitation Framework (ISF) to platforma eksploatacyjna oparta na języku Python, która jest podobna do platformy Metasploit. To narzędzie udostępnia różne moduły exploitów, które umożliwiają atakującym włamanie się do docelowych systemów i sieci ICS.

Poniżej wymieniono niektóre z dodatkowych narzędzi do hakowania systemów i sieci OT:

PLCinject (https://github.com)

MODBUS Penetration Testing Framework (https://github.com)

Moki Linux (https://github.com)

Sixnet-tools (https://github.com)

mbtget (https://github.com)

Środki zaradcze ataku OT

W tej sekcji omówiono różne środki bezpieczeństwa OT, luki w zabezpieczeniach OT i ich rozwiązania, środki bezpieczeństwa oparte na modelu Purdue, międzynarodowe organizacje bezpieczeństwa OT, rozwiązania bezpieczeństwa OT i narzędzia. Stosując środki bezpieczeństwa, organizacje mogą wdrożyć odpowiednie mechanizmy bezpieczeństwa w celu ochrony krytycznej infrastruktury przemysłowej i powiązanych systemów IT przed różnymi cyberatakami.

Jak bronić się przed hakowaniem OT

Postępuj zgodnie ze środkami zaradczymi omówionymi poniżej, aby bronić się przed hakowaniem OT:

Regularnie przeprowadzaj ocenę ryzyka, aby zmniejszyć obecną ekspozycję na ryzyko

Używaj specjalnie skonstruowanych czujników do nieaktywnego wykrywania luk w sieci

Wykorzystaj analizę zagrożeń, aby wykrywać zagrożenia i chronić zasoby, ustalając priorytety dla poprawek OT

Regularnie aktualizuj narzędzia sprzętowe i programowe OT

Wyłącz nieużywane porty i usługi

Implementuj bezpieczną konfigurację i praktyki bezpiecznego kodowania dla aplikacji OT

Aktualizuj systemy do najnowszych technologii i regularnie łataj systemy

Prowadź rejestr zasobów, aby śledzić informacje i analizować przestarzałe i nieobsługiwane systemy

Wykonuj ciągłe monitorowanie i wykrywanie danych dziennika generowanych przez systemy OT w celu wykrywania ataków w czasie rzeczywistym

Szkol pracowników w zakresie najnowszych zasad bezpieczeństwa i zwiększaj świadomość najnowszych zagrożeń i ryzyka

Używaj silnych i bezpiecznych haseł za pomocą haszowania i zmieniaj domyślne hasła ustawione fabrycznie

Bezpieczny dostęp zdalny dzięki wielu warstwom ochrony poprzez wdrożenie uwierzytelniania dwuskładnikowego, sieci VPN, szyfrowania, zapór ogniowych itp.

Wdrażaj reagowanie na incydenty i plany ciągłości działania

Zabezpiecz obwód sieci, aby filtrować i zapobiegać nieautoryzowanemu ruchowi przychodzącemu

Regularnie skanuj systemy i sieci za pomocą narzędzi chroniących przed złośliwym oprogramowaniem

Ogranicz ruch sieciowy za pomocą technik, takich jak ograniczanie szybkości i umieszczanie na białej liście, aby temu zapobiec

Ataki typu DoS i brute-force

Utwardź systemy, wyłączając nieużywane usługi i funkcjonalności

Regularnie łataj luki udostępniane przez producentów

Regularnie sprawdzaj dzienniki DNS, aby wykryć nieautoryzowany dostęp

Zabezpiecz i aktualizuj systemy współpracujące z urządzeniami ICS/SCADA, ponieważ systemy te można wykorzystać do ominięcia bram bezpieczeństwa

Zatrudniaj profesjonalne zespoły ds. bezpieczeństwa, aby wykrywać słabe punkty krytycznej infrastruktury przemysłowej

Użyj systemów wykrywania włamań (IDS) i systemów pomiaru przepływu, aby wykrywać próby ataków na wczesnym etapie

Zapewnij odpowiednią sanityzację i weryfikację danych wejściowych, aby zapobiec atakom, takim jak przepełnienie bufora, wstrzyknięcie poleceń i XSS.

Użyj wywołań biblioteki zamiast procesów zewnętrznych, aby odtworzyć pożądaną funkcjonalność

Przetwarzaj wszystkie zapytania SQL używane w systemie ICS przy użyciu przygotowanych instrukcji, zapytań sparametryzowanych lub procedur składowanych

Do obsługi aplikacji internetowych ICS należy używać wyłącznie sprawdzonych i znanych serwerów internetowych innych firm

Upewnij się, że dostawcy ICS projektują swoje systemy tak, aby ograniczać nieautoryzowany dostęp i przyznawać jak najmniejsze uprawnienia do wykonywania funkcji

Zapewnij integralność przesyłanych wiadomości, dołączając do każdej wiadomości sumę kontrolną

Upewnij się, że dostawcy ICS dodają podpisy kryptograficzne do aktualizacji aplikacji

Przeprowadzaj okresowe audyty systemów przemysłowych w celu weryfikacji systemów kontroli bezpieczeństwa, produkcji i zarządzania

Użyj połączeń DMZ między ICS a sieciami korporacyjnymi do bezpiecznej komunikacji

Sprawdź powiązania i integralność danych sieciowych w aplikacjach serwera, które przetwarzają ruch protokołu ICS

Przeprowadź przegląd kodu źródłowego wszystkich aplikacji ICS, które obsługują ruch sieciowy

Luki w zabezpieczeniach i rozwiązania OT

Luki w systemach przemysłowych, takich jak ICS/SCADA, PLC i RTU, stanowią poważne zagrożenie dla powiązanej infrastruktury krytycznej. Organizacje muszą wdrożyć odpowiednie kontrole i mechanizmy bezpieczeństwa, aby chronić takie systemy przed różnymi cyberatakami. Poniżej omówiono niektóre z najczęstszych luk i rozwiązań OT:

Słabości : Rozwiązania

1. Publicznie dostępne systemy OT:

* Zaimplementuj uwierzytelnianie wieloskładnikowe

* Korzystaj z zapory sieciowej klasy korporacyjnej i rozwiązań dostępu zdalnego

2. Niebezpieczne połączenia zdalne:

* Używaj silnego mechanizmu uwierzytelniania wieloskładnikowego i solidnych zasad dotyczących haseł

* Wdrażaj odpowiednie praktyki łatania zabezpieczeń

3. Brakujące aktualizacje zabezpieczeń:

* Testuj aplikacje w środowisku piaskownicy przed uruchomieniem ich na żywo

* Zastosuj zaporę ogniową i wykonaj hartowanie urządzeń

4. Słabe hasła:

* Używaj oddzielnych konwencji nazw użytkowników dla korporacyjnych sieci IT i OT

* Zmień domyślne poświadczenia w czasie instalacji

* Przeprowadzaj audyty bezpieczeństwa, aby zapewnić zgodność z zasadami bezpieczeństwa haseł zarówno dla sieci IT, jak i OT

5. Niebezpieczna konfiguracja zapory:

* Zaimplementuj bezpieczną konfigurację zapory

* Skonfiguruj listy kontroli dostępu na zaporze

6. Systemy OT umieszczone w ramach Korporacyjnej Sieci Informatycznej:

* Oddziel korporacyjne urządzenia IT i OT

* Ustanowić DMZ (strefę zdemilitaryzowaną) dla wszystkich połączeń w systemach IT i OT

* Regularnie monitoruj strefę DMZ

7. Niewystarczające bezpieczeństwo korporacyjnej sieci IT ze strony systemów OT:

* Ogranicz dostęp do sieci IT/OT w zależności od potrzeb biznesowych

* Stwórz bezpieczną bramę między sieciami OT i IT

* Regularnie przeprowadzaj ocenę ryzyka

8. Brak segmentacji w sieciach OT:

* Określ wyraźny podział między systemami krytycznymi i niekrytycznymi

* Zaimplementuj model podziału na strefy, który wykorzystuje podejście dogłębnej obrony

9. Brak szyfrowania i uwierzytelniania w bezprzewodowych sieciach OT:

* Używaj silnych protokołów szyfrowania sieci bezprzewodowej

* Korzystaj ze standardowych algorytmów kryptograficznych

* Przeprowadzaj regularne audyty bezpieczeństwa

10. Nieograniczony wychodzący dostęp do Internetu z sieci OT:

* Przeprowadź formalną ocenę ryzyka

* Ściśle monitoruj i oddzielaj systemy OT od dostępu zewnętrznego

* Pobierz aktualizacje zabezpieczeń z osobnego repozytorium poza siecią OT

Jak zabezpieczyć środowisko IT/OT

Konwergencja IT/OT jest szeroko stosowana w takich branżach, jak systemy kontroli ruchu, elektrownie, firmy produkcyjne itp. Te systemy IT/OT są często celem atakujących, aby odkryć podstawowe luki i pozwolić sobie na cyberataki. W oparciu o model Purdue środowisko IT/OT podzielone jest na kilka poziomów, z których każdy musi być zabezpieczony odpowiednimi zabezpieczeniami.

W poniższej tabeli opisano różne ataki na różne poziomy Purdue środowiska IT/OT, powiązane zagrożenia i środki kontroli bezpieczeństwa w celu wzmocnienia sieci przed cyberatakami:

Zone	Purdue Level	Attack Vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise Network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, Access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, Network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, Industrial spying, Unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems and Basic Controls)	DoS exploitation, Unencrypted protocols, Default credentials, Application and OS vulnerabilities	Altering industrial process, Industrial spying	IPS, Firewall, Communication encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption to the physical process	Point-to-point communication, MAC authentication, Additional security gateways at levels 1 and 0

Implementacja modelu zerowego zaufania dla ICS/SCADA

Sieci OT stają się coraz bardziej atrakcyjnym celem dla atakujących, którzy chcą zakłócić działanie infrastruktury ICS. Aby wyprzedzić atakujących, organizacje muszą wdrożyć odpowiednie zabezpieczenia i z wyprzedzeniem zająć się lukami w zabezpieczeniach, aby zapobiec wyrafinowanym atakom. Większość sieci ICS opiera się na starszych systemach lub sprzęcie, który nie zawiera nowoczesnych systemów bezpieczeństwa ani kontroli dostępu, co czyni je podatnymi na wyrafinowane ataki. Wdrożenie modelu zerowego zaufania w sieci ICS może pozwolić organizacji na zapewnienie niezawodnego zarządzania dostępem do starszych systemów i sieci. Umożliwia to również wszechstronną widoczność i zapewnia weryfikację wszystkich aplikacji, użytkowników i urządzeń w sieci ICS.

Kroki w celu wdrożenia modelu zerowego zaufania w sieci ICS

Krok 1: Definiowanie sieci

Ponieważ powierzchnia ataku organizacji stale się rozwija, zabezpieczenie całej organizacji jest wyzwaniem. Wdrożenie podejścia opartego na zerowym zaufaniu należy rozpocząć od zdefiniowania obszaru ataku poprzez identyfikację zasobów organizacyjnych, wrażliwych danych i krytycznych aplikacji w centrach kontroli lub halach produkcyjnych.

Krok 2: Mapowanie ruchu

Ogólny przepływ ruchu sieciowego musi być odwzorowany i udokumentowany, aby zrozumieć, w jaki sposób urządzenia sieciowe i inne zasoby współdziałają ze sobą. Mapowanie ruchu umożliwia zespołom OT uzyskanie pełnego wglądu w sieć i zrozumienie wymaganych kontroli bezpieczeństwa w celu zabezpieczenia krytycznych danych i aplikacji.

Krok 3: Tworzenie architektury sieci

Po zrozumieniu przepływów ruchu analitycy bezpieczeństwa mogą wdrożyć architekturę o zerowym zaufaniu (ZTA) w oparciu o wymagania biznesowe, można ją zainicjować wprowadzeniem zapory sieciowej nowej generacji (NGFW), która może dodać bramę segmentacji dla powierzchni to trzeba chronić. Umożliwi to dodatkowe warstwy kontroli dostępu i wewnętrzną ocenę tej powierzchni.

Krok 4: Opracowanie Polityki ZT

Należy wdrożyć zasadę zerowego zaufania (ZT) w celu umieszczania użytkowników i urządzeń na białej liście po stworzeniu architektury sieci. Dzięki temu analitycy bezpieczeństwa mogą określić, kto, dlaczego, kiedy i do jakich zasobów ma mieć dostęp w sieci ICS.

Krok 5: Monitorowanie i konserwacja

Na ostatnim etapie analitycy bezpieczeństwa muszą upewnić się, że architektura zero-trust (ZTA) może monitorować ruch zgodnie z przeznaczeniem, aby uzyskać cenny wgląd w sieć i zarządzać aktualizacjami na wszystkich urządzeniach sieciowych zgodnie z wymaganiami.

Międzynarodowe organizacje bezpieczeństwa OT

Ponieważ OT jest szeroko rozpowszechniony i powiązany z IT, badacze bezpieczeństwa muszą być bardziej ostrożni i wdrażać silne polityki bezpieczeństwa w celu wzmocnienia sieci OT. Niektóre globalne organizacje zajmujące się cyberbezpieczeństwem są zobowiązane do zapewnienia odpowiednich zasad bezpieczeństwa i wglądu w poprawę odporności infrastruktury krytycznej. Poniżej wymieniono kilka międzynarodowych organizacji, które ostrzegają firmy przed zagrożeniami i dostarczają rozwiązania IT/OT w celu ochrony branży OT przed cyberatakami.

OTCSA

Operation Technology Cybersecurity Alliance (OTCSA) kształci operatorów i producentów ze stałą świadomością techniczną i zapewnia wytyczne dotyczące wprowadzania istotnych zmian, aktualizacji, integracji itp. Zespół ds. bezpieczeństwa w OTCSA zapewnia również wsparcie w zrozumieniu wyzwań bezpieczeństwa OT i rozwiązań w celu ochrony zasobów przemysł.

OT-ISAC

Centrum udostępniania i analizy informacji o technologiach operacyjnych (OT-ISAC) to główne centrum wymiany informacji o zagrożeniach między branżami OT, takimi jak sektor energetyczny i wodociągowy. Organizacja oferuje różne narzędzia i techniki do bezpiecznej wymiany informacji między widmem OT/IT w celu ochrony systemów przemysłowych lub sieci przed złośliwymi włamaniami. Będąc powiązanym z różnymi ośrodkami wymiany informacji, OTISAC pozyskuje informacje dotyczące bezpośrednich zagrożeń i dostarcza terminowe rozwiązania wzmacniające systemy przemysłowe zarejestrowanych firm.

NERC

North American Electric Reliability Corporation (NERC) jest międzynarodowym organem regulacyjnym non-profit, którego celem jest zapewnienie skutecznej i wydajnej redukcji zagrożeń dla niezawodności i bezpieczeństwa sieci elektrycznej. NERC opracowuje i egzekwuje standardy niezawodności; corocznie ocenia

niezawodność sezonową i długoterminową; monitoruje masowy system zasilania poprzez świadomość systemu; oraz kształci, szkoli i certyfikuje personel przemysłowy.

Ramy zabezpieczeń Internetu przemysłowego (IISF)

Industrial Internet Security Framework (IISF) odnosi się do ryzyka ataku z nieoczekiwanych źródeł zarówno wewnątrz, jak i na zewnątrz sieci organizacji, co może utrudniać produkcję. Najważniejszym celem tych ram jest identyfikacja i monitorowanie operacji łączących IT i OT oraz ustalanie priorytetów zagrożeń.

ISA/IEC-62443

Międzynarodowe Towarzystwo Automatyki (ISA)/ Międzynarodowa Komisja Elektrotechniczna (IEC) - 62443 jest stowarzyszeniem zawodowym non-profit zrzeszającym inżynierów, techników i kierownictwo zajmujące się automatyką przemysłową. Zapewnia elastyczne ramy do rozwiązywania i łagodzenia obecnych i przyszłych luk w zabezpieczeniach systemów automatyki i sterowania przemysłowego (IACS), które są częścią branży OT. Zawiera również wymagania techniczne dotyczące cyberbezpieczeństwa dla komponentów składających się na IACS, w szczególności związanych z branżami OT, takimi jak urządzenia wbudowane, komponenty sieciowe, komponenty hosta i aplikacje. Norma określa możliwości bezpieczeństwa, które umożliwiają komponentowi łagodzenie zagrożeń dla danego poziomu bezpieczeństwa bez pomocy kompensujących środków zaradczych dla systemów OT.

Rozwiązania bezpieczeństwa OT

Sektor przemysłowy i korporacyjny szybko digitalizują swój operacyjny łańcuch wartości, dając dostęp do urządzeń OT z szerszego zakresu Internetu. Koszt zarządzania bezpieczeństwem w sektorach przemysłu ciężkiego jest w dużej mierze pomijany, co prowadzi do kilku wyzwań związanych z bezpieczeństwem. W związku z tym uważa się, że bezpieczniejsze dla wszystkich sektorów przemysłu jest inwestowanie w programy i rozwiązania w zakresie cyberbezpieczeństwa. - Specjaliści ds. cyberbezpieczeństwa powinni wdrażać rozwiązania, rozsądnie analizując najnowsze wyzwania i wymagania w zakresie cyberbezpieczeństwa, przed którymi stoją w obecnym trendzie, które można połączyć z odpowiednimi zmianami operacyjnymi. Dlatego wielu obecnych dostawców OEM i start-upów opracowało kilka najnowszych taktyk i technologii ochrony środowiska OT. Ponieważ przemysł ciężki ma zdecentralizowaną naturę, rozwiązania bezpieczeństwa można zintegrować ze wszystkimi decyzjami związanymi z technologią w zakresie IT i OT. Ponadto drugą linię obrony można wdrożyć za pomocą zarządzania ryzykiem informacyjnym (IRM). Niektóre branże zapewniają również trzecią linię obrony poprzez wdrożenie funkcji audytu wewnętrznego. Niektóre z pojawiających się rozwiązań technologicznych wykorzystywanych przez organizacje do ochrony środowiska OT są następujące:

Zapory ogniowe

Zapory ogniowe są używane w sieci do monitorowania i kontrolowania przychodzącego i wychodzącego ruchu sieciowego. Zapory ogniowe pomagają w poprawie kontroli bezpieczeństwa, kontrolując ruch przechodzący przez bramę między sieciami OT i IT. Mogą również pomóc w identyfikowaniu i blokowaniu nowych zagrożeń. W ten sposób osoba atakująca może zostać ograniczona do przechodzenia między sieciami po włamaniu się do systemu. Wskazane jest również stosowanie krytycznych zasobów i systemów w strefie zdemilitaryzowanej z dala od systemów SCADA. Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi takich jak SCADAwall, Waterfall i Palo Alto NGFW do ochrony sieci.

Ujednolicone zarządzanie tożsamością i dostępem OT

Zarządzanie dostępem pomaga branżom scentralizować niektóre operacje, takie jak dodawanie, zabezpieczanie, zmienianie i usuwanie dostępu użytkowników do systemów OT. Wszystkie te dane są powiązane z systemem zarządzania tożsamością organizacji, który może zapewnić silne uwierzytelnianie. Zarządzanie dostępem pomaga

zminimalizować ryzyko ataku poprzez nadanie jak najmniejszych uprawnień kontom superużytkownika. Pomaga to personelowi ochrony w śledzeniu krytycznych zasobów i pomaga w identyfikacji źródeł ataku. Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi takich jak OT Access, FireEye itp. do identyfikacji i zarządzania dostępem do systemów przemysłowych.

Inwentaryzacja zasobów i autoryzacja urządzeń

Inwentaryzacja zasobów pomaga w podłączeniu do sieci OT tylko autoryzowanych urządzeń i może wykryć wszystkie podłączone urządzenia. Może również wykrywać luki w zabezpieczeniach urządzeń, które są podzielone na kategorie na podstawie producenta urządzenia, wersji i typu. Narzędzia te mogą być również wykorzystywane do identyfikacji usterek w podłączonych urządzeniach w sieci, a także mogą zwiększyć wydajność urządzenia. Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi takich jak SCADAfence, CyberLens, Guardian i Dragos do inwentaryzacji zasobów i autoryzacji urządzeń.

Monitorowanie sieci OT i wykrywanie anomalii

Monitoring sieci OT służy do ciągłego monitorowania systemów w sieciach przemysłowych. Te narzędzia monitorujące pomagają w śledzeniu ruchu w nieinwazyjny sposób. Narzędzia te wykonują wykrywanie anomalii, czyli proces identyfikowania wszelkich złośliwych lub nieoczekiwanych zdarzeń. Większość z tych narzędzi wykorzystuje algorytmy uczenia maszynowego do łatwego wykrywania i identyfikacji złośliwych zachowań. Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi takich jak Claroty i OT Threat Intelligence do monitorowania sieci OT i wykrywania anomalii.

Wabiki, aby oszukać atakujących

Wabiki to pułapki na miód używane w środowisku OT, które zawierają technologię oszustwa w celu zautomatyzowania tworzenia pułapek lub wabików, aby zwabić atakujących do ujawnienia ich obecności i działań. Dodaje to dodatkową warstwę ochrony przed atakującymi próbującymi przeniknąć do sieci przemysłowej. Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi, takich jak ThreatDefend, Conpot i GasPot, aby chronić sieć.

Narzędzia bezpieczeństwa OT

Poniżej omówiono różne narzędzia, których można użyć do zabezpieczenia systemów i sieci OT:

Flowmon

Flowmon umożliwia producentom i przedsiębiorstwom użyteczności publicznej zapewnienie niezawodności ich sieci przemysłowych w celu uniknięcia przestojów i zakłóceń ciągłości usług. Można to osiągnąć poprzez ciągłe monitorowanie i wykrywanie anomalii, tak aby nieprawidłowo działające urządzenia lub incydenty związane z bezpieczeństwem, takie jak cyberszpiegostwo, dni zerowe lub złośliwe oprogramowanie, mogły być zgłaszane i naprawiane tak szybko, jak to możliwe.

Poniżej wymieniono kilka dodatkowych narzędzi do zabezpieczania środowiska OT:

Tenable.ot (https://www.tenoble.com)

Singtel (https://www.singtel.com)

Forescout (https://www.forescout.com)

PA-220R (https://www.polooltonetworks.com)

Claroty (https://www.cloroty.com)

Podsumowanie modułu

W tym module omówiliśmy koncepcje IoT oraz różne typy modeli komunikacji IoT. Omówiliśmy również szczegółowo różne zagrożenia i ataki na sieci i urządzenia IoT. Ponadto omówiliśmy metodologię hakowania IoT, która obejmuje zbieranie informacji, skanowanie luk w zabezpieczeniach, przeprowadzanie ataków IoT, uzyskiwanie zdalnego dostępu i utrzymywanie dostępu. W tym module zilustrowano również różne narzędzia hakerskie LoT. W tym module omówiliśmy również różne środki zaradcze, które należy zastosować, aby zapobiec próbom hakowania sieci IoT przez cyberprzestępców. Omówiliśmy również szczegółowo, jak zabezpieczyć sieci i urządzenia IoT za pomocą narzędzi zabezpieczających IoT. W tym module omówiliśmy również koncepcje OT oraz zagrożenia i ataki OT. Omówiliśmy szczegółowo metodologię i narzędzia hakerskie OT. Omówiliśmy również różne środki zaradcze w celu obrony przed atakami OT. Moduł ten zakończył się demonstracją rozwiązań i narzędzi bezpieczeństwa OT. W następnym module szczegółowo omówimy, w jaki sposób osoby atakujące, a także etyczni hakerzy i pentesterzy przeprowadzają hakowanie w chmurze w środowisku chmurowym.