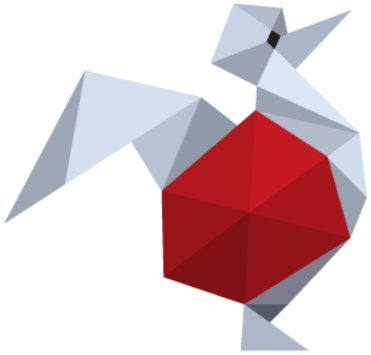
Ochrona informacji na urządzeniach mobilnych

web.lex, Warszawa, 2014

Michał Sajdak, Securitum
sekurak.pl

O prelegencie

- Michał Sajdak
- Założyciel sekurak.pl



sekurak.pl

- Konsultant / trener w securitum.pl
- Certyfikacje: CISSP / CEH / CTT+

O prezentacji

- Prezentacja – tylko do celów edukacyjnych.
- Całość podzielona na dwie części
  - 1. Stare / nowe problemy bezpieczeństwa w systemach mobilnych
  - 2. Jak się zabezpieczyć
- Prezentacja dotyczy przede wszystkim systemów Android / iOS
- Warto pamiętać też o analizie ryzyka

Wstęp

- Obecnie znacznie więcej sprzedaje się smartfonów / tabletów niż „zwykłych PC”
  - Gartner: Worldwide Devices Shipments by Operating System (2014, Thousands of Units):
    - Android: 1,069,503
    - Windows: 397,533
    - iOS/MacOS: 359,483

Wstęp

- Ale w obszarze bezpieczeństwa cofnęliśmy się o co najmniej kilka lat
- Wracają problemy, które od dawna były rozwiązane w świecie „zwykłych” PC

Stare problemy

- Brak aktualizacji
  - Niby w czym jest problem ze zrobieniem aktualizacji OS?
  - Przede wszystkim spora fragmentacja na urządzeniach Android
  - Podejście – działa? Nie ruszać.
  - Za OpenSignal:

Stare problemy

- Brak aktualizacji
  - Ciekawy problem z 2013 roku
    - W systemach Android < 4.2 (czyli globalnie 70% użytkowników)
    - Po kliknięciu na prostego linka (lub wejściu na zainfekowaną stronę) – atakujący otrzymuje nieuwierzytelniony dostęp w systemie operacyjnym

Stare problemy

- Grafika za Rapid7
  - dostarczenie kodu przez QR code

- http://sekurak.pl/przegladarkowe-zdalne-wykonanie-kodu-w-androidzie-4-2/

Stare problemy

- Wykonanie kodu na Androidzie jest…dość proste. Wystarczy taki javascript:

```
<script>
function execute(cmdArgs)
{
    return js2java.getClass().forName("java.lang.Runtime").getMethod("getRunti
me",null).invoke(null,null).exec(cmdArgs);
}
…
</script>
```

  - Za trustlook.com

Stare problemy

- W iOS też mamy różne „niespodzianki”
- Arstechnica.com @02.2014:
  - Extremely critical crypto flaw in iOS

```
1  static OSStatus
2  SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
3                                   uint8_t *signature, UInt16 signatureLen)
4  {
5      OSStatus        err;
6      ...
7
8      if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
9          goto fail;
10     if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
11         goto fail;
12         goto fail;
13     if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
14         goto fail;
15     ...
16
17 fail:
18     SSLFreeBuffer(&signedHashes);
19     SSLFreeBuffer(&hashCtx);
20     return err;
21 }
```

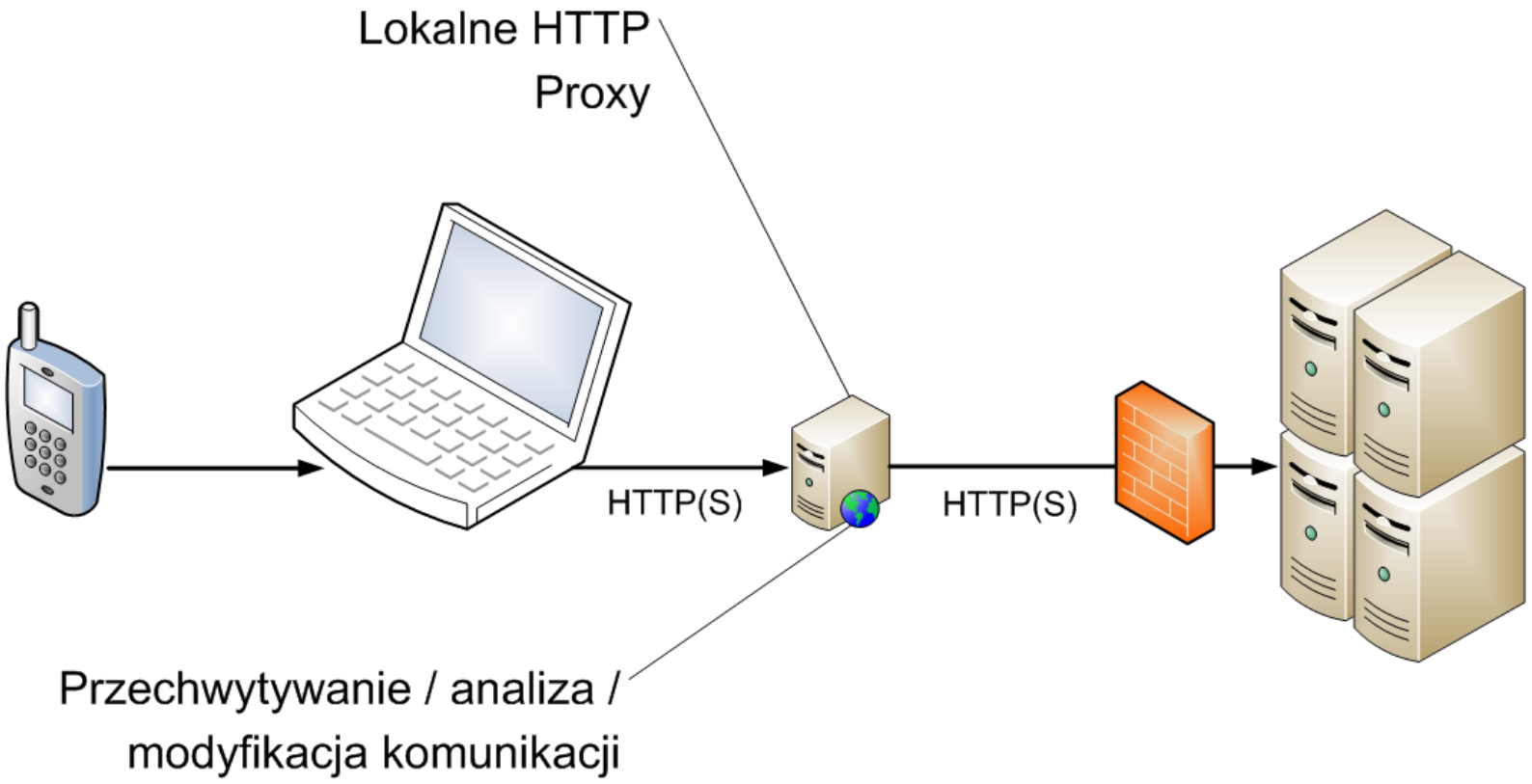
Stare problemy

- Aplikacje pisane z niewielkim naciskiem na bezpieczeństwo
  - Deweloperzy (i klienci) są zachwyceni kiedy aplikacja poprawnie działa. Bezpieczeństwo – tylko przeszkadza ;-)

Stare problemy

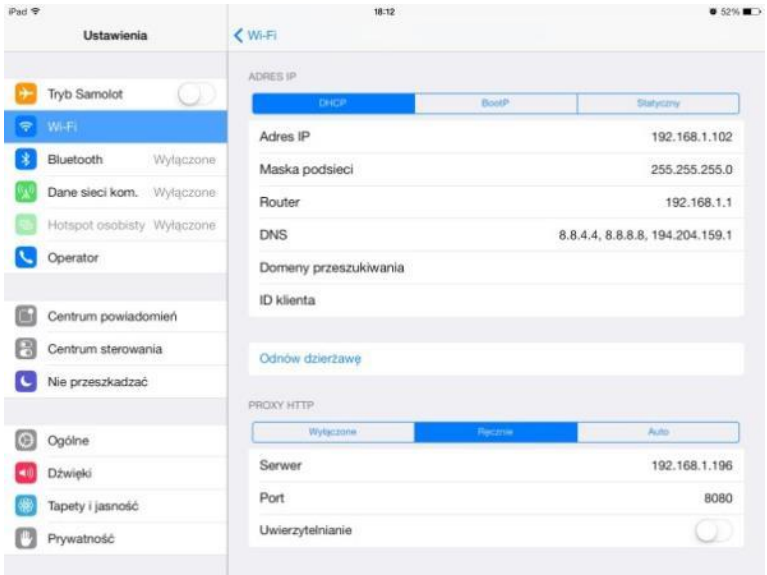
- Aplikacje (c.d.)
  - Słabo zabezpieczona komunikacja z backendem serwerowym (komunikacja HTTP/S)
  - Słabo napisana część backendowa
    - SQL injection
    - Problemy autoryzacyjne
    - Wykonanie kodu w OS
    - Wszystko to już znamy z aplikacji webowych
  - Przechowywanie danych na urządzeniu bez żadnego zabezpieczenia (plaintext)
    - loginy/hasła
    - dane osobowe
    - …

Stare problemy



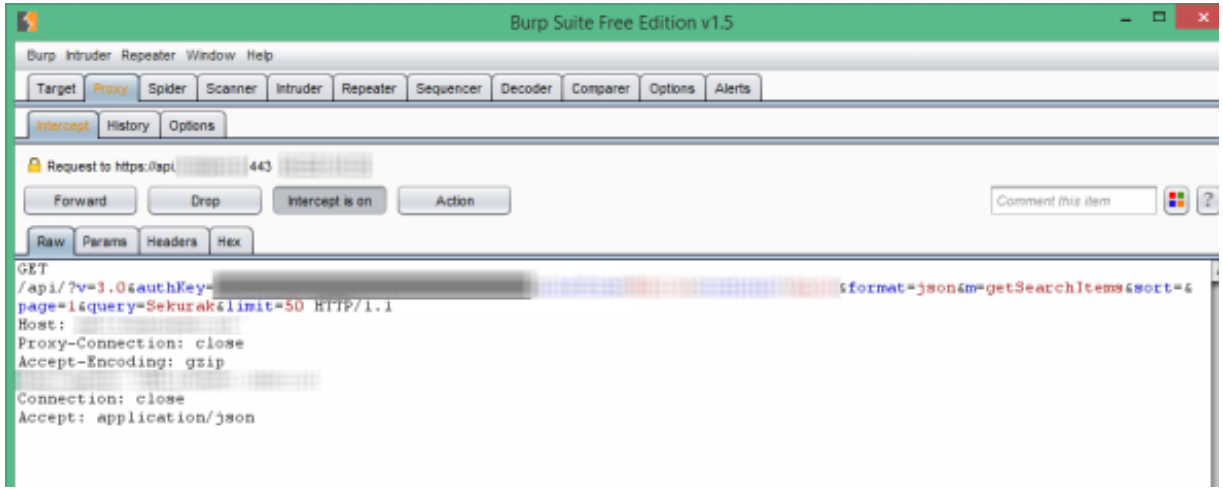
Stare problemy

- Aplikacje (c.d.) – możemy bez problemu analizować komunikację urządzenie - serwer



Stare problemy

- Aplikacje (c.d.) – możemy bez problemu analizować komunikację urządzenie - serwer



Stare problemy

- Aplikacje
  - The Mobile App Top 10 Risks:
    - https://www.owasp.org/images/9/94/MobileTopTen.pdf

Stare problemy

- Aplikacje
  - Specjalnie podatne aplikacje (do trenowania swojej wiedzy)
    - http://carnal0wnage.attackresearch.com/2013_08_01_archive.html

Stare problemy

- Aplikacje
  - Specjalnie podatne aplikacje (do trenowania swojej wiedzy)
    - http://damnvulnerableiosapp.com/
    - *Damn Vulnerable iOS App (DVIA) is an iOS application that is damn vulnerable.*
    - *This application covers all the common vulnerabilities found in iOS applications (following OWASP top 10 mobile risks) and contains several challenges that the user can try.*

Stare problemy

- Brak antywirusa / antymalware
- Malware bankowy
  - ZitMo (Zeus in the Mobile)
    - Kradzież SMS-ów (uwierzytelniających transakcje) i następnie czyszczenie konta
- Czy ogólnie malware mobilny…

Stare problemy

- Przede wszystkim atakowane są systemy Android :
  - instalacja aplikacji z innych źródeł niż Google Play
  - W Google Play też bywa malware…
    - Większa otwartość Google Play (vs. Apple App Store) – również większa otwartość na malware
  - Często źródłem jest piracki software, ale też np. „podrabiane aplikacje”

Stare problemy

- Czy ktoś słyszał o Angry Zombie Birds? ;-)

Stare problemy

- Ciekawostka: „Virus Shield” hitem w Google Play

Stare problemy

- Ciekawostka: „Virus Shield” hitem w Google Play
- Antywirus, cena: $3,99
  - Dobry marketing (wykupione opinie) wywindowały aplikację na Top w Google Play
  - W bardzo krótkim czasie pobrało (kupiło) aplikację około 10 000 osób

Stare problemy

- Ciekawostka: „Virus Shield” hitem w Google Play
  - Bardzo szybkie działanie
  - Nie zajmowanie wiele pamięci
  - Niski wpływ na inne aplikacje

Stare problemy

- Ciekawostka: „Virus Shield” hitem w Google Play
  - Tyle że aplikacja w ogóle nie robiła (!!!) ☺

Stare problemy

- Przede wszystkim atakowane są systemy Android :
  - Nieaktualna przeglądarka
    - wystarczy wejść na odpowiednio spreparowaną stronę
    - odczytać pdf
    - odczytać inny zainfekowany zasób

Stare problemy

- Dostęp do wrażliwych danych
  - Poczta elektroniczna
  - Dane uwierzytelniające do systemów
    - Często przechowywane w plaintext na urządzeniu
  - Dane do VPN
  - Dane do sieci WiFi

Stare problemy

- Dostęp do wrażliwych danych
  - Poczta elektroniczna
    - Loginy / Hasła
    - Poczta przechowywana offline
      - Szyfrowanie end-end
    - Szyfrowana transmisja
    - Sprawdzenie certyfikatu serwera
    - Dostęp do poczty przez VPN

Stare problemy

- Dostęp do wrażliwych danych
  - Dane uwierzytelniające do systemów
    - Przykład: słownik iOS
    - Przykład: dane logowania zapisywane w telefonie
      - Powiązane np. z danymi osobowymi

Stare problemy

- Dostęp do wrażliwych danych
  - Dane do sieci WiFi
  - https://wifipineapple.com/
  - Auto-attack mode switches deliver customized boot-time payloads without the need to login. Simply flip the switches to your attack mode of choice and power on.

Nowe problemy

- Telefon łatwiej zgubić
  - Sprzęt mobilny jest często niezabezpieczony (brak PIN, brak szyfrowania dysku, itd.)
  - Prosty PIN daje tylko podstawowe zabezpieczenie
    - Pamiętajmy też o autoblokadzie podczas pewnej nieaktywności telefonu
  - Łamanie PIN-u
    - http://sekurak.pl/robot-do-lamania-androidowych-pin-ow/

Nowe problemy

- Telefon łatwiej zgubić
  - Rozwiązanie – blokada telefonu (ew. trwałe wymaganie) po podaniu kilku nieprawidłowych PIN-ów
  - **Elcomsoft iOS Forensic Toolkit**
    - Simple 4-digit passcodes recovered in 10-40 minutes
  - Rozwiązanie złożone PINy
    - Niewygodne :/

Nowe problemy

- Telefon łatwiej zgubić
  - iPhone5: możliwość zamiany PIN-u na odcisk palca
  - Problem: można zrobić lateksowy palec – kopia palca oryginalnego
  - Odciski palców na telefonie…

Nowe problemy

- Telefon łatwiej zgubić
  - Szyfrowanie dysku
    - Dane wyglądają jak losowe znaki
    - Warto sprawdzić czy mamy szyfrowane dane również na ew. zewnętrznej karcie pamięci…
    - Często mechanizm powiązany z kodem PIN

Nowe problemy

- Telefon łatwiej zgubić
  - Ciekawostka: Activation Lock dla systemu iOS
  - Po kradzieży / zagubieniu telefonu sprzęt nadaje się do wyrzucenia
    - Nie można przykładowo „sformatować” telefonu i użyć go dla nowego użytkownika

Nowe problemy

- Telefon łatwiej zgubić
  - Hackerom udało się niedawno złamać blokadę
  - Zakupili w cenie $50 znaczną liczbę „zablokowanych” iPhone-ów
  - Zresetowali i sprzedali > $300

Nowe problemy

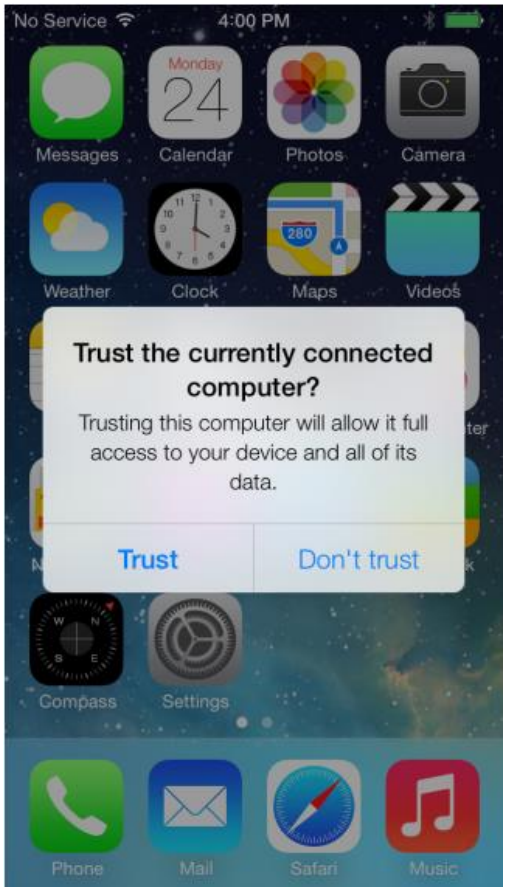
- Wysyłka SMS-ów premium
  - Jeden ze sposobów monetyzacji malware

Nowe problemy

- Podstawione ładowarki
  - Kablem ładującym transmitowane są również dane…
  - Podstawiona ładowarka (np. w punkcie publicznego ładowania), która tak naprawdę jest małym komputerem
  - …atakującym telefon
  - BlackHat USA:
    - Injecting malware into iOS devices via malicious chargers

Nowe problemy

- Podstawione ładowarki
  - iOS od wersji 7 pokazuje odpowiedni komunikat
  - Kto czyta komunikaty? ;-)



Nowe problemy

- Jailbreaking / rooting
  - „jailbreaking essentially reduces ios security to the level of android“ ;-)
  - możliwość korzystania z funkcji systemów mobilnych normalnie niedostępnych
  - pełna kontrola nad urządzeniem

Nowe problemy

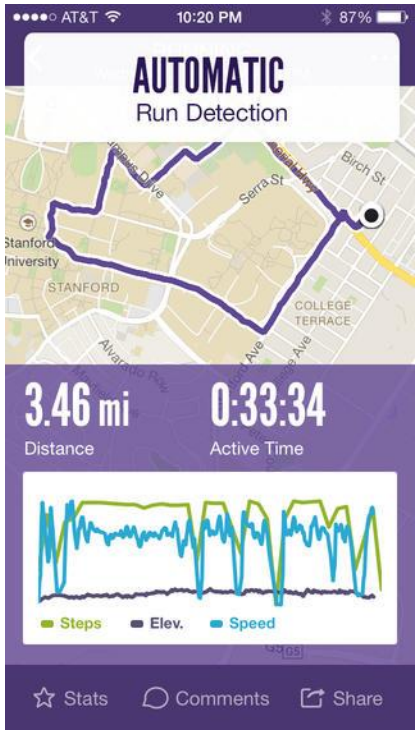
- Częste używanie urządzeń prywatnych w infrastrukturze firmowej
  - Podobnie z laptopami
  - Mniejsza kontrola nad tym co użytkownik posiada na urządzeniu
    - Aplikacje / malware
    - Często sieci o wiele słabiej chronione wewnątrz

Nowe problemy

- Popularny drugi czynnik (poza hasłem) – przy autoryzacji transakcji w bankowości elektronicznej
  - Malware
  - Czy na pewno mamy dwa czynniki?

Nowe problemy

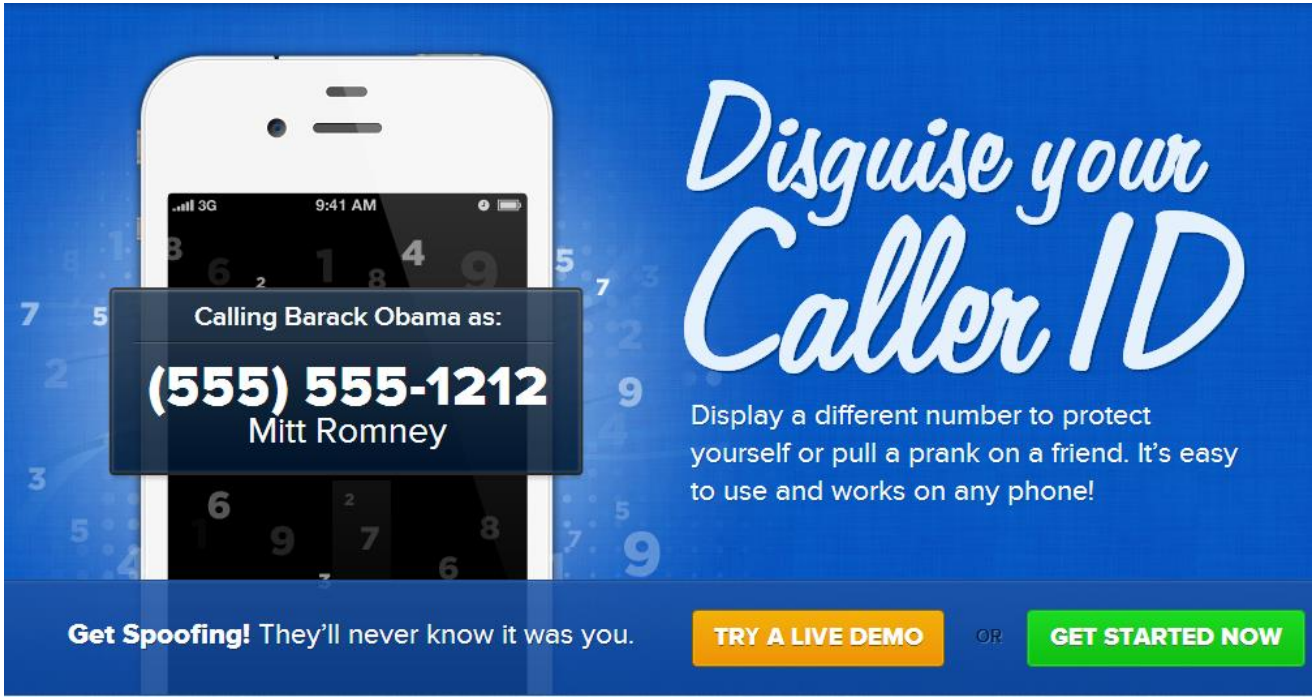
- Wybrany specyficzny problem
- iPhone 5s śledzi ruch użytkownika nawet po wyłączeniu telefonu



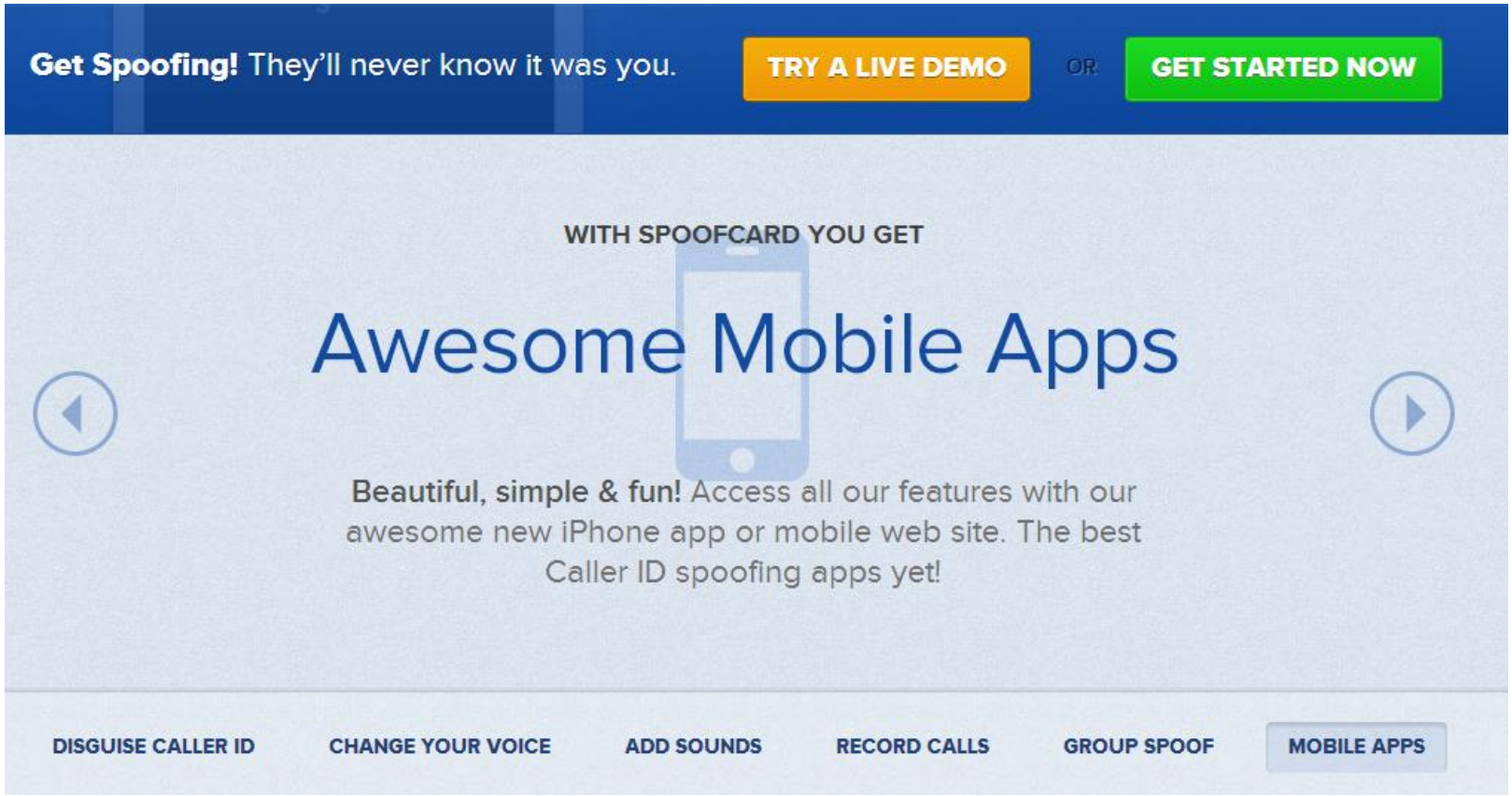
- http://sekurak.pl/iphone-5s-sledzi-twoj-ruch-nawet-po-wylaczeniu-urzadzenia/

Nowe problemy

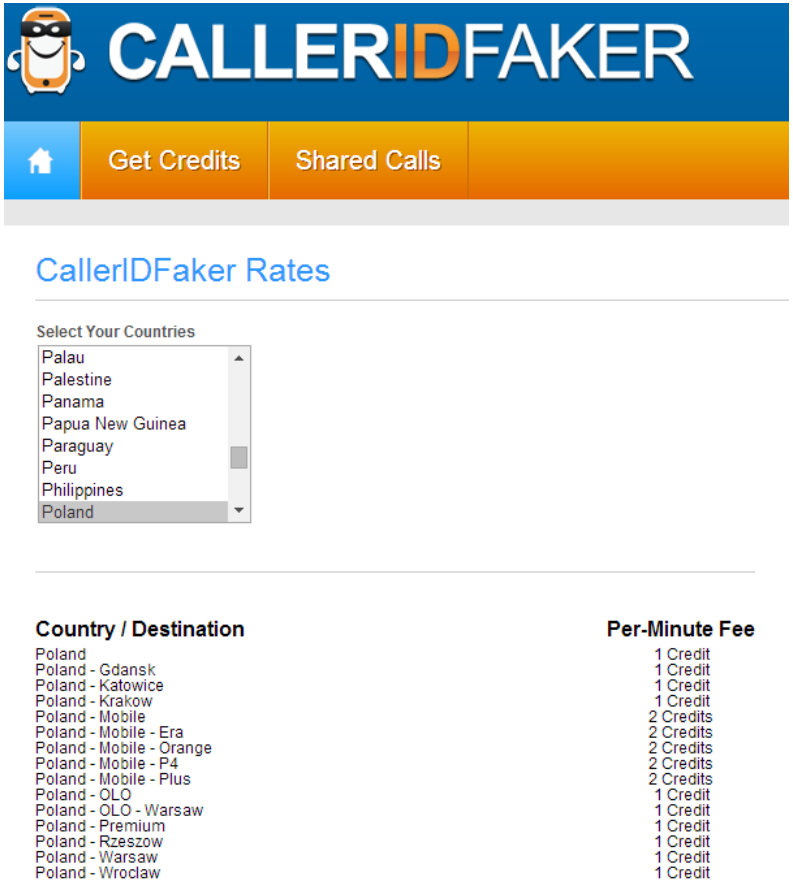
- Możliwość spoofingu numeru dzwoniącego



Nowe problemy



Nowe problemy



Nowe problemy

- Spoofing (realne przypadki)
  - Podawanie się za przedstawiciela wodociągów: zapłać albo odłączamy wodę
  - Żona podająca się za lekarza dzwoni do kochanki męża
  - Wymuszanie pieniędzy „na wnuczka”
  - …

Ochrona

- Trochę już powiedzieliśmy
- Ciekawy case:
  - Blackphone

Ochrona

- Blackphone - bazuje na androidzie, ale posiada pewne udogodnienia:
  - Częste aktualizacje bezpieczeństwa
  - Szyfrowane rozmowy P2P
  - Lepsza kontrola nad połączeniami WiFi
  - Dostępne domyślnie aplikacje – przygotowane z myślą o prywatności
  - Anonimowa możliwość wyczyszczenia telefonu

Ochrona

- Blackphone
  - W dużej mierze bazuje na gotowych aplikacjach, dostępnych na androida, jak np. Silent Phone
    - **Silent Phone** - global encrypted video and voice for your Android devices by Silent Circle.

Ochrona

- Mamy całkiem niezłą (i darmową) dokumentację
  - Podzielona na 3 obszary
    - Bezpieczeństwo urządzeń końcowych
    - Bezpieczeństwo infrastruktury mobilnej
    - Bezpieczeństwo aplikacji mobilnych

Ochrona urządzeń

- CIS Security Benchmarks (Android & iOS)
  - https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

Ochrona urządzeń

- Znajdziemy tu omówienie:
  - ustawienia szyfrowania storage,
  - ustawienia przeglądarki,
  - zarządzania aktualizacjami,
  - ustawień dotyczących Wi-Fi / Bluetooth,
  - ustawień dotyczących blokowania telefonu,
  - ustawień dotyczących poczty elektronicznej,
  - bezpiecznego zerowania sprzętu przed sprzedażą / przekazaniem do serwisu,
  - …

Ochrona infrastruktury

- Jeśli mamy w firmie kilkaset / kilka tysięcy urządzeń mobilnych – ciężko wszystkim sterować ręcznie…
- Mamy zatem do dyspozycji dokumenty umożliwiające odpowiednie przygotowanie infrastruktury:

Ochrona infrastruktury

- Mobile Security Reference Architecture (cio.gov)
  - systemy klasy MDM (Mobile Devices Management),
    - łatwe, scentralizowane zarządzenie naszą “flotą” urządzeń mobilnych,
  - systemy DLP (Data Loss Prevention) –
    - kontrolujące przepływ wrażliwych danych z/na urządzenia mobilne,
  - systemy IDS / VPN
  - …

Ochrona infrastruktury

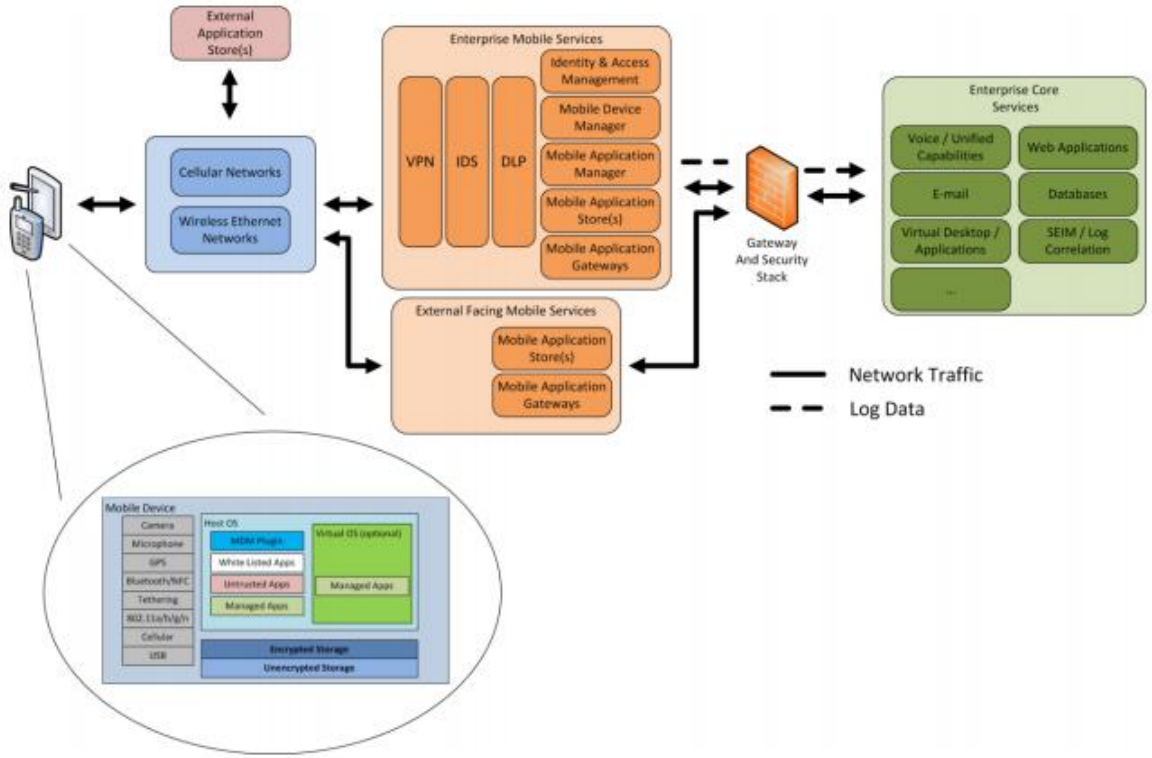


Figure 1: Mobile Security Reference Architecture

- https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf

Podejście całościowe

- Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST)
  - Informacje dotyczące zarówno urządzeń końcowych:
    - używanie niezaufanych aplikacji,
    - brak odpowiednich zabezpieczeń fizycznych na urządzeniach,
    - wykorzystanie w firmie urządzeń, których na co dzień używamy prywatnie (BYOD),
    - problemy wynikające z łączenia się do niezaufanych sieci czy problemy z kodami QR
    - …

Podejście całościowe

- … od rozwiązań klasy MDM (Mobile Device Management)
- umożliwiają zarządzanie scentralizowane:
  - dostęp do komponentów sprzętowych urządzeń (kamera, GPS, port USB, Bluetooth, itd.),
  - polityka uruchamiania aplikacji (np. tylko aplikacji z whitelisty),
  - dostęp tylko do konkretnych app stores,
  - zdalny reset / zerowanie danych urządzenia,
  - zarządzanie szyfrowaniem storage,
  - …

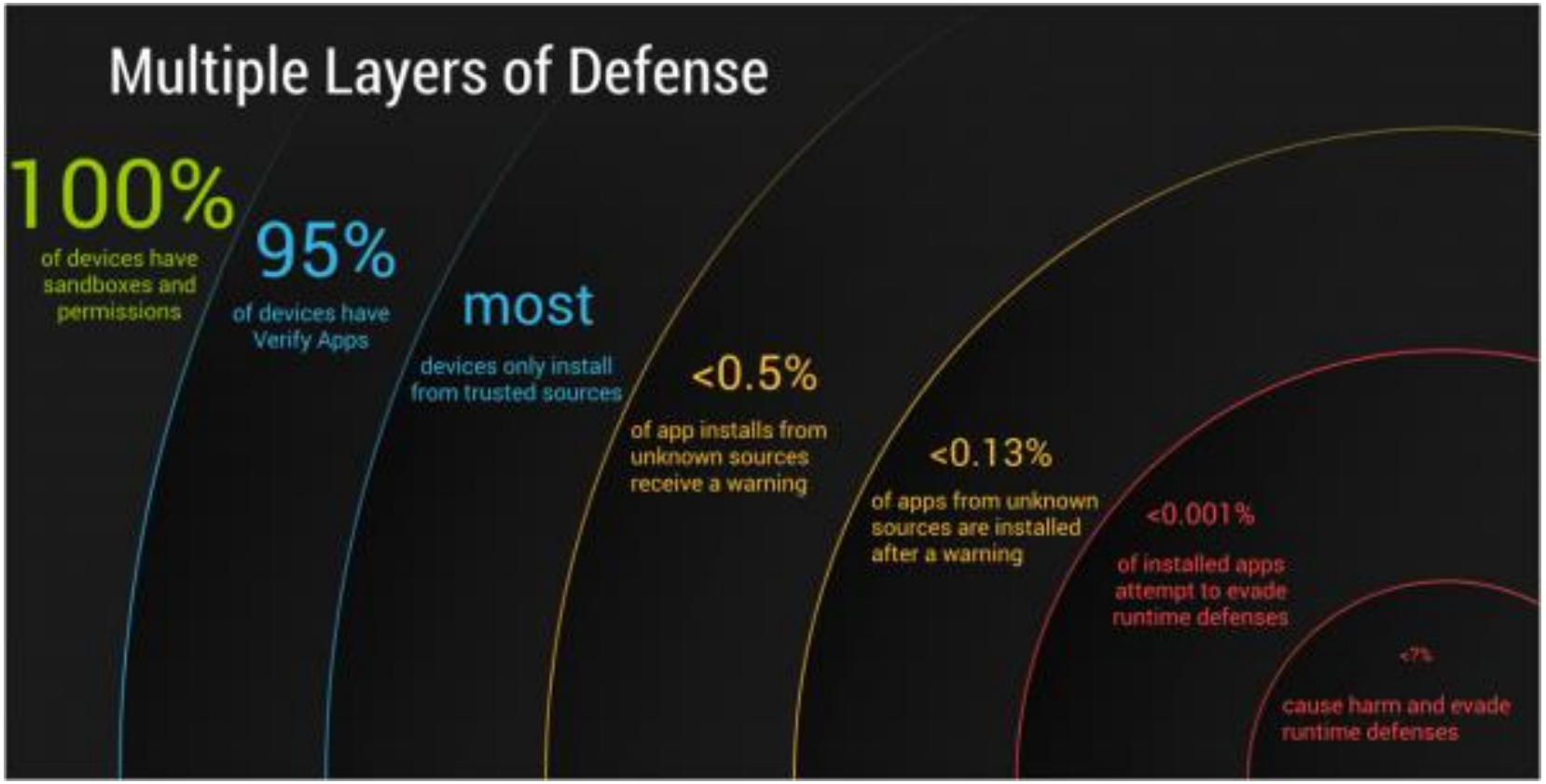
Podejście całościowe

- aż po propozycję: *Mobile Development Life Cycle*,
  - procedury całościowego zarządzania bezpieczeństwem mobilnym
    - od momentu zakupu urządzeń, przez konfigurację oraz zarządzanie zmianami aż do ich bezpiecznej utylizacji.
- http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913427

Prezentacje producentów

- W których oczywiście wszystko będzie różowo i bezpiecznie ☺

Prezentacje producentów



Prezentacje producentów

- Powyższy slajd został pożyczony z prezentacji Google:
  - https://docs.google.com/presentation/d/1YDYUrD22Xq12nKkhBfwoJBfw2Q-OReMr0BrDfHyfyPw/edit?forcehl=1&hl=en#slide=id.g1202bd8e5_044
  - Część funkcjonalności bezpieczeństwa rzeczywiście jest dostępna…ale tylko w najnowszym Androidzie (4.4)

Prezentacje producentów

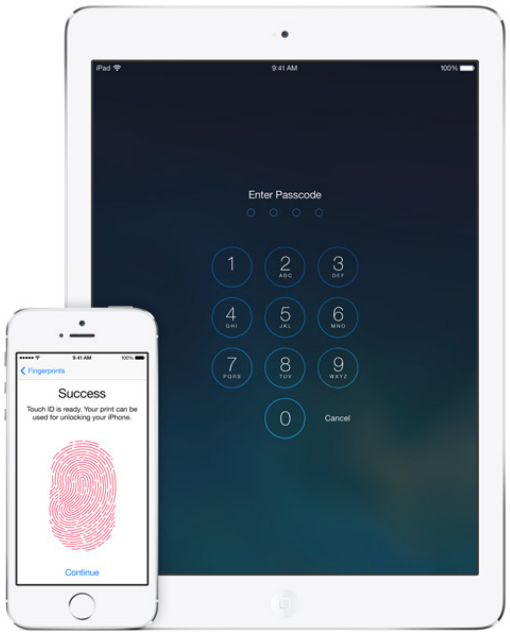
- https://www.apple.com/iphone/business/it/security.html

Secure by design.

iOS is designed with advanced security technologies that offer enterprise-grade protection for corporate data while maintaining a great user experience on all iOS devices. This comprehensive approach to security allows for end-to-end control of your devices, data, and apps and keeps users focused on being productive.

iOS Security

Learn about the features that provide advanced security for iOS devices.
Download the guide ›

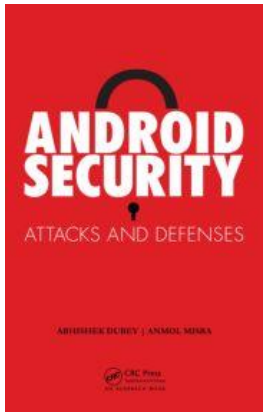


Prezentacje niezależne

- Android vs. Apple iOS Security Showdown
  - http://pittsburgh.issa.org/Archives/Android-vs-iOS-MayUpdate.pdf

Prezentacje niezależne

- Książki
  - *Android Security: Attacks and Defenses*
  - *Hacking Exposed Mobile Security Secrets & Solutions*
  - *iOS Hacker's Handbook*
  - *Android Apps Security*



Ochrona – podsumowanie - użytkownik

- Aktualizacje (!)
- Zabezpieczenie telefonu kodem / autoblokada
- Szyfrowany storage
- Możliwość zdalnego wyczyszczenia telefonu
- Realizacja kopii zapasowych
- Odpowiednio bezpieczny dostęp do poczty
- Ostrożność przy „podejrzanych” aplikacjach
- Nie wchodzenie na „podejrzane” strony www
- Zainstalowany antymalware / antywirus

Ochrona – podsumowanie - firma

- Wdrożenie polityki BYOD
- Zminimalizowanie uprawnień dla firmowych telefonów
  - Wyłączenie USB / zewnętrznych storage
  - Lista aplikacji które mogą być używane
  - …
- IDS / DLP
- Dostęp do zasobów firmy przez VPN
- Testy penetracyjne aplikacji

Dziękuję za uwagę

- Pytania?
  - http://sekurak.pl/bezpieczenstwo-systemow-mobilnych-android-ios-kilka-ciekawych-zasobow/
  - http://securitum.pl/oferta/szkolenia
  - michal.sajdak@securitum.pl