

Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

Wykład #5 – Techniki utrudniające



Plan wykładu



- Zależność między trudnością a wygodą
- Manipulacje semantyczne
- Manipulacje metadanymi
- Enkapsulowanie plików w nagłówki udawanych, innych formatów
- Kasowanie danych i unikanie ich zapisywania
- Przekierowania
- Spoofing
- Fałszowanie danych
- Stosowanie egzotycznego sprzętu i oprogramowania
- Szyfrowanie
- Ukryte partycje
- Steganografia
- Stosowanie ataków ukierunkowanych
- Stosowanie innych zabezpieczeń
- Wykorzystywanie problemów prawnych
- Unikanie inwigilacji (OPSEC)

Zależność między trudnością a wygodą

- Techniki utrudniające operacje mobile forensics, podobnie jak mechanizmy zwiększające bezpieczeństwo nie idą w parze z łatwością użycia i wygodą.



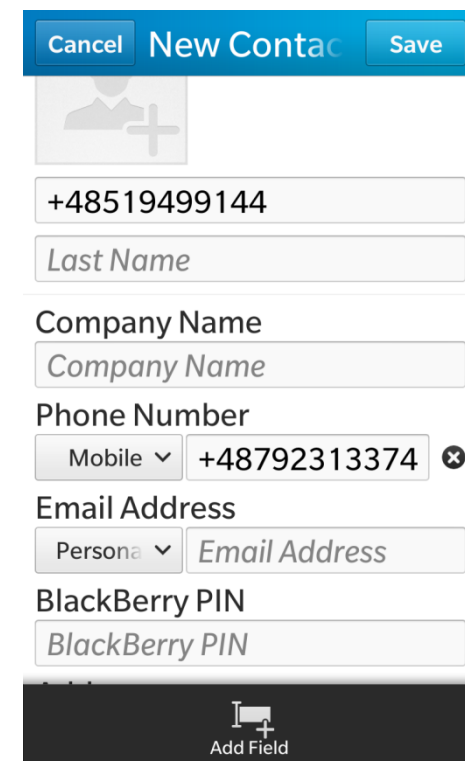
Skrajny przykład: nieposiadanie żadnego urządzenia mobilnego daje 100 % skuteczności w zabezpieczeniu się przed mobile forensics, ale uniemożliwia szybką komunikację z dowolnego miejsca.

Manipulacje semantyczne

- Stosowanie fałszywego nazewnictwa dla plików i kontaktów; np. „Jaś Niewiadomski” zamiast „Zbigniew Stefaniak” (lub „Diler Narkotyków”)
- Stosowanie mylnego nazewnictwa, np. podpisywanie kontaktów odwrotnie, Zbigniew Stefaniak podpisany jako „Jaś Niewiadomski” i odwrotnie; sytuacja może doprowadzić do podważenia wyników analizy
- Podpisywanie kontaktów jako niezapisanych, innych numerów, np. numer 794314372 podpisany jako „+48800500500”
- Niezapisywanie numerów w książce i regularne kasowanie historii wykonanych połączeń (zostają billingi + odczyt fizyczny telefonu)
- Stosowanie kodów słownych

Rozwiązania:

- Świadomość, skupienie, uwaga, brak pośpiechu przy akwizycji i analizie danych
- Analiza spójności z różnych stron (np. czy dane z telefonu nie są sprzeczne z danymi z karty SIM/danymi uzyskanymi od operatora)



A screenshot of a mobile application interface for creating a new contact. At the top, there is a blue header bar with three buttons: 'Cancel', 'New Contact', and 'Save'. Below the header is a grey square icon with a white person silhouette and a plus sign. The form consists of several input fields: a phone number field containing '+48519499144', a 'Last Name' field, a 'Company Name' field, a 'Phone Number' field with a dropdown menu set to 'Mobile' and the number '+48792313374' (with a close icon), an 'Email Address' field with a dropdown menu set to 'Personal' and the text 'Email Address', and a 'BlackBerry PIN' field. At the bottom, there is a dark grey bar with an 'Add Field' button featuring a plus icon.

Manipulacje metadanymi

- Fałszowanie czasów dostępu do plików poprzez:
 - Ustawianie nieprawidłowej daty systemowej
 - Używanie funkcji systemowych, które to wspierają
 - Binarną edycję systemu plików (możliwe głównie w przypadku kart SD)
- Programowy spoofing adresów IP, MAC, IMEI (IMEI często jest też zmieniany w kradzionych telefonach)
- Fałszowanie danych na karcie SIM
- Fałszowanie zawartości SMS-ów
- Stosowanie mylnych nazw i rozszerzeń plików (np. trzymanie zaszyfrowanej bazy haseł w pliku wyglądającym na plik tymczasowy niepowiązany z ciekawymi danymi (np. Desktop.ini))
- Fałszowanie logów, plików tymczasowych systemu etc.
- Stosowanie zmodyfikowanego oprogramowania:
 - Używającego metadanych w formacie niezgodnym ze specyfikacją
 - Ukrywającego procesy i pliki (np. zmodyfikowany Android, zmodyfikowany firmware pamięci flash)

Ciekawostka Symbiana

- Urządzenia z Symbianem jako nieliczne posiadają oddzielną baterię podtrzymującą ustawienie zegara systemowego (data, czas)
- W przypadku jej rozładowania się przy kolejnym uruchomieniu telefon z Symbianem poprosi o podanie daty, domyślnie sugerując 01.01.1970 r (początek ery Uniksa)
- W takim przypadku **należy** postąpić zgodnie z sugestią, ustalając datę z dalekiej przeszłości
- Symbian automatycznie kasuje (nadpisanie bitów jedynką) dane historyczne starsze niż miesiąc; jeśli więc w chwili uruchomienia podamy mu datę bieżącą, stracimy dane historyczne (np. historia połączeń)
- Kasowanie nie obejmuje danych z „przyszłości” (czyli czasu użytkowania telefonu z punktu widzenia daty 01.01.1970)

Enkapsulowanie plików w nagłówki udawanych, innych formatów

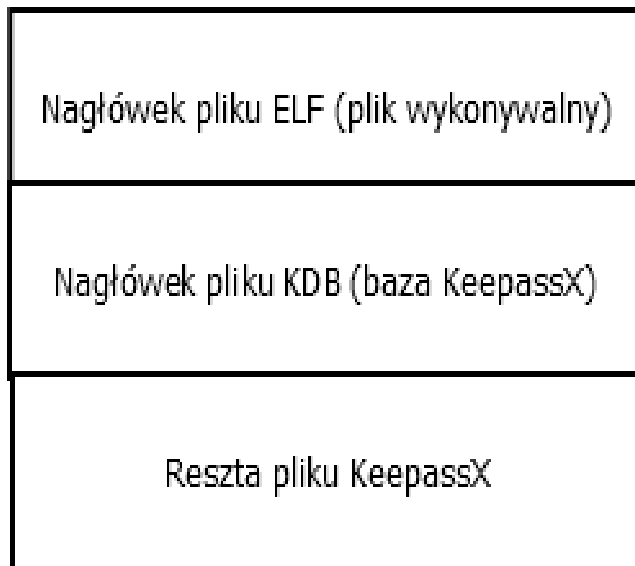
- Technika polega na wykorzystaniu faktu, że przy dużej i stale rosnącej ilości danych przechowywanych na urządzeniach mobilnych niemożliwa jest manualna inspekcja wszystkich plików
- W celu identyfikacji typów danych stosowane są narzędzia rozpoznające pliki po nazwach (w tym rozszerzeniach) oraz indywidualnych „sygnaturach” (unikalnych dla danego formatu ciągach bajtów) [KESSLER]
- Wykorzystanie faktu, iż narzędzie identyfikujące zadowoli się pierwszym przypasowaniem sygnatury
- Umieszczenie pliku zastąpionego fałszywym nagłówkiem w miejscu, które nie wzbudzi podejrzeń

Enkapsulowanie plików w nagłówki udawanych, innych formatów

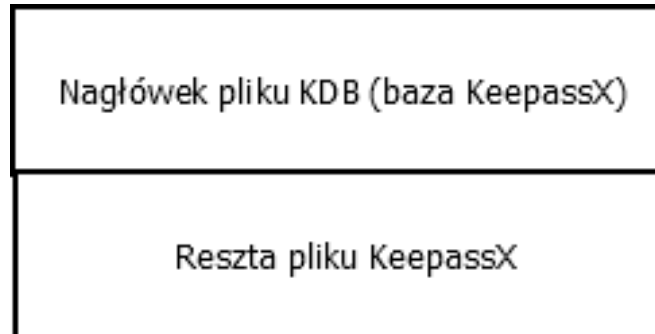
Przykład:

plik KDB (zaszyfrowana baza programu KeepassX) zaenkapsulowana w nagłówek ELF (plik wykonywalny) w katalogu z komendami systemowymi, zastępująca niekrytyczną komendę systemową (np. /bin/wipe)

Plik przechowywany na dysku:



Plik przygotowywany w locie do użytku (po zignorowaniu stałej liczby bajtów z przodu):



Efekt działania programu identyfikującego typy plików: rozpoznanie tylko i wyłącznie plików programów w katalogu z programami (/bin) – żadnej anomalii ani pliku KDB.

Oczywiście anomalią jest tutaj fakt, że komenda /bin/wipe się nie wykonuje (ale tego już nikt nie sprawdzi)

Kasowanie danych

- Zwykłe usuwanie jako usunięcie samych metadanych z systemu plików (oznaczenie zajmowanego obszaru jako wolny, 'zapomnienie' o pliku) – dane zazwyczaj łatwe do odzyskania
- Nadpisywanie nośnika
- Stosowanie wbudowanych funkcji typu security-wipe
- Niszczenie nośników (w przypadku zniszczenia samych urządzeń mobilnych/gniazd dane z nośników zazwyczaj łatwo da się odzyskać)



Unikanie zapisywania danych



[2]

- Niezapisywanie numerów w książce i regularne kasowanie historii wykonanych połączeń
- Stosowanie wszelkich wersji trybu „incognito”, np. w przeglądarkach internetowych (niezapisywanie historii, cookies, e-tagów)
- Wyłączanie/niekorzystanie z urządzeń i usług zbierających dodatkowe dane, np.:
 - Usługi lokalizacyjne i GPS
 - Bluetooth
 - Wi-Fi
 - Akcelerometr
 - Zapisywanie wszelkiej maści logów
 - Dane diagnostyczne

Unikanie zapisywania danych - przykład #1



[2]

- Umieszczanie wiadomości tekstem w obrazku
- Umieszczenie obrazka na serwerze www
- Przesłanie linka zamiast tekstu
- Skasowanie/nadpisanie obrazka po otrzymaniu wiadomości
- Umieszczenie serwera za cloudflare reverse proxy

Unikanie zapisywania danych - przykład #2



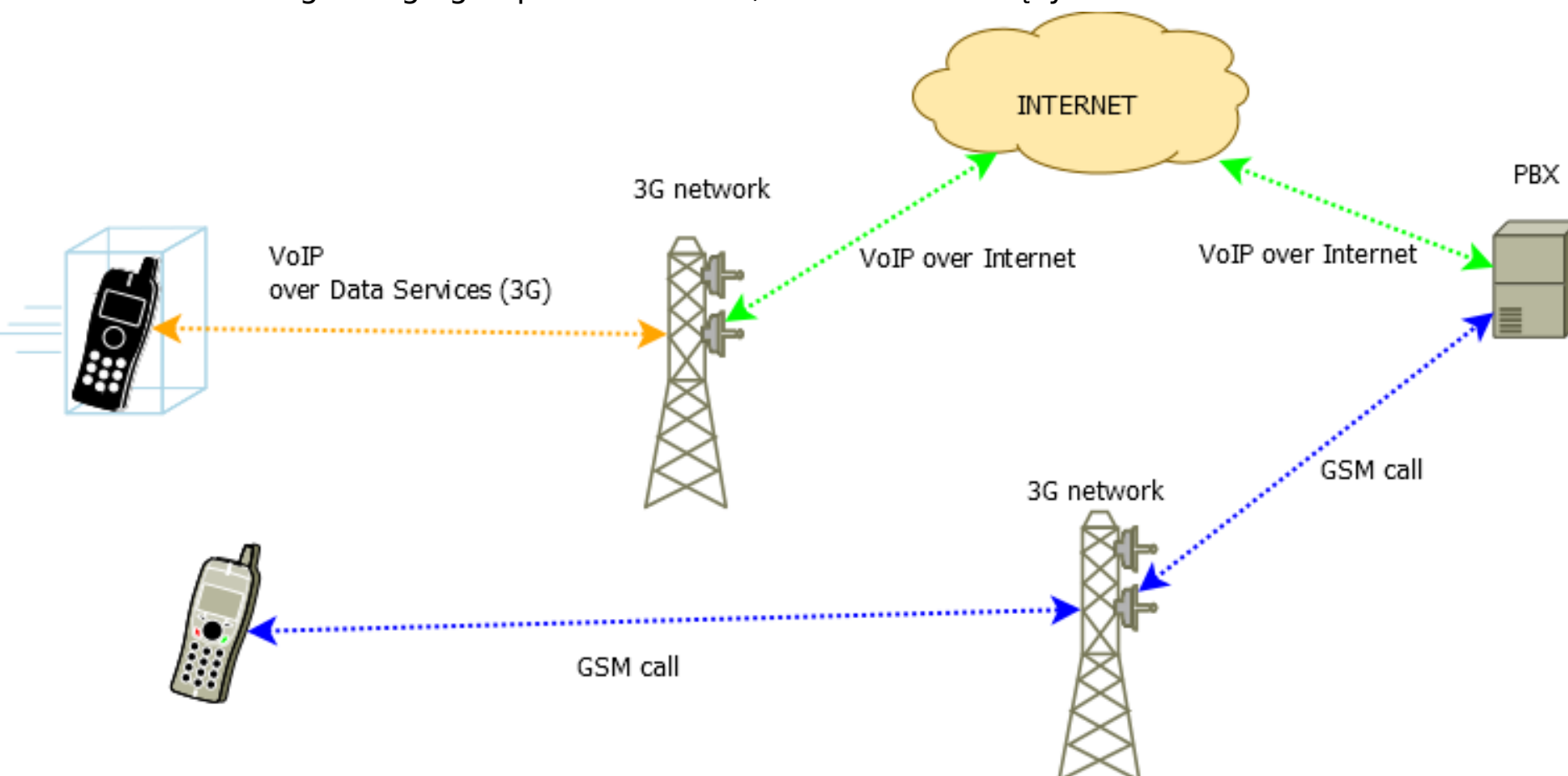
[2]

- Skoro nieodebrane połączenia nie są zapisywane w billingu, można wykorzystać dwa telefony z wyłączoną historią połączeń do implementacji niewidzialnej komunikacji z pomocą alfabetu Morse'a □ (gdyby historia zapisu została włączona, dałoby się odtworzyć treść na podstawie dokładnych czasów)

Przekierowania - VoIP

Bramki VoIP - scenariusz #1

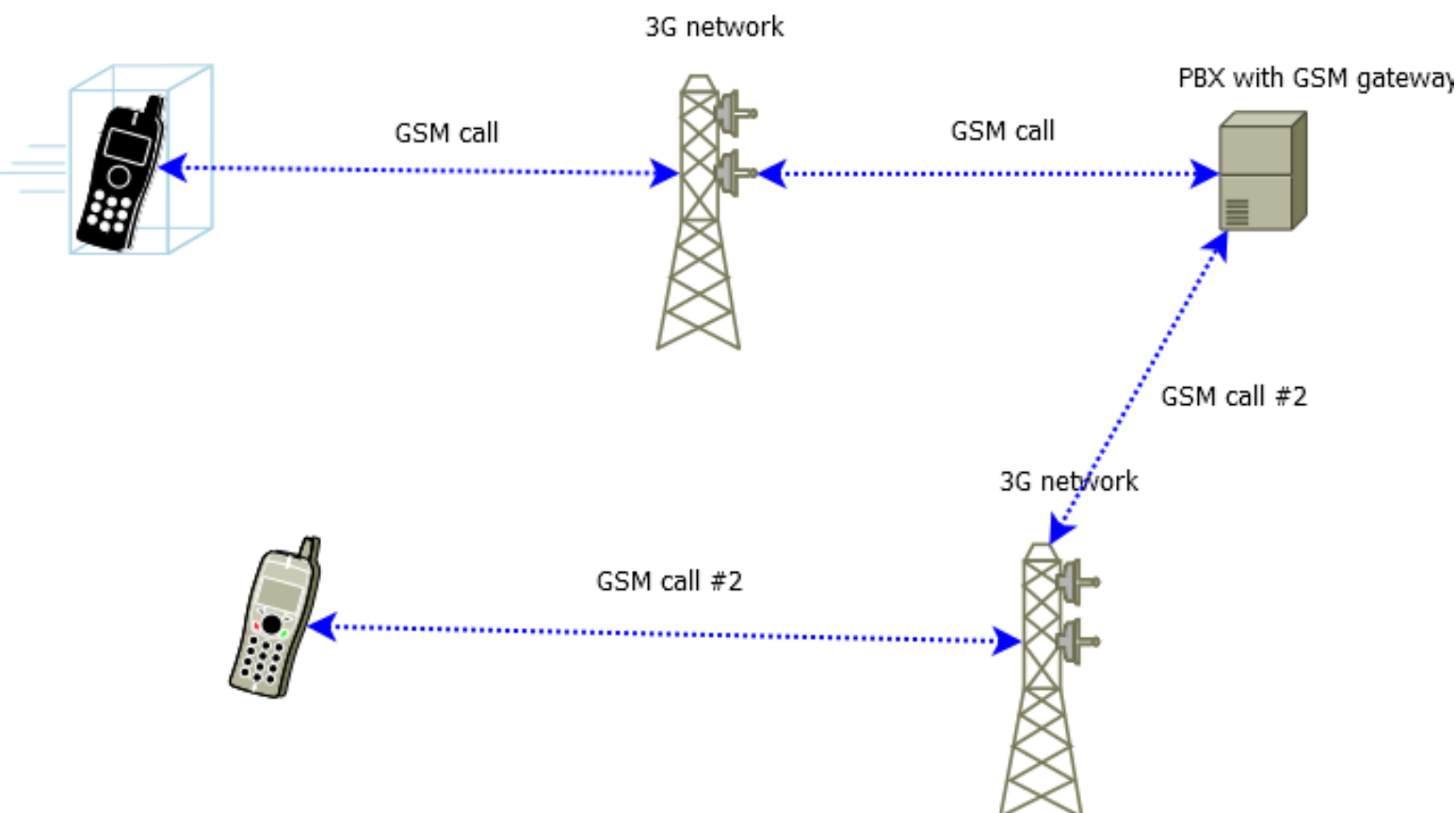
- Zamiast zwykłego połączenia głosowego po GSM, użytkownik **A** komunikuje się z użyciem VoIP z serwerem PBX (np. Asterisk)
- PBX posiada połączenie do publicznej sieci telefonicznej (PSTN), przez którą wykonuje połączenie z innym numerem GSM podanym przez użytkownika tonowo poprzez VoIP
- W standardowym bilingu operatora GSM po stronie dzwoniącego widać jedynie transfer danych
- W bilingu drugiego operatora widać, że numer należący do PBX zadzwonił na numer komórki **B**



Przekierowania - bramka GSM

Bramki VoIP - scenariusz #2

- Wykonywane jest połączenie GSM na numer publiczny podpięty do PBX
- Po nawiązaniu połączenia z PBX, tonowo wybierany jest numer, na który PBX dzwoni z wykorzystaniem bramki VoIP i zestawia połączenia
- W standardowym bilingu operatora GSM użytkownika **A** widać jedynie, że wielokrotnie dzwonił na numer bramki
- W bilingu drugiego operatora widać, że numer należący do PBX zadzwonił na numer komórki **B**



Przekierowania - manipulacja lokalnym rozwiązywaniem nazw

```
/system/etc/hosts  
127.0.0.1      localhost  
111.111.111.111  google.com
```

Zakładając, że IP 111.111.111.111 jest adresem, z którym komunikację ktoś chce ukryć (przynajmniej dla logów takich jak historia przeglądania, ciasteczka itd.), zastosowanie takiej konfiguracji spowoduje, że zapytania kierowane do domeny google.com trafią do tego właśnie adresu IP, logi zaś będą zawierały *google.com*

Plik ten często jest modyfikowany przez złośliwe oprogramowanie (np. fałszywe strony banków itd.).

Spoofing

Możliwe fałszownie adresów źródłowych:

- MAC
- IP
- IMEI
- SMS [SMS SPOOFING]

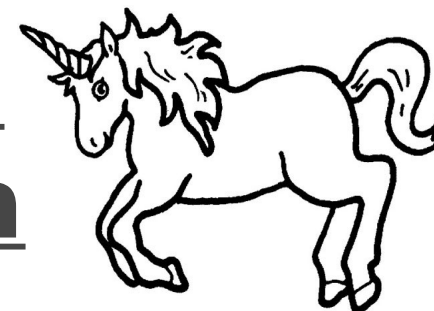
Fałszowanie (preparowanie) danych

Dane elektroniczne można stosunkowo łatwo sfałszować nie pozostawiając śladów

Przykład: SMS

- Możliwe jest edytowanie treści otrzymanych SMS-ów (zarówno w pamięci telefonu – np. sqlite) jak i na karcie SIM
- W billingu operatora jest jedynie informacja, kto, kiedy i do kogo wysłał SMS-a (operator nie przechowuje treści)
- Aby udowodnić sfałszowanie SMS-ów, należy poddać inspekcji obydwa urządzenia (nadawcy i odbiorcy)
- Często spotykany jest spoofing numeru źródłowego SMS

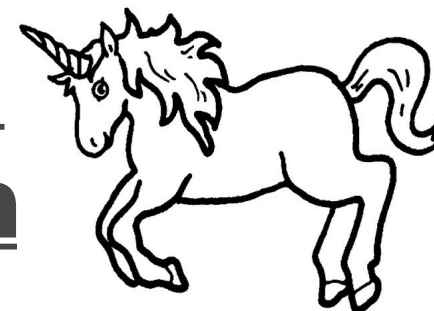
Stosowanie egzotycznego sprzętu i oprogramowania



[3]

- Stosowanie modeli niewspieranych przez narzędzia do mobile forensics
- Stosowanie modeli pozbawionych kluczowych dla mobile forensics funkcji
- Np.:
 - Wyjątkowo stare modele
 - Wyjątkowo kłopotliwe modele (np. Nokia 100 – nie zapisuje dat i godzin)
 - Najnowsze modele z dobrze skonfigurowanymi ustawieniami bezpieczeństwa (np. iOS 10.2.1, Android Nougat 7.0)
 - Mało popularne modele
 - Najnowsze mało popularne modele (Windows Phone :))

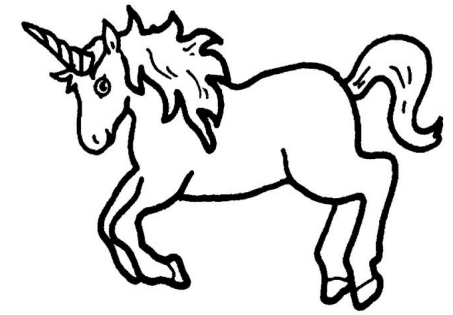
Stosowanie egzotycznego sprzętu i oprogramowania



[3]

- W tak ekstremalnej sytuacji dokonuje się:
 - ręcznego przejrzania zawartości urządzenia mobilnego z wykonaniem zdjęć ekranu
 - chip-off forensics
 - ewentualnego oczekiwania na rozpracowanie urządzenia

Stosowanie egzotycznego sprzętu i oprogramowania - mało popularne modele



[3]

- Lista do ustalenia na podstawie wyników sprzedaży
- Słabą popularność można również szacować sugerując się własnym gustem



Steganografia



- Proces ukrywania danych w większej ilości danych
- Kompletna dowolność w kwestii nośnika, np.:
 - Dla sieci
 - Sekwencje pakietów (np. port knocking)
 - Opcjonalne pola (IP options)
 - Wyglądające na losowe nagłówki HTTP (np. ciastka Session Id)
 - Itd,
 - Dla plików
 - Najmłodsze bity bajtów plików multimedialnych (nie zaburzają działania medium przez co nie wzbudzają podejrzeń)
 - Nieużywane/opcjonalne nagłówki plików
 - Nazwy i inne atrybuty plików
 - Podzbiory znaków w plikach o zawartości wyglądającej na losową (np. pliki z hashami, pliki tymczasowe)
 - Sekwencje białych znaków w plikach tekstowych
 - Slack space
 - itd.
- Steganografię można z powodzeniem stosować do przechowywania dowolnych danych, ograniczeniem jest rozmiar wynikowy wynikający z narzutu

Steganografia



- Wykrywanie treści ukrytej steganograficznie poprzez analizę potencjalnego nośnika (np. analiza LSB)
- Wykrywanie anomalii logicznych (np. setki wysłanych żądań HTTP, wśród których jedyną różnicą jest jedno ciastko, pliki graficzne, które nie pasują do profilu osobowościowego użytkownika)
- Dogłębna analiza zainstalowanych aplikacji (jeśli ktoś chowa dane, używa jakiegoś programu do ich wyciągania i ponownego ukrywania)

Ukryte/szyfrowane partycje

(kontroler flash)

Flash ASIC-based Crypto...

- 1) Flash controllers do wear-leveling
- 2) Encryption key *may* be held in the ASIC, initially set during ASIC programming
- 3) LUNs (drives) can be hidden, locked w/ password AND encrypted
- 4) Flash drives have more space than you know

This is a forensics **NIGHTMARE**

[XABEAN]

Stosowanie innych zabezpieczeń

- Blokada ekranu
- Kody PIN
- Szyfrowanie (FDE, EFS)
- Dodatkowe warstwy kryptograficzne (PGP, Truecrypt)
- Zmodyfikowane oprogramowanie, które w przypadku podania rzekomo poprawnego hasła (które użytkownik dobrowolnie wyjawia) dokona security wipe
- Szyfrowanie SMS-ów
- Stosowanie dwóch handsetów niewłączanych jednocześnie (korelacja danych lokalizacyjnych)
- „Przyjazne trojany”

Stosowanie ataków ukierunkowanych



- Podobnie jak każdy inny rodzaj oprogramowania, narzędzia do mobile forensics mogą być rozpoznane behawioralnie (i odróżnione w ten sposób od sytuacji normalnego użytkownika)
- Otwiera to drogę do modyfikowania oprogramowania w telefonach w taki sposób, by rozpoznawało użycie narzędzia do mobile forensics i podkładało mu fałszywe dane (znane są takie przypadki) **[ANDROID ANTI FORENSIC POC]** <- to tylko jeden przykład

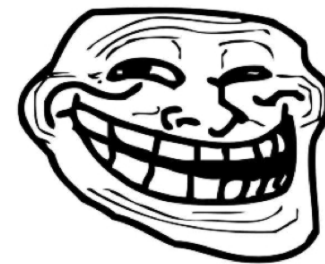
W podanym przykładzie za wzorzec behawioralny posłużyła sekwencja:

1. Połączenie po USB z włączonym USB debuggingiem
2. Przesłanie do urządzenia z Androidem aplikacji (exploita/agenta)

Wnioski

- Manipulacja taka jest **znacznie trudniejsza** do osiągnięcia w przypadku ekstrakcji fizycznej (modyfikacje należałoby umieścić w na poziomie firmware'u kontrolera pamięci NAND, zainstalować na systemie zmodyfikowaną wersję programu recovery lub zmodyfikować firmware odpowiadający za tryb fastboot)
- Potwierdza to sens dokonywania akwizycji więcej niż jednym narzędziem i więcej niż jednym sposobem, aby porównać wyniki i wykryć ewentualne anomalie

Wykorzystywanie problemów prawnych



- Przechowywanie na urządzeniu poufnych danych służbowych
- Przechowywanie danych w lokalizacjach zdalnych będących poza jurysdykcją służb
- Upozorowanie włamania na swoje urządzenie (lub wręcz świadome i celowe zainfekowanie go malware), by podważyć założenie, że obciążające aktywności akcje zostały wykonane przez właściciela
- Zgodnie z polskim prawem można odmówić podania PIN-u, hasła itd., niezależnie czy dotyczy to nośnika lokalnego, czy też lokalizacji zdalnej

Odnośniki

Lista odnośników pod adresem:

https://github.com/ewilded/mobile/W5_URLs.txt