

Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

Wykład #1 – Definicja, klasyfikacja i rola urządzeń mobilnych



Prowadzący

mgr inż. Julian Horoszkiewicz
IT Security Consultant
OSCP, eMAPT, OSWP

<https://www.linkedin.com/in/julian-horoszkiewicz-67075364/>
<https://github.com/ewilded/mobile>



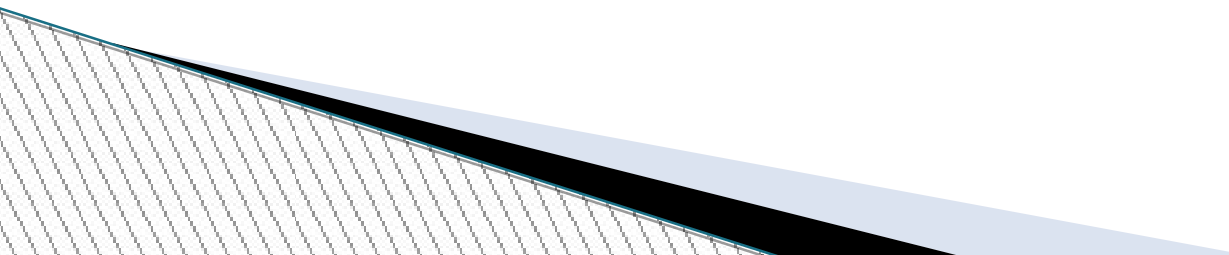
Zasady zaliczenia wykładu

- Ocena końcowa jest oceną z testu w formie pisemnej
- 25 pytań zamkniętych jednokrotnego wyboru
- Pytania bardziej zorientowane na myślenie oraz rozumienie zagadnień, niż na detale technologiczne

Definicja

- Za urządzenia mobilne powszechnie uważane są wszystkie przenośne (o wadze do ok. 1 kg) urządzenia przetwarzające i przechowujące dane
- Z punktu widzenia sieci mobilnych za urządzenie mobilne uważa się takie, które posiada numer IMEI (International Mobile Equipment Number) (wszystkie modemy 3G; nie wszystkie tablety)

Obszar zastosowań

- Życie codzienne
 - Komunikacja
 - Usługi, przemysł, handel, usługi, logistyka
 - Edukacja
 - Sport
 - Obronność
- 

Charakterystyka

- Niewielki rozmiar
- Mobilność
- Osobistość (użytkowanie zazwyczaj przez tylko jedną osobę)
- Bardzo duża różnorodność
 - Sprzętu
 - Oprogramowania
- Bogactwo sensorów (czujniki ruchu, żyroskop, temperatury, światła, barometr, magnetometr, mikrofon, pole magnetyczne (tzw. “proximity”), kamera, podczerwień)
- Trendy
 - Przejmowanie roli klasycznych komputerów osobistych (smartfony, tablety)
 - Nieustannie rosnące
 - Możliwości
 - Popularność
 - Mnogość zastosowań

Podział funkcjonalny

- Wearable Computer (Smart watches, Fit opaski)
- Tablety
- Telefony komórkowe
- Karty inteligentne (Smart Cards)
- Pagery
- Przenośne terminale płatnicze
- E-ink readers
- Kamery
- Modemy 3G
- Nośniki pamięci (karty SD, nośniki pendrive)
- Przenośne konsole do gry
- Beacons [BEACON]
- Dyktafony
- RaspberryPI i pochodne

Podział funkcjonalny c.d.



[MOSQUITO]

- Drony [SMALLEST DRONE]
- Chipy RFID
- Małe roboty, nanoroboty [NANOROBOTS]
- Implanty? :) [Body implants]

Już niefunkcjonujące, wchłonięte przez smartfony:

- PDA - Personal Digital Assistant
- Nawigacje (PND - Personal Navigation Device)
- Mobile Internet Device (MID)
- UMPC - Ultra Mobile PC
- EDA (Enterprise Digital Assistant)

Handheld Game Consoles

- Przenośne gry, historią sięgające 1976 – *Auto Race* (zbudowany na bazie kalkulatora) [13]
- 1997 – *Game Dot Com* (Tiger Electronics) – pierwsza gra z wyświetlaczem dotykowym
- 2001 – *Game Park* (MP3, DivX, e-book reader, karty SmartMedia)
- 2003 – N-Gage (Nokia) – hybryda telefonu, PDA, radia, odtwarzacza muzyki i konsoli do gier
- 2004 – Tapwave Zodiac – hybryda PDA z m.in. dostępem do Internetu
- 2008 – Pandora (konsola/UMPC/PDA) z Linuksem
- 2011 – Sony Ericsson Xperia Play – konsola-smartfon z Androidem 2.3
- 2013 – Nvidia Shield (Android 4.2)
- 2017 – PlayStation Vita (OS oparty o NetBSD)



Auto Race [7]



Nokia N-Gage [6]

PDA-s (Personal Data Assistant)

Docelowe funkcje: notatnik, organizer, kalendarz
Powszechnie spotykane: Wi-Fi, e-mail,
synchronizacja, obsługa nośników zewnętrznych,
touchscreen



[THE PALM TX]

- 1984 - Psion Organizer, 8 bitowy procesor 0.9 Mhz, 4 KB ROM, 2 KB RAM, bateria wytrzymywała kilka miesięcy
- 1991 - Psion Series 3, procesor tekstu, baza danych, modem
- 1992 - powstanie terminu PDA, Apple Newton [PDA NEWTON]
- 1992 - funkcjonalność PDA przechodzi do telefonów komórkowych [11]
- 1996 - początek serii Palm Computing (Palm OS)
- 2006 - urządzenia Palm Computing stają się smartfonami



[PSION ORGANIZER]

PNA/PND (Personal Navigation Assistant/Device)

Urządzenie oferujące wspomaganie w nawigacji z wykorzystaniem usług lokalizacyjnych



[TOMTOM]

- Popularność powstała głównie dzięki nawigacjom samochodowym
- Często spotykaną kombinacją oprogramowania jest
 - Windows CE/Embedded Linux jako OS
 - TomTom Navigator, Navit [NAVIT], I-GO 2006, Netropa IntelliNav iGuidance, Destinator jako program do nawigacji
- Często wykorzystywane przez użytkowników do uruchomienia innych aplikacji, niż nawigacyjne
- Od kilku lat (2007) wchłaniane przez smartfony i tablety [SMARTGPS]
- Większość tych urządzeń przechowuje dane o przejechanych trasach (dokładna lokalizacja i czas)
- Często wyposażone w wejście USB i slot kart SD

[Garmin Foretrex 401 Waterproof Hiking GPS]



MID (Mobile Internet Device)

- Urządzenie mobilne z dostępem do Internetu, zazwyczaj z ekranem większym niż 5 cali
- Wszystkie są wyposażone w Wi-Fi
- Najczęściej używane OS-y to Windows CE, Android, Linux (Ubuntu Mobile, MeeGo, LiMo, Moblin)
- Najczęściej występujące architektury procesora: ARM, x86 (Intel atom)
- Często określane mianem mini-tabletów



[NOKIA N810]

UMPC (Ultra Mobile PC)

- Komputery o wielkości i interfejsie typowym dla tabletów (ekran dotykowy, opcjonalnie klawiatura)
- Praktycznie wszystkie modele wyposażone w procesory x86
- Z uwagi na architekturę należy zaliczyć je do komputerów PC

Wearable computer

Smartwatches [SMARTWATCHES]

- Galaxy Gear
- Sony Smartwatch 2
- Cookoo
- Moto 360
- Google Smartwatch
- Microsoft Smartwatch
- iWatch



[GALAXY GEAR]

Funkcje:

- łączność Bluetooth i NFC z telefonem/tabletem
- Integracja ze smartfonem
- Fit opaski - monitorowanie aktywności fizycznej (czujnik tętna, krokomierz, spalane kalorie, sen)

Inne:

Okulary google [GOOGLE GLASSES]



[Garmin Vivofit]

Pagery

- Bezprzewodowe, mobilne urządzenia telekomunikacyjne
- Historią sięgają lat 50 XX wieku
- Wykorzystują różne protokoły radiowe na niskich częstotliwościach (400 MHz, 900 Mhz)
- Rosnąca popularność załamała się w latach 90 z powodu rozpowszechnienia się technologii GSM
- Obecnie wykorzystywane profesjonalnie w:
 - Restauracjach (wygoda)
 - Szpitalach (bezpieczeństwo, niezawodność)
 - Służbach ratunkowych (bezpieczeństwo, niezawodność)
- Większość pagerów potrafi jedynie otrzymywać wiadomości (jednokierunkowa komunikacja uniemożliwia namierzanie lokalizacji, ale wymusza rozgłoszenie wiadomości do wszystkich stacji bazowych)
- Wiele dzisiejszych pagerów wspiera technologie pozwalające je zintegrować z innymi urządzeniami mobilnymi (Wi-Fi, GSM, etc.)

[TELETRIM]



Tablety

- Przenośny komputer z ekranem dotykowym
- 1989 – GridPad (uznawany za pierwszy współczesny tablet) – pod kontrolą MS DOS [15] □
- Od połowy lat 90 można spotkać hybrydy z podłączanymi klawiaturami (np. Asus Transformer)
- Gwałtowny wzrost popularności od roku 2010
- Architektura, oprogramowanie i wbudowane sensory nie odbiegają od tych obecnych w smartfonach
- Większość tabletów nie posiada modułu GSM (ale posiada modem 3G) [SONY TABLET]
- Obecnie najpopularniejsze:
 - iPad Mini, iPad Air
 - LG G Pad
 - Kindle Fire
 - Google Nexus 7
 - Sony Xperia Z2



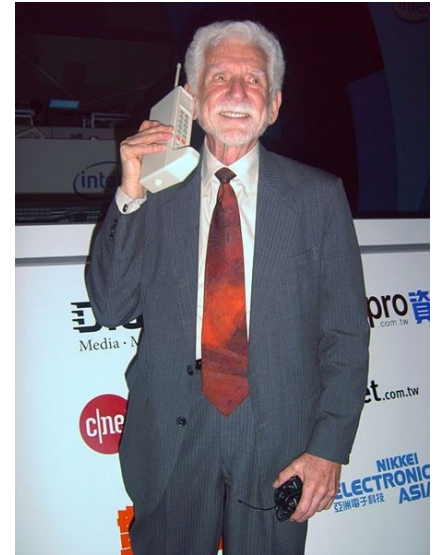
GRiDPad, 1989
[8]



[ASUS TRANSFORMER]

Telefony komórkowe

- Przenośne telefony wykorzystujące bezprzewodową sieć komórkową
- 1G – technologia analogowa (1979 – pierwsza komercyjna sieć)
- Wraz z 2G (GSM - 1991) wymagana jest karta SIM
- Funkcja Short Message Service (SMS) od 1992 [10]
- 1992 – IBM, pierwszy telefon z funkcją PDA [11]
- 1994 – Simon Personal Computer (z dodatkowymi funkcjami, uznawany za pierwszy smartfon)
- 1996 – Nokia 9000 z GEOS v.3.0
- 1998 – początek ery multimediiów w telefonach komórkowych [10]
- 2000 – pierwsze urządzenie nazwane smartfonem (Sony Ericsson, [12])
- 2002 – pierwszy smartfon z Windows Mobile
- 2007 – pierwszy iPhone
- 2008 – pierwszy telefon z Androidem



Dr Martin Cooper,
Motorola, pierwszy telefon
komórkowy, 1973 [2]



Nokia 9000 z GEOS v.3.0, [4]

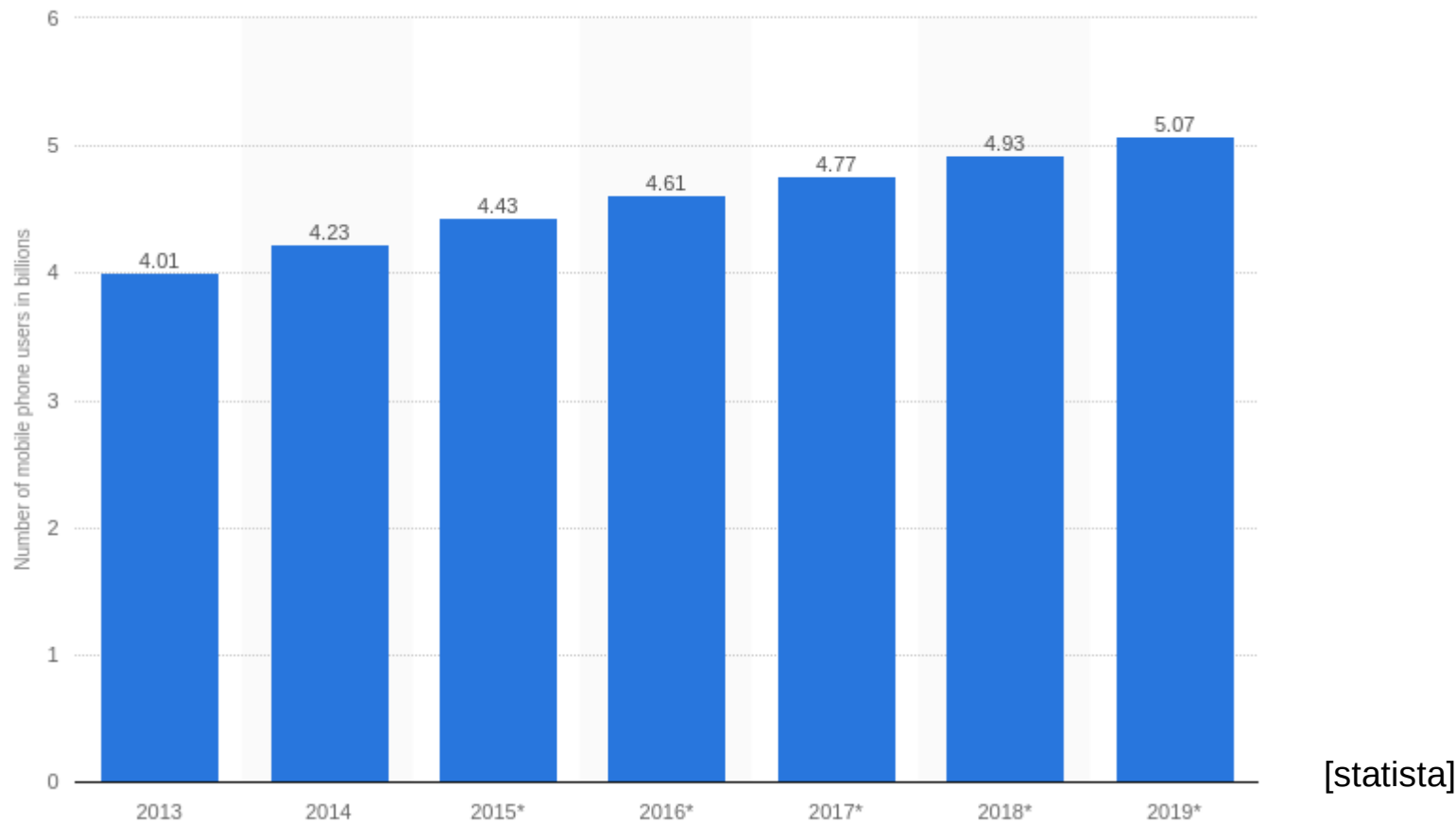
Skala trendu

(dane tylko dla telefonów komórkowych)

- Z końcem roku 2012 używanych było 6,8 mld. urządzeń mobilnych
- Z końcem roku 2013 liczba ta wzrosła o ok. 500 mln. (ok 7,3 mld.), przekraczając liczebność populacji na Ziemi [2][3][5]
- Ponad 1.9 mld. Używanych w 2014 urządzeń mobilnych to smartfony (wzrost ok **50 % w stosunku do 2012**) [6][7]

Skala trendu (dane tylko dla telefonów komórkowych)

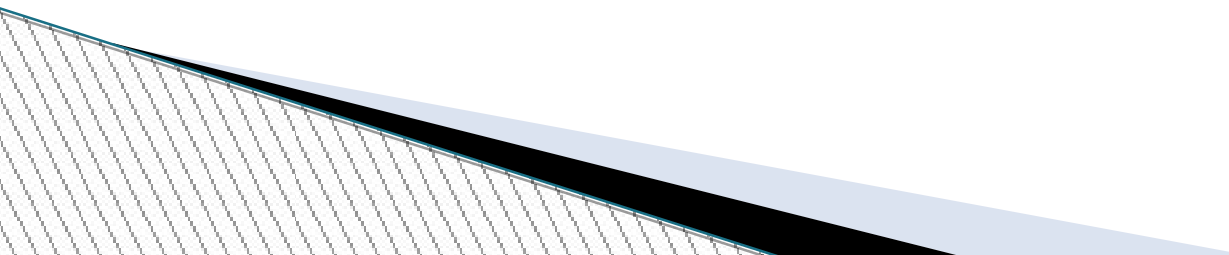
Szacowana ilość użytkowników telefonów komórkowych w miliardach



Skala trendu

(dane tylko dla telefonów komórkowych)

Ciekawostki o zwyczajach użytkowników [4]:

- 68 % podczas snu trzyma telefon przy łóżku
 - 37 % sprawdza swój telefon co pół godziny lub częściej
 - 34 % przyznaje, że nie może funkcjonować bez telefonu komórkowego
 - 32 % przyznaje, że preferuje komunikację za pośrednictwem SMS-ów
 - 29 % przyznaje, że telefon jest pierwszą i ostatnią rzeczą, jaką widzi każdego dnia
- 

Obecne zastosowania

- Przeglądanie Internetu
- Serwisy społecznościowe
- News
- Robienie zdjęć
- Słuchanie muzyki
- Gry
- Nawigacja z GPS
- Wideo czat
- Zakupy online
- Bankowość i płatności
- Połączenia telefoniczne
- Wiadomości SMS/MMS
- E-mail
- Zarządzanie czasem
- Sport i rekreacja
- Praca biurowa (dokumenty, nagrania)
- Nauka
- Optymalizacja snu
- Optymalizacja diety
- Integracja innych urządzeń
- Monitoring
- Nagrywanie dźwięku
- Zbieranie i analiza informacji o lokalizacji, temperaturze, promieniowaniu magnetycznym, ruchu itd.
- ...?

Efekty uboczne

Przyczyny:

- Przytłaczająca ilość informacji o użytkowniku i otoczeniu
- Niska świadomość użytkowników o:
 - Możliwościach urządzeń mobilnych
 - Zagrożeniach prywatności
- Bardziej dynamiczny rozwój technologii niż zabezpieczeń
- Zaangażowanie ze strony rządów i korporacji w technologię i przepisy prawa celem ograniczania prywatności i utrzymania kontroli

Efekty uboczne

Skutki:

- Inwigilacja (przez rządy, instytucje, korporacje, przestępców)
- Mnóstwo danych i luk bezpieczeństwa przydatnych zarówno dla działań wywiadowczych jak i informatyki śledczej



"Nie posiadam i nie zamierzam posiadać telefonu komórkowego (...) To marzenie Stalina, narzędzie Wielkiego Brata. Nie zamierzam nosić urządzenia zbierającego informacje o tym, gdzie przebywam w każdym momencie, urządzenia które może w każdej chwili stać się aktywnym narzędziem podsłuchowym (...)" [9] - Richard Stallman, 2011, założyciel Fundacji Wolnego Oprogramowania

[3]

- 2013 – Dzięki rewelacjom Edwarda Snowdena na światło dzienne wychodzi skala nielegalnego szpiegostwa cybernetycznego prowadzonego w USA i na świecie przez NSA
- 2014 – Badacze na konferencji BlackHat pokazują, jak większość smartfonów może być zamieniona w narzędzie podsłuchowe przy pomocy protokołów kontrolnych OMA-DM
- 2017 – wikileaks.org ujawnia Vault7, ukazujący skalę i rozmiar aresnału inwigilacyjnego (w tym złośliwego oprogramowania i exploitów na urządzenia mobilne) stosowanego przez CIA (niezależnie od NSA)... nad którym CIA utraciło kontrolę
- Co jeszcze... ?!

Częste zagrożenia

- **Luki w oprogramowaniu** i rosnąca popularność malware (np. [16][17] [18] [27] [mobile malware trend])
- **Złośliwe aplikacje** w zaufanych repozytoriach (np. w Google Play Store)
 - Szpiegowskie [19]
 - Ransomware
 - Trojany [21]
 - Dialery (drogie połączenia, SMS-y premium) [20]
 - Ataki na narzędzia do płatności i kryptowaluty
- **Tylne furtki** pozostawione przez producentów i służby specjalne (np. [23], [24], [29], [43][mockingbird])
- **Słabe zabezpieczenia i luki protokołów** komunikacyjnych (np. GSM, Wi-Fi)
 - Przejęcie kontroli [22]
 - Podśluch (np. przez fałszywy BTS)
 - Information disclosure (CreepyDOL - [26])
 - Denial of Service (DoS) [25]
 - Wymuszenie wysyłania SMS-ów [36]

Częste zagrożenia

- Nieprzewidziane następstwa nowych funkcji
 - Ataki Side Channel/Covert Channel/Inference (keylogger, identyfikacja biometryczna z użyciem akcelerometru [35] itd.)
 - Ataki na inne technologie (np. karty PayPass [28])
- Nowe narzędzia ataków przeciwko sieciom i innym technologiom (keylogger z akcelerometru, odtworzenie klucza kryptograficznego przez podsłuch dźwięków wydawanych przez procesor, Android Network Toolkit itd.) [30][31][32]
- Kradzież telefonu równa się praktycznie z kradzieżą tożsamości w Internecie
- Smartfon jako popularne narzędzie stalkingu
- Ataki socjotechniczne
 - Puszczanie „strzałek” z drogich numerów celem uzyskania połączenia zwrotnego
 - Podawanie się za kogoś innego
 - Wyciąganie informacji, których nie powinniśmy nikomu udzielać

Zwiększenie bezpieczeństwa telefonu

(kilka porad)

Dla wszystkich użytkowników (socjotechnika):

- Przezorność, świadomość, nieudzielanie drugiej stronie żadnych informacji przed jej uwierzytelnieniem się (telefon z banku, urzędu skarbowego, „pomyłka” z pytaniem o imię etc.)

Dla wszystkich telefonów:

- Włączenie uwierzytelniania kodem PIN
- OTA firewall* (Nokia 111)
- Wyłączenie zbędnych usług u operatora (potencjał do nadużyć)
 - Możliwość wysyłania SMS-ów premium, zakupów mobilnych itd.
 - Blokada progów kwotowych
 - Możliwość wykonywania połączeń wychodzących i SMS na drogie numery
 - Możliwość doładowania telefonu innym abonentom
 - Możliwość odbierania połączeń z zastrzeżonych numerów
 - Innych zbędnych dla nas (np. wysyłania maili, jeśli nie korzystamy)

Zwiększenie bezpieczeństwa telefonu

(kilka porad)

Dla smartfonów:

- Ustawienie blokady ekranu (długie hasło alfanumeryczne)
- Włączenie automatycznych aktualizacji systemu i aplikacji
- Blokada SMS-ów klasy 0 (bywa, że zawieszają system) [37]
- Blokada niechcianych połączeń (przychodzących, wychodzących, np. Mr Number)
- Zaszyfrowanie systemu plików [38]
- Włączanie Bluetooth i Wi-Fi tylko, gdy ich używamy + bezpieczna konfiguracja [BLUE_BAG]
- Pakiet antywirusowy [41]
- VPN w niezaufanych sieciach
- Wyłączenie zbędnych sensorów
- Stosowanie unikatowych haseł
- Stosowanie dwuskładnikowego uwierzytelniania
- Instalacja „przyjaznego trojana” [39][40]
- Instalacja i konfiguracja firewalla (np. Droidwall)
- Instalacja IMSI-catchera (wykrywacz fałszywych BTS-ów) [33]
- W zastosowaniach firmowych wprowadzenie MDM (Massive Device Management)

Odnośniki

Lista odnośników dostępna pod adresem:

https://github.com/ewilded/mobile/W1_URLs.txt

