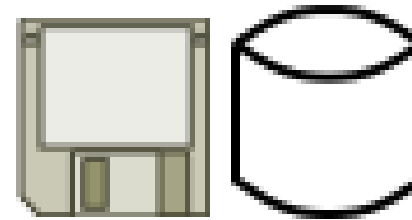


Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

Wykład #3 – Systemy operacyjne, nośniki danych, systemy plików



Plan wykładu



- Firmware a system operacyjny
- Nośniki danych
 - RAM
 - Flash
 - Pamięć telefonu
 - Karty przenośne
 - Smart Cards; karta SIM
 - Warstwy abstrakcji
- Systemy operacyjne

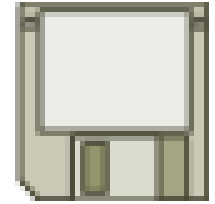
Firmware a OS

Jedno i drugie jest oprogramowaniem; ciągiem instrukcji maszynowych zrozumiałych przez procesor, dla którego zostało zbudowane.

	Firmware	System Operacyjny
rozmiar	mały (liczony w KB)	duży (MB, GB)
przeznaczenie	dedykowane zadania	wszechstronne
rozszerzalność	nie	tak
dostarcza środowisko dla obsługi aplikacji	nie	tak

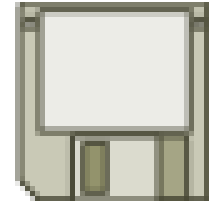
- Firmware może istnieć bez OS, OS może istnieć bez firmware
- Często firmware jest wykorzystywany jako podstawowy interfejs przed załadowaniem systemu operacyjnego (np. boot loader w PC czy smartfonie)
- Na niewielkich urządzeniach wbudowanych istnieje sam firmware, bez systemu operacyjnego (nie ma takiej potrzeby)
- Od niedawna termin często używany niepoprawnie (np. „firmware” dla domowych routerów, który jest GNU/Linuksem)

Nośniki danych - RAM



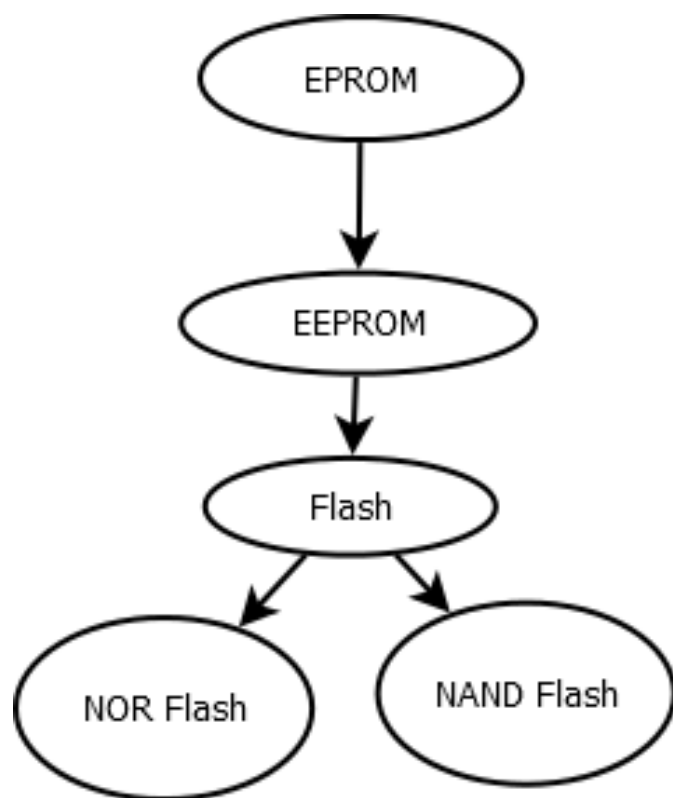
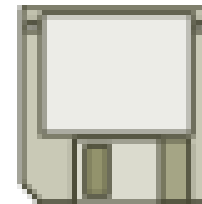
- **RAM** – Random Access Memory (pamięć oferująca dostęp do dowolnego obszaru w bardzo zbliżonym czasie, bez względu na kolejność)
- Stosowana do przechowywania danych tymczasowych, operacyjnych
- Wymaga stałego źródła zasilania celem zachowania danych (pamięć ulotna)

Nośniki danych - ROM



- **ROM** – Read Only Memory – zgodnie z pierwotną definicją pamięć przeznaczona wyłącznie do odczytu
- Z praktycznego punktu widzenia określenie to zaczęto stosować wobec nośników pamięci, które nie wymagają ciągłego źródła zasilania do zachowania danych, stąd też obecnie ROM jest stosowany jako synonim do **pamięci telefonu** (stąd też wzięło się używanie terminu ROM jako synonimu dla obrazów z oprogramowaniem dla telefonu, np. Android ,stock ROM’)
- **MROM** – Masked ROM (pamięć zapisywana jednokrotnie przez producenta, używana obecnie przez część mikrokontrolerów do przechowywania swoich bootloaderów/całego firmware-u)

Nośniki danych - flash



EPROM (Erasable Programmable Read Only Memory), pamięć nieulotna, nośnik wymazywalny z użyciem UV, używany przed EPROM (bateria tranzystorów)

EEPROM - Electrically Erasable Programmable Read Only Memory, nie wymaga wymontowania celem przeprogramowania (w przeciwieństwie do swojego poprzednika)

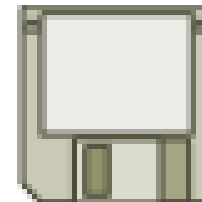
Flash - forma EEPROM, w której tranzystor odpowiedzialny za operację kasowania jest przydzielany dla całego bloku komórek pamięci (w EEPROM kasowanie, odczyt i zapis wymagają osobnych tranzystorów)

NOR - bezpośredni dostęp do każdej komórki pamięci, niska prędkość zapisu (zazwyczaj wykorzystywana do rzadko aktualizowanych danych, np.. Jako ROM), pozwala na szybki dostęp losowy (niesekwencyjny) na poziomie bloków

NAND - większa prędkość zapisu, większa gęstość upakowania danych, sekwencyjny dostęp do danych (niższa prędkość odczytu) na poziomie sektorów (odczyt i zapis), stosowana na szeroką skalę w pamięciach przenośnych, dyskach SSD jak i w tzw. pamięciach telefonu (trwałe przechowywanie OS i danych)

Wiele urządzeń mobilnych posiada jednocześnie pamięć NOR dedykowaną na oprogramowanie i pamięć NAND jako pamięć główną.

Nośniki danych - flash



Sektor – jednostka najmniejsza

Blok – składa się z sektorów

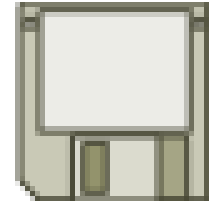
Spotykane kombinacje (obszar na dane + ECC (Error Correction Code)):

- 32 sektory o rozmiarze 512+16 bajtów dają blok o rozmiarze 16 KB
- 64 sektory o rozmiarze 2,048+64 bajtów dają blok o rozmiarze 128 KB
- 64 sektory o rozmiarze 4,096+128 bajtów dają blok o rozmiarze 256 KB
- 128 sektory o rozmiarze 4,096+128 bajtów dają blok o rozmiarze 512 KB

Zarówno pamięci typu NOR jak i NAND

- rozróżniają operację kasowania od zwykłego zapisu
- pozwalają na odczyt/zapis na poziomie sektorów
- pozwalają na kasowanie wyłącznie na poziomie bloków

Nośniki danych - flash

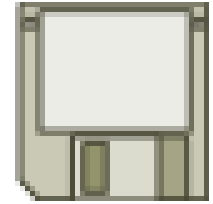


- Zarówno pamięci NOR jak NAND dotyka problem bad sektorów (zarówno montowanych fabrycznie jak i powstałych podczas normalnej pracy)
- W przypadku NOR zazwyczaj jest on obsługiwany na poziomie sterownika [ECC ON FLASH]
- Komórka typowej pamięci flash pozwala na zachowanie dwóch możliwych stanów (0 albo 1, SLC (Single Level Cell))

Współczesne pamięci NAND

- Współczesne pamięci NAND stosują MLC (Multi Level Cell), co zwiększa zapotrzebowanie na detekcję i korekcję błędów (zróżnicowanie algorytmów)
- Powoduje to również potrzebę omijania uszkodzonych sektorów (mapowanie fizycznie sprawnych sektorów na logiczne), co z wraz ze stopniowym zużyciem kolejnych komórek powoduje spadek dostępnej widocznej pojemności nośnika
- Optymalizacja zużycia sektorów przez tzw. wear-leveling (przechowywanie liczników ilości zapisów na danym sektorze celem równomiernego rozkładania nowych zapisów tej samej informacji) [FLASH SURVEY]

Nośniki danych - współczesna pamięć NAND

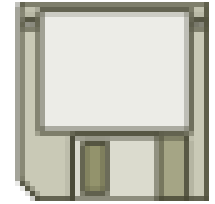


Faktyczne zagospodarowanie sektora w pamięci NAND flash

METADANE FLASH
°wirtualny numer bloku °licznik wymazań °bit poprawności °ecc (kody korekcji błędów) °wersja
DANE WIDZIANE JAKO ZAWARTOŚĆ NOŚNIKA

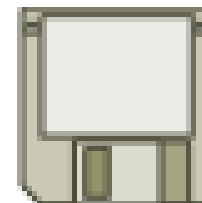
**[FLASH
SURVEY]**

Nośniki danych - flash



- Pamięci NAND zazwyczaj dostarczane są z mikrokontrolerem (najczęściej 8051 lub ARM7 CPU 100MHz)+firmware, który odpowiada za wykrywanie błędów, korekcję błędów, mapowanie oraz wear leveling (np. SD, microSD, MMC, iNAND, eMMC – przeciwieństwo tzw. Raw NAND flash, które są droższe i trudniejsze w eksploatacji) **[BUNNIESTUDIOS]**
- We współczesnych urządzeniach mobilnych poza kością pamięci flash znajduje się również kontroler pamięci (mikrokontroler obsługujący flash)
- W wielu nowych modelach spotyka się moduły pamięci typu iNAND i eMMC z wbudowanym kontrolerem **[iNAND][BUNNIESTUDIOS]**
- Firmware tego rodzaju pamięci często zezwala na interakcje (zmiany konfiguracji bądź nawet nadpisanie kodu firmware-u), co pozwala na:
 - Zmianę sposobu, w jaki urządzenie się przedstawia (typ, rozmiar)
 - Zmianę zachowania (ataki Man In The Middle), potencjalnie możliwość ukrywania danych przy odpowiednio spreparowanym firmware
- Próby standardyzacji pamięci flash są prowadzone przez Open Flash Interface Working Group **[ONFI]**

Nośniki danych - karty pamięci



- **CompactFlash** (CF), standard formatu (46x36 mm), zazwyczaj zawiera pamięć flash, standard stworzony przez SanDisk
- **Secure Digital** (SD), **T-Flash** (microSD), **MultiMedia Card** (MMC), **SmartMedia** (SM), **xD**

Karty w standardzie SD [SD SPEC] oferują dodatkowo:

- Zabezpieczanie hasłem
 - Szyfrowanie i zabezpieczanie przed kopiowaniem (DRM)
 - Blokadę zapisu
-
- **Memory Stick** (MS) – tzw. pendrive
 - USB Mass-Storage (SCSI) również oferuje blokadę zapisu i ochronę hasłem
 - USB Mass-Storage (SCSI) pozwala również na ukrywanie partycji [XABEAN]



Szczególnie polecane źródła
[XABEAN]
[JEFFGRAVES]
[BUNNIESTUDIOS]

Smart Cards



- Znane jako ICC (Integrated Circuit Card) – plastikowe (zazwyczaj polichlorek winylu o grubości 0.76 mm) karty z układem scalonym
- Mikrokomputery wyposażone we własny procesor, pamięć RAM, nośnik danych (EEPROM) i system operacyjny
- Używane głównie do identyfikacji i uwierzytelniania, mogą przechowywać np. klucze szyfrujące
- Opisane normami m. in. ISO/IEC 7810, ISO/IEC 7816, ISO/IEC 14443 [SMARTCARD2] (kształt, właściwości elektryczne, protokoły komunikacyjne, komendy, podstawowa funkcjonalność), [SMARTCARD3] [SMARTCARD4]
- EMV (Europay, MasterCard, Visa) dla kart płatniczych
- Karty SIM, karty płatnicze, karty uwierzytelniające (ten sam chip, inne oprogramowanie)
- Kontaktowe, bezkontaktowe (NFC, RFID), hybrydowe
- Proste (memory cards – tylko mikrokontroler, ROM i RAM) albo z mikroprocesorem (mikroprocesor, RAM, ROM + EEPROM), stosowane jako np. elektroniczne bilety
- Zastosowanie: telekomunikacja, finanse, kontrola dostępu, opieka medyczna, handel, logistyka etc.

Smart Cards - właściwości



EEPROM	1-16 KB
ROM	8-9KB
Taktowanie	1-13.6 MHz
Zapis/odczyt	10-500 000 cykli
Żywotność	10000 operacji odczytu/zapisu
Zasilanie	1.8, 3 lub 5 V DC

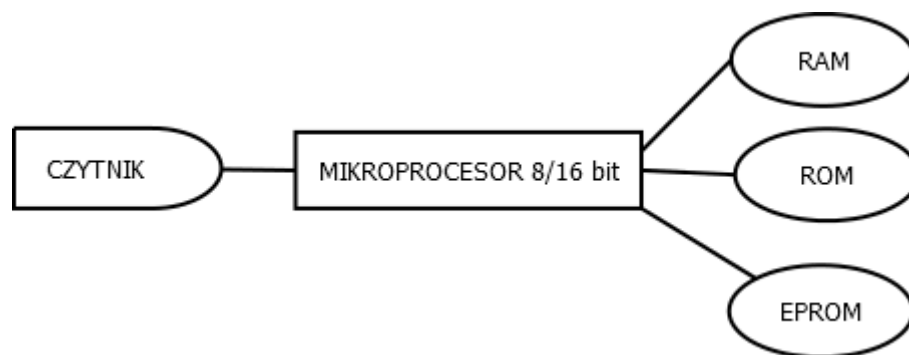
Smart Cards - zasada działania



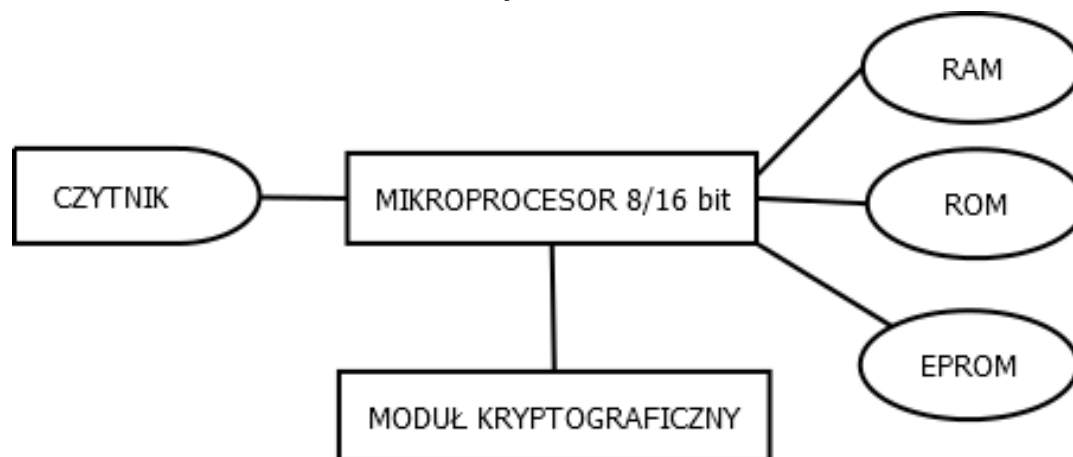
- Zasilanie dostarczane jest przez czytnik karty (zarówno w przypadku kontaktowego jak i bezkontaktowego interfejsu)
- Relacja czytnik/karta jest zawsze typu master/slave (czytnik wysyła komendę, karta odsyła odpowiedź)
- Czytnik dostarcza karcie także sygnału zegarowego
- Komunikacja odbywa się w trybie half-duplex (albo instrukcja jest przesyłana, albo odczytywana jest odpowiedź, nigdy jednocześnie)
- Wiadomości mają wielkość 10-100 B (są buforowane w pamięci RAM karty)
- Nie ma miejsca wykonywanie programu z pamięci RAM (tylko direct execution)
- Jednozadaniowe (brak możliwości uruchomienia wielu aplikacji)

Smart Cards - struktura fizyczna

a) niekryptograficzna karta z mikroprocesorem



b) kryptograficzna karta z mikroprocesorem



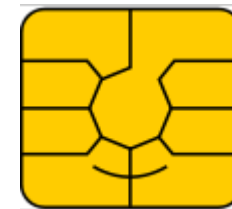
Karta SIM (Subscriber Identity Module)



- Rodzaj karty inteligentnej (Smart Cards)
- Przechowuje dane i aplikacje identyfikujące i uwierzytelniające użytkownika telefonii komórkowej, zgodna ze standardami Smart Card [\[SMARTCARD\]](#)
- Grubość 0.76mm (Nano SIM ma grubość 0.67), regulowana normą ISO/IES_7810
- Komunikacja z pomocą APDU (Application Protocol Data Unit) [\[APDU\]](#)
- Rozmiary:
 - Full size (jak karta kred.) – 85 x 54 mm
 - Mini (25x15 mm)
 - Mikro (15x12 mm)
 - Nano (12.3 x 8.8 mm)
 - Embedded SIM (6 x 5 mm)
- System Operacyjny: JavaCardOS (znany również jako JavaCard) [\[MULTOS vs JavaCardOS\]](#)[\[JavaCards\]](#)
- Pojemność do 256 KB



ICCID - Integrated Circuit Card ID



- Identyfikuje kartę SIM
- ICCID - 19 cyfr, można odczytać bez znajomości PIN/PUK
- 2 cyfry - urządzenie mobilne (89)
- 2 cyfry - kod kraju (48 dla PL)
- 2 cyfry - kod operatora
- 2 cyfry - rok wydania karty
- 10 cyfr - unikalny numer karty (znajduje się również w IMSI)
- Ostatnia cyfra - suma kontrolna
- Zazwyczaj nadrukowany i widoczny na karcie

Karta SIM - najważniejsze atrybuty



ICCID, IMSI

Klucz uwierzytelniający (K_i), jego kopia znajduje się u operatora

Klucz szyfrujący K_c

LAI (Location Area Identifier)

LND - Last Numbers Dialed (historia połączeń)

ADN - Abbreviated Dialing Numbers (spis kontaktów)

SMS - treść SMS-ów

PIN, PIN2, PUK, PUK2, co się dzieje przy blokadzie PUK

FDN - Fixed Dialing Number (numery ustalone)

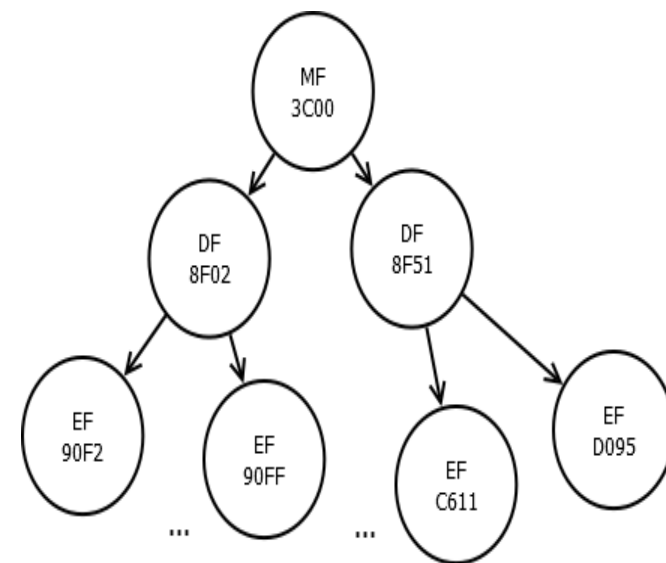
Kod PIN (4 do 8 cyfr)



Karta SIM - system plików



- System plików SmartCards posiada 2 typy plików;
 - DF (Dedicated File) zawierające tylko nagłówek
 - EF (Elementary File) zawierający nagłówek i zawartość
- Drzewiasta struktura rozpoczynająca się od korzenia (MF, który jest DF)
- EF występują w 4 podtypach:
 - **Transparent EF (sekwencja bajtów dowolnej długości, „tablica”)**
 - **Linear fixed EF (rekordy o stałej długości, „struktura”)**
 - Linear variable EF (rekordy o zmiennej długości, „tablica struktur”), nie występuje w kartach SIM
 - **Cyclic EF (cykliczny rekord, „lista dwukierunkowa”)**
- Numeryczne ID jest unikalną nazwą pliku
- Przestrzeń nazw zawiera 65536 elementy (od 0000 do FFFF)



Karta SIM - bezpieczeństwo



Prawa dostępu do systemu plików

Wartość	Dostęp	Znaczenie
0	ALWays	Zawsze dostępny
1	CHV1 (Card Holder Verification 1)	Tylko przy uwierzytelnieniu PIN-em (jeśli wymagany)
2	CHV2	Tylko przy uwierzytelnieniu PIN-em 2
3	Zarezerwowane na przyszłość	
4-14	ADM	Zależne od wydawcy karty
15	NEVer	Nigdy

Karta SIM - aplikacje



- Na karcie SIM może działać wiele aplikacji (aplety Javy)
- Sandboxing (aplety nie mają dostępu do siebie wzajemnie oraz do kodu OS i systemu plików)
- Instalacja/aktualizacja aplikacji odbywa się za pośrednictwem specjalnych SMS-ów binarnych (OTA – Over The Air) podpisanych cyfrowo przez operatora
- Proces ten zachodzi bez żadnej notyfikacji ze strony telefonu

SIM - uwierzytelnianie z GSM



1. Telefon po włączeniu odczytuje IMSI i przekazuje go wraz z numerem IMEI do operatora prosząc o uwierzytelnienie (SIM wymaga PIN do podania IMSI)
2. Operator odnajduje K_i dla danego IMSI
3. Operator generuje losowo liczbę, którą następnie szyfruje kluczem K_i
4. Operator wysyła tę liczbę w jawnej postaci do telefonu, który przekazuje ją karcie SIM
5. Karta SIM również szyfruje liczbę swoją kopią klucza i odsyła wynik do operatora
6. Operator porównuje odpowiedź z zaszyfrowaną liczbą uzyskaną w kroku 3
7. Jeśli wartości się zgadzają, karta SIM zostaje uwierzytelniona do sieci

SIM a USIM

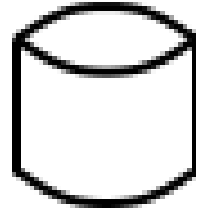


Od czasu pojawienia się 3G operatorzy wydają karty SIM z dwiema partycjami

- SIM (przeznaczona dla 2G)
- USIM (przeznaczona dla 3 G)

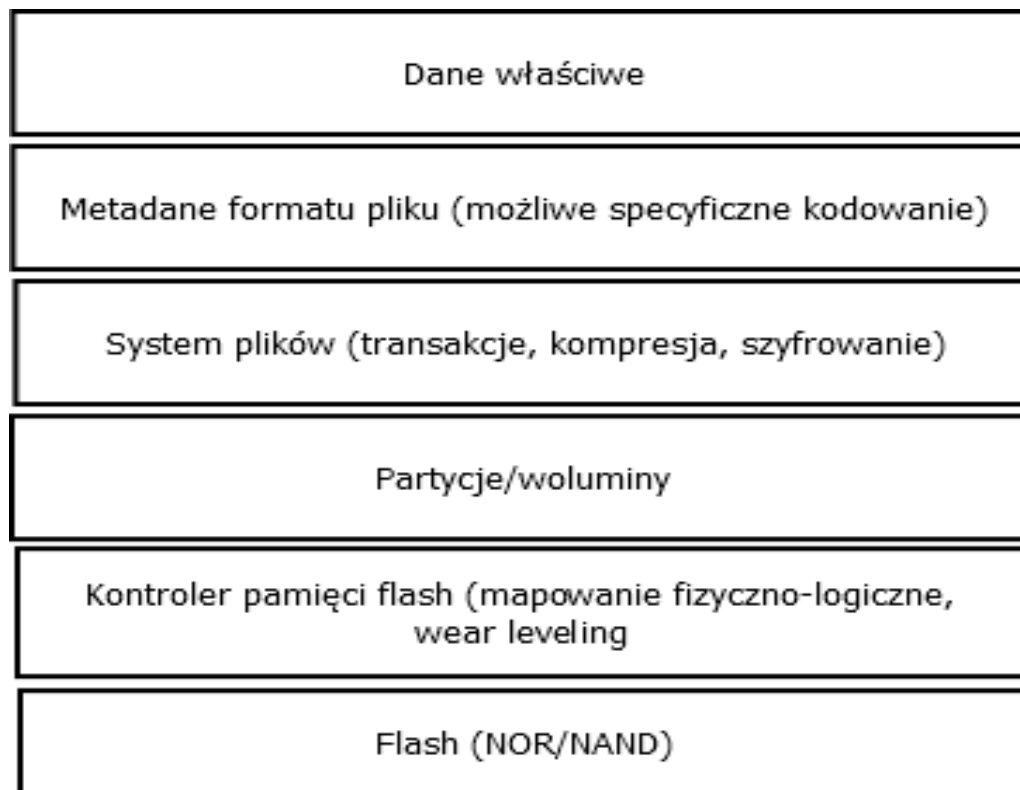
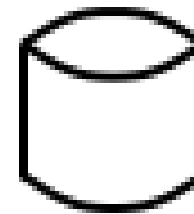
W takim wypadku to, która partycja jest używana, zależy od generacji telefonu.

Systemy plików urządzeń mobilnych



- FAT (VFAT,FAT12,FAT16,FAT32,exFAT)
- RFS (Robust File System, Samsung; FAT rozszerzony o log transakcyjny)
- F2FS (Flash-Friendly File System (Linux), Samsung)
- EXT2, EXT3, EXT4
- YAFFS, YAFFS2 [HOW YAFFS WORKS]
- ETFS (Embedded Transactional File System; QNX, NAND)
- FFS3 (Embedded Transactional File System; QNX, NOR)
- JFFS, JFFS2
- NVFS (Non-Volatile File System,Palm OS))
- RFS (Robust File System, Samsung)
- PM records (Nokia)
- NFS, CIFS
- Inne

Dane na nośniku - warstwy abstrakcji (analogicznie do OSI/ISO)



Systemy Operacyjne urządzeń mobilnych

- Inne
- Windows
 - Windows CE
 - Windows PocketPC
 - Windows XP Tablet Edition
 - Windows 7
 - Windows Mobile
 - Windows Phone
 - Windows RT
- Symbian
- PalmOS
- iOS
- BlackBerry OS/Blackberry 10
- Android

Skala: samych znanych producentów urządzeń jest ok. 500 (dane z 2014).

Systemy Operacyjne - Inne

- Nokia S40 (najpopularniejszy OS Nokii nieoparty o Symbiana), występuje na większości klasycznych Nokii
- webOS (oparty o Linuksa z interfejsem opartym o przeglądarkę web, stworzony przez Palm Computing)
- OpenMoko (oparty o Linuksa) [openmoko]
- LiMo (oparty o Linuksa)
- MeeGo (oparty o Linuksa, połączenie Maemo Nokii i Moblina Intela)
- Palm OS (wersja 5 znana jako Garnet, dla procesorów ARM)
- Nucleus
- Bada (Samsung)
- REX
- DOS
- Bardzo dużo innych, mniej popularnych własnościowych systemów

Symbian



- Występuje na wielu modelach Nokii (ale również Samsunga, Motoroli i Sony Ericsson-a i dwóch modelach Siemens)
- Jako Symbian OS stworzony przez Symbian Ltd. (wykupionego przez Nokię w 2008) jako zastępca Psion EPOC (OS dedykowany dla PDA)
- Od 2008 do 2010 rozwijany przez Nokię pod opieką Symbian Foundation
- Najpopularniejszy smartfonowy OS do roku 2010 (wyparty przez Androida)
- W roku 2011 przekazany przez Nokię firmie Accenture (przejście na Windows Phone) z planowanym wsparciem do roku 2016 [ACCENTURE]
- Często używanym sposobem przechowywania danych jest również SQLite
- Posiada trzy alternatywne interfejsy graficzne: S80, S90, S60 (głównie S60), UIQ oraz MOAP(S)
- Najważniejsze wersje:
 - Do wersji 5 był to EPOC
 - Symbian OS 6.0, 6.1 (2001)
 - Symbian OS 7.0, 7.0s z wieloma UI (2003)
 - Symbian 8.0 (2004), dwa alternatywne jądra, EKA1, EKA2 (realtime) [SYMBIAN INTERNALS]
 - Symbian 9.x – ulepszenia w obszarze bezpieczeństwa (2004-2007)
 - S60 5th Edition (znany również jako Symbian^1)
 - Symbian^2 (wersja używana wyłącznie przez japońskich producentów, 2010)
 - Symbian^3 (Symbian OS 9.5, Symbian Anna)

Blackberry 10



BlackBerry

- Zastępca BlackBerry OS (1.0-1999; 7.1-2012)
- Dedykowany dla urządzeń BlackBerry produkcji RIM (Research In Motion)
- Najnowsza wersja 10.2.1
- Jedyny mobilny OS oparty o QNX (system czasu rzeczywistego, zastosowania przemysłowe + komputery samochodowe)
- Posiada środowisko uruchomieniowe dla aplikacji napisanych dla Androida
- Często spotykany w zastosowaniach biznesowych (dostarczany jest również natywny MDM (Mobile Device Management) – BlackBerry Enterprise Server)
- Sprzedawany z urządzeniami Z10, Z30, Q10, Q5, P'9982
- Oparty o ten sam kod źródłowy, co BlackBerry Tablet OS (dla urządzeń BlackBerry PlayBook)
- Ciekawostką jest UI eliminujące konieczność używania przycisku ,wstecz'
- Relatywnie dobrze zabezpieczony [BLACKBERRY HACKING] [BLACKBERRY FLAWS]
- Obecnie u schyłku popularności

Windows Phone

- Niekompatybilny wstecznie z Windows Mobile
- Rozpoznawalny głównie przez nowy interfejs (Metro)
- Windows Phone 7 (2010)
- Windows Phone 7.5/Mango (2011)
- Wersja 8.1 wydana 14.04.2014
- Od wersji 8.1 dostępny personalny asystent Cortana
- Aplikacje dostarczane przez Windows Phone Store
- Spotykany głównie na urządzeniach z serii Nokia Lumia (ale również HTC, Hauwei, Samsung, Dell, LG, Acer, Alcatel)
- Podobnie jak inne systemy z rodziny Windows posiada rejestr systemowy (używany wyłącznie przez OS, nie przez aplikacje)
- Jedyny OS mobilny wspierający TPM
- Popularną usługą jest OneDrive (usługa zdalnego przechowywania plików)
- Zawartość lokalna i zdalna jest dostępna we wspólnym interfejsie, jako tzw. „huby” (np. zdjęcia, kontakty)
- Znacznie podwyższony poziom zabezpieczeń od wersji 8, odpowiednio skonfigurowany telefon jest problematyczny z punktu widzenia zabezpieczenia danych [WINDOWS 8 PHONE FEATURES]
- U schyłku swej egzystencji (0.3 % rynku) [Windows Phone is dead]

iOS



- Zastępca iPhone OS
- Obecny na urządzeniach iPhone, iPad, iPod Touch, Apple TV
- Podobnie jak OS X, iOS wykorzystuje uniksowego mikrokernels Darwin
- Główne wersje wydawane raz do roku
- Przechowywanie większości danych w bazach sqlite
- Obecna wersja to 10.2.1

iPhone



- 1st gen: lipiec 2007
- 3G: lipiec 2008
- 3GS: czerwiec 2009
- 4: czerwiec 2010
- 4S: październik 2011
- 5: 21 wrzesień 2012
- 5C, 5S: wrzesień, 2013 (5S – pierwszy 64-bitowy iPhone)
- 6 / 6 Plus: wrzesień, 2014
- 6S / 6S Plus: wrzesień 2015
- SE: 31 marzec 2016
- 7 / 7 Plus: wrzesień 2016

Android



- Linux pełni rolę jądra (lekko zmodyfikowany)
- Przestrzeń użytkownika to oprogramowanie Google
- Open Source (AOSP) – licencja Apache
- Większość aplikacji to oprogramowanie własnościowe (płatne/o zamkniętym kodzie)
- Zdecydowanie najwyższa popularność
- Smartfony, tablety, kamery, przenośne konsole (prawdopodobnie niebawem standardowy OS urządzeń przenośnych)
- Duża fragmentacja powodująca problemy z aktualizacjami (więc i bezpieczeństwem)

Android - wersje



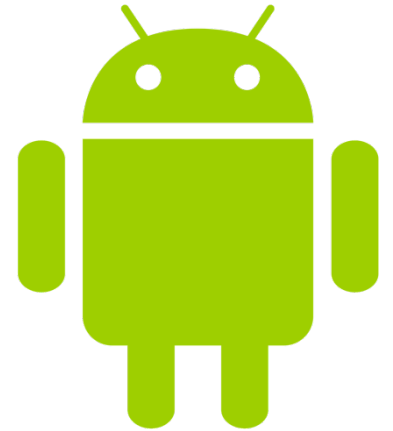
Oficjalne

- Android 1.0
- Android 1.1
- Android 1.5 Cupcake (Linux 2.6.27)
- Android 1.6 Donut (Linux 2.6.29)
- Android 2.0-1 Eclair (Linux 2.6.29)
- Android 2.2-2.2.3 Froyo (frozen yogurt, 2.6.32)
- Android 2.3-2.3.7 Gingerbread (Linux 2.6.35, wsparcie dla NFC)
- Android 3.0-2 Honeycomb
- Android 4.0-4.0.4 Ice Cream Sandwich (Linux 3.0.1)
- Android 4.1-3 Jelly Bean (Linux 3.0.31), od 4.3 SELinux w trybie permissive
- Android 4.4 KitKat (SELinux w trybie enforcing, prewencja ataków przez buffer overflow) [\[KITKAT SECURITY\]](#)
- Android 5.0 Lollipop (wprowadzenie mechanizmu SmartLock)
- Android 6.0 Marshmallow
- Android 7.0 Nougat

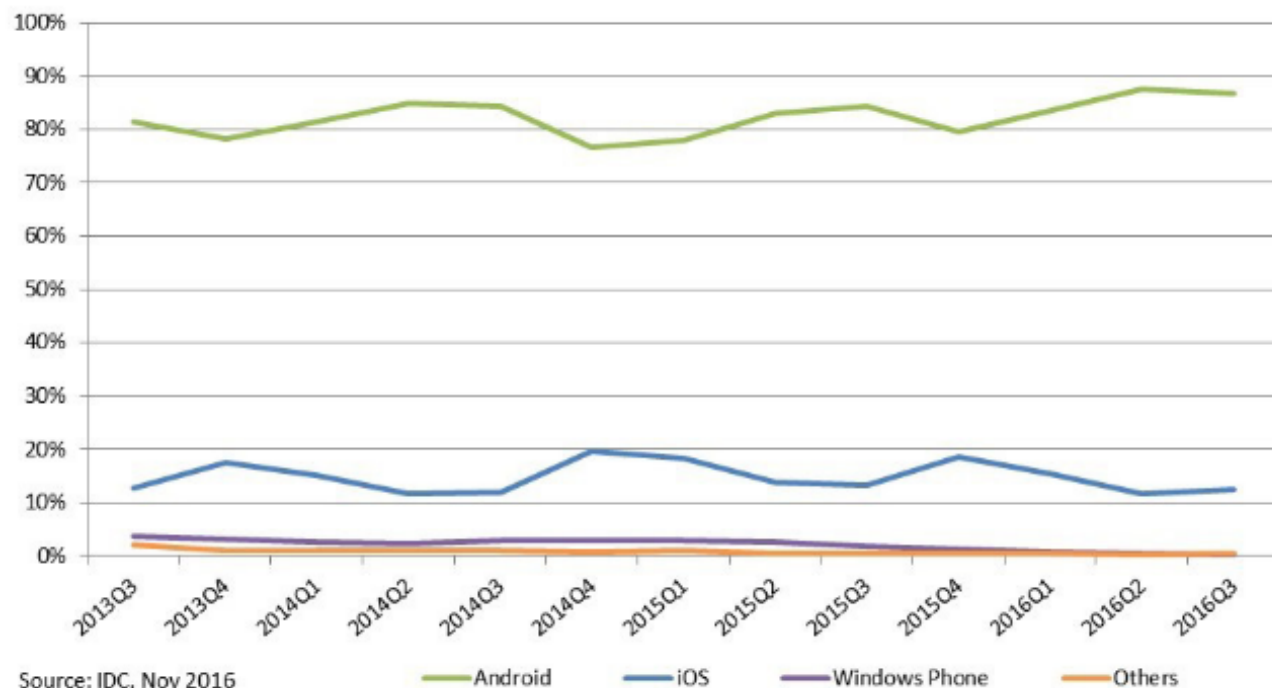
Android - wersje rootowane

Rootowane

- Cyanogenmod
- Replicant



Udział w rynku



Period	Android	iOS	Windows Phone	Others
2015Q4	79.6%	18.7%	1.2%	0.5%
2016Q1	83.5%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%

Source: IDC, Nov 2016

[Market Share]

Odnośniki

Lista odnośników pod adresem:

https://github.com/ewilded/mobile/W3_URLs.txt