KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

11. Získavanie firmvéru jednoúčelových zariadení a jeho analýza

Architektúra ukladania dát: Flash pamäte

- **NOR Flash:**
  - **Topológia:** Bunky sú zapojené paralelne k bitovým linkám, čo umožňuje individuálny prístup ku každému bajtu (čítanie).
  - **Vlastnosti:** Extrémne rýchle čítanie, pomalý zápis a mazanie. Nízka hustota dát, vyššia cena za bit.
  - **XIP (Execute-in-Place):** Kľúčová vlastnosť, ktorá umožňuje procesoru (CPU) čítať inštrukcie priamo z pamäťového čipu cez systémovú zbernicu, rovnako ako z RAM.
  - **Využitie:** Uloženie primárneho bootloadera (BIOS, UEFI, U-Boot), RTOS, kritické konfiguračné dáta.
- **NAND Flash:**
  - **Topológia:** Bunky sú zapojené do série, čo šetrí miesto na čipe (o 40% menšia plocha bunky oproti NOR).
  - **Vlastnosti:** Prístup iba po celých stránkach (Pages) a blokoch (Blocks), nie po bajtoch.
  - **No-XIP:** CPU nemôže vykonávať kód priamo z NAND. Obsah sa musí najprv skopírovať do operačnej pamäte (RAM) pomocou malého zavádzača v ROM alebo NOR pamäti (tzv. Shadowing).
  - **Využitie:** Veľkokapacitné úložiská (USB kľúče, SSD, eMMC), uloženie súborových systémov a užívateľských dát.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Špecifiká NAND a eMMC úložísk

- **Nedokonalosť NAND technológie:**
  - **Bad Blocks:** Výrobný proces NAND nie je dokonalý; čipy opúšťajú továreň s povoleným množstvom nefunkčných blokov, ktoré musia byť mapované.
  - **Bit-flips:** Čítanie alebo zápis môže spôsobiť náhodné preklopenie bitov. Hustejšie technológie (MLC, TLC, QLC) sú na to náchylnejšie.
  - **OOB (Out-Of-Band) dáta:** Každá stránka (napr. 2048 bajtov) má pridruženú "spare area" (napr. 64 bajtov) pre uloženie ECC parít a metadát.
- **Výzva pre analytika:** Bitový (raw) dump NAND pamäte obsahuje "deravé" dáta (zlé bloky) a premiešané paritné bity, čo znemožňuje priamu analýzu súborového systému bez znalosti použitého ECC algoritmu (BCH, Hamming, LDPC).
- **Riešenie: eMMC (embedded MultiMediaCard):**
  - **Architektúra:** Puzdro (BGA) obsahujúce surový NAND čip a dedikovaný mikrokontrolér (Flash Controller).
  - **Flash Translation Layer (FTL):** Firmvér radiča transparentne rieši ECC, Bad Block Management, Wear Leveling (rovnomerné opotrebenie) a Garbage Collection.
  - **Rozhranie:** Navonok poskytuje štandardizované blokové rozhranie (podobné SD karte), čím skrýva fyzikálne nedokonalosti pamäte.
  - **Výhoda:** Extrahovaný obraz z eMMC je "čistý" a logicky usporiadaný, pripravený na okamžité pripojenie (mount).
- **Evolúcia eMMC:** Pre úplnosť moderných trendov (najmä ak sa analyzujú mobilné telefóny alebo pokročilé smart zariadenia) treba spomenúť UFS (Universal Flash Storage). UFS nahradilo eMMC – kým eMMC je half-duplex, UFS je full-duplex.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Neinvazívna extrakcia – UART

- **UART (Universal Asynchronous Receiver-Transmitter):**
  - Asynchrónny sériový protokol, často ponechaný aktívny pre potreby továrenského testovania a ladenia.
  - **Signály:** TX (Transmit - výstup dát), RX (Receive - vstup dát), GND (spoločná zem). VCC nie je nutné pripájať, slúži len na referenciu napäťovej úrovne.
- **Identifikácia a Pinout:**
  - Hľadanie neosadených konektorov (4 piny v rade) na PCB.
  - **Metóda multimetra:** TX pin má pri bootovaní vysokú impedanciu; po inicializácií je v konfigurácii push-pull (idle stav - logická 1) a pravidelne sa napäťový stav mení, keď sa posielajú znaky logu. VCC je stabilné, GND je skratované na tienenie konektorov.
  - **Pokročilé nástroje:** Jtagulator alebo logický analyzátor (Saleae Logic) pre automatickú detekciu baudovej rýchlosti (typicky 115200, 57600, 38400 - moderné zariadenia až do 1.5M).
- **Úroveň napätia (Logic Levels):**
  - Kritické upozornenie: Väčšina moderných SoC pracuje s 1.8V alebo 3.3V logikou. Pripojenie 5V prevodníka (Arduino style) môže mikrokontolér (procesor) nenávratne zničiť. Vždy zmerajte napätie na TX pred pripojením prevodníka!
- **Proces extrakcie:**
  - Prerušenie bootovania (stlačenie klávesy počas "Hit any key to stop autoboot").
  - Prístup do shellu bootloadera (U-Boot, RedBoot, CFE).
  - Použitie príkazov na výpis pamäte: `md.b` (memory dump byte), `sf read` (SPI Flash read), `nand read`.
  - Logovanie výstupu do textového súboru a konverzia hexadecimálneho textu späť na binárny súbor (skriptom).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Debugovacie rozhrania – JTAG a SWD

- **JTAG (Joint Test Action Group - IEEE 1149.1):**
  - Pôvodne štandard pre testovanie spojov na doske (Boundary Scan) bez nutnosti fyzických sond na každom pine. Dnes primárne pre hardvérové ladenie.
  - **Architektúra:** Daisy-chain zapojenie zariadení (TAP Controller).
  - **Signály:**
    - **TCK (Test Clock):** Hodinový signál.
    - **TMS (Test Mode Select):** Riadenie stavového automatu TAP.
    - **TDI (Test Data In):** Vstup dát.
    - **TDO (Test Data Out):** Výstup dát.
    - **TRST (Test Reset):** Voliteľný reset debug logiky.
- **SWD (Serial Wire Debug):**
  - Alternatíva optimalizovaná pre nízky počet pinov. SWD je štandardné debug rozhranie pre všetky moderné ARM jadrá (Cortex-M, Cortex-A, Cortex-R).
  - Dvojvodičové rozhranie: **SWCLK** (hodiny) a **SWDIO** (obojsmerná dátová linka). Poskytuje rovnakú funkcionalitu ako JTAG pri nižšej spotrebe pinov.
- **Proces extrakcie:**
  - Identifikácia pinov (často 10 alebo 20-pinový header, alebo testovacie plôšky).
  - Použitie **OpenOCD** (Open On-Chip Debugger) a hardvérového adaptéra (ST-Link, J-Link, Bus Pirate, Raspberry Pi).
  - Pripojenie k cieľu (Target Halt) – zastavenie CPU.
  - Príkaz `dump_image <file> <address> <size>` vytvorí bitovú kópiu pamäťového priestoru.
  - Možnosť čítať obsah interných registrov a mapovanej RAM.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Invazívna extrakcia – ISP a Chip-Of

- **ISP (In-System Programming):**
  - Čítanie obsahu pamäte priamo na PCB bez odspájkovania, pripojením na piny čipu.
  - **Nástroje:** Testovacie klipy (SOIC-8 clip, Pomona 5250), pogo-piny.
  - **Problém "Bus Contention":** Pri pokuse o čítanie pamäte externým programátorom sa môže interný CPU tiež pokúsiť o prístup na zbernicu. To vedie k poškodeniu dát alebo elektrickému skratu signálov.
  - **Riešenie:** Uvedenie CPU do stavu Reset, alebo externé napájanie iba pamäte (ak to obvod dovoľuje), prípadne prerušenie VCC cestičky k CPU.
- **Chip-Off Forenzka:**
  - Najradikálnejšia a deštruktívna metóda – fyzické odstránenie čipu z dosky.
  - **Postup:**
    - Aplikácia tavidla (flux) a predohrev dosky.
    - Použitie teplovzdušnej stanice (Hot Air Rework Station) pri kontrolovanej teplote.
    - Očistenie pinov/guličiek čipu (reballing pre BGA nie je nutný pre čítanie v kvalitnej pätici).
    - Vloženie do programátora (Xeltek, TL866II Plus) s príslušným adaptérom (TSOP48, BGA153).
  - **Výhody:** Eliminácia akéhokoľvek rušenia od ostatných komponentov na doske. 100% istota čítania (ak je čip funkčný).
  - **Riziká:** Tepelné poškodenie pamäťovej bunky (data retention loss) alebo mechanické poškodenie puzdra.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prekonávanie ochrán – Fault Injection

- **Readout Protection (RDP/CRP):** Bezpečnostný bit v konfigurácii mikrokontroléra (napr. STM32, nRF52, ESP32), ktorý zakazuje prístup cez JTAG/SWD k internej Flash pamäti.
- **Teória Fault Injection (FI):**
  - Polovodičové obvody sú deterministické len v rámci špecifikovaných prevádzkových podmienok (napätie, frekvencia, teplota).
  - Vybočenie z týchto podmienok (Glitch) spôsobí nedefinované správanie – preskočenie inštrukcie, chybné dekódovanie inštrukcie, alebo neuloženie výsledku.
- **Voltage Glitching (Útok chybou napájania):**
  - Zámerné, extrémne krátke (nanosekundy) zníženie napájacieho napätia jadra (VCC_CORE) v presne načasovanom okamihu.
  - **Cieľ:** Narušiť vykonávanie inštrukcie, ktorá kontroluje RDP bit (typicky `LDR` hodnota + `CMP` porovnanie + `B.NE` skok). Ak glitch spôsobí, že skok sa nevykoná (napr. inštrukcia sa interpretuje ako `NOP`), procesor pokračuje do debugovacieho režimu, akoby bol odomknutý.
- **Implementácia:**
  - **Crowbar obvod:** Hardvérový obvod s výkonným MOSFETom, ktorý na chvíľu skratuje napájanie.
  - **FPGA riadenie:** Nutnosť presnosti na úrovni hodinového cyklu procesora. Nástroje ako **ChipWhisperer** synchronizujú glitch s resetom alebo iným spúšťacím signálom.
- **Iné metódy FI:** Clock Glitching (manipulácia hodín), EMFI (Electromagnetic Fault Injection).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Architektúra ARM (AArch64)

- **Dominancia:** De-facto štandard pre mobilné telefóny, tablety a moderné IoT brány.
- **Základné vlastnosti:** 64-bitová RISC architektúra, pevná dĺžka inštrukcií (32-bitov), veľký počet registrov.
- **Register File (AArch64):**
  - **X0 - X30:** 64-bitové všeobecné registre.
  - **X0 - X7:** Slúžia na odovzdávanie argumentov funkciám a návratové hodnoty (podľa konvencie AAPCS64).
  - **X8:** Adresa pre návratovú štruktúru (indirect result location).
  - **X29 (FP - Frame Pointer):** Ukazuje na začiatok aktuálneho stack frame-u (dôležité pre debugovanie).
  - **X30 (LR - Link Register):** Uchováva návratovú adresu pri volaní podprogramu (inštrukcia `BL`). Na rozdiel od x86 sa návratová adresa neukladá automaticky na stack!
- **Stavové príznaky (PSTATE):**
  - Architektúra je silne závislá na stavových bitoch **N** (Negative), **Z** (Zero), **C** (Carry), **V** (Overflow).
  - Väčšina aritmetických inštrukcií má variantu, ktorá nastavuje flagy (napr. `SUBS` vs `SUB`).
  - Podmienené skoky (`B.EQ`, `B.MI`) sa rozhodujú výhradne na základe týchto bitov.
- Pri ARM je potrebné tiež spomenúť inštrukčnú sadu Thumb / Thumb-2 (32-bit ARM). AArch64 dominuje u výkonných zariadení, ale miliardy IoT zariadení (smart žiarovky, senzory) stále bežia na Cortex-M jadrách, ktoré používajú exkluzívne 16/32-bitový Thumb-2 mód.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Architektúra RISC-V

- **Charakteristika:** Open Source Hardware ISA (Instruction Set Architecture). Umožňuje implementáciu bez licenčných poplatkov. Rýchlo naberá na popularite v embedded sfére (diskové radiče, AI akcelerátory).
- **Modulárny dizajn:** Základná sada (RV32I/RV64I) + voliteľné rozšírenia (M-násobenie, A-atomické operácie, F-floating point, C-kompresia).
- **Kľúčové rozdiely oproti ARM pre analytika:**
  - **Register `x0` (Zero):** Je hardvérovo "prednastavený" na hodnotu 0. Zápis do neho sa ignoruje. Používa sa na syntetické inštrukcie (napr. `J` skok je len `JAL x0, offset`).
  - **Absencia globálnych príznakov (Flags):** RISC-V nemá stavový register (CPSR/EFLAGS). Podmienené skoky vykonávajú porovnanie priamo v rámci inštrukcie (napr. `BEQ x1, x2, label` - skoč ak x1 == x2). To zjednodušuje Out-of-Order execution, ale mení vzorce pri disassemblovaní.
  - **Návratová adresa:** Ukladá sa do registra `x1` (alias `ra`), podobne ako LR v ARMe.
- **Privilege Levels:** Machine Mode (M-mode) pre firmvér, Supervisor Mode (S-mode) pre OS, User Mode (U-mode) pre aplikácie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Embedded súborové systémy

- **Hierarchia firmvéru:** Bootloader -> Kernel -> Root Filesystem. Súborový systém obsahuje všetku aplikačnú logiku (web server, konfiguračné skripty, heslá).
- **SquashFS:**
  - Komprimovaný súborový systém len na čítanie (Read-Only).
  - Extrémna kompresia (podpora LZMA, XZ, LZO, ZSTD).
  - Využitie: Štandard pre distribúciu systému v routeroch (OpenWrt, DD-WRT).
  - **Identifikácia:** Magické bajty `hsqs` (Little Endian) alebo `sqsh` (Big Endian). Pozor na neštandardné mutácie výrobcov (napr. `shsq`, `alebo` `qshs`).
- **JFFS2 (Journaling Flash File System version 2):**
  - Navrhnutý priamo pre raw Flash pamäte (bez FTL).
  - **Log-structured:** Dáta sa nepíšu na miesto, ale vždy na koniec (sekvenčne). Staré dáta sú označené ako neplatné.
  - **Mounting:** Pri pripojení musí ovládač prejsť (scan) celé médium a v RAM vytvoriť mapu súborov. To spomaľuje boot pri veľkých kapacitách.
  - **Identifikácia:** Magické číslo `0x1985` na začiatku každého uzla (inode).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Pokročilé súborové systémy – UBIFS

- **Limitácie JFFS2:** Nutnosť skenovania celého disku pri štarte a vysoká spotreba RAM robí JFFS2 nepoužiteľným pre pamäte väčšie ako 128MB.
- **Riešenie: UBIFS (UBI File System):**
  - Pracuje nad vrstvou **UBI (Unsorted Block Images)**.
- **Architektúra vrstiev:**
  - **MTD (Memory Technology Device):** Raw prístup k hardvéru (čítaj/zapisuj/zmaž fyzický blok).
  - **UBI Subsystem:** Vrstva abstrakcie. Mapuje **Logické mazateľné bloky (LEB)** na **Fyzické mazateľné bloky (PEB)**. Rieši manažment zlých blokov a wear leveling transparentne pre vyššiu vrstvu.
  - **UBIFS:** Samotný súborový systém, ktorý používa B+ stromy pre rýchle vyhľadávanie súborov (indexing) bez nutnosti skenovania média.
- **Postup analýzy v Linuxe:**
  - Nestačí jednoduchý `mount`.
  - Nutnosť emulácie NAND pamäte v RAM
  - Formátovanie emulovanej pamäte a nahranie obrazu (`dd`).
  - Pripojenie UBI vrstvy (`ubiattach /dev/mtdX`).
  - Až následne pripojenie zväzku (`mount -t ubifs /dev/ubi0_0 /mnt`)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Praktické nástroje (Linux)

- **Flashrom:** Univerzálny nástroj na čítanie/zápis SPI Flash čipov. Podporuje stovky programátorov (od profesionálnych po Raspberry Pi).
  - Príklad: `flashrom -p ch341a_spi -c "W25Q64.V" -r firmware_dump.bin`
- **Binwalk (klasický, etablovaný nástroj):** "Švajčiarsky nožík" a vhodný pre prvotnú analýzu firmvéru.
  - **Signature Scan:** Hľadá známe hlavičky (GZIP, LZMA, SquashFS, Linux Kernel ARM boot code) v binárnom blobe.
  - **Entropy Analysis (`-E`):** Vizualizuje náhodnosť dát. Vysoká entropia (blízko 1.0) indikuje kompresiu alebo šifrovanie. Nízka entropia indikuje kód alebo prázdne miesto (padding).
  - **Extraction (`-eM`):** Automaticky extrahuje nájdené artefakty a rekurzívne skenuje ich obsah.
- **Unblob** (de facto moderný štandard)
  - Koniec "False Positives" (Falošných zhôd) oproti binwalk
  - Architektúra "Chunkingu" (Presné ohraničenie) - nájde začiatok súboru, ale presne vypočíta (na bajt presne) aj jeho koniec
  - Hlboká rekurzívna extrakcia (Matrioška efekt) - funguje plne automaticky a rekurzívne. Sám sa "prehryzie" všetkými vrstvami až na úroveň základných súborov bez nutnosti manuálnych zásahov analytika.
  - Natívna podpora pre komplexné pamäťové štruktúry:
- **Emulácia a Súborové systémy:**
  - `block2mtd`: Umožňuje pripojiť bežný súbor ako MTD zariadenie (pre JFFS2).
  - `jefferson`: Nástroj na extrakciu JFFS2 súborových systémov (alternatíva k mountovaniu).
  - `ubi_reader`: Python nástroje na extrakciu dát z UBI/UBIFS obrazov bez nutnosti root práv a modulov jadra.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Záver

- **Syntéza poznatkov:** Úspešná analýza vyžaduje multidisciplinárny prístup – od spájkovania a elektrotechniky, cez znalosť operačných systémov, až po assembler a kryptografiu.
- **Kľúčový workflow:** Identifikácia HW -> Zvolenie metódy extrakcie (UART/JTAG/Chip-off/Glitch) -> Dekódovanie štruktúry binárky -> Statická a dynamická analýza kódu.
- **Aktuálne trendy a výzvy:**
  - **Secure Boot & Encrypted Flash:** Moderné MCU majú šifrovanie pamäte "on-the-fly". Statická analýza dumpu je nemožná bez extrakcie kľúča (často cez Fault Injection).
  - **Nástup RISC-V:** Nová architektúra prináša nové nástroje a potrebu učiť sa nové inštrukčné sady.
  - **AI v Reverse Engineeringu:** Využitie LLM a strojového učenia na automatické komentovanie dekompilovaného kódu a hľadanie zraniteľností.
- **Výzva pre študentov:** Experimentujte. Začnite so starým routerom, skúste získať root shell, vydumpovať pamäť a nájsť svoje WiFi heslo v binárnom súbore.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť.