Laboratórium hardvérovej a dátovej analýzy

Úvod

Zriadenie špecializovaného laboratória pre hĺbkovú analýzu hardvéru predstavuje pre organizáciu fundamentálny posun v paradigme kybernetickej bezpečnosti. V ére Industry 5.0 a masívnej konvergencie IT/OT systémov už nestačí chrániť len softvérové vrstvy a sieťové perimetre. Moderné hrozby, ako sú útoky na dodávateľské reťazce, hardvérové trójske kone či pokročilé perzistentné hrozby (APT) cielené na firmvér, vyžadujú prístup, ktorý sleduje aj najnižšiu úroveň.

Hlavnou výhodou tohto laboratória je **holistický vertikálny prístup**, ktorý umožňuje analyzovať zariadenie od fyzikálnych prejavov (napätie, elektrický prúd, teplo, RF žiarenie a podobne) až po logickú úroveň (firmvér, komunikácia, súborové systémy). Laboratórium integruje metodiky reverzného inžinierstva a forenznej vedy do jedného ekosystému.

Potenciálne možnosti laboratória

1. **Prelomenie kryptografických ochrán cez fyzickú vrstvu** (Side-Channel Analysis). Umožňuje realizáciu ofenzívnych aktivít s cieľom obísť matematickú bezpečnosť šifier (ako AES či RSA) útokom na ich fyzickú implementáciu.
2. **Analýza spotreby** (Power Analysis). Využitím osciloskopov s extrémnym vertikálnym rozlíšením, laboratórium dokáže detegovať mikroskopické fluktuácie v spotrebe energie procesora. Tieto fluktuácie korelujú so spracovávanými dátami, čo umožňuje extrahovať tajné šifrovacie kľúče bez znalosti hesla alebo prístupu do systému.
3. **Vysoká presnosť merania**. Nasadenie profesionálneho multimetra spoločnosti Keysight s rozlíšením 7½ miest umožňuje detegovať anomálie v prúdoch na úrovni pikoampérov, čo je kľúčové pre odhalenie pasívnych implantátov alebo analýzu kryptografických operácií v režime spánku.
4. **RF analýza (**Screaming Channels). Spektrálny analyzátor rozširuje vyššie popísané analytické možnosti do rádiofrekvenčného spektra, v ktorom umožňuje detegovať neúmyselné vyžarovanie výpočtových jednotiek prenášaných do rádiového signálu, čím odhaľuje informácie o vnútorných procesoch čipov na diaľku.

5. **Voltage Glitching.** Kombináciou precízneho programovateľného laboratórneho zdroja a generátorov ľubovoľných priebehov (vstavaných v PicoScope) dokáže laboratórium injektovať presne načasované poklesy napätia. Cieľom je dostať procesor do nedefinovaného stavu, kedy preskočí bezpečnostné inštrukcie (napr. kontrolu hesla alebo Secure Boot).
6. **Extrakcia dát**. Technológie spoločnosti ACELab, ako sú PC-3000 Flash a UDMA poskytujú svetovú špičku v oblasti záchrany dát. Umožňujú obísť poškodené radiče pamätí, pristupovať priamo k NAND čipom a rekonštruovať ich dáta.
7. **Chip-off a ISP metódy**. Vďaka opravárenskej stanici ZM-R5860C s optickým zarovnávaním a precíznym riadením teploty je možné bezpečne odspájkovať BGA pamäťové čipy (napr. z havarovaných dronov alebo mobilov) bez ich tepelného zničenia.
8. **Univerzálna čipová konektivita**. Programátor ASIX Forte umožňuje priamu komunikáciu s tisíckami typov mikrokontrolérov a pamätí v širokom spektre napätí (1.8V – 5.5V), čo je kľúčové pre extrakciu firmvéru z neznámych IoT zariadení.
9. **Vizuálna inšpekcia**. Boroskop spoločnosti Fluke s vysokým rozlíšením a makro optikou umožňuje inšpekciu vnútra zariadení cez ventilačné otvory. Analytici môžu odhaliť pridané "bodge wires", neautorizované modifikácie PCB alebo cudzie telesá (implatnáty) bez porušenia záručných plomb.
10. **Termálna analýza**. Termokamera spoločnosti Fluke s citlivosťou 40 mK dokáže odhaliť hardvérové trójske kone na základe ich tepelnej stopy (leakage power), aj keď nie sú permanentne aktívne. Taktiež umožňuje identifikovať falšované alebo prebrúsené čipy na základe rozdielnej emisivity povrchu.
11. **Detekcia odposluchov**. Spektrálny analyzátor umožňuje v režime spektrogramu odhaliť skryté vysielače, ktoré komunikujú v krátkych dávkach (bursts) alebo využívajú techniky rozprestretého spektra, a tým verifikovať, či zariadenie neodosiela dáta na neznáme servery.
12. **Neinvazívne trasovanie**. Sonda SEGGER J-Trace PRO s technológiou Streaming Trace umožňuje nahrávať tok inštrukcií procesora v reálnom čase po neobmedzenú dobu. To umožňuje analytikom vidieť presnú príčinu pádu systému alebo zraniteľnosti (napr. Buffer Overflow) bez toho, aby zastavenie behu výpočtovej jednotky zamaskovalo chybu.
13. **Man-in-the-Middle (MitM) na hardvérovej úrovni**. Schopnosť vložiť “interposer” (medziprvok) pod BGA čipy pomocou stanice ZM-R5860C umožňuje odpočúvať vysokorýchlostné zbernice (DDR, PCIe) a analyzovať komunikáciu, ktorá je inak vnútri čipov neviditeľná.
14. **Automatizácia a AI**. Využitie jednodoskových počítačov Raspberry Pi 5 a skriptovania v Pythone umožňuje automatizovať zber dát, fuzzing protokolov a riadenie komplexných útokov, čím sa zvyšuje efektivita a opakovateľnosť testov.

Špecifikácia a oblasti využitia jednotlivých laboratórnych zariadení

1. Osciloskopy

V kontexte moderného laboratória zameraného na embedded systémy a sieťovú infraštruktúru prestáva byť osciloskop len nástrojom na vizualizáciu elektrických priebehov. Stáva sa kľúčovým senzorom pre **ofenzívnu aj defenzívnu bezpečnostnú analýzu**. Schopnosť vidieť "neviditeľné" – mikroskopické fluktuácie spotreby pri kryptografických operáciách, nanosekundové poruchy na napájacích pnoch či anomálie v časovaní signálov – umožňuje odhaliť zraniteľnosti, ktoré sú pre tradičné softvérové nástroje nezistiteľné. Laboratórium disponuje dvoma komplementárnymi technológiami: stolným osciloskopom **Teledyne LeCroy HDO4034A-MS** pre úlohy vyžadujúce extrémnu precíznosť a USB osciloskopom **PicoScope 5444D MSO** pre flexibilnú analýzu s veľkokapacitnou pamäťou.

Teledyne LeCroy HDO4034A-MS

Prístroj je definovaný technológiou HD4096, ktorá integruje 12-bitové analógovo-digitálne prevodníky (ADC). Oproti štandardným 8-bitovým osciloskopom (256 úrovní) poskytuje 12-bitové rozlíšenie až 4096 úrovní kvantovania, čo je kritické pre detekciu signálov skrytých v šume.

Aplikácia A: Analýza postranných kanálov (Side-Channel Analysis - SCA)

- Detekcia slabín. Moderné procesory v IoT zariadeniach (napr. STM32, ESP32) spotrebúvajú energiu v závislosti od spracovávaných dát. Pri 8-bitovom osciloskope by mikroskopické zmeny napätia na bočníkovom rezistore (rádovo v stovkách mikrovoltov) zanikli v kvantizačnom šume. 12-bitové rozlíšenie HDO4034A-MS umožňuje tieto zmeny jasne zaznamenať.
- Príklad z praxe. Pri analýze implementácie AES šifrovania na inteligentnom merači môžeme pomocou Diferenciálnej analýzy napájania (DPA) získať tajný kľúč. Osciloskop zachytí tisíce priebehov spotreby synchronizovaných so začiatkom šifrovania. Vďaka nízkemu šumu prístroja je možné znížiť počet potrebných meraní na úspešné prelomenie kľúča o 50 – 80 % oproti bežným prístrojom. Pri asymetrickej kryptografii (RSA) môžeme metódou Simple Power Analysis (SPA) vizuálne rozlíšiť operácie "Square" a "Multiply" priamo na displeji osciloskopu a pokúsiť sa prečítať súkromný kľúč z tvaru krivky spotreby v závislosti na implementácii.

Aplikácia B: Analýza a detekcia útokov “vstrekovaním” chýb (Fault Injection)

Aktívne útoky, ako je Voltage Glitching, cielia na narušenie integrity vykonávaného kódu krátkodobým poklesom napätia.

- Detekcia slabín. Cieľom je presne načasovať pokles napätia tak, aby procesor nesprávne prečítal inštrukciu (napr. preskočil kontrolu hesla), ale neresetoval sa.
- Využitie osciloskopu. HDO4034A-MS so šírkou pásma 350 MHz a vzorkovaním 10 GS/s slúži na presnú vizualizáciu tvaru "glitchu" (impulzu), ktorý môže trvať len 10 – 100 ns. Analytik sleduje, či glitch nespôsobuje nežiaduce zákmity (ringing) a či má dostatočnú hĺbku na vyvolanie chyby. Funkcie ako Glitch Trigger umožňujú automaticky zachytiť len úspešné injektáže.

PicoScope 5444D MSO

Osciloskop sa vyznačuje architektúrou FlexRes® (flexibilné rozlíšenie až do 16-bitov) a extrémne kapacitnou pamäťou 512 miliónov vzoriek (512 MS), čo ho predurčuje na analýzu dlhodobých dejov a komplexných protokolov.

Aplikácia A: HĺbkovÁ analýza bootovacieho procesu a "Deep Memory"

Mnoho bezpečnostných chýb v sieťových zariadeniach (routery, kamery) sa vyskytuje počas štartu systému, ktorý môže trvať niekoľko sekúnd až minút.

- Príklad z praxe. Bežný osciloskop s malou pamäťou nedokáže zachytiť celý boot proces pri vysokom vzorkovaní. PicoScope s 512 MS pamäťou umožňuje zachytiť sekvenciu trvajúcu stovky milisekúnd pri plnom rozlíšení. Analytik môže následne "zoomovať" z makro pohľadu (celý boot) až na mikro úroveň (jednotlivé bity na SPI zbernici) a hľadať anomálie, ako sú nezvyčajné príkazy odosielané do Flash pamäte alebo chyby v inicializácii Secure Boot.

Aplikácia B: Reverzné inžinierstvo rozhraní (JTAG, UART, SPI)

Výrobcovia často ponechávajú na doskách neoznačené testovacie body, ktoré môžu slúžiť ako vstupná brána pre útočníka (získanie administrátorského prístupu, extrakcia firmvéru).

- Identifikácia UART. Pomocou PicoScope v režime MSO (Mixed Signal Oscilloscope) môžeme monitorovať neznáme piny. Namiesto metódy pokus-omyl analytik zmeria šírku najužšieho pulzu na linke. Ak je napríklad šírka pulzu 8,68 µs, softvér okamžite vypočíta prenosovú rýchlosť 115200 baudov a začne dekódovať textovú komunikáciu (boot logy, login prompt) priamo na obrazovke.

- Identifikácia JTAG. Pomocou 16 digitálnych kanálov môžeme vizualizovať stavy na viacerých pinoch súčasne a identifikovať charakteristické správanie JTAG protokolu.

Aplikácia C: Forenzná analýza dronov a elektromechanických systémov

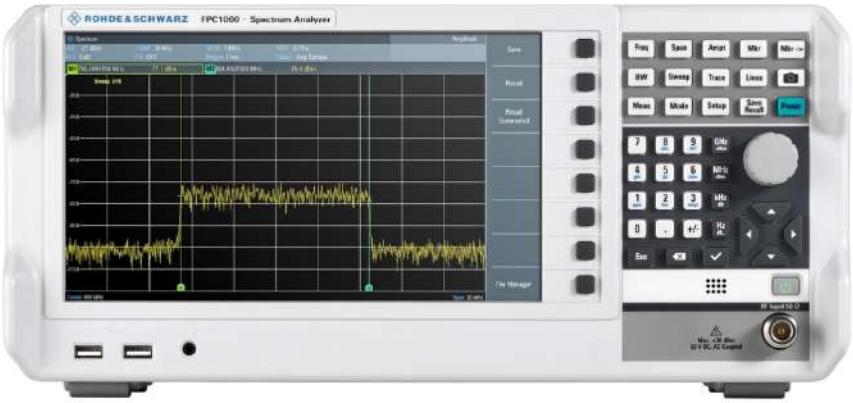
Bezpečnosť dronov závisí od integrity riadiacich signálov motorov.

- Detekcia slabín. Útočník alebo malvér môže modifikovať firmvér regulátora otáčok (ESC) tak, aby spôsobil pád drona.
- Využitie osciloskopu. PicoScope umožňuje analyzovať PWM (Pulse Width Modulation) signály medzi letovým kontrolérom a motormi. V reálnom čase je možné sledovať zmeny v šírke pulzov. Analytik tak môže odhaliť zmeny v riadení – napríklad, ak letový kontrolér pošle neplatný, príliš krátky pulz, ktorý spôsobí desynchronizáciu motora, čo by bežný multimeter nezaregistroval.

Aplikácia D: Injektovanie chýb pomocou AWG

Model 5444D obsahuje integrovaný generátor signálnych priebehov (AWG). V laboratóriu ho využívame na generovanie presne definovaných "glitchov" (napr. krátky pokles napätia), ktoré sú následne injektované do napájania cieľového čipu s cieľom obísť bezpečnostné ochrany.

2. Spektrálny analyzátor



Zatiaľ čo osciloskopy analyzujú signály v časovej doméne (napätie v čase), spektrálny analyzátor poskytuje pohľad do frekvenčnej domény (výkon na frekvencii). V kontexte bezpečnosti embedded systémov a IoT je tento pohľad nenahraditeľný.

Moderné zariadenia komunikujú bezdrôtovo a často vyžarujú informácie aj neúmyselne. Spektrálny analyzátor **Rohde & Schwarz FPC1000** v laboratóriu slúži primárne na detekciu anomálií v RF spektre, odhaľovanie skrytých vysielačov (ploštíc), analýzu proprietárnych protokolov dronov a realizáciu pokročilých útokov postrannými kanálmi (RF Side-Channel Analysis).
S rozšíreným frekvenčným rozsahom do 3 GHz a extrémne nízkym šumovým pozadím dokáže tento prístroj odhaliť aj tie najslabšie signály, ktoré by bežné detektory prehliadli.

Aplikácia A: Diferenciálna spektrálna analýza

Najspoľahlivejšou metódou na odhalenie neautorizovaného vysielania je porovnanie spektra zariadenia s referenčným pozadím (Baselining).

- Detekcia hrozby. Akákoľvek energia v pásmach, ktoré zariadenie nemá používať (napr. aktivita v GSM/LTE pásme na zariadení, ktoré má mať len Wi-Fi, alebo signál 433 MHz), indikuje prítomnosť implantátu alebo ploštice.
- Lokalizácia na PCB. Po detekcii anomálie sa pripojí sada sond blízkeho poľa (Near-Field Probes, napr. R&S HZ-17). Analytik prechádza H-field sondou ponad dosku plošných spojov a hľadá "hotspot" – miesto s maximálnou amplitúdou signálu. Týmto spôsobom je možné fyzicky lokalizovať čip implantátu s presnosťou na milimetre.

Aplikácia B: RF Side-Channel Analysis (Screaming Channels)

Analytická technika využíva fakt, že v moderných zmiešaných čipoch (SoC), ktoré obsahujú procesor aj rádio (napr. ESP32, nRF52), sa digitálny šum z procesora indukuje do rádiového vysielača.

- Princíp. Keď procesor vykonáva kryptografickú operáciu (napr. AES šifrovanie), zmeny v odbere prúdu modulujú signál vysielača. Tento jav sa nazýva "Screaming Channels".
- Využitie FPC1000. Prístroj sa prepne do režimu **Zero Span** (Nulové rozpätie). V tomto režime analyzátor nemeria frekvenčné spektrum, ale funguje ako precízny rádiový osciloskop naladený na jednu konkrétnu frekvenciu.

Aplikácia C: Analýza IoT a Dronov: Spektrogram a Modulácia

Komunikácia dronov a IoT zariadení je často dynamická a využíva techniky na sťaženie detekcie, ako je Frequency Hopping (FHSS) alebo rozprestretie spektra (LoRa).

- Forenzná analýza dronov. Spektrogram umožňuje vizualizovať vzor skokov (hopping pattern) riadiaceho signálu drona. To umožňuje identifikovať protokol (napr. Futaba vs. DJI OcuSync) a odlíšiť signál ovládača od iných zdrojov rušenia,. Pri LoRa komunikácii spektrogram jasne zobrazí "chirpy" (šikmé čiary), z ktorých sklonu môžeme určiť faktor rozprestretia (Spreading Factor) a detegovať anomálie v prevádzke.

3. Programovateľný laboratórny zdroj

Laboratórium využíva laboratórny zdroj **Rohde & Schwarz NGA100. Tento** prístroj bol zvolený pre svoju hybridnú architektúru, ktorá kombinuje efektivitu s lineárnou reguláciou na výstupe, čím zabezpečuje extrémne nízky šum (≤ 1 mVrms). Táto čistota napätia je kritickou podmienkou pre pokročilé techniky, ako je analýza postranných kanálov (Side-Channel Analysis), kde by šum bežného spínaného zdroja maskoval mikroskopické zmeny v odbere prúdu spôsobené kryptografickými operáciami.

Aplikácia A: Metóda injektáže napätia (Voltage Injection)

Ak pasívne meranie odhalí skrat na napájacej vetve je možné využiť režim konštantného prúdu (Constant Current - CC) na bezpečnú lokalizáciu chyby.

- Postup. Zdroj sa nastaví na bezpečné napätie (napr. 1V pre 3.3V logiku) a limitovaný prúd. Prúd sa injektuje do skratovanej vetvy. Podľa Jouleovho zákona sa energia mení na teplo najintenzívnejšie v mieste poruchy (napr. prerazený MLCC kondenzátor).
- Lokalizácia. V kombinácii s termokamerou sa toto miesto prejaví ako "hotspot". Režim CC chráni vodivé cesty PCB pred prepálením.

Aplikácia B: Analýza postranných kanálov (Side-Channel Analysis - SCA)

Ide o jednu z najsofistikovanejších aplikácií zdroja. Využíva fakt, že spotreba CMOS procesorov je priamo úmerná počtu preklápajúcich sa tranzistorov, čo závisí od spracovávaných dát.

- Detekcia kľúčov. Pripojením osciloskopu cez bočník k napájaniu zo zdroja je možné sledovať dynamickú spotrebu. Stabilita zdroja a nízky šum sú nevyhnutné, aby sa v šume nestratila informácia o jednotlivých bitoch šifrovacieho kľúča,.
- Detekcia hardvérových trójskych koní. Aj neaktívny škodlivý čip (implantát) má určitý zvodový prúd (Leakage Current). Porovnaním profilu spotreby s referenčným zariadením napájaným z presného zdroja je možné pomocou štatistických metód odhaliť anomálie indikujúce prítomnosť cudzieho hardvéru.

Aplikácia C: Brown-out testovanie a obchádzanie ochrán

Okrem pasívneho merania sa zdroj využíva na aktívne testovanie robustnosti hardvéru voči útokom na napájanie. Útočníci často využívajú krátkodobé poklesy napätia na to, aby dostali procesor do nedefinovaného stavu (napr. preskočenie inštrukcie overenia hesla).

- Simulácia. Programovateľnosť zdroja umožňuje vytvárať komplexné profily napätia – pomalé poklesy (ramps) alebo rýchle skoky. Cieľom laboratória je nájsť "slepé miesto", kedy je napätie

dostatočne nízke na vyvolanie chyby v logike, ale detektor poklesu napätia (Brown-out Detector - BOD) v čipe ešte neresetuje zariadenie.

- Požiadavka na zdroj. Pre tieto testy je kritická rýchla prechodová odozva zdroja (Transient Recovery Time ≤ 100 µs), aby sa napätie po "glitch" okamžite vrátilo na nominálnu úroveň a procesor mohol pokračovať v (teraz už kompromitovanom) behu.

Aplikácia D: Energetická detekcia malvéru (Fingerprinting)

Bootovacia sekvencia moderných zariadení (Linux, RTOS) má charakteristický energetický "podpis". Rôzne typy škodlivého kódu zanechávajú špecifické stopy v odbere prúdu, ktoré je možné detegovať dlhodobým logovaním spotreby.

- Ransomvér. Vykazuje unikátny vzor vysokej spotreby s periodickými výkyvmi zodpovedajúcimi intenzívnemu zápisu šifrovaných dát do Flash pamäte.
- Cryptojacking. Ťažba kryptomien na IoT zariadeniach sa prejavuje trvalou, maximálnou spotrebou, ktorá neklesá ani v čase nečinnosti.
- Botnet. Pravidelné komunikačné okná s C&C serverom vytvárajú v grafe spotreby viditeľné vzory odlišné od bežnej prevádzky.

Aplikácia E: Simulácia vnútorného odporu

Reálne batérie majú vnútorný odpor, ktorý spôsobuje pokles napätia pri záťaži (napr. pri vysielaní LoRaWAN signálu).

- Testovanie stability. V laboratóriu je možné simulovať tento jav sériovým zapojením rezistora, alebo programovaním zdroja. Tým sa overí, či sa IoT zariadenie alebo dron neresetuje pri vysielaní v dôsledku poklesu napätia, čo je častá zraniteľnosť lacných senzorov.

4. Profesionálny stacionárny multimeter

V bežnej elektrotechnickej praxi je multimeter vnímaný ako základný nástroj na overenie napätia. V kontexte laboratória pre analýzu hardvérovej bezpečnosti však **digitálny multimeter (DMM) Keysight 34470A** zohráva fundamentálne odlišnú rolu. Slúži ako referenčný štandard, ktorý umožňuje detegovať anomálie na hranici fyzikálnych zákonov – od pikoampérových únikov indikujúcich prítomnosť hardvérových trójskych koní až po miliohmové odchýlky odhaľujúce manipuláciu s plošnými spojmi. Tento prístroj triedy Truevolt s rozlíšením 7½ miest.

Aplikácia A: Meranie zvodových prúdov (Leakage Current)

Každý pridaný tranzistor na čipe, aj keď je neaktívny, zvyšuje celkový zvodový prúd. Hardvérový trójsky kôň (škodlivý obvod pridaný do procesora počas výroby) sa často prezradí práve týmto spôsobom.

- Detekcia. Na najnižšom prúdovom rozsahu (1 µA) poskytuje Keysight 34470A rozlíšenie až 1 pikoampér (pA). To umožňuje laboratóriu triediť čipy do klastrov na základe ich pokojovej spotreby. Čip s implantátom sa v tejto viacrozmernej analýze prejaví ako "outlier" (odľahlá hodnota), pretože jeho zvodový prúd bude nepatrne vyšší než u referenčnej vzorky.
- Truevolt technológia. Vďaka patentovanej architektúre A/D prevodníka prístroj eliminuje parazitné injektované prúdy, ktoré by mohli ovplyvniť citlivé obvody, čím zaisťuje, že samotné meranie nespustí anti-tamper mechanizmy skúmaného zariadenia.

Aplikácia B: Detekcia "Always-On" odposluchov (TSCM)

Pri kontrole priestorov sa stretávame s odposluchmi implantovanými do bežnej elektroniky (napr. dymové senzory).

- Korelačná analýza. Pripojením 34470A do série s podozrivým zariadením môžeme digitalizovať jeho spotrebu rýchlosťou 50 000 vzoriek za sekundu. Ak v miestnosti vygenerujeme tón 1 kHz a spektrálna analýza prúdového profilu ukáže zložku 1 kHz, potvrdili sme prítomnosť analógového odposluchu, ktorý moduluje odber prúdu v rytme zvuku.

Aplikácia C: Identifikácia malvéru podľa spotreby

Na rozdiel od osciloskopov, ktoré sa zameriavajú na rýchle deje, multimeter exceluje v presnom dlhodobom profilovaní energetickej stopy zariadenia (Energy Fingerprinting). Rôzne typy škodlivého kódu zanechávajú špecifické stopy v odbere prúdu embedded zariadení.

- Cryptojacking. Ťažba kryptomien na IoT zariadeniach sa prejavuje trvalým posunom priemernej spotreby (Mean Power Shift) smerom nahor, ktorú 34470A vďaka vysokej presnosti spoľahlivo deteguje aj v rádoch desatín percenta.
- Logic Bombs. Malvér, ktorý čaká na aktiváciu, môže v režime spánku vykonávať periodické kontroly času. Rozlíšenie pikoampérov umožňuje odhaliť tieto mikro-prebudenia procesora, ktoré nie sú súčasťou legitímneho firmvéru.

Aplikácia D: Identifikácia debuggovacích (ladiacich) portov (JTAG/UART)

Výrobcovia často nechávajú na doskách neoznačené testovacie body.

- Vysokoimpedančné meranie. Vstupný odpor prístroja > 10 GΩ zaručuje, že pripojenie voltmetra neovplyvní logické úrovne bežiaceho systému.
- Pull-up/down analýza. Presným zmeraním odporu voči napájaniu a zemi na vypnutom zariadení môžeme identifikovať charakteristické rezistory definujúce JTAG piny (TDI, TMS), a tak nájsť vstupnú bránu pre extrakciu firmvéru.

Aplikácia E: Diagnostika Dronov a Elektromechanických systémov

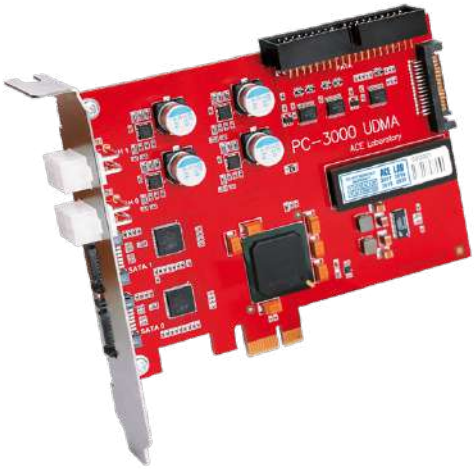
Pre autonómne systémy je kritická spoľahlivosť pohonu.

- Symetria vinutí. Presnosť multimetra 34470A umožňuje detegovať asymetriu odporu vinutí motora na úrovni mikroohmov, čo indikuje medzizávitové skraty spôsobené prehriatím, ešte pred fatálnym zlyhaním drona.
- Testovanie tranzistorov MOSFET. Rýchly a presný diódový test umožňuje skontrolovať polia tranzistorov v regulátoroch otáčok (ESC) a odhaliť prierazy, ktoré by mohli viesť k pádu stroja.

5. Extraktory dát spoločnosti ACELab

V tradičnej digitálnej forenznej analýze sa vyšetrovatelia často spoliehajú na logický prístup k dátam cez operačný systém alebo štandardné rozhrania. V kontexte hardvérovej bezpečnosti a analýzy embedded zariadení (IoT, routery, drony) je však tento prístup často nemožný – či už kvôli fyzickému poškodeniu zariadenia, proprietárnym súborovým systémom, alebo aktívnym bezpečnostným ochranám (heslá, šifrovanie).

Z tohto dôvodu laboratórium integruje špičkové technológie spoločnoti ACELab, konkrétne produkty **PC-3000 Flash** a **PC-3000 UDMA.** Tieto systémy umožňujú ignorovať štandardné komunikačné protokoly a pristupovať k dátam na najnižšej fyzickej úrovni. Kľúčovou stratégiou je obídenie radiča (Controller Bypass), čo poskytuje významnú výhodu pri analýze zariadení, ktoré sú pre bežné nástroje "čiernou skrinkou".



Aplikácia A: Metóda Chip-off a priamy prístup (Raw Dump)

Pri bezpečnostnej analýze smerovačov alebo IoT brán je často nutné získať bitovú kópiu firmvéru na hľadanie zadných vrátok (backdoors). Ak sú porty JTAG/UART uzamknuté, laboratórium využíva metódu Chip-off.

- Proces. Pamäťový čip sa fyzicky odspájkuje z dosky plošných spojov a vloží do špecializovaného adaptéra PC-3000.

- Monolity. Pre miniatúrne pamäťové karty (microSD) alebo integrované čipy bez vývodov (Monoliths), ktoré sa často nachádzajú v špionážnej technike alebo dronoch, je možné využiť adaptér "Spider Board" dodávaný s analyzátorom. Ten umožňuje pripojenie k mikroskopickým technologickým bodom na povrchu čipu a automatickú detekciu rozloženia signálov (Pinout Auto-Detection).

Aplikácia B: Read-Retry a prekonávanie degradácie dát

Jedným z kritických problémov moderných NAND pamätí (TLC, QLC) je vysoká chybovosť čítania. Pre bezpečnostnú analýzu, kde zmena jedného bitu môže zneplatniť dekompiláciu kódu alebo extrakciu kryptografického kľúča, je integrita dát kľúčová.

- Technologické riešenie. PC-3000 Flash implementuje funkciu Read-Retry. Tento proces emuluje správanie radiča a dynamicky mení referenčné napätia na bránach pamäťových buniek. Tým dokáže prečítať aj tie bunky, ktoré sú na hranici čitateľnosti (napr. vplyvom tepla pri požiari alebo zastarania), a zrekonštruovať bezchybný obsah pamäte, čo bežné programátory nedokážu.

Aplikácia C: Rekonštrukcia Flash Translation Layer (FTL)

Surové dáta z NAND čipu sú pre bežný softvér nečitateľné (obsahujú bitové chyby, sú premiešané a fragmentované).

- XOR Descrambling a ECC. Systém automaticky deteguje a odstraňuje XOR "scrambling" a aplikuje ECC korekciu chýb.
- Virtuálny prekladač. Najnáročnejšou fázou je rekonštrukcia virtuálneho obrazu disku. PC-3000 využíva metadáta z OOB (Out-of-Band) oblasti na zostavenie logického obrazu, ktorý presne zodpovedá tomu, čo vidí operačný systém zariadenia. To umožňuje exportovať dáta do formátu .bin pre analýzu v nástrojoch ako Binwalk.

Aplikácia D: Manipulácia so servisnou oblasťou a obchádzanie hesiel

Pre analýzu pevných diskov (HDD) a SSD v priemyselných systémoch (ICS) a kamerových systémoch sa využíva systém PC-3000 UDMA. Mnohé priemyselné systémy využívajú ATA heslá na uzamknutie diskov, čím bránia analýze.

- Servisný režim. PC-3000 UDMA dokáže prepnúť disk do servisného režimu a pristupovať priamo k servisnej oblasti (Service Area) na platniach disku.
- Obídenie ochrany. Umožňuje analytikom čítať moduly s heslom priamo zo servisnej oblasti, alebo ich resetovať bez straty užívateľských dát. To je kľúčové pre forenznú analýzu obsahu diskov z kompromitovaných priemyselných počítačov.

Aplikácia E: Analýza proprietárnych súborových systémov (DVR/NVR)

Pri vyšetrovaní bezpečnostných incidentov je často nutné analyzovať záznamy z kamerových systémov. Tieto zariadenia často nepoužívajú štandardné súborové systémy (NTFS/EXT4), ale proprietárne formáty (napr. WFS0.x) optimalizované pre sekvenčný zápis.

- FS Data Extractor. Softvér v laboratóriu obsahuje moduly pre detekciu a rekonštrukciu týchto exotických súborových systémov, čo umožňuje extrakciu videa a metadát, ktoré by inak boli pre bežné nástroje neviditeľné.

6. Univerzálny programátor

V kontexte výrobného procesu slúži programátor na nahrávanie firmvéru a dát do čipov. V prostredí bezpečnostného laboratória sa však jeho rola invertuje. ASIX Forte sa stáva primárnym nástrojom pre extrakciu (dumping) obsahu pamätí, manipuláciu s bezpečnostnými nastaveniami (fuses) a injekciu inštrumentovaného kódu pre dynamickú analýzu. Na rozdiel od bežných programátorov postavených na mikrokontroléroch, **ASIX Forte** využíva architektúru založenú na FPGA (Field Programmable Gate Array). Táto architektúra poskytuje deterministické časovanie a hardvérovú paralelizáciu, čo je kritické pre komunikáciu s modernými čipmi pri vysokých rýchlostiach (až 30 MHz pre hodiny) bez rizika jitteru, ktorý by mohol spôsobiť chyby pri prenose kritických dát.

Aplikácia A: Adaptabilná logika a nízkonapäťová analýza

Analýza neznámeho hardvéru (IoT, routery, drony) vyžaduje flexibilitu v napájaní a komunikačných protokoloch. Moderné IoT zariadenia (napr. senzory s ESP32 alebo nRF52) často pracujú s logickými úrovňami 1.8V alebo 2.5V. Pripojenie bežného 5V programátora by tieto obvody zničilo.

- Technické riešenie. ASIX Forte disponuje pokročilými napájacími obvodmi, ktoré automaticky prispôsobujú logické úrovne v rozsahu od 1.8V až do 5.5V bez potreby externých adaptérov (level shifters). To umožňuje bezpečné pripojenie priamo k nízkonapäťovým SPI Flash pamätiam a extrakciu firmvéru bez rizika poškodenia cieľového zariadenia.

Aplikácia B: Generovanie vysokého napätia (HVP) pre prelomenie ochrán

Niektoré mikrokontroléry (napr. Microchip PIC) vyžadujú pre vstup do programovacieho režimu alebo pre resetovanie bezpečnostných poistiek aplikáciu vysokého napätia.

- Využitie. Forte integruje menič schopný generovať napätie v rozsahu 6.5V až 17V na pin VPP. V laboratóriu sa táto funkcia využíva na "unbricking" zariadení, kde bol deaktivovaný štandardný nízkonapäťový prístup, alebo na pokusy o obídenie bezpečnostných zámkov (Lock Bits) prostredníctvom manipulácie s napätím.

Aplikácia C: In-Circuit Serial Programming (ICSP) a izolácia CPU

Preferovanou metódou je nedeštruktívna analýza priamo v obvode (In-Circuit). Pri pokuse čítať externú SPI Flash pamäť routera pomocou klipu však často dochádza ku konfliktu s hlavným procesorom zariadenia, ktorý sa tiež snaží komunikovať s pamäťou.

- Riešenie. Programátor Forte umožňuje “držať” procesor v stave RESET. Tým sa výstupy procesora prepnú do stavu vysokej impedancie (Hi-Z), čo uvoľní zbernicu pre programátor a umožní bezchybné stiahnutie binárneho obrazu firmvéru (dump).

Aplikácia D: Forenzná analýza dronov (SWD a STM32)

Letové kontroléry moderných dronov sú často postavené na platforme STM32 (architektúra ARM Cortex-M), ktorá využíva rozhranie SWD (Serial Wire Debug).

- Blackbox analýza. Pomocou Forte je možné cez SWD rozhranie vyčítať obsah internej Flash pamäte mikrokontroléra. Táto pamäť často obsahuje logy – telemetrické dáta o poslednom lete (GPS súradnice, výška, zásahy pilota). Analýza týchto dát umožňuje rekonštruovať priebeh letu aj po havárii, keď je dron fyzicky poškodený, ale čip prežil.
- Modifikácie. Porovnaním extrahovaného firmvéru s originálom (diffing) je možné identifikovať neautorizované modifikácie, napríklad odstránenie geofencingu (No-Fly Zones).

Aplikácia E: Diagnostika ochrany proti čítaniu

ASIX Forte v laboratóriu neslúži len na čítanie, ale aj na testovanie robustnosti zabezpečenia čipov. Výrobcovia MCU (napr. STM32) implementujú stupne ochrany (Read-Out Protection - RDP), ktoré blokujú debug rozhranie.

- Analýza. Softvér UP pre Forte umožňuje prečítať stav konfiguračných bitov (Option Bytes) ešte pred pokusom o prístup k hlavnej pamäti. To umožňuje analytikovi zistiť úroveň ochrany a zvoliť vhodnú stratégiu útoku bez rizika spustenia autodestrukčného mechanizmu (vymazania pamäte).

7. Ladiaca sonda spoločnosti Segger

Pri analýze kybernetickej bezpečnosti embedded systémov (smerovače, drony, IoT) tradičné metódy ladenia typu "stop-and-stare" (zastav a pozeraj) často zlyhávajú. Mnohé zraniteľnosti, ako sú súbehy (race conditions) alebo časovo závislé chyby v sieťových stackoch, sa prejavia len počas plnej prevádzky zariadenia. Zastavenie procesora pomocou bežného debuggera spôsobí stratu spojenia, vypršanie watchdog časovačov a zmenu správania systému, čím sa chyba zamaskuje. Z tohto dôvodu laboratórium disponuje sondou **SEGGER J-Trace PRO.** Kľúčovou vlastnosťou tohto zariadenia je technológia Streaming Trace. Na rozdiel od bežných sond, ktoré ukladajú históriu inštrukcií do malého interného buffera čipu (ETB - rádovo v KB), J-Trace PRO využíva rozhranie USB 3.0 SuperSpeed na streamovanie dát z procesora priamo do PC v reálnom čase. To umožňuje zaznamenávať tok inštrukcií (Instruction Trace) a dát (Data Trace) po neobmedzenú dobu, limitovanú len kapacitou disku analytickej stanice.

Aplikácia A: Spätná analýza pretečenia zásobníka (Buffer Overflow)

Využitie hardvérového trasovania umožňuje laboratóriu aplikovať pokročilé analytické techniky, ktoré sú pre bežné nástroje nedostupné. Pretečenie zásobníka je jednou z najčastejších príčin zlyhania a zraniteľností v C/C++ kóde. Pri bežnom ladení, keď dôjde k pádu (HardFault), je zásobník už poškodený a analytik nevidí príčinu.

- Riešenie. Vďaka neustálemu záznamu histórie je možné realizovať "spätnú analýzu" (Backwards Analysis). V nástroji Ozone, ktorý je rovnako produktom spoločnosti Segger, sa môže analytik posúvať v čase dozadu od momentu pádu a presne identifikovať inštrukciu, ktorá prepísala návratovú adresu alebo prekročila hranice buffera. To umožňuje vidieť nielen následok (pád), ale aj presnú príčinu.

Aplikácia B: Detekcia súbehov (Race Conditions)

Vo viacúlohových systémoch (RTOS v dronoch, Linux v routeroch) vznikajú chyby, ak viacero vlákien pristupuje k zdieľanej pamäti bez synchronizácie. Tieto chyby sú často zneužiteľné.

- Data Trace Watchpoints. J-Trace PRO umožňuje nastaviť hardvérové sledovacie body na konkrétne premenné (napr. príznak `admin_logged_in`). Sonda zaznamená každý prístup (čítanie/zápis) k tejto premennej s presnou časovou značkou. Analýzou chronológie prístupov je môžné odhaliť nebezpečné sekvencie, ktoré by softvérový debugging nezachytil.

Aplikácia C: Timing Attacks a Kryptografická analýza

Niektoré implementácie šifier (napr. PIN overenie pomocou `memcmp`) môžu prezradiť tajomstvo na základe času, ktorý potrebujú na vykonanie (Timing Attack).

- Cycle Accurate Tracing. Sonda dokáže merať trvanie vykonávania funkcií s presnosťou na jeden takt procesora. Je tak možné experimentálne overiť, či čas overovania hesla koreluje s počtom správnych znakov, a tým potvrdiť zraniteľnosť voči útokom postrannými kanálmi bez potreby osciloskopu.

Aplikácia D: Hardvérovo asistovaný "Silent Fuzzing"

Fuzzing je metóda testovania odolnosti softvéru posielaním náhodných dát. Efektívny fuzzing vyžaduje informáciu o tom, ktorú časť kódu test zasiahol (Code Coverage).

- Zero-Overhead. J-Trace PRO poskytuje túto informáciu pasívne cez ETM (Embedded Trace Macrocell) rozhranie. To umožňuje vykonávať tzv. "Silent Fuzzing", kde sa testuje cieľové zariadenie bez akejkoľvek softvérovej inštrumentácie (ktorá by inak spomaľovala beh a menila veľkosť binárky). Dáta o pokrytí kódu sú streamované späť do fuzzeru na PC, ktorý podľa nich optimalizuje generovanie ďalších vstupov.

Aplikácia E: Debugovanie Secure Boot na routeroch

Pri analýze zabezpečených routerov s procesormi Cortex-A (napr. bežiacich na Linuxe) je kritická fáza bootovania (zavádzania operačného systému).

- Využitie. J-Trace PRO sa dokáže pripojiť k procesoru okamžite po resete a sledovať vykonávanie bootloadera (U-Boot/SPL) ešte pred inicializáciou RAM. To umožňuje detailne analyzovať proces overovania digitálneho podpisu firmvéru a identifikovať miesta, kde by mohol útočník tento proces narušiť.

8. Profesionálna opravárenská stanica s mikroskopom

Pre prístup k chráneným dátam v moderných zariadeniach (smartfóny, IoT, riadiace jednotky dronov) už často nestačia logické metódy. Je nutné fyzicky oddeliť pamäťové čipy pre forenznú extrakciu alebo vložiť hardvérové sondy priamo na komunikačné zbernice. Laboratórium je preto vybavené infračervenou BGA opravárenskou pretavovacou stanicou **Seamark ZM-R5860C**. Tento prístroj nie je len nástrojom na opravu, ale kľúčovým prostriedkom pre invazívnu hardvérovú analýzu. Umožňuje bezpečnú manipuláciu s puzdrami typu BGA (Ball Grid Array), CSP a QFN, a to s presnosťou potrebnou na realizáciu pokročilých útokov, ako sú hardvérové Man-in-the-Middle (MitM) implantácie.

Aplikácia A: Precízne riadenie teplotných profilov

Pri extrakcii pamäťových čipov s dôkazmi je kritické neprekročiť teplotu, ktorá by poškodila dátové bunky (retention loss).

- Trojzónový ohrev. Stanica kombinuje horný horúkovzdušný ohrev (800 W) cielený na čip, spodný ohrev (1200 W) pre elimináciu vertikálneho gradientu a masívny spodný IR predohrev (2700 W) pre celú dosku.
- Význam pre forenziu. IR predohrev je kľúčový pri analýze veľkých viacvrstvových dosiek (napr. serverové matičné dosky alebo routery), kde lokálny ohrev spôsobuje deformáciu (warping) a delamináciu spojov. Stanica s termočlánkom riadi teplotu s presnosťou ±3 °C, čo garantuje, že čip dosiahne bod tavenia spájky, ale neprekročí deštruktívnu hranicu.

Aplikácia B: Analýza "Black Box" havarovaného drona

Po havárii drona sú štandardné porty často nefunkčné a doska je lakovaná proti vlhkosti.

- Riešenie. Stanica ZM-R5860C sa použije na jemný predohrev pre odstránenie laku. Následne sa bezpečne odspájkuje eMMC čip s letovými záznamami. Ak je pôvodná doska zlomená, laboratórium vykoná "Board Swapping" – prenesenie (transplantáciu) kľúčových čipov na funkčnú darcovskú dosku, čo umožní stiahnutie dát.

Aplikácia C: Útok na šifrovanú pamäť (DDR4 Interposer)

Cieľom je získať šifrovacie kľúče z RAM pamäte bežiaceho systému.

- Riešenie. Je možné odpájkovať RAM čip, pričom na dosku sa následne prispájkuje tenký interposer a naň pôvodný čip. Vďaka optickému zarovnávaniu a mikroskopu, ktorými stanica disponuje je možné vytvoriť tento funkčný "sendvič" a pripojiť logický analyzátor na sledovanie komunikácie v reálnom čase, čím sa preukáže zraniteľnosť systému voči fyzickým útokom.

9. Boroskop

V procese analýzy hardvérovej bezpečnosti predstavuje fyzické otvorenie zariadenia často nezvratný krok, ktorý môže porušiť záručné plomby, zanechať forenzné stopy, alebo v prípade zariadení s aktívnou ochranou (tamper-responsive) spustiť vymazanie kľúčov. Moderné laboratórium preto musí implementovať aj metodiku Nedeštruktívneho vstupu (NDE) a Nedeštruktívneho testovania (NDT). Primárnym nástrojom pre túto fázu je diagnostický videoskop (boroskop, endoskop) **Fluke DS703 FC.** Tento prístroj, vybavený 7-palcovým kapacitným dotykovým displejom s HD rozlíšením (1280 x 720), umožňuje analytikom vykonať detailný hardvérový prieskum (Hardware Reconnaissance) vnútra zariadenia cez

ventilačné otvory a porty ešte predtým, než sa pristúpi k demontáži. Schopnosť vidieť dovnútra "čiernej skrinky" bez jej narušenia je kritická pre overenie integrity dodávateľského reťazca a detekciu hrubých hardvérových anomálií. Bežné priemyselné endoskopy často zlyhávajú pri inšpekcii elektroniky kvôli nízkemu rozlíšeniu a nevhodnej optike. Fluke DS703 FC bol vybraný pre špecifické vlastnosti, ktoré riešia výzvy mikroelektroniky. Súčasne disponuje pokročilými možnosťami značkovania vyhotovených obrazových záznamov, ktoré sú cenným artefaktom v procese forenznej anlýzy.

Aplikácia A: Orientácia v komplexnej topológii

Pri navigácii sondou cez kľukaté chladiace kanály serverov alebo routerov stráca operátor pojem o priestorovej orientácii.

- Technológia. DS703 FC využíva akcelerometer v sonde a technológiu Up is Up, ktorá v reálnom čase digitálne rotuje obraz tak, aby bol vždy vertikálne správne orientovaný, bez ohľadu na rotáciu sondy.
- Bezpečnostný význam. To umožňuje presné mapovanie polohy komponentov. Analytik môže s istotou určiť, či sa podozrivý vodič nachádza na hornej alebo spodnej strane dosky plošných spojov (PCB), čo je kľúčové pre plánovanie ďalších, invazívnych krokov.

Aplikácia B: Makro inšpekcia

Pre detekciu manipulácie na úrovni SMD komponentov (veľkosti 0402 a menšie) je nutné vysoké zväčšenie.

- Zoom a Optika. Funkcia digitálneho zoomu (1x až 8x) v kombinácii s makro optikou umožňuje prechod od celkového pohľadu na rozloženie dosky k detailu jednotlivých pinov čipu.

Aplikácia C: Analýza kvality spájkovania

Hlavným cieľom vizuálnej inšpekcie je odhaliť anomálie, ktoré indikujú zásah do hardvéru po opustení výrobnej linky (Supply Chain Interdiction). Automatizovaná výroba (reflow/wave soldering) produkuje konzistentné spoje. Ručný zásah útočníka zanecháva stopy.

- Indikátory. Pomocou vysokého rozlíšenia DS703 FC je možné nájsť nepravidelnosti ako sú "špičky" (icicles), zvyšky taviva (flux residue) v okolí čipov, alebo guľôčky spájky roztrúsené na maske PCB. Tieto znaky prezrádzajú, že čip bol vymenený, alebo prepájkovaný ručne.
- Bodge Wires. Boroskop dokáže odhaliť tenké smaltované vodiče (magnet wire), ktoré útočníci používajú na prepojenie bodov na doske. Vďaka makro optike je možné vidieť ich špecifický lesk a neorganizované vedenie cez komponenty, často fixované kvapkami lepidla.

Aplikácia D: Identifikácia čipov a "Black-on-Black" značenie

Identifikácia presného typu čipov je nutná pre vyhľadanie zraniteľností. Výrobcovia však používajú laserové gravírovanie na čiernom puzdre, čo je pri priamom osvetlení nečitateľné (nízky kontrast).

- Technika šikmého osvetlenia. Boroskop umožňuje techniku Oblique Lighting, kedy sa sonda umiestni pod ostrým uhlom k povrchu čipu. Integrované LED svetlo vytvorí tiene v gravírovaní a odlesk od hladkého povrchu smeruje mimo kameru. Tento "dark field" efekt dramaticky zvyšuje čitateľnosť značenia čipov bez nutnosti otvárať šasi.

Aplikácia E: Topologická identifikácia

Pred spustením elektronickej analýzy je efektívne lokalizovať testovacie body vizuálne.

- Postup. Sonda sa zavedie do zariadenia a hľadajú sa charakteristické zhluky pinov alebo pokovovaných otvorov. UART sa často prejavuje ako rad 3-4 pinov, zatiaľ čo JTAG ako dvojradová lišta (2x5, 2x7).
- Silkscreen. Vďaka HD rozlíšeniu je možné prečítať miniatúrne popisy na doske (silkscreen), ako sú "TX", "RX", "TMS" alebo "TCK".

10. Termovízna kamera

Z hľadiska analýzy hardvéru predstavuje teplo viac než len odpadový produkt prevádzky. Práve naopak, je cenným informačným kanálom, ktorý odhaľuje vnútornú logiku zariadenia, kvalitu výroby a prítomnosť skrytých hrozieb. Každá operácia procesora, či už ide o legitímny výpočet alebo škodlivú aktivitu malvéru, je fyzikálne podmienená pohybom elektrónov, ktorý generuje teplo. Laboratórium preto využíva termokameru **Fluke TiS55+.** Tento prístroj bol zvolený pre svoju excelentnú tepelnú citlivosť, čo znamená schopnosť rozlíšiť teplotné rozdiely už od 0,04 °C. Táto citlivosť je kritická hranica pri hľadaní mikroskopických energetických stôp hardvérových trójskych koní alebo pri analýze spotreby v režimoch hlbokého spánku. V kombinácii s manuálnym zaostrovaním a technikou makro-termografie umožňuje analyzovať komponenty na úrovni jednotlivých čipov a SMD súčiastok.

Aplikácia A: Analýza statickej spotreby (Leakage Power Analysis)

Dôležitou aplikáciou termografie je detekcia neautorizovaných modifikácií priamo v kremíku alebo na doske plošných spojov (PCB). Hardvérový trójsky kôň (škodlivý obvod pridaný do čipu) môže byť väčšinu času neaktívny ("dormant"), čím uniká funkčným testom. Avšak aj neaktívne tranzistory majú určitý zvodový prúd (leakage current), ktorý generuje teplo.

- Metodológia "Golden Chip". Umožňuje porovnávať tepelný profil analyzovaného čipu s referenčnou "zlatou vzorkou". Vďaka vysokej citlivosti dokáže Fluke TiS55+ odhaliť lokálne tepelné ostrovčeky spôsobené zvodovým prúdom trójskeho koňa, ktoré by menej citlivá kamera nezachytila.

Aplikácia B: Detekcia falšovaných komponentov (Counterfeit Detection)

V dôsledku nedostatku čipov sa na trhu objavujú "recyklované" alebo "preznačené" komponenty.

- Blacktopping. Falšovatelia často brúsia povrch lacných čipov a prekrývajú ho epoxidom ("blacktop") pre nové gravírovanie. Tento materiál má inú emisivitu ako originál. Termokamera dokáže takýto povrch zobraziť ako nehomogénny a "šupinatý".
- Vnútorné poškodenie. Recyklované čipy môžu mať poškodené vnútorné spoje (bond wires). Pri záťaži sa tieto poškodenia prejavia ako asymetrické tepelné výkyvy priamo na púzdre čipu.

Aplikácia C: Detekcia útokov "Denial of Sleep"

Bezpečnosť IoT zariadení je často ohrozená útokmi zameranými na vyčerpanie energie (Energy Depletion Attacks). Batériovo napájané senzory musia tráviť väčšinu času v režime hlbokého spánku. Útočník im v tom môže brániť neustálym posielaním paketov.

- Nedeštruktívna verifikácia. Termokamera slúži ako neinvazívny nástroj. Ak má mikrokontrolér (napr. ESP32) teplotu vyššiu oproti okoliu v čase, kedy má "spať", je to dôkaz, že procesor stále beží alebo rádio vysiela. Táto metóda je lepšia ako meranie prúdu, pretože nevyžaduje prerušenie obvodu, čo by mohlo zmeniť správanie zariadenia.

Aplikácia D: Lokalizácia funkčných blokov (Side-Channel Mapping)

Pri analýze neznámeho čipu (Black Box) môžeme spustiť špecifickú operáciu (napr. AES šifrovanie) a sledovať, ktorá časť kremíka sa zahreje. Tým vytvoríme "tepelnú mapu" čipu a zistíme, či sa používa hardvérový akcelerátor (lokalizovaný hotspot) alebo či šifrovanie beží neefektívne softvérovo na hlavnom CPU (celkový ohrev).

Aplikácia E: Prediktívna údržba VRM v routeroch

Moderné routery majú extrémne prúdové nároky. Prehriatie napájacej kaskády (VRM) nad 105 °C vedie k nestabilnému napätiu ("ripple"), čo spôsobuje chyby pri spracovaní paketov (CRC errors). Termokamera umožňuje identifikovať tento hardvérový problém skôr, než technik začne zbytočne hľadať chybu v softvérovej konfigurácii.

Aplikácia F: Detekcia skrytých odposluchov

Každá elektronika, aj skrytá kamera alebo ploštica v stene, generuje teplo. TiS55+ dokáže v tepelne stabilizovanej miestnosti odhaliť anomálie (body teplejšie o 0,5 – 2 °C) na povrchoch, kde by nemali byť, čím odhalí skrytý zdroj napájania alebo vysielač.

11. Jednodoskové počítače Raspberry Pi 5

V kontexte moderného hardvérového laboratória nepredstavuje jednodoskový počítač **Raspberry Pi 5** len lacný minipočítač, ale strategickú, modulárnu pracovnú stanicu pre reverzné inžinierstvo a kybernetickú bezpečnosť. Piata generácia prináša zásadný architektonický posun zavedením RP1 vstupno-výstupného radiča a plnej podpory kryptografických rozšírení Armv8 v procesore BCM2712. Táto zmena transformuje platformu na nástroj schopný akcelerovanej kryptoanalýzy, vysokorýchlostného sieťového monitoringu a riadenia komplexných hardvérových útokov, ako je Fault Injection. Vďaka rozhraniu PCIe 2.0 laboratórium využíva RPi 5 nielen ako samostatný radič, ale ako rozšíriteľný hub pre pripojenie NVMe diskov (pre rýchly zápis zachytených dát) alebo špecializovaných sieťových kariet.

Aplikácia A: Transparentný sieťový most (Network Tap)

Pre analýzu komunikácie medzi IoT zariadením a cloudom (alebo dronom a ovládačom) vytvárame transparentný L2 most.

- Konfigurácia. Využitím interného Ethernet portu a druhej sieťovej karty pripojenej cez PCIe (napr. Gigabit ETH HAT) sa vytvorí most, cez ktorý prechádza prevádzka. Nástroje ako Wireshark alebo tcpdump bežiace priamo na RPi 5 zachytávajú a filtrujú pakety bez toho, aby cieľové zariadenie detegovalo prítomnosť analyzátora.

Aplikácia B: Fuzzing a Video Analýza

Výkon RPi 5 umožňuje realizovať úlohy, ktoré predtým vyžadovali desktopové PC.

- RTSP Fuzzing. Pri analýze IP kamier sa využíva RPi 5 na beh fuzzerov, ktoré posielajú malformované požiadavky na RTSP port kamery s cieľom vyvolať pád a odhaliť pretečenie zásobníka. Veľká pamäť RAM (8GB) umožňuje efektívne logovanie stavov fuzzera.
- Hardvérová akcelerácia. Grafické jadro VideoCore VII s podporou HEVC dekódovania umožňuje plynulú analýzu video streamov z bezpečnostných kamier alebo dronov vo vysokom rozlíšení.

Aplikácia C: Emulácia periférií (USB Gadget Mode)

Cez USB-C port dokáže RPi 5 emulovať rôzne USB zariadenia.

- Využitie. Laboratórium využíva tento režim na emuláciu sieťových adaptérov (pre získanie prístupu do zariadení bez Ethernetu).