Název projektu: Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI

Identifikační kód: VJ02010010

Odborná zpráva - Etapa 16 - Testování a dokončení nástrojů pro analýzu certifikačních reportů. Implementace SW modulu pro analýzu implementací kryptografických algoritmů.

Období: 07/2024 - 12/2024

Příjemce:	Vysoké učení technické v Brně Antonínská 548/1 Brno 60190
Jméno hlavního řešitele:	doc. Ing. Jan Hajný, Ph.D. Tel.: +420541146961 Email: hajny@vut.cz
Další účastník 1:	Masarykova univerzita Žerotínovo náměstí 617/9 Brno 602 00
Jméno řešitele:	doc. RNDr. Petr Švenda, Ph.D. Tel.: +420549491878 Email: svenda@fi.muni.cz
Další účastník 2:	České vysoké učení technické v Praze Jugoslávských partyzánů 1580/3 Praha 160 00
Jméno řešitele:	Ing. Martin Novotný, Ph.D. Tel.: +420224358715 Email: martin.novotny@fit.cvut.cz

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

MUNI

ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Obsah

Číslo a název aktivity: Etapa 16 - Testování a dokončení nástrojů pro analýzu certifikačních reportů. Implementace SW modulu pro analýzu implementací kryptografických algoritmů.	
Období řešení:	07/2024 - 12/2024
Cíl aktivity:	Návrh, testování a dokončení sady otevřených nástrojů pro analýzu stávajících certifikačních reportů (mapování certifikovaných zařízení na zveřejněné zranitelnosti pro podporu automatizovaného analytického zpracování s využitím strojového učení (AI)). Implementace SW modulu pro analýzu implementací kryptografických algoritmů.
Krátký popis řešení:	Ve spolupráci s aplikačním garantem a odbornou veřejností proběhlo testování dvou nových a dvou již dříve vytvořených a nyní rozšířených nástrojů včetně dokumentace souvisejících postupů v relevantních scénářích využití.
Řešitel zodpovědný za realizaci:	Petr Švenda (Masarykova univerzita).
Stav plnění aktivity:	Splněno
Výstupy:	1x shrnující zpráva (CZ), 4x GitHub repositář nástroje sec-certs, pyecsca, cooltest a opal-test-suite.
Výsledky:	V rámci této etapy došlo k doplnění implementace čtyř nástrojů, jejich testování s odbornou veřejností a přijetí dvou výzkumných článků popisující výstupy projektu: *Ján JANČÁR, Vojtěch SUCHÁNEK, Petr ŠVENDA, Vladimír SEDLÁČEK a Lukasz Michal CHMIELEWSKI. pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis. CHES'24, 2024, s. 355-381. ISSN 2569-2925. Dostupné z: https://dx.doi.org/10.46586/tches.v2024.i4.355-381.* *Adam JANOVSKÝ, Ján JANČÁR, Petr ŠVENDA, Lukasz Michal CHMIELEWSKI, Jiří MICHALÍK a Václav MATYÁŠ. sec-certs: Examining the security certification practice for better vulnerability mitigation. Computers & Security. 2024, roč. 2024, č. 143, s. 1-13. ISSN 0167-4048.*
Doložení splnění aktivity:	Odborná zpráva – Etapa 16
Shrnutí:	Všechny podmínky pro přechod do další aktivity byly splněny.

1 Úvod

V rámci etapy #16 (07/2024 - 12/2024) jsme prováděli práce na vylepšování uživatelského rozhraní softwaru pro analýzu certifikátů bezpečnosti vydávaných v rámci Common Criteria a FIPS140. V nástrojové části pak bylo provedeno testování a úprava prototypových softwarových modulů pro verifikaci a testování odolnosti kryptografických implementací na čipových kartách, jim příbuzných čipech (TPM, MCU), testování kvality generovaných náhodných dat a také hardwarového diskového šifrování (SED).
Rozšíření nástroje sec-certs pro zpracování certifikátů a extrakci užitečných dat pro posouzení bezpečnosti kryptografických modulů (popsáno v sekci 2.1) pokračovalo vylepšením snadné dostupnosti výsledků přes webové rozhraní, zapojením algoritmů zpracování přirozeného jazyka a aktualizací vhledu do celého ekosystému.
Nástroj pyecsca pro testování a analýzu (nejen) uzavřených implementací na bázi eliptických křivek (popsán v sekci 2.1) byl rozvinut o dodatečné testovací moduly, doplněn databází implementačních rozhodnutí knihoven s otevřeným zdrojovým kódem. Použití nástroje pyecsca bylo testováno v rámci dvou tutoriálů pro odborné publikum v rámci letní školy aplikované kryptografie v Chorvatsku a při konferenci CHES'24 v Kanadě. Vědecký článek popisující metody použité v nástroji byl na tuto špičkovou konferenci také přijat a související softwarový nástroj obdržel ocenění Best Artifact Award. Nástroj Cooltest (sekce 2.3) rozšířil citlivost statistických testů náhodnosti a zjednodušil použití samotného nástroje díky sadě základních nastavení vhodně vybraných na základě rozsáhlého testování dat z různě poškozených pseudonáhodných generátorů.
Na základě zájmu aplikačního garanta a dle domluvy v roce 2023 proběhlo zařazení dodatečné analýzy hardwarově šifrovaných disků (SED, sekce 2.4) a jejich kryptografických implementací. V rámci prací byl vytvořen nástroj pro otestování podporovaných funkcí a analýzu jeho kryptografických vlastností, včetně generátoru náhodných čísel a detekci pravděpodobného chování při přešifrování dat a jejich odstranění. Vytvořený nástroj, spolu s doporučením pro jeho použití a interpretaci výsledků, je součástí výstupů za rok 2024 a je v současné době také zpracován v podobě výzkumného článku, který je nyní v recenzním řízení.
Tato zpráva shrnuje v českém jazyce nejdůležitější zjištění, pro plný rozsah analýz doporučujeme přílohy v anglickém jazyce. Část prací úzce souvisí i s výsledky dosaženými v rámci etap #15 a #17, pro omezení překryvu popisu nástrojů uvádíme potřebné informace na jednom místě a doporučujeme tedy přečíst i související výsledky etapy #15 a #17.

Veškeré plánované činnosti v rámci Etapy 16 byly úspěšně dokončeny a průběžné výsledky byly prezentovány aplikačnímu garantovi (NUKIB) v těchto termínech:

- **15.5.2024, online.** Představení výsledků od posledního kontrolního bodu, představení plánů chystaných v rámci etapy 2024.

- **31.7.2024 odpoledne, Havraníky.** Setkání v rámci brokerage event, diskuze uživatelského testování.
- **25.10.2024 online.** Představení výsledků v oblasti šifrovaných disků, TPM čipů, analýzy úniku časovým postranním kanálem knihovny pro čipové karty a reverzní inženýrství implementací kryptografie eliptických křivek. Diskuze prací plánovaných pro 2025. Rozšířená diskuze formou workshopu.
- **4.12.2024, Praha.** Shrnutí výsledků za rok 2024.

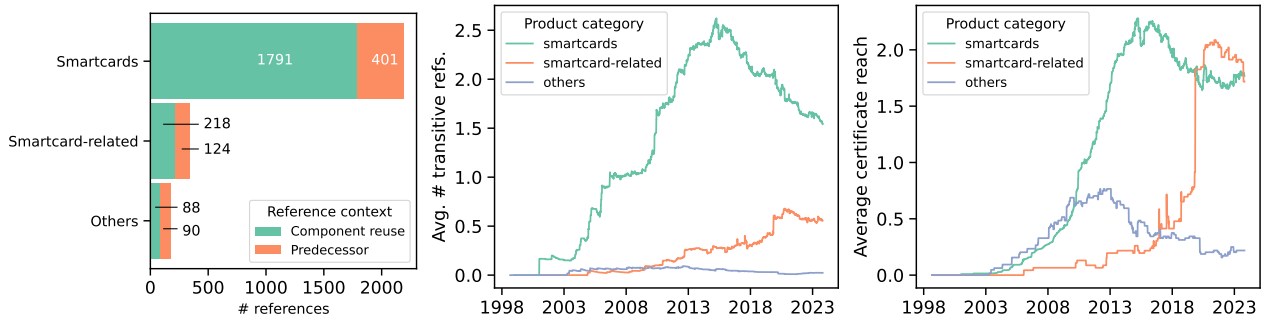
2 Nástroje pro analýzu certifikačních reportů a kryptografických implementací

2.1 *sec-certs*: Analýza certifikačních reportů

Návrh a základní funkčnost nástroje sec-certs pro analýzu stávajících certifikačních reportů schémat Common Criteria a FIPS 140-2/3 byla detailně popsána v roční zprávě pro rok 2022 (viz. zpráva Etapa 3). V roce 2023 bylo doplněno rozšíření o automatické mapování zranitelností v databázi NIST NVD na certifikované položky včetně vyhodnocení celkové úspěšnosti (viz. zpráva Etapa 10).
V roce 2024 doplňujeme inferenci významu referencí mezi certifikovanými zařízeními, provádíme datovou analýzu v ekosystémech produktů certifikovaných ve schématech Common Criteria i FIPS 140, a finalizujeme analýzu proveditelnosti pro použití algoritmů zpracování přirozeného jazyka (NLP) ve vyhledávání nad certifikačními artefakty.
Letošní výsledky vedly k přijetí článků v časopise Computers & Security. Taktéž jsme výsledky projektu prezentovali odborné veřejnosti na několika konferencích: IFIP SEC v Edinburghu, EU CyberAct v Bruselu, ICMC v San Jose, a ICCC v Kataru.

2.1.1 Inference významu referencí

S téměř šesti tisíci bezpečnostními certifikáty vytvořilo certifikační schéma Common Criteria ekosystém propletený různými typy vztahů mezi certifikovanými produkty. Přesto zůstala prevalence a povaha závislostí mezi certifikovanými produkty převážně neprozkoumaná. Naše studie navrhla novou metodu pro sestavení grafu referencí mezi certifikovanými produkty, určení různých kontextů těchto odkazů pomocí algoritmu strojového učení, a měření toho, jak často odkazy představují skutečné závislosti mezi certifikovanými produkty. S pomocí výsledného grafu referencí tato práce identifikuje jen tucet certifikovaných komponent, na kterých závisí alespoň 10% celého ekosystému, což z nich činí hlavní cíl pro škodlivé aktéry. Ve vydaném článku posuzujeme dopad jejich kompromitace a diskutují se potenciálně problematické reference na archivované produkty. Některé důležité trendy zachycené ve světě referencí jsou zobrazeny na Obrázku 1.Z výsledků je jasně patrná dominance kategorie produktů čipových karet nebo s nimi souvisejícími mezi certifikáty obsahující alespoň nějaké reference. Průměrný počet referencí na jiné certifikáty dosahoval maxima cca 2.5 referencí pro čipové karty v roce 2015 a od té doby setrvale klesá na cca 1.5 průměrných referencí. Produkty z jiných kategorií obsahují jen zanedbatelné množství referencí. Tranzitivní závislost produktů pro čipové karty také rostla do roku 2015 a pak jen mírně poklesla. U produktů souvisejících s čipovými kartami výrazně vzrostla po roce 2018.



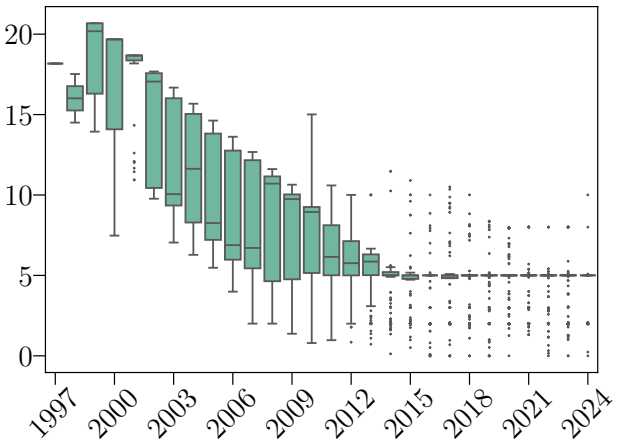
(a) Frekvence významů ref. (b) Avg. # trans. ref. (c) Average product reach

Obrázek 1: Pod-obrázek (a) zobrazuje popularitu jednotlivých významů referencí napříč kategoriemi certikovaných zařízení. Pod-obrázek (b) dokumentuje vývoj průměrného počtu tranzitivních referencí (vztahu component-reuse) v čase. Třetí pod-obrázek (c) pak ukazuje, jak se v čase vyvíjí průměrný dosah produktu.

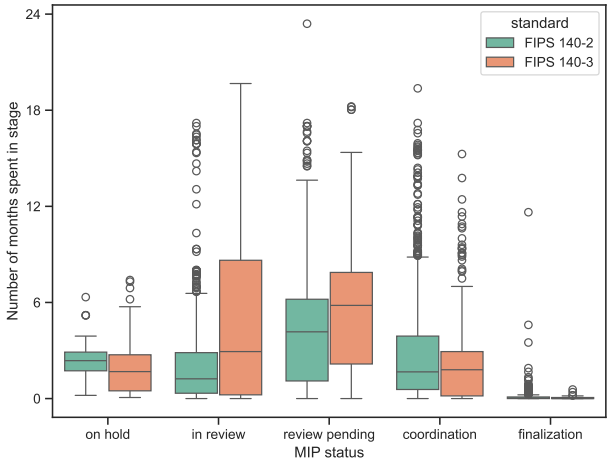
2.1.2 Vhled do ekosystému

Data, která dlouhodobě získáváme pomocí nástroje `sec-certs` nám umožňují hlouběji prozkoumat certifikační praxi a odhalit její zvyklosti. Pomocí našeho nástroje jsme se zaměřili na vývoj certifikační praxe v čase a odhalili zajímavé trendy. Nejprve okomentujeme výsledky získané ze schématu Common Criteria. Zde sledujeme lineárně narůstající počet ročně certifikovaných zařízení, i vývoj průměrné úrovně certifikace (zvyšující se pro čipové karty, oscilující v jiných kategoriích). Taktéž jsme zaznamenali odklon od politiky certifikátů vydávaných na dobu neurčitou k certifikátům s fixní platností 5 let. Naše data nám umožňují monitorovat počet vydávaných certifikátů jednotlivými národními schématy, kde v současnosti nejpopulárnějším národním schématem je schéma nizozemské, které v roce 2023 předstihlo jak německé, tak francouzské národní schéma.

V oblasti FIPS 140 jsme pozornost zaměřili především na popularitu jednotlivých verzí tohoto schématu (starší verze 2 a novější verze 3). Vidíme, že přechod na novější verzi je stále blokován komplikovaností procesu, jakož i jeho dlouhou dobou trvání. Náš nástroj také umožňuje unikátní vhled do délky trvání jednotlivých fází certifikačního procesu, a umožňuje vzájemné porovnání právě mezi verzemi 2 a 3. Tyto výsledky byly prezentovány na konferenci International Cryptoraphic Module Conference v San Jose, CA. Vybrané trendy jsou zachyceny na Obrázku 2 a ukazují, že po roce 2013 je již průměrná doba platnosti certifikátu stabilizována na 5 let s pouze občasnými výjimkami předčasně archivovaných nebo naopak prodloužených certifikátů. Doba trvání fází certifikačního procesu v rámci FIPS 140 ukazuje na prodloužení doby pro FIPS 140-3 vůči svému předchůdci FIPS 140-2 (již tak relativně dlouhé, běžně dosahující 12 až 18 měsíců).



(a) Rozptyl délek platností certifikace v čase. Na ose y je zobrazen počet let, po které je certifikát platný.



(b) Délka trvání jednotlivých fází certifikačního procesu FIPS

Obrázek 2: Pod-obrázek (a) zobrazuje boxploty délky platnosti certifikátů v čase. Konvergence k současné platnosti 5 let (prakticky s nulovým rozptylem) je snadno viditelná. Pod-obrázek (b) porovnává délku trvání jednotlivých certifikačních fází schématu FIPS 140 pro různé verze standardu: FIPS 140-2 (zeleně) a FIPS 140-3 (oranžově). Z obrázku je zřejmé, že úzkým hrdlem nového standardu FIPS 140-3 je samotné hodnocení bezpečnosti produktu, které může trvat i více než jeden rok.

2.1.3 Analýza využití algoritmů NLP pro vyhledávání v dokumentech

V rámci realizované diplomové práce jsme studovali techniky zpracování přirozeného jazyka k pokroku v analýze artefaktů certifikačního schématu Common Criteria, které jsou dostupné jako nestrukturované dokumenty PDF s technickým obsahem. Primárním cílem bylo navrhnout a implementovat řešení proof-of-concept, které uživatelům umožní získat relevantní segmenty (pro jejich dotaz) v rámci těchto certifikátů – segment je definován jako souvislý blok textu v PDF. Byl využit následující přístup:

- Byl proveden průzkum stávajících přístupů a vybrán ten nejschůdnější s ohledem na požadavky projektu.
- Byl vyvinut systém pro vyhledávání informací. Systém je schopen zvýraznit segmenty, které jsou pro daný uživatelský dotaz nejrelevantnější. Systém prohledává jednotlivé soubory PDF.
- Relevance získaných segmentů byla vyhodnocena pomocí předem definované sady uživatelských dotazů. Dále byly navrhnuty kroky vedoucí ke zlepšení přesnosti tohoto řešení, jakož i kroky vedoucí k jeho implementaci na webové stránky projektu.

2.1.4 Plány pro rok 2025

V současnosti pracujeme na několika vylepšeních, které budeme dále rozvíjet v následujícím roce. Jedná se o uživatelskou studii zabývající se použitelností naší webové prezentace (user study), jakož i o vizuální znázornění vhledů do ekosystému získaných dříve v tomto roce. Taktéž prozkoumáváme možnosti automatického vyhledávání špatně konfigurovaných kryptografických algoritmů v certifikačních dokumentech, což by umožnilo automaticky identifikovat konkrétní zranitelnosti v certifikovaných zařízeních.
Dále probíhá příprava vizualizací analýz přímo na webu sec-certs v sekci pro Common Criteria (`https://sec-certs.org/cc/analysis/`) i FIPS 140 (`https://sec-certs.org/fips/analysis/`). V současné době jsou k dispozici statické výsledky, které budou nahrazeny dynamicky generovanými během pravidelné aktualizace.
Dále připravujeme repositář s komplexními vyhledávacími řetězce pro specifickou oblast, například detekce postkvantových algoritmů nebo varianty RSA knihovny obsahující zranitelnost ROCA.

2.1.5 Další informace

Webová stránka projektu se zpracovanými daty z certifikačních reportů a možností pokročilého vyhledávání je dostupná na `https://sec-certs.org`.
Detailní popis nástroje a zdrojové kódy jsou dostupné v repositáři `https://github.com/crocs-muni/sec-certs`.
Publikované výsledky jsou uvedeny v článku: Adam JANOVSKÝ, Ján JANČÁR, Petr ŠVENDA, Lukasz Michal CHMIELEWSKI, Jiří MICHALÍK a Václav MATYÁŠ. sec-certs: Examining the security certification practice for better vulnerability mitigation. Computers & Security. 2024, roč. 2024, č. 143, s. 1-13. ISSN 0167-4048. Dostupné z: https://dx.doi.org/10.1016/j.cose.2024.103895.

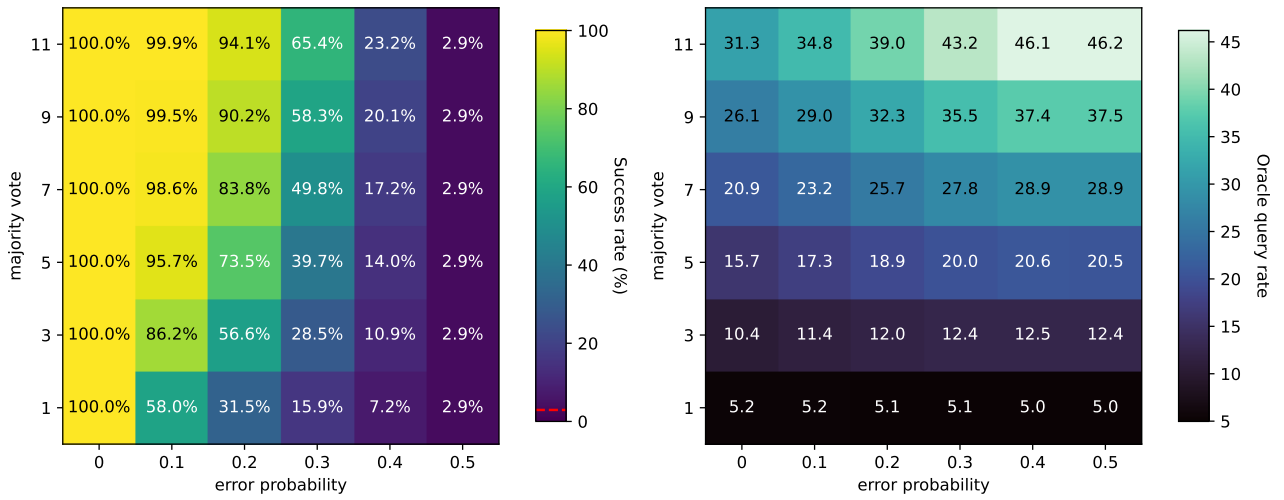
2.2 *pyecsca*: Analýza uzavřených ECC implementací

Návrh a základní funkčnost nástroje *pyecsca* byla detailně popsána v roční zprávě pro rok 2023 (viz. zpráva Etapa 10). V roce 2024 přidáváme shrnutí nových rozšíření publikovaných v článku "pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis"[1] a diskuzi využití pro analýzu posuzovaných kryptografických implementací.

2.2.1 Analýza a reverzní inženýrství black-box ECC implementací

Nástroj pyecsca využívá známé útoky postranními kanály (Refined Power Analysis (RPA), Zero-ValuePoint (ZVP) a Exceptional Procedure Attack (EPA)) a jejich závislost na konfiguracích implementace a přetváří je na metody reverzního inženýrství. Dokáže změřit a odvodit použitý algoritmus na skalární násobení, souřadnicový systém a sčítací formuli. Zároveň jsou tyto metody imunní vůči některým protiopatřením proti útokům postranními kanály jako jsou randomizace souřadnic nebo randomizace křivky. Obecně lze říct, že nástroj pyecsca měří únik informací o detailech dané ECC implementace.
Jako příklad uvádíme výsledky simulace reverzního inženýrství pomocí jedné z našich metod (RPA) zaměřující se na algoritmus skalárního násobení. RPA-RE metoda opakovaně dává na vstup dané implementaci speciálně zkonstruovaný bod, který vyvolává výpočty s nulovými hodnotami, což má za následek snížení celkové hammingové váhy. Ta se projeví v úbytku napětí na rezistoru, který lze měřit a z kterého uniká informace o použitém algoritmu skalárního násobení. Opakováním tohoto postupu jsme pak schopni z částkových uniklých informací zjistit použitý algoritmus. Obrázek 3a ukazuje úspěšnost této metody v závislosti na šumu při měření (error probability) a v závislosti na počtu SCA měření – každé měření totiž opakujeme vícekrát a výsledek se vyhodnotí většinovým hlasováním (majority vote). Například při nulovém šumu má tato metoda 100% úspěšnost. Obrázek 3b pak ukazuje celkový počet potřebných měření celé metody. Celkově lze zhodnotit, že tato metoda je úspěšná i při značném šumu.
Existující protiopatření proti útokům postrannímy kanály se typicky zaměřují na ochranu tajného klíče. Naše metody a provádí reverzní inženýrství a v principu tedy mohou být účinná i v případě existence těchto protiopatření v dané implementaci.

[1] Jan Jancar, Vojtech Suchanek, Petr Svenda, Vladimir Sedlacek and Lukasz Chmielewski. pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis, IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES'24), Ruhr-University of Bochum, 2024, 355–381.



(a) Míra úspěšnosti (- - odpovídá náhodnému hádání).

(b) Rychlost dotazování na orákulum.

Obrázek 3: Výsledky pro RPA-RE metodu se přítomností symetrického šumu.

2.2.2 Analýza ECC knihoven

Pro lepší pochopení vývoje reálných ECC implementacích jsme analyzovali zdrojové kódy 18 open-source kryptografických knihoven v jejich nejnovější vydané verzi (k lednu 2024): BearSSL, BoringSSL, Botan, BouncyCastle, fastecdsa, Go crypto, Intel IPP cryptography, libgcrypt, LibreSSL, libsecp256k1, libtomcrypt, mbedTLS, micro-ecc, Nettle, NSS, OpenSSL, SunEC a Microsoft SymCrypt. Zaměřovali jsme se na kód implementující ECDH, ECDSA na prvočíselných křivkách a X25519, Ed25519. Tento průzkum open-source knihoven nám dal i představu o black-box implementacích, jako jsou kryptografické čipové karty nebo uzavřené embedded systémy.

Naše analýza ukázala, že open-source knihovny zjevně využívají širokou škálu možných algoritmů na skalární násobení, souřadnicových systémů, modelů křivek a sčítacích formulí. Kromě toho je upravují, kombinují a transformují pro další optimalizace. Na základě těchto pozorování jsme odhadli, že celkový prostor ECC implementací obsahuje statisíce konfigurací. Tyto výsledky jsou silnou motivací pro hledání metod pro reverzní inženýrství black-box implementací. Sesbírané poznatky ze zmíněných knihoven jsou zdokumentovány v našem repozitáři `https://github.com/J08nY/pyecsca/tree/master/docs/libraries`.

2.2.3 Rozšířené možnosti nástroje pyecsca

Nástroj pyecsca je komplexní a popis všech jeho možností přesahuje úroveň zaměření tohoto textu. Celkově nástroj pyecsca nabízí širokou funkcionalitu včetně:

- Výčet milionů možných konfigurací implementace ECC a jejich simulace (na úrovni operací na konečných tělesech). Generování C kódu (pro ARM mikrokontrolery, či x86 zařízení) implementace ECC v libovolné konfiguraci.
- Odběrová analýza pomocí osciloskopů PicoScope/ChipWhisperer. Možnosti zpracování získaných odběrových křivek, např. zpracování signálu, filtrování, průměrování, řezání, zarovnání.
- Komunikace přes PCSC/LEIA s implementací ECC na čipové kartě.
- GPU-akcelerované implementace algoritmů na analýzu postranních kanálu (jako například počítání korelačního koeficientu apod.) výrazně zrychlující celý proces.
- Tři metody na analýzu a reverzní inženýrství black-box ECC implementací.

Pro detailní dokumentaci využití pokročilých funkcí lze nalézt na `https://pyecsca.org`.

2.2.4 Další informace

Další informace jsou dostupné v článku vzniklém v rámci projektu a prezentovaném na konferenci CHES'24: *Ján JANČÁR, Vojtěch SUCHÁNEK, Petr ŠVENDA, Vladimír SEDLÁČEK a Lukasz Michal CHMIELEWSKI. pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis. In IACR Transactions on Cryptographic Hardware and Embedded Systems. Německo: Ruhr-University of Bochum, 2024, s. 355-381. ISSN 2569-2925. Dostupné z: https://tches.iacr.org/index.php/TCHES/article/view/11796/11301*. Na konferenci CHES'24 nástroj získal ocenění Best Artifact Award `https://artifacts.iacr.org/tches/2024/`.
Detailní popis nástroje a zdrojové kódy jsou dostupné v repositáři `https://pyecsca.org/`.
Související analytické skripty jsou dostupné v repositáři `https://github.com/J08nY/pyecsca/`.
Tutoriály pro použité nástroje pyecsca jsou dostupné na
`https://github.com/J08nY/pyecsca-tutorial-croatia2024` a v aktualizované podobě v září 2024 na `https://github.com/J08nY/pyecsca-tutorial-ches2024`.

2.3 *CoolTest*: Testování výstupů generátorů (pseudo-)náhodných čísel

V rámci této etapy jsme vyvinuli nástroj na testování náhodnosti CoolTest. Principiálně nástroj vychází z našeho dřívějšího testu náhodnosti BoolTest[2]. Na rozdíl od běžně používaných sad testů náhodnosti, jako je NIST STS, Dieharder nebo TestU01, poskytují naše nástroje lepší informaci o nenáhodnosti nalezené v datech – konkrétní bity a jejich vztah. Další výhodou našich nástrojů je že pro detekci nenáhodnosti typicky potřebují menší množství dat. V tomto ohledu nově vytvořený nástroj CoolTest překonává i svého předchůdce BoolTest. CoolTest díky vyšší senzitivitě dokáže typicky najít nenáhodnost v menším množství dat, než jaké potřebuje BoolTest pro stejný výsledek.

2.3.1 Princip fungování CoolTestu

Základní myšlenka CoolTestu je zkoušet velké množství Boolovských funkcí. Ty jsou vyhodnoceny na testovaných datech a pokud se některá na daných datech chová výrazně jinak, než by se očekávalo u opravdu náhodných dat, pak jsou data prohlášena za nenáhodná.
Podrobněji proces funguje následovně. Vstupní data se rozdělí na bloky uživatelem definované velikosti a takto upravená data se dál rozdělí na dvě částí – trénovací a testovací. Poté se prochází všechny Boolovské funkce na každé kombinaci k bitů, kde k je parametr volený uživatelem. Pro každou funkcí f se vykonají následující kroky:

1. Funkce se aplikuje na každý blok trénovacích dat a spočítáme kolikrát funkce vrátila 1 značené jako #1.
2. Vypočítáme pravděpodobnost p, že funkce f vrátí 1 pro náhodně zvolený blok. Očekávaný počet vrácených 1 je potom pn, kde n je počet bloků v trénovacích datech.
3. Vypočítáme pro danou funkci *Z-score*, jako $Z\text{-}score = \frac{(\#1 - pn)}{\sqrt{p(1-p)n}}$.

Poté ze všech těchto funkcí vybereme tu s nejvyšší absolutní hodnotou *Z-score* a tu obdobným způsobem vyhodnotíme na testovacích datech jen v tomto případě vypočítáme *p-value*. Toto *p-value* je potom výsledkem celého testu společně s Boolovskou funcí, která nám popisuje, které bity jsou spolu závislé a jaký je jejich vztah.
Hlavní rozdíl mezi CoolTestem a jeho předchůdcem BoolTestem je volba funkcí f. Zatímco BoolTest procházel pouze funkce uživatelem definované algebraické normální formy, CoolTest prochází funkce v libovolné algebraické formě omezené pouze počtem proměnných. Pro urychlení výpočtu používá CoolTest chytrý proces při kterém pro nalezení nejlepší z 2^{2^k} funkcí stačí vyhodnotit 2^k z nich.

[2] https://github.com/crocs-muni/booltest

2.3.2 Srovnání s jinými testy

Pro srovnání CoolTestu s dalšími testy jsme použily běžné kolové kryptografické funkce jako je AES, MD5, SHA-2 a další. Vstup pro tyto funkce byl generován tak, že vstupy na liché pozici, byly generovány náhodně a vstup na pozici $m+1$, kde m je liché, byl vytvořen z bloku na pozici m náhodnou změnou hodnoty jednoho bitu.
Na 100 MB těchto dat jsme kromě CoolTestu vyhodnotili i BoolTest a baterie testů NIST STS, Dieharder a TestU01. Tabulka 1 ukazuje pro kombinaci nástroj a kryptografická funkce maximální počet kol kryptografické funkce v jejíchž výstupech daný nástroj dokázal najít nenáhodné vzory. Pro BoolTest a CoolTest tabulka navíc ukazuje i signifikaci daného výsledku, pro baterie testů tuto hodnotu neuvádíme, protože kvůli velkému počtu testů v bateriích a různé přesnosti výstupních *p-value* by takové srovnání bylo komplikované.
Z výsledků můžeme vidět, že CoolTest překonává náš dřívější nástroj BoolTest a ve všech případech kromě blokové šifry Simon poskytuje silnější rozlišovač. V případě hashovací funkce SHA-1 dokonce dokázal najít rozlišovač pro vyšší počet kol než BoolTest. I ve srovnání s bateriemi testů vychází CoolTest nejlépe, kdy pouze ve 4 případech ze 14 dokázala některá baterie najít nenáhodné vzory ve vyšším počtu kol, zatímco z baterií nejlépe vycházející TestU01 byl překonaný jiným nástrojem v 5 případech. Tady je nutné dodat, že s vyšším množstvím dat by baterie oproti CoolTestu dosahovaly lepších výsledků, naopak s nižším množstvím dat by se pravděpodobně zvyšovala výhoda CoolTestu.

2.3.3 Využití v rámci procesu testování

CoolTest je užitečným nástrojem pro testování náhodnosti dat hlavně v případě, kdy jsou data generována v blocích fixní délky. Když se poté velikost bloků, na kterých CoolTest pracuje, nastaví jako malý násobek (např. 2) výstupního bloku generující funkce, dosahuje CoolTest velmi dobrých výsledků. Obzvlášť v případě, kdy máme k dispozici jen omezené množství dat (do stovek MB) nám CoolTest může poskytnout lepší výsledky než standardní baterie testů.
CoolTest má dva parametry, jedním je délka bloku a druhým je velikost množin bitů, na kterých se hledá závislost. Druhý parametr je vhodné nastavit na co nejvyšší hodnotu, při které CoolTest ještě stále dokončí výpočet v přijatelné době. Obvyklá volba je 3, nebo 4.

2.3.4 Další informace

Detailní popis nástroje a zdrojové kódy jsou dostupné v repositáři `https://github.com/jirigav/cooltest/`.

Tabulka 1: Výsledky nástrojů CoolTest, BoolTest, NIST STS, Dieharder a TestU01 na 100 MB dat vygenerovaných běžnými kryptografickými funkcemi se sníženým počtem kol. *P-value* 0 označuje jakoukoli *p-value* menší než 10^{-300}. Zvýrazněné buňky ukazují nejvyšší počet kol, ve kterém byly detekovány nenáhodné vzory.

	CoolTest		BoolTest		NIST STS	Dieharder	TestU01
	kola	*p-value*	kola	*p-value*	kola	kola	kola
AES	2	0	2	0	2	3	3
Camellia	3	0	3	0	4	3	3
CAST5	3	$5 \cdot 10^{-66}$	3	$1 \cdot 10^{-34}$	2	3	3
IDEA	1	0	1	0	0	1	1
SHACAL-2	8	0	8	$5 \cdot 10^{-176}$	7	7	7
Simon	17	$8 \cdot 10^{-5}$	17	$2 \cdot 10^{-7}$	13	16	17
Speck	7	0	7	$5 \cdot 10^{-119}$	6	8	8
Twofish	3	0	3	0	2	2	3
BLAKE	1	0	1	0	1	1	1
Keccak	2	0	2	0	2	2	2
MD5	12	$7 \cdot 10^{-220}$	12	$2 \cdot 10^{-67}$	10	11	21
MD6	10	$1 \cdot 10^{-99}$	10	$4 \cdot 10^{-19}$	7	8	9
SHA-1	17	$3 \cdot 10^{-23}$	16	$6 \cdot 10^{-70}$	13	15	16
SHA-256	13	$5 \cdot 10^{-99}$	13	$6 \cdot 10^{-16}$	11	11	12

2.4 *SED*: Hardwarové diskové šifrování

Self-encrypting drive (SED) je úložné zařízení (disk), které zahrnuje šifrování dat přímo v hardware. Současné disky používají standard TCG Opal ve verzi 2. Lze se také často setkat se standardem TCG Pyrite, který však implementuje pouze autentizační funkce, nešifruje samotná data. Tato zařízení umožňují konfiguraci několika nezávislých oblastí s jinými přístupovými právy a odlišným klíčem.
Disky se dodávají se ve formě NVMe zařízení případně SATA/SAS disků a implementovaný TCG standard je obvykle jen dán verzí konkrétního firmware. Některé disky existují i ve FIPS-140/CC verzích.
Vzhledem k proprietárním řešením různých výrobců a problematické použitelnosti existující nástrojů jsme se vyvinuli a rozšířili nástroj *opal-toolset* pro nízkoúrovňovou komunikaci s Opal a Pyrite disky. Tento nástroj slouží pro testování konkrétních scénářů. Nadstavbou je pak sada skriptů *Opal Test Suite*, které implementují navržené testovací scénáře s detekci známých problémů.

2.4.1 Testovací sada disků

Testování proběhlo nad sadou 50 disků (38 podporovalo Opal a 12 Pyrite), které dostatečně silně reprezentují zařízení podporující požadované funkce v současné době. Sada disků obsahuje jak starší modely, které jsou masivně používány v uživatelských systémech, tak i nové disky, které jsou stále v prodeji. Sada obsahuje disky od různých výrobců jako Samsung Western Digital, Seagate, Kingston, Micron, ale i OEM verze dodávané například do notebooků Lenovo.
Společným problémem většiny těchto zařízení je identifikace konkrétních implementovaných TCG standardů. Často se jedná jen o jedno rozdílné písmeno ve verzi, která je pro každého výrobce jiná. Někteří distributoři poté mylně nabízejí zařízení se zabezpečením dat, která ale nešifrují vlastní data (Pyrite místo Opal verze).

2.4.2 Návrh konkrétních testů

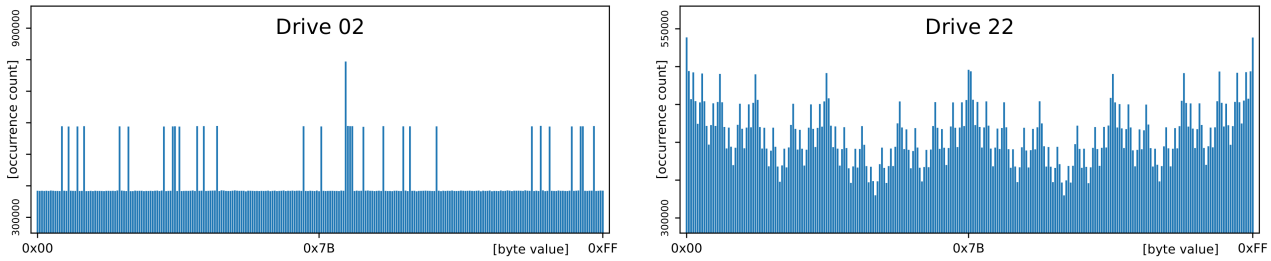
Naše testování proběhlo jen s použitím standardních protokolů, nepředpokládáme interní znalosti o firmware nebo použití technik reverse engineeringu. To umožňuje testy pustit v libovolném systému, jen s nutností vymazání dat. Po testování je zařízení ve stavu dodávaném výrobcem.
V této části jsme navrhli testy založené na reálném scénáři použití SED v Linux LUKS2 diskovém šifrování, které hardwarové šifrování podporuje od verze 2.7 (2024).
Testy zahrnují tyto oblasti:

- skenování vlastností implementovaných vlastností disků,
- analýzu RNG s pomocí exportované funkce *Random*,
- reset do stavu po dodání výrobce s pomocí PSID (kód na zařízení),
- základní nastavení administrátora a uživatele,
- konfigurace šifrované oblasti na disku (locking range),

- velikosti šifrovaných bloků vzhledem k velikosti sektoru disku,
- detekce vzorů po změně klíče.

2.4.3 Příklady nalezených problémů

Pro analýzu RNG jsme ze všech disků nasbírali 100 MB dat, které se vyhodnotili bateriemi pro testování náhodnosti (Dieharder, TestU01, NIST-STS). Z histogramu bytových hodnot je vidět, že některé RNG nemají očekávané vlastnosti. Příklady jsou uvedeny na Obrázku 4 a ukazují na nerovnoměrné zastoupení generovaných bajtů namísto očekávané uniformní distribuce.
Je vhodné poznamenat, že nemůžeme s jistotou říci, zda tento analyzovaný výstup (a tedy i snížená míra entropie) se používá i pro interní generovaní klíče. Ověření takového tvrzení by vyžadovalo analyzovat proprietární firmware disků, které nám v současné době nejsou dostupné.



Obrázek 4: Příklady histogramů vadných RNG z testování SED.

Dalším problémem je analýza vlastního šifrování dat. Všechny disky by měly používat AES se šifrovacím módem XTS. Protože disk nedává k dispozici přímý přístup k šifrovanému textu, použili jsme analýzu cíleně zapsaného vzoru v otevřeném textu s následným překlíčováním zašifrované oblasti. Pokud je šifrování implementováno správně, přečtená pseudonáhodná data by neměla obsahovat vzory. Některé disky správně po překlíčování vrací jen vymazanou oblast, zde tuto analýzu nelze provést. U ostatních disků jsme použili testy náhodnosti a v případě detekovaných problémů pak analyzovali konkrétní nalezený vzor. Ukázalo se, že několik disků zřejmě interně špatně používá inicializační vektor (tweak) pro mód XTS, případně používá větší bloky než jsou sektory disku. Příklad výstupu testování vzorů (zde s hashem obsahu po jednotlivých sektorech) je na Obrázku 5.

```
Initial setup of TPer complete on /dev/nvme1n1
@ Setup LR
@ [LR_START_SECTORS=32768, LR_LENGTH_SECTORS=20480]
LockingRange1 reKeyed
LockingRange1 starting block 32768 for 20480 blocks configured as unlocked range
LockingRange1 enabled ReadLocking,WriteLocking
LockingRange1 set to RW
Plaintext LR checksums
9f56cda75fefeab90f6fa5d5ddc9601544b121732c5ecccab32e631060453a5d  -
9f56cda75fefeab90f6fa5d5ddc9601544b121732c5ecccab32e631060453a5d  -
9f56cda75fefeab90f6fa5d5ddc9601544b121732c5ecccab32e631060453a5d  -
076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560  -
9f56cda75fefeab90f6fa5d5ddc9601544b121732c5ecccab32e631060453a5d  -
```

Obrázek 5: Příklad detekce opakovaného vzoru v blocích disku.

Některé z NVMe disků umožňují konfiguraci velikosti sektoru. Jedním z detekovaných problémů bylo, že tato změna se nepromítla do šifrovací části, což může způsobovat problémy při nastavení šifrované oblasti. Šifrovaná oblast tedy může být menší, nebo naopak větší, než oblast definovaná násobkem reálných sektorů.

2.4.4 Výběr SED

Popisované nástroje umožní uživatelům ověřit reálné vlastnosti zvoleného zařízení. Při tomto procesu je však nutné nutné zohlednit několik bodů:

1. Definice rizik (threat model) a posouzení, zda SED (HW šifrování) je vhodným řešením. Problémem mohou být například rizika spojené s proprietárním firmware (supply chain).
2. Výběr SED hardware s firmware, který poskytuje TCG Opal2 rozhraní.
3. Ověření požadovaných vlastností s pomocí *opal-toolset*, který zobrazí implementovaný interface. Lze tedy ověřit, že disk skutečně implementuje Opal nebo Pyrite rozhraní. Zároveň lze ověřit volitelné funkce, které mohou být kritické pro danou aplikaci (podpora single user módu, kryptograficky bezpečného mazání dat, apod.) Nástroj také zobrazí konkrétní verze firmware a sériová čísla, takže není potřeba používat další nástroje.
4. Spuštění sady testů z *opal-test-suite*. Některé testy vyžadují inicializaci zařízení do továrního nastavení a formát a zašifrování disku. Tyto operace jsou je nutné provést na zařízení bez dat (testy jsou pro uložená data destruktivní).
5. Vyhodnocení testů a kontrola firmware (výrobce stále dodává aktualizace; hardwarové šifrování je stále výrobcem podporováno). Pokud jakýkoliv test detekuje problém, který nelze opravit aktualizací firmwaru, je vhodné zvolit jiné řešení (například softwarové šifrování)

2.4.5 Další informace

Zdrojové kódy nástroje *opal-toolset* jsou dostupné v repositáři `https://github.com/crocs-muni/opal-toolset`. Související testovací skripty jsou pak dostupné v repositáři `https://github.com/crocs-muni/opal-test-suite`.

Nalezené problémy byly reportovány výrobcům. Výsledky byly zpracovány do článku zaslaném na recenzní řízení pro konferenci European Symposium on Security and Privacy (EuroS&P). Vzhledem k tomu, že informace aktivně využíváme i pro vývoj a podporu hardwarového šifrováni open-source projektu LUKS2, je velmi pravděpodobné, že informace budou nadále aktualizovány i po konci tohoto projektu.

3 Závěr

Veškeré plánované činnosti v rámci Etapy 16 byly úspěšně dokončeny a proběhla prezentace výsledků aplikačnímu garantovi v rámci čtyř setkání a workshopů (květen, červenec, říjen a prosinec 2024). V rámci Etapy 16 byly prováděny práce na čtyř různých nástrojích a jejich využití pro analýzu certifikačních reportů, vlastností kryptografických implementací útoků postranními kanály a analýzu disků s hardwarovým šifrováním.

Nástroj *sec-certs* nyní obsahuje možnost detekce změn v certifikátech dle schémat Common Criteria či FIPS140, zasílání reportů, porovnávání více položek mezi certifikovanými produkty a obsahuje rozšířené datové zdroje z národních schémat a pokročilé vyhledávání.

Nástroj *pyecsca* nyní poskytuje velmi rozsáhlou databázi možných implementací operací kryptografie eliptických křivek, reverzního inženýrství neznámých implementací s využitím postranních kanálů a rozsáhlou dokumentaci.

Nástroj *cooltest* poskytuje možnost snadného statistického testování náhodnosti generátoru dat se zvýšenou citlivostí a s použitelností i na relativně menší množství dat.

Nástroj *opal-test-suite* umožňuje snadné otestování kompatibility SED disku se specifikací Opal2 a detekci vybraných kryptografických zranitelností.

V navazujících etapách budeme pracovat na dokončení nástrojů dle konzultací s aplikačním garantem a odbornou veřejností a jejich propagaci.

Příloha: Analýza rizik

Tabulka 2: Analýza rizik relevantních k Etapě 16

Riziko	Možný dopad rizika	Skutečný dopad rizika	Datum rizika	Opatření pro minimalizaci/eliminaci
Nedostupnost zdrojového portálu commoncriteriaportal.org	Nedostupné zdrojové data pro analýzu	Chybějící nové aktualizace certifikátů	-	Ukládání dříve stažených dat, získávání dat ze stránek jednotlivých národních schémat.
Nedostatečný únik informace z postranního kanálu pro aplikace principů útoků nástroje pyecsca	Omezená možnost zjištění detailů blackbox implementace	Omezená možnost zjištění detailů blackbox implementace	-	V případě chybějícího dostatečného úniku informace nelze analýzu pyecsca použít. Stále lze využití databázi znalostí obsaženou v projektu a testovat analýzu na jiných zařízeních stejného výrobce s předpokládanou podobnou implementací.
Nedostatečný objem dat z výstupu náhodného generátoru	Nemožnost dostatečně průkazné detekce existující nenáhodnosti	Data se sníženou entropií jsou použita pro tvorbu citlivého kryptografického materiálu	-	Zajištění většího množství dat z cílového zařízení pro testování.
Odchod výzkumníka anebo vývojáře s hlubokou doménovou znalostí daného nástroje	Nemožnost pokračovat v dalším vývoji a údržbě nástroje	Omezení použitelnosti nástroje, postupné zastarávání	-	Detailní dokumentace nástroje, otevřené zdrojové kódy ve veřejném repositáři, dílčí redundance výzkumníků a vývojářů.