FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Tomáš Rabas
Student:	Jakub Kučera
Název práce:	Aktivní neinvazivní útok na mikrokontroler vkládáním poruch
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	10. června 2024

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Student si dle zadání:
1) nastudoval základy ne-invazivních fault-injection útoků na mikrokontroléry.
2) provedl rešerši vybraných existujících nástrojů na voltage glitching.
3) navrhl a implementoval voltage glitching útok pomocí FPGA pro kontrolu parametrů glitche a jednoduchého crowbar obvodu pro vkládání glitchů. Úspěšně naimplementoval i dle zadání volitelný clock glitching.
4) použil Cmod S7 vývojovou desku pro FPGA
5) provedl úspěšný útok na AVR mikrokontrolér s běžícím AES.

Všechny úkoly ze zadání byly tedy splněny.

2. Písemná část práce 85 / 100 (B)

Vyzdvihnutí:
1) Popis v implementace v kapitole 3 je velmi podrobný a dává detailní obrázek o platformě i bez studia samotného zdrojového kódu.
2) Student dodržuje citační etiku a převzaté věci řádně cituje. Své výsledky přehnaně nevyzdvihuje.

Drobné připomínky/návrhy ke zlepšení:
0) Kapitola 1.4 popisuje vybrané fault injection nástroje, v úvodu popisuje různé charakteristiky, kterými se často liší a zmiňuje i důvody, proč jsou tyto charakteristiky důležité. Na konci kapitoly práce poskytuje tabulku, která tyto charakteristiky pro každou platformu přehledně zobrazuje.
V tabulce jsem ale nenašel zahrnutou i vyvinutou platformu a její porovnání s ostatními. V

ideálním případě by tam mohlo být i slovní hodnocení, případně alespoň formou zvýraznění v tabulce, jak se vyvinuté platformě v těchto charakteristikách daří v porovnání s ostatními (čím je lepší, čím je horší).
1) zdroj s citací [30] navrhuje útoky pro všechny varianty AES-(128,192,256). Student si pro ukázku vybral a implementoval pouze AES-128. To je zcela v pořádku, v textu samotné práce by to ale mělo být přímo řečeno.
2) Útok na [30] mezi 8. a 9. MixColumns byl proveden jak pomocí vyvinuté platformy, tak pomocí ChipWhisperer-Nano, a oba výsledky jsou v práci popsány (kapitoly 5.3 pro platformu a 5.5 pro ChipWhisperer-Nano). Nabízelo by se použít a prezentovat výsledky na obou platformách i pro útok [30] mezi 7. a 8. Columns . V práci jsou ale popsány pouze výsledky pro implementaci útoku na platformě (kapitola 5.4) - to je škoda (nebylo to ale součástí zadání).
3) Nabízelo by se věnovat odstavec porovnání výsledků implementovaných útoků na platformě vs ChipWhisperer-Nano s nějakými závěry pro čtenáře, kdyby se například rozhodoval mezi použitím vyvinuté platformy a ChipWhisperer-Nano.
4) Obecně je práce trochu hůře čitelná, občas působí až příliš suše a technicky, bez doprovodných textů, které by fungovaly jako nit mezi jednotlivými kapitolami.
Jednotlivé kapitoly by si např. zasloužily delší úvody popisující vždy její význam pro práci jako takovou a její vztah ke kapitolám dalším.

3. Nepísemná část, přílohy 90 /100 (A)

V práci bylo použito hned několik technologií a programovacích jazyků, které student dokázal úspěšně propojit a odladit jejcih vzájemné napojení.
Jmenovitě student naprogramoval samotné FPGA na Cmod S7 (jedná se o Xilinx Spartan-7) v jazyce Verilog s nástrojem Vivado, vytvořil firmware microprocesoru v jazyce C kontrolující zmíněný hardware pomocí příkazů přes UART, a pak samotné rozhraní, které umožňuje uživateli kontrolovat glitch parametry a získat zpět výsledky přímo z připojeného počítače, naprogramovaný v jazyce Python.
Student oponentovi předvedl funkční verzi programů včetně použití platformy pro jeden z útoků na AES.
Jako přílohu k práci student vytvořil tutoriál v Jupyter Notebook, který umožňuje seznámení se uživatele s platformou pomocí ukázky části útoku na AES. Tutoriál byl v rámci práce (ale mimo zadání) vyzkoušen na jednom studentovi a na základě jeho zpětné vazby zdokonalen.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Platforma, jenž je stěžejní výsledek práce, lze použít jako nástroj pro výzkum v oblasti fault injection útoků a může také sloužit pro představení této problematiky například studentům v rámci některého z předmětů zaměřených na hardwarovou bezpečnost.
Zcela nové poznatky nebo rozšíření poznatků známých v oboru jsem v práci neshledal.

Celkové hodnocení 90 /100 (A)

Student odvedl velký kus práce při vytvoření platformy, zároveň prokázal její dobrou použitelnost při implementaci několika útoků na AES, které si musel nastudovat a naimplementovat. Samotný text práce vykazuje jisté stylistické nedostatky a jsou možnosti na jeho zlepšení i v jejím strukturování.
Při vytváření platformy ale prokázal student značné technické znalosti a dovednosti, a její

výstup je použitelný pro výzkum i výuku v této problematice.
Se závěrečnou prací jsem spokojen.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.