VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

PLATYPUS: ÚTOK NA POSTRANNÍ KANÁL

SEMESTRÁLNÍ PROJEKT
BEZPEČNÁ ZAŘÍZENÍ

AUTOR PRÁCE **JIŘÍ VÁCLAVIČ**

BRNO 2023

Abstrakt

Cílem této práce je rozšířit povědomí o Platypus útoku, který se řadí do kategorie útoků na postranní kanály. Bylo nutné nastudovat odborné práce týkající se tohoto tématu a na jejich základě vypracovat vypracovat tuto práci. Text je věnován základním a nejdůležitějším pojmům v rámci útoku Platypus, jejich vysvětlení a začlenění v rámci útoku. Jsou zde také zmíněny možné druhy obran.

Klíčová slova

Platypus, postranní kanály, Intel CPU, RAPL, SGX

Citace

VÁCLAVIČ, Jiří. *Platypus: Útok na postranní kanál*. Brno, 2023. Semestrální projekt Bezpečná zařízení. Vysoké učení technické v Brně, Fakulta informačních technologií.

Obsah

Kapitola 1

Úvod

Postranní kanály jsou často využívané pro útoky, které se zaměřují na změny v energii spotřebovávané zařízením během procesu extrakce kryptografických klíčů. Tyto útoky vyžadují fyzický přístup k zařízení a používají specializované nástroje jako jsou sondy a osciloskopy [1].

Nicméně, útok PLATYPUS je sofistikovaným softwarovým útokem, který umožňuje útočníkovi vzdáleně získat kryptografické klíče. Cílí zejména na Intelové procesory, které běží na serverech, desktopech a noteboocích. Tento útok využívá Running Average Power Limit rozhraní (RAPL), které poskytuje přesné údaje o spotřebě energie. Pokud se tento útok podaří, útočník může sledovat řízení aplikací, získat potřebná data a dokonce extrahovat kryptografické klíče [2].

Neprivilegovaný útočník může získat AES-NI klíče z Intel SGX a Linux jádra, prolomit náhodné uspořádání kernelového adresního prostoru (KASLR), zjistit tajné instrukční toky a vytvořit časově závislý skrytý kanál. Privilegovaný útočník cílí na mbed TLS[1], kde v případě úspěchu získá RSA klíče ze SGX enkláv. Společnost Intel donedávna považovala útok na postranní kanály SGX za nemožné, ale jak se ukázalo, tak jsou již v dnešní době velice reálné [2].

[1] mbed TLS je open-source kryptografická knihovna, která poskytuje zabezpečené spojení a šifrování pro různé aplikace, jako jsou webové servery, IoT zařízení, mobilní zařízení a další.

Kapitola 2

Průběh útoku na procesory Intel

Útok na postranní kanály je možný hlavně, protože elektrické obvody CMOS se řídí touto rovnicí, kde $P_{prepinani}$, je výkon potřebný během výpočtu k přepnutí bitu z 0 na 1 a naopak, P_{zkrat} je zkratový výkon a P_{ztrata} je ztrátový výkon, který se odvíjí od kvality materiálu obvodu [3].

$$P = (P_{prepinani}) + (P_{zkrat} + P_{ztrata})$$

Jelikož je v realitě $P_{prepinani}$ daleko větší než ostatní výkon, tak lze odvodit bity ve výpočtu na základě operací, které jsou nad nimi prováděny. Tedy je splněn předpoklad pro útok na postranní kanál.
Existují 3 hlavní techniky útoku na postranní kanály.

- Simple Power Analysis (SPA) představuje techniku, jejíž cílem je získat šifrovací klíč přímo z elektrické spotřeby měřeného zařízení. Podmínkou úspěšného provedení SA útoku je existence nějaké závislosti mezi elektrickou spotřebou a hodnotou šifrovacího klíče, ať už se jedná o přímou nebo nepřímou závislost [1].
- Differential Power Analysis (DPA) spočívá v statistické analýze velkého množství běhů s různými vstupními daty. Na rozdíl od analýzy celé časové osy jako je u Simple Power Analysis (SPA), DPA analyzuje, jak spotřeba energie závisí na zpracovávaných bitech v pevně stanovených časových okamžicích. DPA je výrazně výkonnější než SPA, protože dokáže detekovat i malé závislosti na datech za přítomnosti šumy [1].
- Correlation Power Analysis (CPA) je rozšířením DPA, které zjišťuje korelace mezi variacemi jednotlivých běhů [3].

U Platypus útoku je využit zejména DPA, který provádí jeho analýzu nad daty získanými pomocí Single-Stepping a Zero-Stepping techniky, jež jsou specifikovány níže.

2.1 Running Average Power Limit (RAPL)

Architektura procesorů Intel Sandy Bridge byla rozšířena o funkce pro řízení průměrného výkonu. Tyto funkce dynamicky upravují frekvenci procesoru tak, aby byl výkon maximalizován a zároveň se zajišťovalo, aby průměrný výkon zůstával v rámci konfigurovatelných limit. K tomuto účelu byl přidán mechanismus RAPL, který slouží k zajištění toho, aby procesor zůstával v požadovaných tepelných a výkonových limitech tak, že reportuje informace o spotřebě elektrické energie a řídí množství napětí či frekvenci jádra [4].

2.2 Intel Software Guard Extensions (SGX)

Intel SGX (Software Guard Extensions) je rozšíření instrukční sady, které umožňuje důvěrné provádění kódu v izolovaném paměťovém prostoru zvaném "enkláva". Enkláva je chráněna před přístupem ze strany ostatního softwaru, včetně operačního systému a dalších aplikací, a také před fyzickými útoky na hardwarové úrovni. V enklávě mohou být spuštěny kódy, které pracují s citlivými daty, jako jsou hesla, klíče nebo autentizační tokeny. Tyto data jsou uchovávána v paměti enklávy a chráněna pomocí šifrování. Kromě toho SGX poskytuje mechanismus pro ověření identity a integrity enklávy, aby bylo zajištěno, že se jedná o důvěryhodný prostor pro zpracování citlivých dat [3].

2.3 Neprivilegovaný přístup

Linuxový framework powercap, jehož původní účel je nastavení omezení výkonu, umožňuje neprivilegovaný přístup k technologii Intel RAPL. Tento přístup je realizován prostřednictvím souborového systému sysfs, kde lze číst obsah MSR registrů, tedy registrů z kategorie řídících, které slouží k řízení chodu procesoru a obsahují informace o spotřebě, teplotě a např. i aktuálním využitím CPU. Útočník může číst jednotlivé hodnoty ze souboru umístěného v adresáři /sys/devices/virtual/powercap [3].

2.4 Privilegovaný přístup

V oblasti jádra operačního systému je možné provádět spuštění nativního privilegovaného kódu, což umožňuje útočníkovi přímý přístup k registrům MSR technologie RAPL. Útočník v důsledku toho získá plnou kontrolu nad operačním systémem a tudíž také nad přístupem k paměti běžících aplikací. Může tedy získat RSA klíče[1], které jsou často jeho cílem [3].

2.5 Detaily útoku

Pro úspěšné rekonstruování signálu je nutné vzorkovat vysokou vzorkovací frekvenci, abychom získali dostatečné množství dat na časové ose.

Během útoku je měřena spotřeba provádění jednotlivých instrukcí v přesně určených časových intervalech, aby bylo možné provádět tato měření přesně nad pořád stejnými intervaly a instrukcemi a získat, tak relevatní data jsou využívány dvě techniky časování:

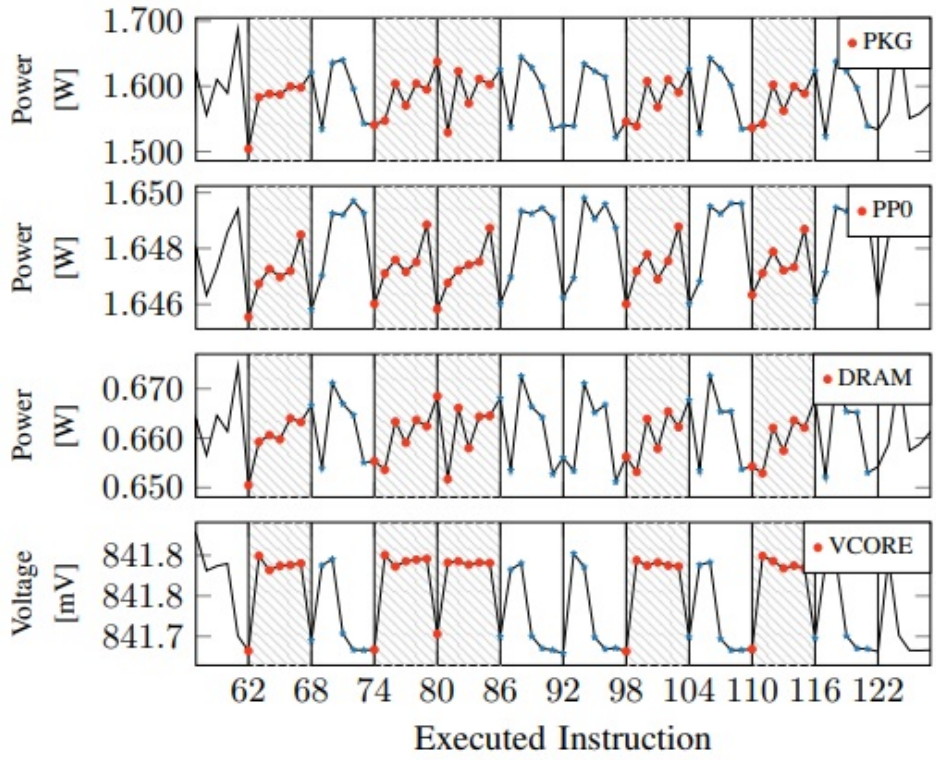
- Single-Stepping se zaměřuje na nastavení místního APIC časovače přerušení tak, že přerušení vznikne během vykonání první instrukce, která je spuštěna po zotavení po přerušení. Přerušení nastene ihned po provedení instrukce ERESUME[2], která slouží pro obnovení vykonávání instrukcí po přerušení. Pokud se Single-Stepping opakuje, tak je umožněno odděleně a postupně za sebou spuštět všechny instrukce a provádět nad nimi příslušná měření odběru elektrické energie. Lze také přeskočit instrukce, o které útočník nemá zájem a jsou pro jeho meření irelevantní.

[1] RSA je kryptografický algoritmus, který se používá k asymetrickému šifrování např. u autentizace, digitálních podpisů atd. V Intel procesorech jsou jeho kryptografické klíče většinou uloženy v enklávě (SGX), což jeden z nejvyšších stupňů obrany.

[2] ERESUME (Execution RESUME) je instrukce procesoru používaná v Intel SGX pro obnovení běhu enklávy po jeho pozastavení, ke kterému dojde například v případě detekce chyb.

- Zero-Stepping pokud je APIC časovač nastaven jako u Single-Stepping, tak první načtená instrukce po zotavení po přerušení je ta, ve které přerušení vzniklo. Tímto lze danou instrukci spouštět nekonečně mnohokrát než útočník naměří dostatečný počet vzorků.

Obvykle se tyto dvě techniky používají společně a to tak, že útočník posune čítač na instrukci, kterou chce měřit pomocí Single-Stepping. Následně danou instrukci vykonává cyklicky pořád dokola pomocí Zero-Stepping dokud nenasbírá dostatečné množství dat. Na obrázku 2.1 lze vidět rozdílný výkov výkonu a napětí pokud je instrukcí zpracován bit s hodnotou 1 nebo bit s hodnotou 0.



Obrázek 2.1: Výkon a napětí během provádění Single-Step a Zero-Step technik. Modrá znázorňuje bity s hodnotou 0 a červená bity s hodnotou 1.

2.6 Obrana

Neprivilegovanému útoku se dá jednoduše zabránit omezením práv přístupu k rozhraní RAPL neoprávněným uživatelům přes framework powercap. Linux tuto opravu kódu také v nedávné aktualizaci provedl, a proto by tento útok neměl být již hrozbou, pakliže je stáhnuta nejnovější aktualizace operačního systému. Obrana vůči privilegovanému útoku je skrze aktualizaci mikrokódu procesorů Intel, která zobraňuje jednoduché čtení údajů o spotřebě v registrech RAPL pomocí výše zmíněných Stepping technik [2].

Kapitola 3

Útok na procesory jiných značek

I když tato práce byla zejména zaměřena na útok na procesory Intel, je tento typ útoku realizovatelný i na architekturách procesorů jiných značek. Každé CPU je různě odolné vůči tomuto útoku, a proto vyžadují trochu odlišný přístup. Níže jsou zmíněny pouze ti největší zástupci, ale problémy se dále také mohou týkat například firem jako je Marvell, Ampere, Hygon atd [3].

3.1 AMD

AMD procesory od generace Zen obsahují také rozhraní RAPL. Dokonce je zde umožněno měření spotřeby energie pro jednotlivá jádra a tak nevzniká nadbytečný šum od ostatních jader. Největší nevýhodou pro útočníka je, že framework powercap nepodporuje AMD, takže je zapotřebí práv root, aby bylo umožněno čtění MSR registrů.

3.2 ARM

ARM mikrokontrolér obsahuje rozhraní Energy Probe, které je určeno pro sběr dat o spotřebě elektrické energie. Nejvetší nevýhodou pro útočníka je nutnost fyzického přístupu do zařízení. Rozhraní získává informace za pomocí voltmetru či jiných senzorů.

3.3 Nvidia

Procesory nejsou jediným zařízením, na které mohou být vedeny útoky, ale ohrozeny mohou být také celá individuální, komplexní zařízení. Například Nvidia uvedla na trh modul JetsonTX2, což je samostatné zařízení určené pro výpočetně náročné úlohy v oblastech jako jsou počítačové vidění, umělá inteligence a robotika, obsahuje mimo jiné i výkonné CPU a GPU. Toto zařízení však umožňuje čtení jeho elektrického proudu, napětí. Jeho využití je v autonomních vozidlech, dronech, robotech.

Kapitola 4

Shrnutí

V této práci byly představeno dělení typů útoků na postranní kanály. Byl zde podrobně popsán konkrétní útok Platypus, který využívá nově přidanou funkci Running Average Power Limit pro procesory Intel. V rámci popisu bylo vysvětleno provedení tohoto útoku v neprivilegovaném a privilegovaném režimu. Byly zde vysvětleny Stepping techniky, které slouží pro provedení úspěšného měření odběru elektrické energie jednotlivých instrukcí a bylo znázorněno, že lze pozorovat jasný rozdíl mezi tím, když do instrukce vstupuje bit s hodnotou 1 nebo 0. V reakci na útok byly uvedeny možnosti aktuální obrany. Nakonec byl probrán tento problém v kontextu jiných firem než-li Intel.

Literatura

[1] Hanáček, P. *Útoky na postranní kanály* [online]. Brno, Česká republika: VUT FIT, 2022 [cit. 2023-10-04]. Dostupné z: https://moodle.vut.cz/pluginfile.php/562095/mod_resource/content/1/BZA05_Postr_MNG.pdf.

[2] Ježek, D. *Útok Platypus: měření spotřeby jako postranní kanál k citlivým datům* [online]. Praha, Česká republika: root.cz, 2020 [cit. 2023-08-04]. DOI: 10.1145/3548606.3560682. Dostupné z: https://www.root.cz/clanky/utok-platypus-mereni-spotreby-jako-postranni-kanal-k-citlivym-datum/.

[3] Lipp, M. et al. *PLATYPUS: softwarebased power side-channel attacks on x86* [online]. San Francisco, CA, USA: IEEE Computer Society Press, 2021 [cit. 2023-10-04]. DOI: 10.1109/SP40001.2021.00063. Dostupné z: http://pure-oai.bham.ac.uk/ws/files/115385754/platypus.pdf.

[4] Liu, C. et al. *Frequency Throttling Side-Channel Attack* [online]. Los Angeles, CA, USA: Intel Corporation, 2022 [cit. 2023-09-04]. DOI: 10.1145/3548606.3560682. Dostupné z: https://dl.acm.org/doi/pdf/10.1145/3548606.3560682.