Analýza postranních kanálů (kryptoanalýza hardvérových zařízení)

J.Breier, M.Vančo, J.Ďaďo, M.Klement, J.Michelfeit, M.Moráček, J.Kusák, J.Hreško

Masarykova univerzita
Fakulta informatiky

6.5.2010

Klasifikace útoků na HW zařízení

- **dle vlivu útočníka na průběh výpočtu**
  - aktivní útoky
  - pasivní útoky

Klasifikace útoků na HW zařízení

- **dle vlivu útočníka na průběh výpočtu**
  - aktivní útoky
  - pasivní útoky
- **dle použitého rozhraní**
  - invazivní útoky
  - semi-invazivní útoky
  - neinvazivní útoky

Klasifikace útoků na HW zařízení

Pasivní a neinvazivní = Útoky analýzou postranních kanálů

Klasifikace útoků na HW zařízení

Pasivní a neinvazivní = Útoky analýzou postranních kanálů

- časová analýza (Timing attack)

Klasifikace útoků na HW zařízení

Pasivní a neinvazivní = Útoky analýzou postranních kanálů

- časová analýza (Timing attack)
- útoky odběrovou analýzou (Power analysis attacks)
  - jednoduchou analýzou spotřeby (Simple power analysis - SPA)
  - diferenciální analýzou spotřeby (Differential power analysis - DPA)

Klasifikace útoků na HW zařízení

Pasivní a neinvazivní = Útoky analýzou postranních kanálů

- časová analýza (Timing attack)
- útoky odběrovou analýzou (Power analysis attacks)
  - jednoduchou analýzou spotřeby (Simple power analysis - SPA)
  - diferenciální analýzou spotřeby (Differential power analysis - DPA)
- útoky elektromagnetickou analýzou (Electromagnetic analysis - EMA - méně časté)

Časové útoky I

Časové útoky

- jsou založeny na měření časů výpočtů operací
- tyto měření můžou vést k informaci o tajném klíči
- důkladným měřením času potřebného k vykonání operace s privátním klíčem, může útočník získat Diffie-Hellmanove exponenty, faktor RSA klíče nebo prolomit jiné kryptografické systémy
- jestli je zařízení zranitelné, útok je výpočetně jednoduchý a často vyžaduje pouze známý kryptogram

Časové útoky II

Časové útoky

- kryptosystémy sa často mírně liší v množství času potřebném ke zpracování různých vstupů
- mezi důvody těchto odlišností patří výkonové optimalizace kvůli vynechání nepotřebných operací, větvení a podmíněné příkazy, zásahy do RAM cache, procesorové instrukce, které běží v různém čase, a celá řada jiných příčin
- výkonostní charakteristiky obvykle závisí jak na šifrovacím klíči tak i na vstupu dat (např. prostý text nebo kryptogram).

Časové útoky – Modulární snížení kroků I

Modulární snížení kroků

- obvykle způsobí nejvíce časových změn při modulárním násobení operací

Čínská věta o zbytcích (CRT)

- je často používána pro optimalizaci operací RSA soukromého klíče
- (Y mod P) a (Y mod Q) jsou počítány jako první, kde Y je zpráva
- toto prvotní modulární snížení kroků může být zranitelné na načasování útoků

Časové útoky – Modulární snížení kroků II

Čínská věta o zbytcích (CRT)

- nejjednodušší útok je výběr hodnot Y, která jsou v blízkosti P nebo Q
- pak pomocí měření času operací zjistit, zda je získaná hodnota je větší nebo menší než je aktuální hodnota P nebo Q
- jestliže Y je menší než P, výpočet Y mod P nemá žádný vliv, zatímco pokud Y je větší než P, bude nutné odečíst od P Y alespoň jednou
- určité časové vlastnosti závisí na implementaci

Opatření proti časovým útokům

Časové útoky – obrana

Opatření proti časovým útokům

- přidání zpoždění
  - nejjednodušší způsob, jak zabránit časovým útokům, je zařídit, aby všechny operace trvaly přesně stejnou dobu

Časové útoky – obrana

Opatření proti časovým útokům

- přidání zpoždění
  - nejjednodušší způsob, jak zabránit časovým útokům, je zařídit, aby všechny operace trvaly přesně stejnou dobu
- vyrovnání časové náročnosti násobení a mocnění
  - čas, který zabere jednotce vykonání operací násobení a mocnění, by měl být nastaven na podobnou hodnotu

Časové útoky – obrana

Opatření proti časovým útokům

- přidání zpoždění
  - nejjednodušší způsob, jak zabránit časovým útokům, je zařídit, aby všechny operace trvaly přesně stejnou dobu
- vyrovnání časové náročnosti násobení a mocnění
  - čas, který zabere jednotce vykonání operací násobení a mocnění, by měl být nastaven na podobnou hodnotu
- vyhnutí se podmíněnému větvení

Útoky odběrovou analýzou - SPA I

Jednoduchá analýza spotřeby

- všeobecně založena na hledání vizuální reprezentace spotřeby energie na jednotku v průběhu šifrovací operace
- technika, která zahrnuje přímou interpretaci měření spotřeby elektrické energie v průběhu kryptografické operace
- zkoumá zachycené odběrové vzorky za účelem zjištění tajného klíče
- může přinést i informace o operacích zařízení
- dělíme ji na útoky
  - útoky vizuální inspekcí odběrových vzorek
  - šablonové útoky
  - kolizní útoky

Útoky odběrovou analýzou - SPA II

Jednoduchá analýza spotřeby

- útočník přímo pozoruje spotřebu energie systému
- hodnota spotřeby se mění v závislosti na právě vykonávané instrukci mikroprocesoru
- velké operace jako např. opakování DES, RSA operace atd. mohou být identifikovány, protože operace prováděné mikroprocesorem se mohou výrazně lišit v jednotlivých místech těchto velkých operací
- SPA analýza může být použita např. k prolomení RSA implementací odhalením rozdílů mezi násobícími a mocnícími operacemi
- podobně tak mnoho DES implementací má viditelné rozdíly mezi permutacemi a posuny a tím pádem může být prolomena za pomoci SPA

Útoky odběrovou analýzou - DPA I

Diferenciální analýza spotřeby

- útokům touto technikou se lze hůře bránit
- neskládají se jen z vizuální, ale také ze statistické analýzy, také obsahují statistické opravy chyb metod pro získání informací o klíči
- analýza se obvykle skládá ze dvou fází
  - sběr dat - vyžadují velký počet vzorků (kontrola zařízení)
  - analýza dat, která používá statistické funkce pro filtrování šumu pro získání dalších informací o procesech, které zařízení provádí
- vedle poměrně velkých změn spotřeby způsobených posloupností instrukcí, jsou zde také změny související s daty, se kterými se pracuje
- tyto rozdíly jsou obvykle menší a někdy jsou zastíněny chybami měření a šumem

Útoky odběrovou analýzou - DPA II

Diferenciální analýza spotřeby

- obvykle je nutná pouze znalost šifrovacího algoritmu
- je možné prolomit systém pomocí statistických funkcí, které jsou šité na míru cílového algoritmu
- vzhledem k tomu, že DPA automaticky vyhledává korelované oblasti ve spotřebě energie zařízení, mohou být útoky automatizovány i s malými či žádnými informacemi o implementaci cílového zařízení
- tento typ útoku patří mezi nejpopulárnější typy odberové analýzy
- hlavně z důvodu, že nevyžaduje detailní znalost napadnutého zařízení
- umí odhalit tajný klíč i v případech, kdy zachycené vzorky obsahují vysoký podíl šumu

Útoky odběrovou analýzou - DPA III

Diferenciální analýza spotřeby - všeobecná strategie útoku

- zvolení výsledku vykonávaného algoritmu
- měření spotřebované energie
- výpočet hypotetických mezivýsledků
- výpočet spotřebované energie z hypotetických mezivýsledků
- porovnání hypotetických hodnot se zachycenými vzorky

Útoky odběrovou analýzou – obrana

Útoky odběrovou analýzou – obrana

- vyhýbání se podmíněnému větvení a skrytým meziproduktům
  - maskuje mnoho SPA charakteristik
  - omezení IF klauzulí, výpočty pomocí elementárních operací (AND,OR,XOR)
  - zabraňuje všem druhům časových útoků na asymetrické šifry i vetšině útoků na základě odběru energie

Útoky odběrovou analýzou – obrana

- vyhýbání se podmíněnému větvení a skrytým meziproduktům
  - maskuje mnoho SPA charakteristik
  - omezení IF klauzulí, výpočty pomocí elementárních operací (AND,OR,XOR)
  - zabraňuje všem druhům časových útoků na asymetrické šifry i vetšině útoků na základě odběru energie
- vyrovnávání spotřeby energie
  - provádění nadbytečných operací nad falešnými elementy
  - konstantní spotřeba zabraňuje všem útokům na základě odběru energie

Útoky odběrovou analýzou – obrana

- vyhýbání se podmíněnému větvení a skrytým meziproduktům
  - maskuje mnoho SPA charakteristik
  - omezení IF klauzulí, výpočty pomocí elementárních operací (AND,OR,XOR)
  - zabraňuje všem druhům časových útoků na asymetrické šifry i vetšině útoků na základě odběru energie
- vyrovnávání spotřeby energie
  - provádění nadbytečných operací nad falešnými elementy
  - konstantní spotřeba zabraňuje všem útokům na základě odběru energie
- redukce velikosti signálu
  - použití kódu ke degradaci signálu
  - pouze ztíží útok

Útoky odběrovou analýzou – obrana

- vyhýbání se podmíněnému větvení a skrytým meziproduktům
  - maskuje mnoho SPA charakteristik
  - omezení IF klauzulí, výpočty pomocí elementárních operací (AND,OR,XOR)
  - zabraňuje všem druhům časových útoků na asymetrické šifry i vetšině útoků na základě odběru energie
- vyrovnávání spotřeby energie
  - provádění nadbytečných operací nad falešnými elementy
  - konstantní spotřeba zabraňuje všem útokům na základě odběru energie
- redukce velikosti signálu
  - použití kódu ke degradaci signálu
  - pouze ztíží útok
- přidání šumu
  - pouze zvyšuje počet vzorků potřebných pro útok
  - změna pořadí instrukcí, náhodné výpočty
  - potřeba balancovat trade-off

Diskuze

Diskuze

Děkuji za pozornost