Posudek vedoucího diplomové práce:

MARTIN HLAVÁČ: ÚTOKY POMOCÍ POSTRANNÍCH KANÁLŮ

Martin Hlaváč se ve své diplomové práci vypracované na Katedře algebry MFF UK zaměřil na útoky založené na předpokladu, že útočník má k dispozici postranní informaci o určitých dočasných proměnných existujících během výpočtu asymetrických kryptografických transformací. Zpracování takové informace úzce souvisí s takzvaným problémem skrytého čísla, který patří do oblasti teorie čísel a poprvé byl formulován právě pro účely kryptoanalýzy v roce 1996 (Boneh a Venkatesan). Martin Hlaváč samostatně nastudoval známé varianty tohoto problému a způsoby jejich řešení založené na využití algoritmických úloh na číselných mřížkách. V rámci nepublikované úvodní studie vybrané metody rovněž samostatně implementoval a porovnal jejich efektivitu s ohledem na výpočetní náročnost a nutnou míru postranní informace. Přitom si diplomant povšiml práce (Percival 2005) upozorňující na postranní kanál v rychlé vyrovnávací paměti (L1 cache) vícevláknových procesorů Intel Pentium (technologie hyper-threading). V této práci byl ukázán útok na RSA za předpokladu dostupnosti postranní informace získané analýzou rychlé vyrovnávací paměti uvedených procesorů. Po dohodě s vedoucím diplomové práce bylo další úsilí zaměřeno na ukázání toho, že obdobný útok je možné vést i proti implementacím schématu DSA.

Nejprve bylo nutné najít vhodnou formulaci problému skrytého čísla, na který by bylo možné úlohu útoku na DSA převést. Martin Hlaváč vyzkoušel existující přístupy a jejich přímé modifikace a ukázal, že bude nutné problém formulovat významně jinak. Tak vznikl rozšířený problém skrytého čísla, který lze stručně charakterizovat jako multidimensionální formu původního problému. Uvedená vícerozměrnost souvisí s formou, v jaké je postranní informace z vybraného typu kanálu k dispozici. Dále Martin Hlaváč navrhl, dokázal a prakticky ověřil metodu na řešení rozšířeného problému skrytého čísla. Jeho metoda účelně kombinuje obecné matematické principy se specifickými ideami přístupů vyvinutých pro řešení předchozích variant problému skrytého čísla.

Po formální analýze a praktickém ověření metody pro řešení rozšířeného problému skrytého čísla diplomant přistoupil k prověření existence uvedeného postranního kanálu a dostupnosti předpokládané postranní informace. Samostatně odladil implementaci jednoduchého měřicího programu, který hypotézu proveditelnosti útoku potvrdil.

Přínos předložené práce vidím jednak v novém teoretickém výsledku, jehož praktická uplatnitelnost byla úspěšně experimentálně ověřena, jednak v přesvědčivé demonstraci zranitelnosti vícevláknových procesorů se sdílenou rychlou vyrovnávací pamětí. Rozšířený problém skrytého čísla je kromě analýzy DSA možné spojit i s útoky postranními kanály na další běžná schémata asymetrické kryptografie, namátkou uveďme Diffieho-Hellmanův protokol dohody na klíči nebo El Gamalovu šifru. Kvalitu diplomanta vidím zejména ve schopnosti samostatně analyticky zpracovat předloženou úlohu a najít stabilní metodu pro její řešení. Při tom využívá kvalitní matematické základy, které dokáže rychle dle potřeby doplňovat o specifické partie. Je schopen kombinovat matematický a technický pohled na předmětnou problematiku.

Předloženou práci navrhuji uznat jako diplomovou a klasifikovat jako výbornou.

Tomáš Rosa, Ph.D.
vedoucí diplomové práce

25. 5. 2006