HARDWARE ACCELERATED SYSTEM FOR SECURING NETWORK TRAFFIC

Karel Koranda
Master Degree Programme (2), FIT BUT
E-mail: xkoran01@stud.fit.vutbr.cz

Supervised by: Libor Polčák
E-mail: ipolcak@fit.vutbr.cz

Abstract: This paper proposes the design of hardware acceleration of a security mechanism which ensures data integrity and confidentiality through encryption within the Lawful Interception System developed as a part of Sec6Net project. The design is following the principles of HW/SW codesign. It is based on existing library that implements commonly used SSH protocol. The proposed architecture aims on acceleration of performance heavy computation of SSH protocol, namely integrity assuring algorithm SHA-1 and encryption algorithm AES.

Keywords: HW/SW codesign, SSH acceleration, SHA-1, AES

1 ÚVOD

Se stále se zvyšující konektivitou uživatelů do sítě Internet jsou spojené především dva problémy. První problém se týká potřeby přenést přes počítačovou síť stále větší objemy dat, aby byla zajištěna dostupnost služeb v reálném čase připojeným uživatelům. Druhým problémem je pak narůstající počítačová kriminalita spojená s nedokonalým zabezpečením existujících systémů. Cílem potenciálního útočníka mohou být například citlivá data uživatelů přenášená po síti v otevřené podobě.

S výše zmíněnými problémy se potýká například systém pro zákonné odposlechy, jehož součástí je sonda, která zajišťuje odposlech komunikace osoby podezřelé z páchání kybernetické kriminality. Tato sonda je koncipována jako samostatné vestavěné zařízení, ze kterého jsou data následně přenášena počítačovou sítí. Protože se jedná o citlivá data, musí být zajištěna jejich důvěrnost a integrita. Cílový systém realizující odposlech musí pracovat na co nejvyšší rychlosti, aby byl záznam komunikace pro další zpracování úplný. Softwarové realizace zabezpečení tohoto přenosu by však na daném zařízení byly příliš pomalé, a proto je potřeba proces zabezpečení vhodně hardwarově akcelerovat.

2 CÍLOVÁ PLATFORMA A TECHNOLOGIE

Cílovou platformou, pro kterou je systém navrhován, je vestavěné zařízení nazývané mikrosonda [1]. Tato mikrosonda je schopná pracovat v sítích s maximální rychlostí přenosu 1 Gb/s. Hlavním výpočetním prvkem na mikrosondě je čip FPGA, v rámci jehož architektury je instancován nevýkonný softcore procesor MicroBlaze, na kterém pracuje OS Linux zajišťující softwarové prostředky pro řízení mikrosondy. V současné době neexistuje pro tuto platformu použitelné řešení, které by bylo schopné zajistit bezpečný přenos dat na požadované přenosové rychlosti 1 Gb/s.

3 PROTOKOL SSH

Při výběru metody zabezpečení přenosu dat z mikrosondy byl jako nejvhodnější vybrán [2] protokol SSH (RFC 4251). Tento protokol pracuje nad transportní vrstvou síťového modelu ISO/OSI. V rámci

standardu protokolu SSH je určeno použití několika kryptografických algoritmů pro šifrování dat, zajištění jejich autentizace a integrity.

Vzhledem k výpočetní náročnosti kryptografických operací, neexistenci výkonného procesoru na mikrosondě a požadavku na přenos zabezpečených dat při rychlostech dosahujících 1 Gb/s, je zapotřebí navrhnout vhodnou architekturu, která s využitím dostupných prostředků technologie FPGA urychlí kritické výpočetní operace. Současně není v rámci cílové technologie možné implementovat všechny podporované algoritmy protokolem SSH. Proto byly do akcelerované architektury zvoleny pouze algoritmy AES pro šifrování dat a SHA-1 pro zajištění integrity dat.

3.1 ALGORITMUS AES

Symetrický šifrovací algoritmus AES [3] byl standardizován americkou organizací NIST a v současné době je považován za jednu z nejbezpečnějších blokových šifer. AES zpracovává datové bloky o velikosti 128 bitů. Dle standardu umožňuje použití klíčů teoreticky libovolné délky, reálně se používají klíče o velikosti 128, 192 a 256 bitů. Princip šifrování tímto algoritmem spočívá v aplikaci rozličných aritmetických a logických operací na vstupující blok dat v několika kolech. Dnes je tento algoritmus běžně podporován v dostupných knihovnách implementujících protokol SSH.

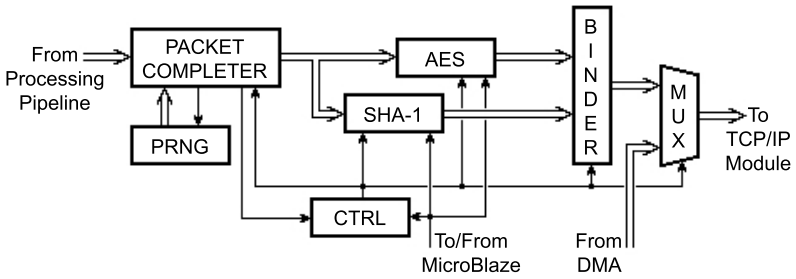
3.2 HASHOVACÍ FUNKCE SHA-1

SHA-1 (RFC 3174) je kryptografická hashovací funkce používaná pro zajištění integrity dat. Funkce pracuje s 512 bitovými bloky dat a jejím výstupem je hash těchto dat dlouhý 160 bitů. Výpočet trvá 80 kol, během kterých jsou na slova vstupního bloku aplikovány aritmetické a logické operace.

Bezpečnost této hashovací funkce již byla zpochybněna a jejím nástupcem jsou hashovací funkce SHA-2 a SHA-3. Použití funkce SHA-3 není v rámci protokolu SSH v současné době definováno. SHA-2 je sice podporována platnými standardy (RFC 6668), realita je však jiná a ne všechny dostupné knihovny implementující protokol SSH tento algoritmus podporují. Aby tedy byla zajištěna kompatibilita řešení s dalšími implementacemi protokolu SSH, byl pro účely této práce zvolen právě algoritmus SHA-1.

4 NAVRŽENÁ ARCHITEKTURA

Navržený systém se skládá ze dvou částí, softwarové a hardwarové. Softwarová část vychází z knihovny libssh2 [4], která implementuje protokol SSH a je dostupná pod licencí GNU LGPL. Protože algoritmy zajišťující zabezpečení budou převedeny do hardwarové části, činnost softwaru spočívá především v ustanovení spojení mezi mikrosondou a vzdáleným počítačem, dohodnutí klíčů vzniklé relace a jejich průběžné obnově. Hardwarová část systému je reprezentována akcelerační jednotkou provádějící zabezpečení přenášených dat v čipu FPGA. Schéma architektury této jednotky je možné shlédnout na obrázku 1.



Obrázek 1: Architektura navržené akcelerační jednotky.

Data, která budou systémem zabezpečena, přichází do hardwarové jednotky z procesní linky. Tato data jsou zapouzdřena hlavičkou protokolu SSH, je vypočtena jejich celková délka a provedeno zarovnání (jednotka PACKET COMPLETER) náhodnou výplní generovanou pseudonáhodným generátorem označeným jako PRNG. Výsledná zpráva protokolu SSH je šifrována v bloku AES paralelně s výpočtem jejího hashe blokem SHA-1. Vypočtený hash musí být přidán na konec šifrované zprávy, aby byla zpráva protokolu SSH kompletní. Toto zajišťuje komponenta BINDER.

Na obrázku 1 je vyznačena jednotka MUX, která reprezentuje multiplexor přepínající přenos dat ze softwaru a z hardwarové části. Výstup dále pokračuje do TCP/IP nebo jiného hardwarového modulu, který zajistí přenos po nižších vrstvách modelu ISO/OSI.

Komponenta CTRL je konečný automat řídící celý proces zabezpečení dat, především kvůli synchronizaci modulů AES a SHA-1 s ohledem na jejich různé doby výpočtu a možnou různou délku zabezpečované zprávy. Tato jednotka a bloky AES a SHA-1 jsou současně připojené na řídicí sběrnici procesoru MicroBlaze, přes kterou se provádí konfigurace těchto jednotek ze softwaru (např. nastavení platných kryptografických klíčů).

Aby softwarová a hardwarová část systému správně spolupracovaly, je potřeba zajistit důkladnou synchronizaci mezi procesorem MicroBlaze a dedikovanou jednotkou. K tomu je zapotřebí nejen úprav knihovny, ale také vytvoření ovladače pro použitý operační systém. Pečlivé zajištění synchronizace je nutné zejména kvůli tomu, že obě dvě části systému potřebují zasílat zprávy přes stejné síťové rozhraní a že v rámci existujícího spojení musí být zajištěno správné pořadí těchto zpráv.

5 ZÁVĚR

Součástí cílového vestavěného zařízení není výkonný výpočetní prvek, který by umožňoval zabezpečit přenos dat dosahující rychlosti 1 Gb/s softwarovým řešením. Proto je zapotřebí hardwarově akcelerovat výpočetně náročné operace, u zvoleného protokolu SSH se jedná o operace kryptografické. V rámci tohoto článku je představena architektura jednotky urychlující zabezpečení přenosu dat poskytované tímto protokolem. Výsledná jednotka bude reálně nasazena v rámci systému pro zákonné odposlechy.

PODĚKOVÁNÍ

Tato práce je součástí projektu VG20102015022 podporovaného MVČR. Tento příspěvek vznikl za podpory grantu FIT-S-11-1 a výzkumného záměru MSM 0021630528.

REFERENCE

[1] KOŘENEK, J., KORČEK, P., KOŠAŘ, V. ET AL. A New Embedded Platform for Rapid Development of Networking Applications. In *Proceedings of the 2012 Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2012)*. Austin, US: IEEE Computer Society, 2012. S. 81-82. ISBN 978-1-4503-1684-2.

[2] KAJAN, M., KORANDA, K. A POLČÁK, L. *Spolehlivá a zabezpečená komunikace v rámci systému pro zákonné odposlechy*. Brno, Česká republika: Fakulta informačních technologií, Vysoké učení technické v Brně, 2012. 26 s. Technická zpráva, FIT-TR-2012-007.

[3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. Announcing the ADVANCED ENCRYPTION STANDARD (AES). *Federal Information Processing Standards Publication*. Listopad 2001.

[4] *WWW stránky knihovny libssh2*. [online]. [cit. 1. března 2013]. Dostupné na: <http://www.libssh2.org>