HARDWARE ACCELERATED ENCRYPTION OF NETWORK COMMUNICATION

Jiří Novotňák
Master Degree Programme (2), FIT BUT
E-mail: xnovot87@stud.fit.vutbr.cz

Supervised by: Martin Žádník
E-mail: izadnik@fit.vutbr.cz

ABSTRACT

The aim of this paper is to design hardware accelerated encryption machine utilized to encrypt network communication at high bitrates. The implementation is targeted to CESNET's COMBO v2 cards containing FPGA chip Xilinx Virtex5. The encryption will be done using AES algorithm and the whole solution will be compatible with standard IPSec.

1 ÚVOD

Vzhledem ke stále zvyšujícímu se rozšíření počítačů a počítačových sítí ve světě spolu se zvyšující se snahou o zjednodušení jejich vzájemné komunikace bývá často za potřebí propojit 2 počítače či 2 sítě nacházející se v relativně velké vzdálenosti od sebe. Protože stavět fyzické propojení mezi těmito uzly by bylo neefektivní, bývá pro tento účel využita celosvětová počítačová síť Internet.

Jelikož se po síti často přenáší důvěrná data, jsme při využití takovéto sítě postaveni před problém zajistit důvěrnost komunikace a též autentizaci druhé strany. Utajení důvěrných dat je navíc citlivou otázkou nejen ve firemním prostředí, ale zejména orgánů státní zprávy. Zařízení schopné šifrovat přenášená data vysokou rychlostí může v tomto ohledu velmi vypomoci jak s bezpečností, tak s jednoduchostí přenosu důvěrných dat.

2 STANDARDY IPSEC A AES

Pro zabezpečení síťové komunikace existují v dnešní době různé standardy. Velmi používaný je standard IPSec, který zajišťuje zabezpečení na úrovni protokolu IP. Tento stadnard není spojen s konkrétním algorimem šifrování, ale umožňuje používat různé symetrické šifrovací algoritmy v závislosti na aktuální konfiguraci obou stran. [7]

Jedním s používaných algoritmů pro symetrické šifrování je algoritmus nazývaný AES (Advanced Encryption Standard), který byl standardizován organizací americkou NIST (National Institute of Standards and Technology) 26.listopadu 2001. AES je blokový symetrický šifrovací algoritmus, používající délku klíče 128, 192 nebo 256 bitů. Algoritmus pracuje s bloky o velikosti 128 bitů na které cyklicky aplikuje jednotlivé operace (přičtení klíče, posun v řádcích, substituce a promíchání ve sloupcích). Pro klíč o velikosti 128b se cyklus opakuje 10-krát,

pro 192b 12-krát a pr klíč o 256b 14-krát. [1] AES je dodnes standardem a je stále považován za bezpečný. Z tohoto důvodu jsem se rozhodl ve své implementaci použít tento algoritmus.

3 SOUČASNÁ SITUACE

Na trhu již existuje velké množství zařízení, zejména síťových routerů podporujících zpracování IPSec včetně šifrování na hardwarové úrovni. Jejich propustnost se pohybuje v řádech desítek Mb/s. Dále existují i vysokorychlostní řešení mající propustnost řádově stovky Mb/s až jednotky Gb/s. Některá řešení umožňují propojení několika zařízení pro zvýšení propustnosti. [2] [3]

Existující vysokorychlostní řešení jsou proprietární a velmi nákladné. Cílem mého projektu je tedy vytvořit šifrátor síťového provozu schopný pracovat s propustností 10Gb/s, který by byl otevřený a rozšiřitelný.

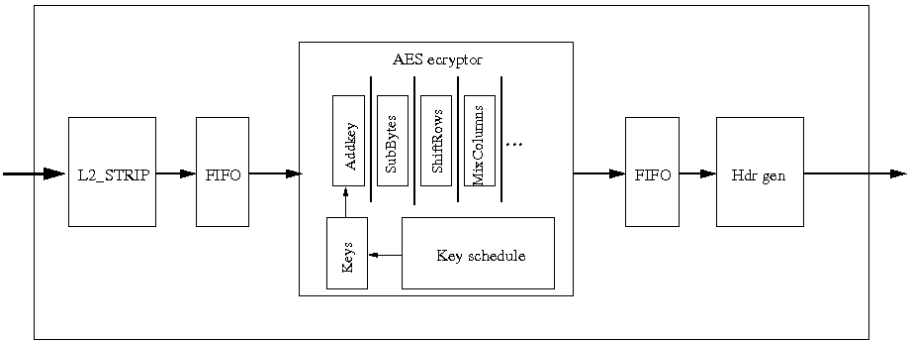
4 NÁVRH IMPLEMENTACE

Šifrování dat za pomoci software neumožňuje dosažení potřebné propustnosti. Experimentálně jsem zjistil, že například procesor Intel Pentium®s jádrem Core2 na frekvenci 2,17GHz je programem *mcrypt* schopný šifrovat algoritmem AES rychlostí asi 32MB/s (256Mb/s), což je velmi silně nedostačující i v případě vícejádrového řešení. Vzhledem k omezené propustnosti interních sběrnic je navíc nutné provádět v hardware všechny potřebné úkony pro vlastní přenos dat. Oproti softwarovému zpracování může zřetězná implementace v hardware dosahovat propustnosti až 128b/takt, tedy při 100MHz se jedná o propustnost 12,8Gb/s.

Cílovou platformou projektu je programovatlné hradlové pole FPGA Xilinx Virtex5 [6] umístěné na kartě COMBOv2-LXT s přídavnou kartou COMBOIO10G2 obsahující 2 porty s propustností 10Gb/s. Pro tyto karty je vyvinuta síťová platforma NetCOPE, umožňující napojení univerzálního designu na hardware konkrétní karty.

Výkonnostně kritické komponenty jsou umístěny v FPGA, zatímco úlohy nevyžadující vysoký výpočetní výkon jsou zpracovávány v software. Mezi takové patří zejména úvodní konfigurace a správa klíčů. Při této činnosti poskytuje hardware pouze nešifrované síťové rozhraní a programové vybavení obstará výměnu klíčů a nahrání klíče a konfigurace do hardware. Tam se nakonfigurují jednotlivé komponenty a zejména je spuštěn proces generování rundovních klíčů. Po dokončení této činnosti je design připraven k šifrování komunikace, která je odstartována příkazem ze software.

Během procesu šifrování jsou jednotlivé pakety zbaveny hlaviček L2 vrstvy. Následně jsou data zarovnána a uložena do vyrovnávací paměti FIFO ze které jsou odebírány komponentou pro šifrování. Po dokončení šifrovacího procesu jsou data opět uložena do paměti FIFO. Jsou vygenerovány nové hlavičky L3 (původní jsou zašifrované v datech) včetně hlaviček ESP, ke kterým jsou připojena zašifrovaná data. Takto vzniklý paket je opatřen hlavičkami L2 a odeslán síťovým rozhraním. Schéma celé architektury ilustruje obrázek 1. Dešifrování je prováděno analogicky.



Obrázek 1: Schéma architektury

5 ZÁVĚR

Šifrování přenášených dat na vysokých rychlostech vyžaduje hardwarovou akceleraci. V tomto článku jsem se snažil nastínit implementaci takohoto akcelerátoru postaveného dle standardu IPSec s využitím šifrovacího algoritmu AES. Celý produkt je v současnosti realizován s ohledem na co nejvyšší propustnost a modularitu pro možnost dalšího rozšíření.

PODĚKOVÁNÍ

Tato práce vznikla částečně za podpory grantu VUT FIT, FIT-S-10-1 a specifického výzkumu MSM0021630528.

REFERENCE

[1] National Institute of Standards and Technology: Advanced encryption standard [online], 2001 [cit. 1.3.2010], Dostupný z WWW <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[2] CipherOptics: CipherEngine Enforcement Point datasheed [online], 2009 [cit. 1.3.2010], Dostupný z WWW <http://www.cipheroptics.com/pdf/datasheet-cep1000.pdf>

[3] Cisco: Cisco IPsec and SSL VPN Solutions Portfolio [online], 2009 [cit. 1.3.2010], Dostupný z WWW <http://72.163.4.161/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_brochure09186a00801f0a72.pdf>

[4] CESNET: NetCOPE [online], [cit 1.3.2010], Dostupný z WWW <http://www.liberouter.org/netcope/index.php>, [cit. 1.3.2010],

[5] CESNET: Description of COMBO cards [online], [cit. 1.3.2010], Dostupný z WWW <http://www.liberouter.org/hardware.php?flag=2>

[6] Xilinx: Product Specification [online], 2009 [cit. 1.3.2010], Dostupný z WWW <http://www.xilinx.com/support/documentation/data_sheets/ds100.pdf>

[7] Kent S., Atkinson R.: Security Architecture for the Internet Protocol [online], 1998 [cit. 1.3.2010], Dostupný z WWW <http://www.ietf.org/rfc/rfc2401.txt>