VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Informace o obhajobě doktorské disertační práce

Ing. Tomáš Fukač z Ústavu počítačových systémů Fakulty informačních technologií ve středu 11.12.2024 úspěšně obhájil svoji disertační práci.

Studijní program: Výpočetní technika a informatika

Název práce: Vyhledávání vzorů založené na hash funkcích pro vysokorychlostní sítě/ Hash-Based Pattern Matching for High-Speed Networks

Abstrakt/Abstract:

Neustále se zvyšující rychlost síťových linek zvyšuje požadavky na výkonnost systémů zajišťujících zabezpečení a monitorování sítě, zejména Intrusion Detection System (IDS). Systémy IDS provádějí hloubkovou kontrolu paketů a detekují síťové hrozby pomocí sady pravidel obsahující velké množství vzorů. Vzhledem k vysoké výpočetní náročnosti musí systémy IDS využívat hardwarovou akceleraci, aby dosáhly propustnosti 100 Gb/s. Vyhledávání vzorů v síťovém provozu je výpočetně nejnáročnější částí zpracování paketů v IDS a bývá proto obvykle hardwarově akcelerováno. Současné hardwarové architektury však používají masivní replikaci pamětí a datových struktur a mohou podporovat pouze malé sady vzorů. Pro podporu velkých sad pravidel mohou rychlé aproximované pre-filtry předzpracovat síťový provoz a výrazně snížit zátěž na následující přesné vyhledávání vzorů realizovaní v softwaru nebo hardwaru. Tato práce se proto zabývá návrhem vysoce efektivní architektury pre-filtru založené na hashování, která nahrazuje složité vyhledávání vzorů podstatně jednodušším vyhledáváním krátkých řetězců. Pre-filtr provádí vyhledávání pomocí několika paralelních hashovacích funkcí a vhodně sdílené sady paměťových bloků uchovávajících krátké řetězce. Díky absenci replikace obsahu paměti jsou efektivně využívány hardwarové prostředky. Architektura dosahuje vysoké míry pre-filtrace, podporuje velké sady pravidel a její propustností je škálovatelnost na stovky Gb/s. Kromě toho práce dále představuje optimalizace zaměřené na zvyšování efektivity využití hardwarových zdrojů a ukazuje jejich přínos pro open-source systém akcelerující IDS Snort - Pigasus. Navržený koncept hardwarové architektury je navíc použit v hardwarově akcelerovaných zařízeních pro zabezpečení a monitorování sítí používaných Ministerstvem vnitra ČR a byl také komercializována firmou BrnoLogic./ Constantly increasing speeds of network links push up requirements on the performance of network security and monitoring systems, especially intrusion detection systems (IDSes). IDSes perform deep packet inspection and detect network threats using a ruleset with many signatures. Due to high computation complexity, IDSes must use hardware acceleration to achieve wire-speed 100 Gbps throughput. Pattern matching - the most computationally intensive part of packet processing in an IDS - is usually accelerated in

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Božetěchova 2, 612 00 Brno
tel.: +420-5-4114 1139, fax: +420-5-4114 1270, http://www.fit.vut.cz

Informace o obhajobě doktorské disertační práce

hardware. However, current hardware architectures use massive replication of memories and data structures and can support only small sets of signatures. To support large rulesets, fast approximate pre-filters can sift the network traffic and significantly decrease the load of further exact signature matching in software or hardware. Therefore, this thesis deals with designing a highly efficient hash-based pre-filtration architecture that replaces the complex signature matching with a significantly simpler short string matching. The pre-filter performs the matching by several parallel hash functions and a suitably shared set of memory blocks storing short strings. Due to the lack of memory replication, hardware resources are efficiently utilized. The architecture achieves a high level of pre-filtration, supports large sets of signatures, and its throughput is scalable to hundreds of Gbps. In addition, the thesis further presents optimizations focused on efficient hardware resources utilization and shows their benefits for an open-source IDS Snort acceleration system, Pigasus. Moreover, the proposed concept of hardware architecture is used in hardware accelerated network security and monitoring devices used by the Ministry of the Interior of the Czech Republic and has been commercialized by BrnoLogic company.

Školitel: doc. Ing. Jan Kořenek, Ph.D., FIT VUT, Česká republika

Oponenti: doc. RNDr. Zdeněk Matěj, Ph.D., FI MU, Česká republika

prof. Salvatore Pontarelli, Sapienza Università di Roma, Italská republika