



Záverečná karta projektu

Názov projektu

Evidenčné číslo projektu

APVV-0008-10

Modelovanie, simulácia a implementácia architektúr vysokopriepustných nástrojov sieťovej bezpečnosti s podporou GPGPU

Zodpovedný riešiteľ **prof. Ing. Liberios Vokorokos, PhD.**

Príjemca **Fakulta elektrotechniky a informatiky TUKE**

Názov pracoviska, na ktorom bol projekt riešený

1. Fakulta elektrotechniky a informatiky TUKE
- 2.
- 3.
- 4.
- 5.

Názov a štát zahraničného pracoviska, ktoré spolupracovalo pri riešení

- 1.
- 2.
- 3.

Udelené patenty/podané patentové prihlášky, vynálezy alebo úžitkové vzory, ktoré sú výsledkami projektu

- 1.
- 2.
- 3.

Najvýznamnejšie publikácie (knihy, články, prednášky, správy a pod.) zhrňujúce výsledky projektu – uveďte aj publikácie prijaté do tlače

1. VOKOROKOS, Liberios et al.: A Distributed Network Intrusion Detection System Architecture Based on Computer Stations Using GPGPU / - 2013. In: INES 2013 : IEEE 17th International Conference on Intelligent Engineering Systems : proceedings : June 19-21, 2013, Costa Rica. - Budapest : IEEE, 2013 P. 323-326. - ISBN 978-1-4799-0828-8
2. MIHÁLYI, Daniel - NOVITZKÁ, Valerie: Towards the Knowledge in Coalgebraic model of IDS / - 2014. In: Computing and Informatics. Roč. 33, č. 1 (2014), s. 61-78. - ISSN 1335-9150 (Current Contents)
3. BACULÍKOVÁ, Blanka - DŽURINA, Jozef: On certain inequalities and their applications in the oscillation theory / - 2013. In: Advances in Difference Equations. P. 1-8. - ISSN 1687-

1847 (Current Contents)

4. VOKOROKOS, Liberios – BALÁŽ, Anton – MADOŠ, Branislav: Intrusion Detection Architecture Utilizing Graphics Processors/ - 2012. In: Acta Informatica Pragensia, Vol. 1, No. 1 (2012), p. 50-59. – ISSN 1805-4951

5. TOMÁŠEK, Martin: Security Properties Verification of Security Protocols / - 2014. In: Acta Electrotechnica et Informatica. Roč. 14, č. 2 (2014), s. 15-18. - ISSN 1338-3957

Uplatnenie výsledkov projektu

Najvýznamnejšími výsledkami projektu sú nové architektúry sieťových systémov na detekciu prienikov s podporou GPGPU a najmä ich formálne a simulačné modely, ktoré boli verifikované a validované pomocou formálnych techník a experimentov. Modely budú uplatnené v ďalšom výskume a vývoji v oblasti bezpečnosti počítačových systémov a sietí, ktorý smeruje k návrhu spoľahlivejších, výkonnejších a bezpečnejších riešení. Implementačné softvérové výstupy budú využité pre potreby vzdelávania a výskumu v rámci doktorandského štúdia.

CHARAKTERISTIKA VÝSLEDKOV

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v slovenskom jazyku (max. 20 riadkov)

Hlavným cieľom projektu bol návrh modelu, simulácia a implementácia univerzálneho systému detekcie prienikov s podporou GPGPU a jeho experimentálne overenie vo vysokorýchlostnej sieti. Na základe analýzy architektúr NIDS systémov a bezpečnostných špecifik vysokorýchlostných sietí boli identifikované možnosti využitia GPGPU v NIDS. Pomocou koalgebry bol zostavený formálny model IDS a zvolené boli vhodné formálne metódy pre verifikáciu a validáciu takýchto modelov. Navrhnutých bolo viacero modelov architektúr IDS, ktoré boli následne simulované. Ďalší výskum sa sústredil na trojvrstvový model architektúry NIDS pozostávajúci z mentora a niekoľkých elementárnych NIDS staníc využívajúcich GPU. Tento model bol implementovaný a testovaný v reálnej prevádzke vo viacerých konfiguráciách, pričom boli porovnávané parametre priepustnosti, zaťaženia systémových zdrojov a presnosti detekcie. Najdôležitejšími výsledkami projektu sú formálne a simulačné modely architektúr NIDS, ktoré boli verifikované a validované pomocou formálnych techník a experimentov. Aplikačným výstupom projektu je softvérový nástroj FEIIDS-GPU, ktorý obsahuje vyvinuté komponenty NIDS. Výsledky projektu boli publikované v 9 karentovaných časopisoch, 32 recenzovaných periodikách a 75 nerecenzovaných periodikách a zborníkoch, pričom získali 25 SCI citácií v zahraničných publikáciách.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v anglickom jazyku (max. 20 riadkov)

The main project goal was a model design, simulation and implementation of general-purpose GPGPU-enabled intrusion detection system and its experimental verification in high-speed network. Potential usage of GPGPU in NIDS was identified based on the analysis of NIDS architectures and security features of high-speed networks. A formal model of IDS was designed using coalgebras and appropriate formal methods have been selected for verification and validation of such models. Several models of IDS architecture have been proposed and simulated subsequently. Further research was focused on the three-tier NIDS architecture model consisting of a mentor and several elementary NIDS stations using GPU. This model was implemented and tested in real conditions using multiple configurations while the parameters like throughput, system resource load and accuracy of detection were compared. The most important project results are both formal and simulation models of NIDS architectures that have been verified and validated using formal techniques and experiments. Application output of the project is the FEIIDS-GPU software tool containing components of developed NIDS. The project results were published in 9 CC journals, 32 peer-reviewed journals and 75 non-reviewed journals and proceedings, gaining 25 foreign SCI citations.

Svojím podpisom potvrdzujem, že údaje uvedené v záverečnej karte sú pravdivé a úplné a súhlasím s ich zverejnením.

Zodpovedný riešiteľ

prof. Ing. Liberios Vokorokos, PhD.

V Košiciach 24.11.2014

Štatutárny zástupca príjemcu

Dr.h.c. prof. Ing. Anton Čižmár, CSc.

V Košiciach

.....
podpis zodpovedného riešiteľa

.....
podpis štatutárneho zástupcu príjemcu