APVV
Agentúra na podporu výskumu a vývoja
Mýtna 23, P.O.BOX 346, 814 99 Bratislava

Formulár ZK - Záverečná karta projektu

Riešiteľ: prof. Ing. Liberios Vokorokos, PhD.	**Evidenčné číslo projektu:** APVV-0073-07
Názov projektu: Metódy identifikácie a analýzy bezpečnostných ohrození v architektúrach distribuovaných počítačových systémov a dynamických sietí.	

Na ktorých pracoviskách bol projekt riešený:	Fakulta elektrotechniky a informatiky TUKE
Ktoré zahraničné pracoviská spolupracovali pri riešení (názov, štát):	

Udelené patenty alebo podané patentové prihlášky, vynálezy alebo úžitkové vzory vychádzajúce z výsledkov projektu:	
Publikácie (knihy, články, prednášky, správy a pod.) zhrňujúce výsledky projektu (uveďte i publikácie prijaté do tlače): ***Uvádzajte maximálne päť najvýznamnejších publikácií.***	VOKOROKOS, Liberios - BALÁŽ, Anton: Architecture of Computer Intrusion Detection Based on Partially Ordered Events. In: Petri Nets: Applications. Vukovar: In-Tech, 2010, pp 13-28. ISBN 978-953-307-047-6. *(kapitola v zahraničnej monografii, 1,1 AH)*
	VOKOROKOS, Liberios – BALÁŽ, Anton – CHOVANEC, Martin: Distributed Detection System of Security Intrusions Based on Partially Ordered Events and Patterns, In: Towards Intelligent Engineering and Information Technology. Series: Studies in Computational Intelligence, Vol. 243, Budapest, September 1-2, 2009, Berlin, Springer, 2009, pp. 389-404. ISBN 978-3-642-03736-8.
	VOKOROKOS, Liberios - BALÁŽ, Anton - MADOŠ, Branislav: Anomaly and Misuse Intrusions Variability Detection. In: Acta Electrotechnica et Informatica, Vol. 10, No. 4 (2010), Košice 2010, pp. 5-9, ISSN 1335-8243.
	VOKOROKOS, Liberios - BALÁŽ, Anton: Host-based Intrusion Detection System, In: INES 2010: IEEE 14th International Conference on Intelligent Engineering Systems, May 5-7, 2010, Las Palmas of Grand Canaria, Spain [CD-ROM]. Budapest: IEEE, 2010, pp. 43-47, ISBN 978-1-4244-7651-0.
	VOKOROKOS, Liberios - ÁDÁM, Norbert - BALÁŽ, Anton - PERHÁČ, Ján: High-Performance Intrusion Detection System for Security Threats Identification in Computer Networks. In: Computer Science and Technology Research Survey. Košice: TU, 2009. s. 54-61. ISBN 978-80-8086-131-5.
V čom vidíte uplatnenie výsledkov projektu:	Verifikované a validované modely sieťových útokov sú dôležitým predpokladom pre modelovanie a simuláciu v procese identifikácie, analýzy, návrhu, testovania a hodnotenia bezpečnosti architektúr distribuovaných počítačových systémov a dynamických sietí. Vyvinuté modely a softvérový nástroj vytvárajú komplexnú platformu umožňujúcu modelovanie, simuláciu a detekciu narušení na sieťovej vrstve ISO/OSI modelu. Výsledky je možné využiť v základnom i aplikovanom výskume pre potreby rozličných simulácií ako aj priamo pri vývoji systémov detekcie a prevencie narušenia. V konečnom dôsledku výsledky projektu môžu prispieť k vývoju spoľahlivejších a bezpečnejších informačných a komunikačných systémov.

APVV

Agentúra na podporu výskumu a vývoja
Mýtna 23, P.O.BOX 346, 814 99 Bratislava

Charakteristika výsledkov

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu (max. 20 riadkov) - slovensky:

Projekt bol zameraný na návrh metód identifikácie a analýzy bezpečnostných ohrození v architektúrach distribuovaných systémov a dynamických počítačových sietí. Stanovené boli dva hlavné ciele:

1. Návrh formálnej špecifikácie, verifikácia a validácia modelov sieťových útokov na sieťovej vrstve bezpečnostných architektúr distribuovaných výpočtových systémov a dynamických počítačových sietí.
2. Vytvorenie komplexnej softvérovej platformy na modelovanie a simuláciu sieťových útokov na sieťovej vrstve ISO/OSI modelu.

Na základe analýzy a klasifikácie podstaty znakov prienikov bola navrhnutá abstraktná klasifikačná hierarchia a formálny aparát pre popis bezpečnostných prienikov do architektúr distribuovaných systémov. Navrhnuté modely útokov boli verifikované a validované využitím automatizovaných metód a následne využité pri simuláciách a experimentoch.

V rámci projektu bola vyvinutá softvérová platforma s názvom FEIIDS umožňujúca modelovanie a simuláciu sieťových útokov na sieťovej vrstve ISO/OSI modelu a tiež simuláciu detekcie narušenia. Systém podporuje modelovanie pomocou farbených Petriho sietí a detekciu prienikov na báze čiastočne usporiadaných udalostí a vzorov. V súčasnej verzii je možné produkt využívať pre podporu návrhu systémov detekcie a prevencie narušenia.

V súvislosti s riešením stanovených úloh a dosahovaním cieľov projektu vznikli výstupy v kategóriách: publikácie, aplikované výstupy, výstupy do vzdelávania a popularizácie vedy, ostatné výstupy a pridaná hodnota, a to v nasledujúcej štruktúre: 2 práce v zahraničných karentovaných časopisoch, 11 prác v recenzovaných časopisoch, 36 článkov v nerecenzovaných časopisoch a zborníkoch, 1 monografia, 1 knižná publikácia, 3 zborníky z konferencií v elektronickej podobe, 1 softvérový produkt, 15 školených doktorandov, 21 obhájených diplomových prác, 2 vzdelávacie kurzy, 111 účastníkov vzdelávania, 2 popularizačné články, 3 zorganizované konferencie, 1 workshop a 3 vyvolané projekty.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu (max. 20 riadkov) - anglicky:

The project was focused on method design for analysis and identification of security threats in distributed system architectures and dynamic computer networks. The two main objectives were set:

1. A design of formal specification, verification and validation of network attack models at the network layer of distributed computing systems and dynamic networks security architectures.
2. A complex software platform for modelling and simulation of network attacks at the network layer of ISO/OSI model.

Based on the analysis and classification of intrusion patterns principles, the abstract classification hierarchy and the formal apparatus for description of security intrusions into distributed system architectures were developed. Proposed attack models were verified and validated using automated methods and then used for simulations and experiments.

Within the project a software platform called FEIIDS was developed that enables modelling and simulation of network attacks at the network layer of ISO/OSI model and simulation of intrusion detection as well. The system supports modelling using coloured Petri nets and intrusion detection based on partially ordered events and patterns. The current version of the product can be used for the intrusion detection and intrusion prevention systems design support.

In relation to the project tasks solving and goals achievement, the outcomes aroused in the following categories: publications, applied outcomes, outcomes to the education and popularization of science, other outcomes and value added outcomes in the following structure: 2 foreign current content articles, 11 articles in peer-reviewed journals, 36 articles in non-reviewed journals and proceedings, 1 monograph, 1 book publication, 3 conference proceedings in electronic form, 1 software product, 15 doctoral students trained, 21 master thesis defended, 2 educational courses, 111 trainees, 2 promotional articles, 3 conferences organized, 1 workshop and 3 induced projects.

Podpisom záverečnej karty riešiteľ vyjadruje svoj súhlas so zverejnením údajov v nej uvedených.

Podpis zodp. riešiteľa: ..... **Dátum: 25.1.2011.....**

Podpis štatutárneho zástupcu: ..... **Pečiatka:**