

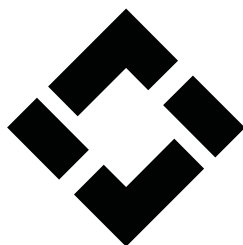
Univerzita obrany
www.unob.cz



Veletrhy Brno, a.s.
www.bvv.cz

PŘEDBĚŽNÁ INFORMACE

o konferenci



Security and Protection of Information 2009

která proběhne pod záštitou
bezpečnostního ředitele Ministerstva obrany České republiky

5. – 7. května 2009

jako součást sady konferencí CATE
(Community – Army – Technology – Environment)

v rámci doprovodného programu
10. mezinárodního veletrhu obranné a bezpečnostní techniky
a speciálních informačních systémů IDET

webové stránky konference: **www.unob.cz/spi**

Majitelé předplatitelské karty DSM - 1000 Kč sleva
(netýká se zvláštní sazby pro státní správu a školství)

Přednášky na konferenci

Tutoriály

Dobromir Todorov: Security for Unified Communications

Předmětem tutoriálu je bezpečnost Unified Communications (UC). Budou vysvětlena specifika identifikace a autentizace ve světě UC, ochrany systémů pro okamžitou komunikaci (instant messaging), bezpečnosti signalizace a také zabezpečení cest přenášejících hlasová a obrazová data.

Autor pracuje v Londýně jako Unified Communications Architect u společnosti BT Global Services. Jeho kniha *Mechanics of User Identification and Authentication* nabízí zasvěcený pohled na technické a bezpečnostní aspekty správy identit.

Anne-Marie Eklund Lowinder: DNSSEC the .SE way: Overview, deployment and lessons learned

DNS typicky přiřazuje jménu počítače IP adresu. Pokud by byl kompromitován, a takové případy se staly, uživatel by nedokázal odlišit, zda je opravdu připojen k požadovanému stroji či nikoliv. DNSSEC definuje do systému DNS nové záznamy, které kryptograficky zajišťují integritu dat poskytovanou DNS serverem a dá se očekávat, že na tuto technologii budeme i v České republice od letošního roku přecházet. Bylo by omylem si ale myslet, že tím je bezpečnost DNS definitivně vyřešena; je pouze zvýšena a přichází problémy jiné.

Autorka pracuje ve švédské společnosti .SE. Problému bezpečnosti DNS se věnuje od roku 2005 a během let získala nepřehledné množství konkrétních zkušeností při řešení DNSSEC v rámci Švédska.

Richard Clayton: Searching for evil, and what we find

Internetové zločince lze zhruba rozdělit na ty, co si nepřejí, aby byl jejich web nalezen vyhledávacími nástroji (roboty), neboť organizují phishing apod., a na ty, kteří právě naopak chtějí, aby byli na Internetu co nejvíce viditelní (například vnucují reklamu). V příspěvku budou analyzovány obě kategorie internetových zločinců a vysvětleny způsoby, jak jim jejich zločinnou činnost znemožňovat.

Autor je světovým expertem v oblasti anonymity a trasovatelnosti zdrojů toků zpráv na Internetu. Je rovněž spoluautorem loňské zprávy sdružení ENISA "Security Economics and the Internal Market", ze které vyplynula řada doporučení pro EU a její členské státy.

Zvaní řečníci

Lorenz Müller: A system to assure authentication and transaction security

Bezpečnost transakcí prováděných pomocí Internetu je dnes ohrožena novým typem počítačové kriminality (Man-in-the-middle, Man-In-The-Browser, Malicious Software). Autentizace koncového uživatele pomocí technologie SSL/TLS již není pro transakce e-businessu postačující ochranou. Příspěvek ukazuje, jak i za těchto podmínek vytvořit mezi dvěma partnery v rámci e-businessu bezpečný kanál.

Autor je spoluzakladatelem švýcarské společnosti of AXSionics AG, v níž nyní zastává funkci Chief Technology Officer. Je mezinárodně uznávaným expertem na poli kryptografie, počítačové bezpečnosti a biometrie, kde získal několik patentů, cen a ocenění.

Petr Švenda: Cryptographic Protocols in Wireless Sensor Networks

Autor je odborným pracovníkem Katedry počítačových systémů a komunikací Fakulty informatiky Masarykovy univerzity v Brně. Přednáší problematiku počítačové bezpečnosti a kryptografie a je respektovaným odborníkem i v zahraničí.

Příspěvek je věnován bezpečnostním aspektům sítí bezdrátových senzorů. Tato technologie, která vznikla v oblasti vojenství a dnes se stále více používá i ve zdravotnictví, zemědělství, průmyslu atd., se dnes stává i předmětem nebezpečných útoků. Cílem příspěvku je tyto útoky popsat a vysvětlit některé způsoby obrany proti nim (ochrana klíčů, bezpečné směrování atd.).

Abstrakta

Byla schválena abstrakta příspěvků na tato témata:

- Flow-Based Security Awareness Framework for High-Speed Networks
- Measuring of the Time Consumption of the WLAN's Security Functions
- Experiences with Massive PKI Deployment and Usage
- Possibility of Use Position Information as Part of User Authentication
- Safeguard your Data wherever it Resides
- Security Analysis of the New Microsoft MAC Solution
- Trusted Security Network
- Adaptive Authentication Approach to the Governmental Portals
- Processes Improvement Towards the Information Security
- System Engineering on the way to Information Superiority
- Validation of the Network-based Dictionary Attack Detection
- Video CAPTCHAs

V současnosti se texty příspěvků nalézají ve stádiu finálního zpracování, bližší informace budou postupně uváděny na webu konference.

<http://www.unob.cz/spi>