



**Projekt Výzkum, Vývoj, Vysočina  
spolu s katedrou elektrotechniky a informatiky Vás zvou na**

**Seminář pro studenty**

## **Kryptografie a síťová bezpečnost**

**přednáší Ing. Tomáš Vaněk, Ph.D. (ČVUT Praha)**

Seminář je členěn na pět částí, které se uskuteční od 11.10.2012 vždy ve čtvrtek od 17:50 do 20:20 v posluchárně P4

**Seminář bude mít tyto části:**

### **1) Moderní symetrické a asymetrické kryptosystémy – 11.10.2012**

Tématem semináře jsou moderní symetrické a asymetrické šifrovací algoritmy. Kromě symetrických blokových šifer (AES, Camelia) budou probírány i vybrané proudové šifry (A5, RC4 a algoritmy z projektu E-Stream). Součástí semináře bude demonstrace plně funkční repliky historického šifrovacího stroje Enigma, která vznikla jako diplomová práce na ČVUT.

### **2) PKI - Public Key Infrastructure – 18.10.2012**

Hlavním tématem semináře bude problematika elektronického podpisu, certifikátů X.509 a PGP, certifikačních autorit, časových razítek. Součástí semináře bude i praktická ukázka, jak si jednoduše pořídit certifikát k podepisování elektronické pošty.

### **3) Zabezpečení datových sítí – 25.10.2012**

Seminář je věnován problematice zabezpečení v lokálních sítích (IEEE 802.3 - Ethernet, IEEE 802.11 - Wifi, případně i IEEE 802.15 - Bluetooth a IEEE 802.16 WiMAX) z pohledu zajištění integrity, utajení a autentizace komunikujících stran. Součástí semináře bude demonstrace inteligentní rušičky v pásmu 2,4 GHz sestavené v rámci diplomové práce na katedře telekomunikační techniky.

### **4) Zabezpečení mobilních sítí a VoIP komunikace – 1.11.2012**

Seminář je věnován problematice zabezpečení v mobilních sítích 2G (GSM), 3G (UMTS), případně i 4G (LTE) a zabezpečení VoIP protokolů (SIP, H.323, Skype). Součástí semináře bude i prezentace evropského projektu FREEDOM, který se zabýval výzkumem v oblasti femtobuněk v mobilních sítích.

### **5) Virtuální privátní síť – 8.11.2012**

Seminář o protokolech pro VPN. Nejvíce prostoru je věnováno protokolu IPSec, ale jsou zmíněny i VPN na bázi SSL/TLS a další protokoly jako L2TP, PPTP, SSTP. Součástí semináře bude prezentace projektu Bender – systému pro automatizovaný sběr dat a komunikaci české polární základny na ostrově Jamese Rosse v Antarktidě s Prahou.



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Pokud budete mít o seminář zájem, pošlete nám email na adresu [vvv@vspj.cz](mailto:vvv@vspj.cz) (v předmětu uveďte název semináře)

**Ing. Tomáš Vaněk, Ph.D.**

Odborný asistent působící na Katedře telekomunikační techniky Fakulty elektrotechnické ČVUT v Praze. V roce 2008 získal titul Ph.D. v oboru aplikovaná kryptografie na ČVUT v Praze. Zajišťuje výuku předmětů Informační bezpečnost, Základy síťových technologií, Počítačové a komunikační sítě. Zabývá se výzkumem v oblasti broadcastových autentizačních protokolů a zabezpečení VoIP komunikace. Od roku 2005 pracuje jako lektor regionální Cisco Akademie CESNET, z.s.p.o., kde vyučuje v kurzy CCNA Exploration1-4 a CCNA Security.



Projekt „Výzkum, Vývoj, Vysočina – Cesty k vědění VŠPJ“, reg. č. CZ.1.07/2.3.00/35.0029.



evropský  
sociální  
fond v ČR



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY



V Š P  
J  
Vysoká škola  
polytechnická  
Jihlava

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ