0x5DLaBAKx5FC517D0FEA3

Laboratoř bezpečnosti a aplikované kryptografie

Vašek Matyáš

LaBAK – výzkum

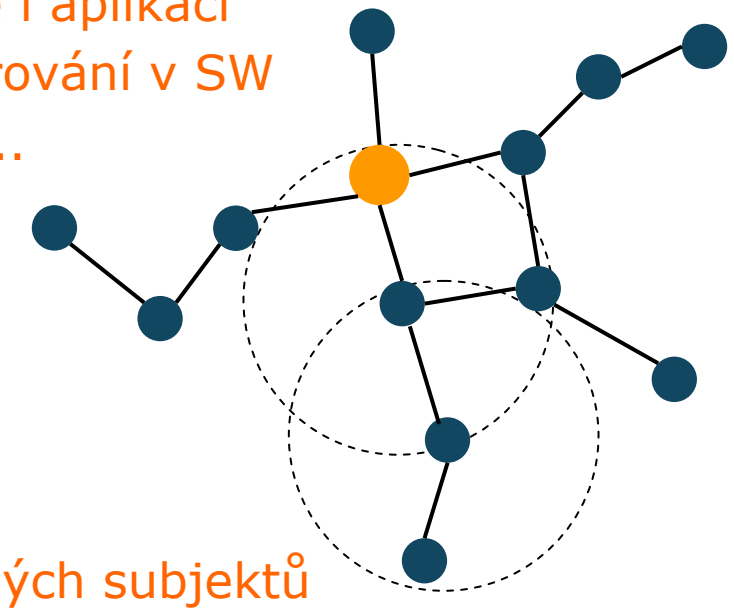
- Spolupráce s MV ČR, NBÚ
- Spolupráce se zahraničními institucemi (Cambridge, Dresden, Malaga, Leuven)
- Spolupráce s komerční sférou
  - Běžící projekty: Y Soft, CEPIA Technologies, Trusted Network Solutions
  - Dříve mj.: Monet+, ANECT, XT Card
  - PhDs a postdocs v laboratoři pracují např. ve firmách: CEPIA Technologies, Trusted Network Solutions, ESET, Honeywell

LaBAK – výuka

- Magisterský obor a zaměření na bakalářské úrovni
  - Široké spektrum předmětů
  - Výuka z velké části v angličtině (i laborní)
- Zapojení studentů do projektů
  - Projekty vědy a výzkumu
  - Projekty vývojové ve spolupráci s průmyslovými partnery
  - Projekty dle návrhu studentů

Bezpečnost sítí

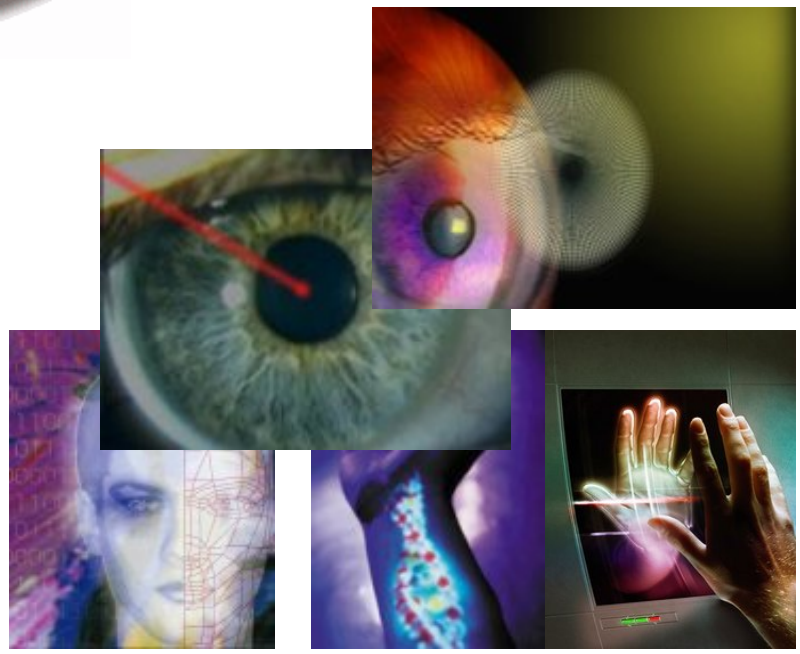
- Bezpečnost metalických a bezdrátových sítí
  - Způsoby ochrany na úrovni sítě i aplikací
  - Zajištění důvěrnosti pomocí šifrování v SW
  - Anonymita, nesledovatelnost, ...



- Bezdrátové senzorové sítě
  - Kryptografické protokoly
  - Detekce průniku do sítě
  - Ochrana soukromí monitorovaných subjektů
  - Zabezpečení sítě jako celku a zajištění jejího fungování

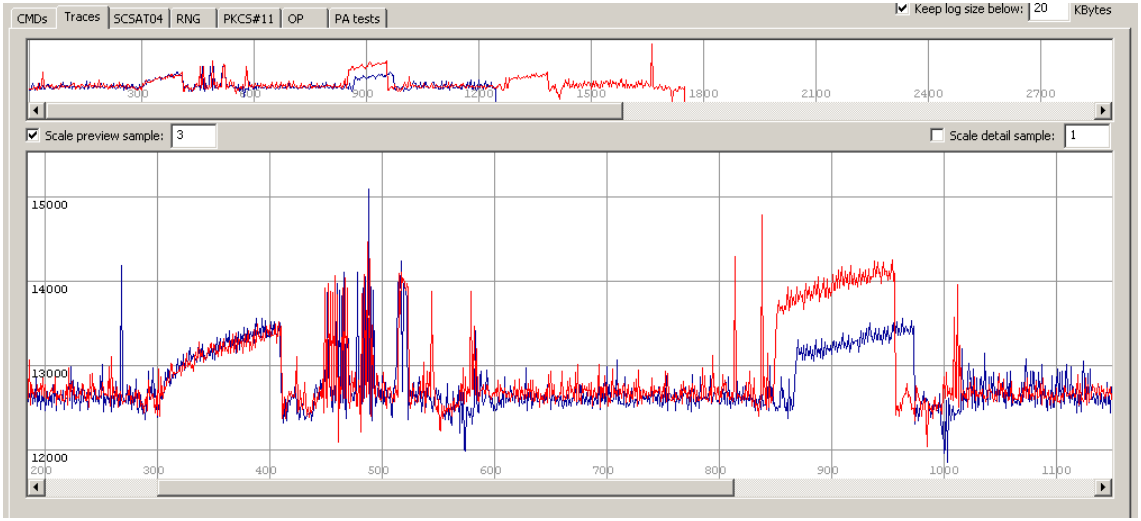
Metody autentizace a autorizace

- Kryptografické protokoly
  - I mikroplatební schémata
- Tokeny
  - Čipové karty
  - Autentizační kalkulátory
  - Mobily
- Bezpečnost biometrik



Bezpečný hardware a čipové karty

- Využití: bankovnictví, elektronické doklady, SIM karty
- Kontaktní/bezkontaktní čipové karty (a RFID)
  - Nutná je bezpečnostní analýza (postranní kanály)
  - Odběrové charakteristiky mohou vést např. k odhalení PINu



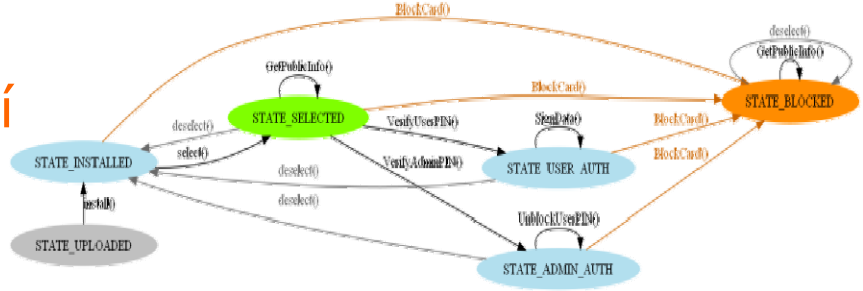
- Kryptografické moduly a akcelerátory
  - Zabezpečení komunikace (např. mezi bankami a bankomaty)

Programování a bezpečnost

- Programování bez bezpečnostních chyb
  - Korektní implementace kryptografických schémat
- Programování (a správa) bezpečnostních aplikací
  - PC, kapesní počítače (PDA), mobilní telefony
    - Šifrování SMS, šifrování privátních dat
    - Symbian OS, JavaME
- Programování bezpečného hardwaru
  - Čipové karty s podporou JavaCard, .NET
  - Kryptografické moduly a hardwarové akcelerátory
  - Různá aplikační programovací rozhraní (API)
- Bezpečnost operačních systémů
  - Souborové systémy, šifrování disků

Automatické transformace kódu - CesTa

- Code Enhancing Security Transformation and Analysis
  - nástroj pro automatické nahrazení zranitelných konstrukcí ve zdrojovém kódu za jejich bezpečné ekvivalenty
- Zvýšení odolnosti vůči odběrové a chybové analýze
- Robustní kontrola změny stavu programu včetně vizualizace
- Detekce problematických konstrukcí při využití transakcí



- Testováno na reálných Java Card appletech
  - OpenPGPCard, CardCrypt/TrueCrypt, implementace SHA-512,AES...
  - Open source projekt http://CesTa.sourceforge.net

Děkuji za pozornost...

www.fi.muni.cz/labak

- Konference EurOpen
  - 2.-5. 10., klášter Želiv, D1 exit Humpolec
  - zaměření na praktickou bezpečnost a aplikovanou kryptografii
  - tutoriály, zvané přednášky, vlastní příspěvky a zkušenosti účastníků
  - příjemný kolektiv lidí z průmyslu a univerzit
  - podání návrhu příspěvku do 13.6. (europen.cz)