CRoCS OpenLab – Bc/Mgr thesis topics
21.9.2018 (Friday 10:00-11:00), A403

https://crocs.fi.muni.cz/openlab
OpenLab – basic idea

• Informal collection of active students and CRoCS’s members
• Wide range of topics: security, cryptography, lockpicking, 3D print, Bitcoin, UAV, juggling, CPU tuning…
  – See archives of the previous years at https://crocs.fi.muni.cz/openlab/
• Running every week the during teaching semester
  – but not a formal course (come as you like)
• Don’t forget to register for info emails 💌
WORK ON (GREAT) THESIS TOPIC
Selection of thesis topic

• How to pick great thesis topic
  – Interesting and hard problem with the right colleagues and supervision
  – Not expert knowledge (at start) but continuous learning is expected
  – Be picky first then heavily committed after

• Always talk to potential supervisors
  – Get a feeling of future collaboration, more fit topic can be newly opened

• How to search for CRoCS thesis (CRoCS labels)
  – Rozpisy témat → Přehled témat → pokročilý výběr → aktuální & dle zadaných štítků → má přiřazen štítěk ‘CRoCS’
  – Take a look also on past and already taken topics
Main research and development themes in CRoCS

- Cryptanalysis
- Randomness Testing
- Wireless Sensor Networks
- Smartcards Security
- Disk Encryption
- Usable Security
- Software Security and Secure Programming
- Secure Cryptographic Implementations

https://crocs.fi.muni.cz/projects
Randomness testing

- How to recognize non-random data? How to exploit the weakness?
- How to empower normal user to test easily?

- RTT: String and easy to use randomness testing
- BoolTest: Automatic generation of tests adapting to data
- CryptoStreams: 100+ cryptographic functions with unified interface
The ID-card maker has violated the most important security principle and 12,500 cards need to be replaced by people.
Randomness testing – thesis topics

- Randomness testing toolkit extensions
- Continuous monitoring of crypto libraries using biased RSA keys
- CryptoStreams cipher database extensions
- Interpretation of BoolTest results
Cryptographic smartcards

• Is smartcard really secure? What algorithms are supported?
• Can we solve hard problem with piece of secure hardware?

• ROCA: vulnerability in Infineon RSA keypair generation
• JCAIgTest.org – performance and algorithm support
• Secure multiparty protocols on 120 smartcards
• Open-source development for JavaCards
Cryptographic smartcards – open topics

- Automatic performance profiler for cryptographic smartcards
- Bezpečná vzdálená instalace aplikací pro kryptografické čipové karty
- Bezpečnostní transformace zdrojového kódu
- Constant-time implementation of low-level ECC library for smartcards
- Návrhové vzory pro vývoj bezpečné JavaCard aplikace
- Schnorr signatures with application to Bitcoin
- …
Cryptanalysis

• BoolTest – cryptanalysis of cryptographic primitives (hash functions, block ciphers)

• Elliptic curve attacks
  – factorisation of integers (attack on RSA)
  – ECDLP (attacks on ECDH)

• Algebraic attacks based on:
  – LLL algorithm
  – Coppersmith algorithm
Cryptanalysis - open topics

- Vylepšenie BoolTest-u
- Zlepšenie ROCA útoku - optimalizácia Coppersmithovho algoritmu
- Zlepšenie ROCA útoku - minimalizácia počtu iterácií
- Knížnica pre Coppersmithov algoritmus
- Interpretácia výsledkov RTT
- LLL a jeho použitie
- Hladké čísla a LLL algoritmus
- Faktorizácia pomocou ECC
Usable security

• Usable security for IT professionals
  – e.g. usability of crypto APIs

• Usable security for end-users
  – e.g. authentication, SSL warnings, experiences with security, …
Usable security – open topics

- Analysis of certificate manipulation errors across multiple libraries
- Automatizované testovanie kryptografických knižníc pracujúcich s X.509 certifikátmi
- …

- We are looking for a student to support us with research on end-user SSL warnings!
WIRELESS SENSOR NETWORK
MULTIPARTY COMPUTATION
PRIVACY CRYPTOCOINS
Every Friday 9:00, A403
https://crocs.fi.muni.cz/openlab