CRoCS OpenLab – Bc/Mgr thesis topics

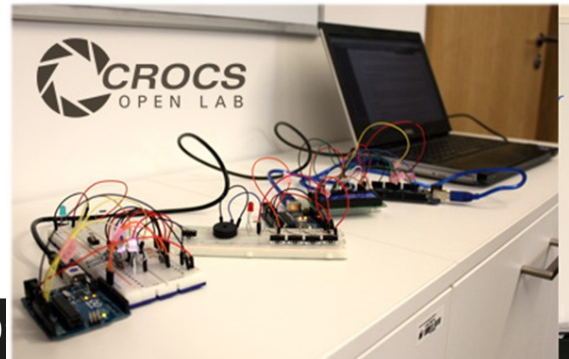
21.9.2018 (Friday 10:00-11:00), A403

https://crocs.fi.muni.cz/openlab

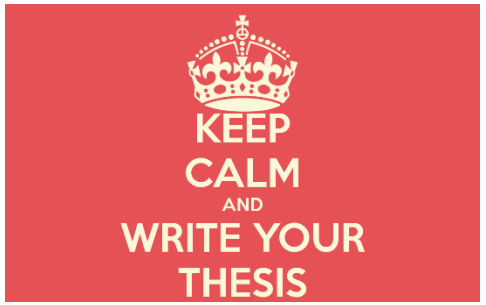
Centre for Research on Cryptography and Security

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



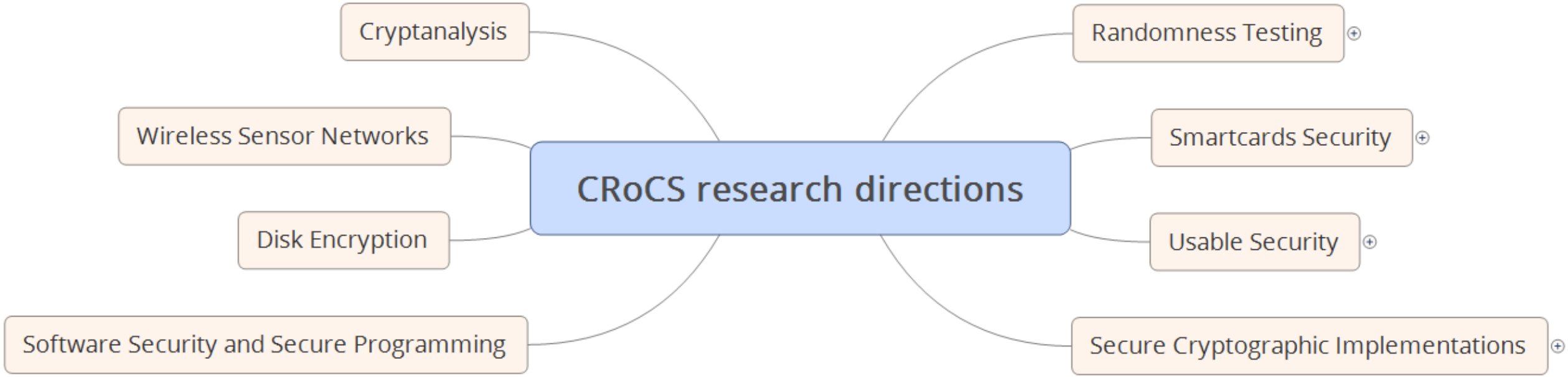
WORK ON (GREAT) THESIS TOPIC



Selection of thesis topic

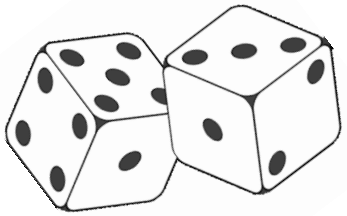
- How to pick great thesis topic
  - Interesting and hard problem with the right colleagues and supervision
  - Not expert knowledge (at start) but continuous learning is expected
  - Be picky first then heavily committed after
- Always talk to potential supervisors
  - Get a feeling of future collaboration, 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 štítek ‘CRoCS’
  - Take a look also on past and already taken topics

Main research and development themes in CRoCS



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

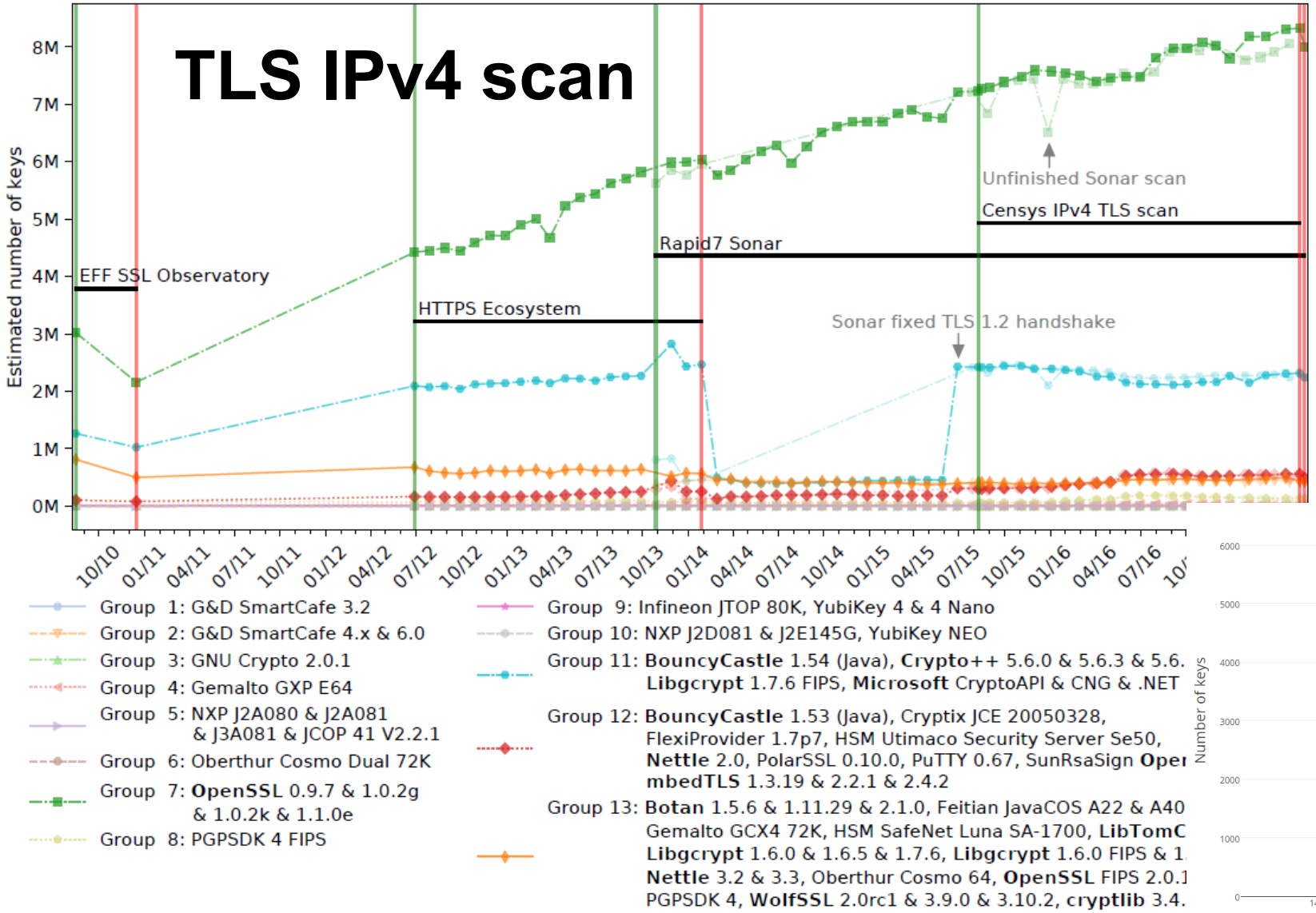
Randomness testing



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

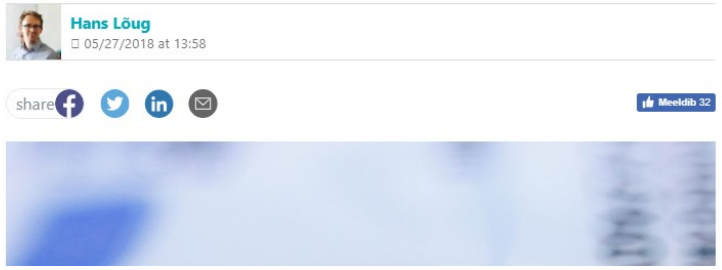
- RTT: String and easy to use randomness testing
- BoolTest: Automatic generation of tests adapting to data
- CryptoStreams: 100+ cryptographic functions with unified interface

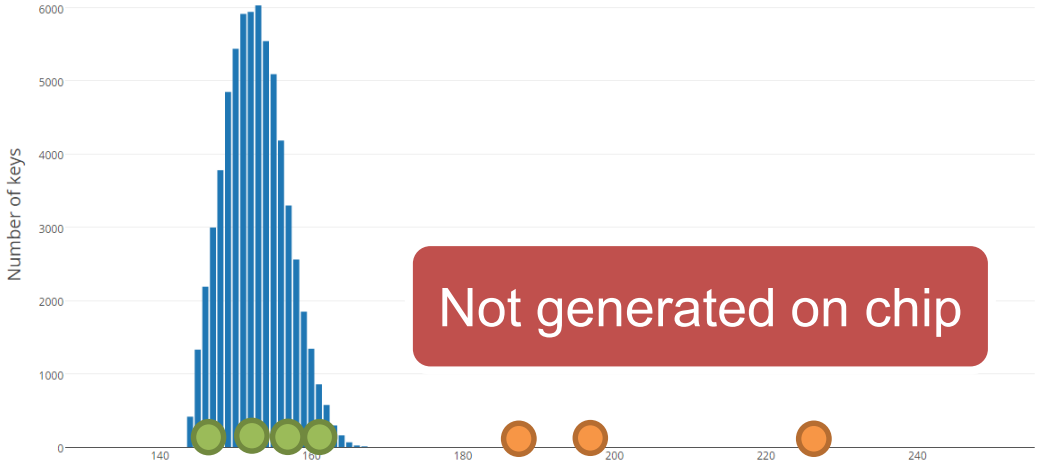
EE eID injected keys (Arnis Paršovs, 05/2018)



Group 1: G&D SmartCafe 3.2
Group 2: G&D SmartCafe 4.x & 6.0
Group 3: GNU Crypto 2.0.1
Group 4: Gemalto GXP E64
Group 5: NXP J2A080 & J2A081 & J3A081 & JCOP 41 V2.2.1
Group 6: Oberthur Cosmo Dual 72K
Group 7: **OpenSSL** 0.9.7 & 1.0.2g & 1.0.2k & 1.1.0e
Group 8: PGPSDK 4 FIPS
Group 9: Infineon JTOP 80K, YubiKey 4 & 4 Nano
Group 10: NXP J2D081 & J2E145G, YubiKey NEO
Group 11: **BouncyCastle** 1.54 (Java), **Crypto++** 5.6.0 & 5.6.3 & 5.6. **Libgcrypt** 1.7.6 FIPS, **Microsoft** CryptoAPI & CNG & .NET
Group 12: **BouncyCastle** 1.53 (Java), Cryptix JCE 20050328, FlexiProvider 1.7p7, HSM Utimaco Security Server Se50, **Nettle** 2.0, PolarSSL 0.10.0, PuTTY 0.67, SunRsaSign **Oper mbedTLS** 1.3.19 & 2.2.1 & 2.4.2
Group 13: **Botan** 1.5.6 & 1.11.29 & 2.1.0, Feitian JavaCOS A22 & A40 Gemalto GCX4 72K, HSM SafeNet Luna SA-1700, **LibTomC Libgcrypt** 1.6.0 & 1.6.5 & 1.7.6, **Libgcrypt** 1.6.0 FIPS & 1. **Nettle** 3.2 & 3.3, Oberthur Cosmo 64, **OpenSSL** FIPS 2.0.1 PGPSDK 4, **WolfSSL** 2.0rc1 & 3.9.0 & 3.10.2, **cryptlib** 3.4.

The ID-card maker has violated the most important security principle and 12,500 cards need to be replaced by people.





Not generated on chip

MSB value

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
- JCAlgTest.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

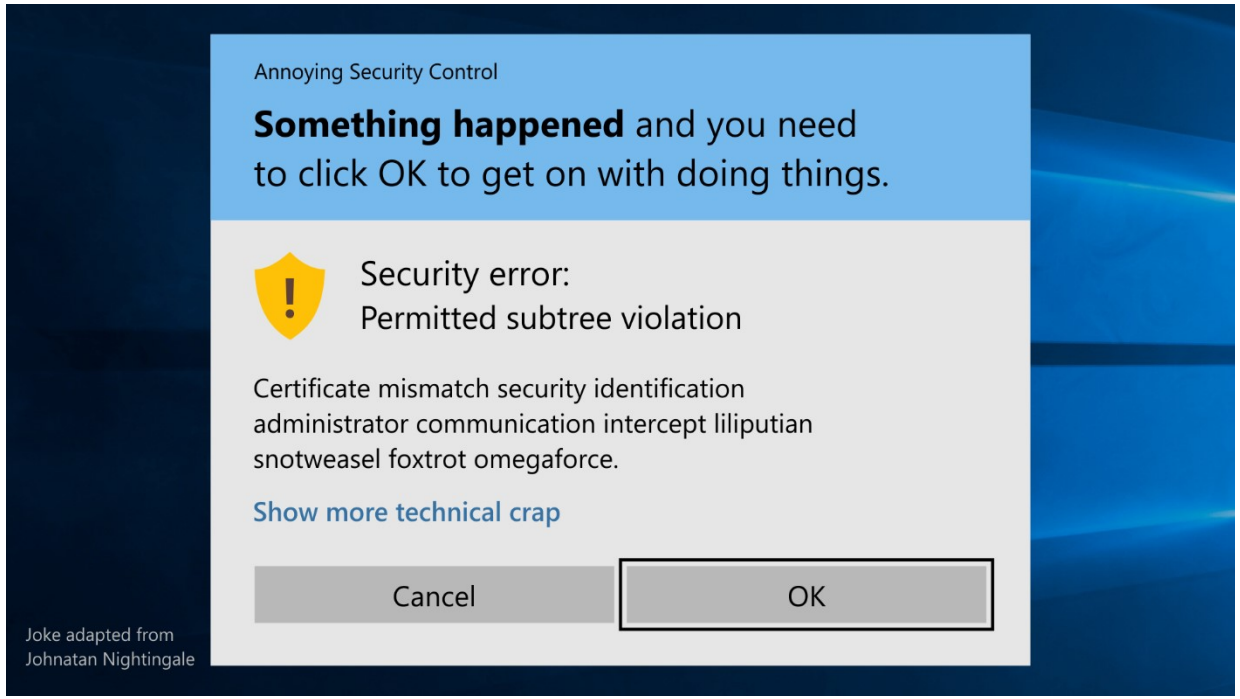
- BoolTest – cryptanalysis of cryptographic primitives (hash functions, block ciphers)
- Elliptic curve attacks
  - factorisation of integers (attack on RSA)
  - ECDLP (attacks on ECDH)
- Algebraic attacks based on:
  - LLL algorithm
  - Coppersmith algorithm

Cryptanalysis - open topics

- Vylepšenie BoolTest-u
- Zlepšenie ROCA útoku - optimalizácia Coppersmithovho algoritmu
- Zlepšenie ROCA útoku - minimalizácia počtu iterácií
- Knižnica pre Coppersmithov algoritmus
- Intepretácia 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