



CEPIA
TECHNOLOGIES

About Cepia



- Small research company
- Started operation 3rd January 2009
- Located in Brno (Platinum at Veveri)
 - Secure offices for 12 people over 2 floors + meeting rooms and reception
 - Own ICT with high level of security for own research and production
 - Very comfortable working environment for staff

What we do?

- Main focus on developing crypto analytical systems for governmental customers
 - Strong focus within research activities
 - Maintaining high academic standards for our staff
- Building a generic processing platform for cryptanalysis
 - State-of-the-art of used components/technology
 - Prototype FPGA processing unit



Current and future projects

- Time-memory Trade-off (TMTO) attacks
 - A5/1, A5/2, A5/3 & Kasumi, GEA1/2, GMR1/2, etc.
- High Performance Computing (HPC)
 - Building a generic platform, HW/SW co-design
 - Cryptanalysis, financial analysis
- HW assisted password crackers
- Proximity systems security
 - DESfire, Keeloq, etc.



Why work for Cepia?

- Research in cryptology, information security and signal/protocol processing
- Allowing employees to publish results
- Ensuring employees have time to keep up to date in their fields of expertise
- Very high education level among colleagues
- Competitive salaries

Who are we looking for?

- Master or doctoral graduates in the fields of:
 - Number theory, algebra, statistics and probability
 - Cryptography and communication/IT security
 - VHDL, GPU and DSP algorithms design and programming
- Ability to think out-side 'the box' & to consume new ideas quickly
- Work in international teams

Typical roles

- Research:
 - Feasibility studies
 - Construction of models
 - Design of innovative algorithms
 - Large scale testing
- Implementation:
 - C/C++ programming
 - Perl/scripting in general
 - VHDL/GPU/DSP programming
 - HW/SW co-design

Pushing hardware to the maximum



Topics of theses for Spring 2013

- GPU accelerated encryption/decryption of communication (OpenCL)
 - Creating of fast GPU-based implementations of cryptographic algorithms
 - Attacking selected algorithms by using GPU acceleration
- Contactless cryptographic Smartcards & RFIDs
 - Analysis of RFID technology with Proxmark3

Competitions

- Competition for talented students at FI
 - In cooperation with:
TNS, Ysoft, Lexical Computing
 - Awards: Paid working positions
in several laboratories at FI MU
- Best Bachelor/Master thesis in IT security and cryptology
 - In cooperation with: TNS
 - Deadline for applications: 31.5.2012
 - Awards: Up to 30K CZK for all winners



CEPIA TECHNOLOGIES **tns** TRUSTED NETWORK SOLUTIONS

SOUTĚŽ!

Přihlaš svoji diplomku nebo bakalárku a vyhraž!

Laboratoř bezpečnosti a aplikované kryptografie FI ve spolupráci se společností Cepia Technologies s.r.o. a Trusted Network Solutions a.s. vyhlašuje soutěž o nejlepší diplomovou a bakalářskou práci řešící problematiku z oblasti **bezpečnosti informačních technologií a kryptologie**. Hlavní cíle soutěže jsou z atraktivnější výše uvedených vědních oborů a podpora nadaných studentů vysokých škol při překonávání bariér v počátcích vlastní odborné kariéry.

Přihášky do soutěže mohou zaslat pouze studenti obhajující na Fakultě informatiky Masarykovy univerzity v semestru jaro 2012 závěrečnou práci v češtině, slovenštině, nebo angličtině. Pro přihlášení práce je zapotřebí zaslat do **31. 5. 2012** (včetně) e-mail s předmětem zprávy „Soutez“ na adresu xrhovj@fi.muni.cz.

Mezi řešitele vítězných prací bude rozdělena částka **30 000 Kč**.

tns TRUSTED NETWORK SOLUTIONS
CEPIA TECHNOLOGIES

Best thesis winners

- Bachelor's thesis
 - Ondřej Koutský
 - Power analysis attacks on smart cards using the PicoScope oscilloscope
 - Tomáš Dragoun
 - Implementation of covert channels in IPv6
- Master's thesis
 - Alexandr Kuckir
 - Detection of attacks on VoIP using NetFlow data
 - Ivan Hutyra
 - Analysis and entering into encrypted traffic at the firewall
 - Matej Prišťák
 - Automated search for dependencies in eStream stream ciphers

Thank you for your attention