POLITECNICO DI MILANO

Dipartimento di
Elettronica, Informazione
e Bioingegneria

Cryptography & Hardware Security research at Politecnico di Milano

Nicholas Mainardi

January 22*nd*, 2018

Research team

- The team is included in the larger research line of the Computer Engineering – System Architecture group
- Research topics:
  - Embedded systems and Cyber Physical Systems
  - Design Methodologies
  - Low-power Design
  - Hardware Security and Cryptography
  - Compiler Construction
- Cryptography & Hardware Security research team

  Gerardo Pelosi (Asst. Prof. – gerardo.pelosi@polimi.it)
  Alessandro Barenghi (Asst. Prof. – alessandro.barenghi@polimi.it)
  Nicholas Mainardi (Ph.D. student – nicholas.mainardi@polimi.it)
  Luca Breveglieri (Ass. Prof. – luca.breveglieri@polimi.it)

Research lines and current results

Side-channel cryptanalysis and countermeasures

- Side-channel cryptanalysis employs the (unintended) information leakage coming from implementations of mathematically secure ciphers
- Side channel attacks are known-plaintext/ciphertext attacks using physical information (e.g. energy consumption) of the implementation
  - passive attack techniques (execution time, power/EM consumption)
  - active attack techniques (intentional fault injection)
- On simple computing devices, the engineering efforts to perform side-channel attacks are still relatively low
- On the other hand, the development of effective countermeasures is a challenging research task

Research lines and current results

Side-channel cryptanalysis and countermeasures - Contributions

- Countermeasures:
  - A compiler-based code morphing methodology to prevent passive side channel attacks with a fully automated application toolchain
  - Two new side channel countermeasures augmenting the regular information leakage with false targets, and encasing any secure cipher within a novel and efficiently protected primitive
- Compiler Automated Cryptanalysis:
  - A security oriented *data flow analysis* to evaluate the resistance of software ciphers against power-(EM-)based cryptanalyses
  - An automated conservative differential fault analysis for block ciphers
- An active side channel attack and countermeasure against ECDSA

Research lines and current results

Scalable and Energy Efficient Realizations

- Efficient implementations of cryptographic primitives across the entire computing platform spectrum (from μ-controllers to servers) allow to
  - exploit the benefits provided by cryptographic techniques
  - prevent exhaustive cryptanalysis in a cost effective manner

Contributions

- Design and realization of industry grade, high-efficiency software cryptographic libraries for smart-cards
- Design and implementation of dedicated hardware accelerators for identity based cryptosystems
- Pioneered the use of GPUs for scalable implementations of symmetric-key cryptographic primitives
- Efficiency and cost estimations of parallel password cracking on GPUs

Research lines and current results

Cryptographically Enforced Security & Privacy in Online Social Networks (OSNs)

- Existing OSNs require the the *social interaction graphs* to be known to the provider to function (user contents may be encrypted though)
- Designed *Snake*, an OSN where social interactions management is entirely performed on the client on end-to-end encrypted data
- The storage provider provides only a flat billboard to post messages

Access Privacy Aware Data Structures for Cloud Data Outsourcing

- Even if data confidentiality is provided via encryption, an honest but curious service provider may violate access confidentiality, i.e. infer information from the locations of the accessed data
- In collaboration with UNIMI, designed an encrypted data structure and the related client-server protocol to make accesses to distinct or repeated remote private items indistinguishable to one another

Research lines and current results

Code based Cryptography

- Integer factoring and discrete log problems admit polynomial time solvers running on a quantum computer
- Decoding a general linear code is an NP-complete problem, thus highly unlikely to be solved in polynomial time with a quantum computer
- Cryptosystems relying on decoding trapdoors require large keypairs and longer running times than current public-key based cryptosystems

Contributions

- In collaboration with UnivPM, participation to the U.S. NIST *Post-quantum Cryptography* standardization initiative, proposing:
  - a key encapsulation module (KEM)
  - a Public Key Cryptosystem (PKC)

  based on quasi-cyclic low-density parity-check (QC-LDPC) codes

  `csrc.nist.gov/Projects/Post-Quantum-Cryptography`

  `www.ledacrypt.org`

Research lines and current results

Language Theoretic Security

- Application of Formal language recognition techniques (parsing) to ensure the soundness of input interpretation for security critical data
- Allows to highlight data format specifications which are flawed in principle (i.e., the ones where the string correctness problem is undecidable)

Contributions

- Found syntactic ambiguities in the X.509 digital certificate format
- Pointed out non systematic parsing of X.509 in the 7 most used TLS libraries leading to server impersonation vulnerabilities
- Devised a new *regular* (type-3) format for X.509 certificates amenable as a drop in replacement for the current ITU format
- Analyzed the certificate format of OpenPGP highlighting ambiguities

Ongoing research activities

- Investigating the impact of μ-architectural features on the side-channel security of software cryptographic implementations running on superscalar CPUs
- Investigating security and privacy issues in emerging non-volatile memories
- Providing accurate security analysis and optimized hardware & software implementations for code based cryptosystems
- Providing data confidentiality while retaining computational capabilities in outsourcing scenarios with Homomorphic Encryption (HE)
  - ↪ Cryptanalysis of Noise Free Fully Homomorphic Encryption (FHE) schemes
  - ↪ Design protocols to perform necessary operations (division, string search, sorting) for encrypted data analytics

Organization of Workshops

Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)

- reached its 14th edition (`www.fdtc-workshop.eu`)
  - **Topics**: active side channel attacks, countermeasures, models and security metrics

Workshop on Cryptography and Security in Computing Systems (CS^2)

- reached its 5th edition (`www.cs2.deib.polimi.it`)
  - **Topics**: architectural, compiler and systems aspects of designing trustworthy and secure computing systems

Mobile System Technologies (MST)

- reached its 3rd edition (`www.mstworkshop.eu`)
  - **Topics**: system and security aspects of modern and emerging memory technologies for mobile systems

Contacts

Thanks for your attention !

Contact us:

Team Personal Email – *name.surname*@polimi.it

Cryptography Group Website – `http://crypto.dei.polimi.it/`