Bachelor @ IAIK 2019/2020

Welcome!

Stefan Mangard
The Bachelor thesis is a milestone of your studies
Compulsory/basic topics vs. specialized/elective topics
Bachelor Thesis

You choose – you have your own individual topic
Information Security
What to do?
The Research Questions:

We need Cryptography!
Cryptology & Privacy

• **Research Questions**
  • How can we design efficient and secure cryptographic algorithms/protocols?
  • How can we compute on encrypted data?
  • How can we attack current cryptographic schemes?
  • How can we build cryptography that cannot be broken by quantum computers?
  • ...

---

If |A| > 0 then
\[ A_1 \ldots A_s \leftarrow r \text{-bit blocks of } A_j \]
\[ \text{for } i = 1, \ldots, s \text{ do} \]
\[ S \leftarrow S \oplus ((S_r \oplus A_i) \parallel S_c) \]
\[ S \leftarrow S \oplus (0219 \parallel 1) \]
\[ S \leftarrow \text{Processing Ciphertext} \]
\[ C \leftarrow \text{r-bit blocks of } C_t \]
\[ t \leftarrow 1 \text{do} \]
The Research Questions

We need to look inside our devices to analyze and understand them!

We need to build secure systems!
System Security

• Research Questions:
  • What are the weaknesses of current systems?
  • How can we design systems (compiler, software, hardware, ...) to prevent an attacker from hacking a computer?
  • How can we cope with side channels?
  • ...

DEVELOPING STORY

COMPUTER CHIP FLAWS IMPACT BILLIONS OF DEVICES

LIVE

NEWS STREAM
The Research Questions

We need to show/prove that the implementations indeed do what we specified.
Formal Methods

• **Research Questions**
  • How can we formally proof the security of a system?
  • How can we generate suitable test vectors?
  • How can we synthesize secure systems?
  • How can we verify the security of systems using deep learning?
  • ...
We need to bring everything together correctly to build secure applications!
Secure Applications

• How can we design secure cloud solutions?

• How can we do fine grained identity management?

• How can we design complex and secure applications (e.g. in E-government)?

• ...

; IAIK, www.iaik.tugraz.at
Secure Applications
System Security

Formal Methods
Cryptography & Privacy

Topic Tables
Bachelor Thesis

• Find a topic → talk to people, look at topics on IAIK website

• Get it done → classic mode or Bachelor@IAIK mode

Today

Summer Term 2020
Bachelor Thesis – Getting it Done

• Classic Mode
  • Individual timeline – you can start any time

• Bachelor@IAIK
  • Work @ IAIK
  • Get part of the team
  • Get free coffee
  • Discuss, meet, research with us and other students working on their thesis
  • Fixed timeline
Timeline for Bachelor@IAIK

- Nov 29: Presentation of topics
- Dec – Jan: Meet with supervisors @ IAIK and decide on mode for Bachelor thesis

- Feb 24 – March 6: 1st working block
  - Feb 28: Writing lab (optional)
  - March 6: Lightning Talks 12:00-13:30
- April 13 – April 24: 2nd working block

- April 25-26: Presentation Lab (optional)
- June 5: Final presentations
2019 Student Research Excellence Awards
Student Research Excellence Awards

• Many excellent student projects have been completed during the last year

• Any student that contributes to a publication at an international conference in IT security receives this award.
Bachelor Thesis

A Systematic Evaluation of Transient Execution Attacks and Defenses
Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtyushkin, Daniel Gruss

USENIX Security Symposium 2019

Santa Clara, CA, USA
Summer Internship

Big Numbers - Big Troubles: Systematically Analyzing Nonce Leakage in (EC)DSA Implementations
Samuel Weiser, David Schrammel, Raphael Spreitzer, Lukas Bodner

USENIX Security Symposium 2020

Boston, MA, USA
Bachelor Thesis

Page Cache Attacks
Daniel Gruss, Erik Kraft, Trishita Tiwari, Michael Schwarz, Ari Trachtenberg, Jason Hennessey, Alex Ionescu, Anders Fogh

CCS 2019

London, UK
Bachelor Thesis

JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits

Michael Schwarz, Florian Lackner, Daniel Gruss

NDSS 2019

San Diego, CA, USA
Master Project

Bounded Synthesis of Register Transducers

Ayrat Khalimov, Benedikt Maderbacher, Roderick Bloem

ATVA 2018

Los Angeles, CA, USA
Bachelor Thesis

SGXJail: Defeating Enclave Malware via Confinement
Samuel Weiser, Luca Mayr, Michael Schwarz, Daniel Gruss

RAID 2019

Beijing, China
Bachelor Thesis / Master Project

Analyzing the Linear Keystream Biases in AEGIS
Maria Eichelseder, Marcel Nageler, Robert Primas

FSE 2020

Athens, Greece
Master Thesis

Mind the Gap: Finding what Updates have (really) changed in Android Applications

Johannes Feichtner, Lukas Neugebauer, Dominik Ziegler

SECRYPT 2019

Prague, Czech Republic
Master Thesis

Cloud Data Sharing and Device-Loss Recovery with Hardware-Bound Keys
Felix Hörandner, Franco Nieddu

ICISS 2019

Hyderabad, India
Bachelor Thesis

A Systematic Evaluation of Transient Execution Attacks and Defenses
Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtyushkin, Daniel Gruss

USENIX Security Symposium 2019

Santa Clara, CA, USA
Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC

Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, Christian Rechberger

Eurocrypt 2019

Darmstadt, Germany
Master Thesis

NetSpectre: Read Arbitrary Memory over Network
Michael Schwarz, Martin Schwarzl, Moritz Lipp, Daniel Gruss

ESORICS 2019

Luxembourg, Luxembourg
Master Thesis

Efficient FPGA Implementations of LowMC and Picnic
Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, Mario Werner

CT-RSA 2020

San Francisco, CA, USA
What’s next?
Secure Applications
System Security

Formal Methods
Cryptography & Privacy

Topic Tables