Bachelor Thesis in Digital Security

Bram Westerbaan
awesterb@cs.ru.nl

May 31, 2023

Bachelor Thesis in Digital Security

- What topics do you find interesting?

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like?

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point
- For inspiration take a look at: previous theses and a limited set of suggestions

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point
- For inspiration take a look at: previous theses and a limited set of suggestions
- Check the websites of potential supervisors and take a look at their publications

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point
- For inspiration take a look at: previous theses and a limited set of suggestions
- Check the websites of potential supervisors and take a look at their publications
- Some are busier than other; better woo the busy ones with a very interesting topic

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point

- For inspiration take a look at: previous theses and a limited set of suggestions

- Check the websites of potential supervisors and take a look at their publications
- Some are busier than other; better woo the busy ones with a very interesting topic
- But whomever you contact, give them something concrete to work with

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point
- For inspiration take a look at: previous theses and a limited set of suggestions
- Check the websites of potential supervisors and take a look at their publications
- Some are busier than other; better woo the busy ones with a very interesting topic
- But whomever you contact, give them something concrete to work with
  - so that they might suggest an even better topic to you

Bachelor Thesis in Digital Security

- What topics do you find interesting?
- What kind of work do you like? e.g. programming or digging through the literate
- A good research question/topic is the best starting point
- For inspiration take a look at: previous theses and a limited set of suggestions
- Check the websites of potential supervisors and take a look at their publications
- Some are busier than other; better woo the busy ones with a very interesting topic
- But whomever you contact, give them something concrete to work with
  - so that they might suggest an even better topic to you
  - or refer you to another colleague and/or Ph.D.-student

Embedded and Mobile Systems

Lejla Batina

- Hacking real-world systems
- Side-channel attacks on
  - Mobile phones
  - Crypto wallets
  - Voice-controlled systems
- Machine and deep learning in security evaluations
- Topics: https://www.cs.ru.nl/~lejla/teaching.html

Ileana Buhan

- (Mathematical analysis of) side-channel attacks
- Security of embedded systems (hardware & software attacks e.g. reverse engineering)
- Implementation of cryptographic algorithms
- “If you like embedded systems and are looking for a project which mixes hands-on work with just the right amount of theory contact me.”

Ph.D.-students of Lejla Batina

Konstantina Miteloudi

- Countermeasures to fault and side-channel attacks

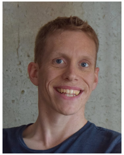
Parisa Amiri Eliasi

- Optimised implementations of cryptography in assembly,
- and their side-channel analysis

Symmetric Cryptography

Joan Daemen

- Design and analysis of symmetric cryptographic primitives
  - Rijndael, now AES
  - Keccak, now SHA3



Bart Mennink

- Symmetric primitives (e.g. hash functions and block ciphers)
- Provable security
- Cryptographic protocols (such as digital signature schemes, credential schemes, and multiparty computation)
- Network applications

Low-Level Implementations and Post-Quantum Cryptography

Peter Schwabe

- Low-level optimisation of cryptographic software
- Cryptography on microcontrollers
- Protection of software against side-channel attacks
- Post-quantum cryptography

Simona Samardjiska

- Various topics in post-quantum cryptography, including
  - Design and optimisation of primitives
  - Cryptanalysis and side channel attacks
  - Provable aspects of PQ crypto
  - Applied PQ crypto
    (such as privacy enhancing schemes and protocols, etc.)

Ph.D.-students of Simona Samardjiska

Krijn Reijnders

- Elliptic curve cryptography
- Post quantum cryptography based on:
  - isogenies between elliptic curves
  - equivalences between error correcting codes

Lars Ran

- Security analysis of Multivariate and Code-based crypto using algebraic methods

Software Security

Erik Poll

- Security testing (e.g., fuzzing or state machine learning)
- Security protocols (e.g., formal analysis of those)

Günes Acar

- Large-scale web measurement studies on:
  - Online tracking
  - Deceptive and manipulative (dark) design patterns
- Privacy and security analysis of mobile apps, IoT devices
- Anonymous communications, website fingerprinting

Privacy and Identity Management

Bart Jacobs (iHUB)

- Identity management, esp. Yivi (formerly k.a. IRMA)
- PubHubs community platform
- Historical crypto/security
  - E.g., reverse engineering of old devices, and analysis

Jaap–Henk Hoepman (iHUB)

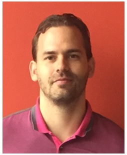
- Privacy enhancing technologies
- Privacy by design; design patterns
- Internet of things
- Identity management
- See also `http://www.cs.ru.nl/~jhh/education.html`

Information Security

Eric Verheul

- Information security consultancy, in the public, private & financial sectors
- Polymorphic encryption and pseudonymisation

AI and Cybersecurity



Stjepan Picek

- Various topics in AI and cybersecurity, e.g.,
  - Security of machine learning (evasion, poisoning, backdoor attacks, etc.)
  - Machine learning for cryptanalysis
  - Deep learning and side-channel attacks
  - Federated learning
  - Evolutionary algorithms for cybersecurity

Network Security

Katharina Kohls

- Mobile network security
  - Implementing attacks using open software stacks
  - Analysing real-world networks
- Information leakage in networks
  - Traffic analysis attacks like end-to-end confirmation, website fingerprinting, tracking, etc.
  - Analysing characteristics of deployed networks

Guido Knips
(Ph.D.-student)

- Automatic/semi-automatic security scans of 5G core networks

Law

Mireille Hildebrandt

- Code versus law:
  - Legal protection by design
  - Machine learning in law
  - ‘Affordance’

Frederik Zuiderveen Borgesius (iHUB)

- Privacy, data protection, discrimination, and freedom of expression in the context of new technologies
- Behavioural targeting

Usability

Hanna Schraffenberger

- Human-centred design
- Usable privacy and security
- Dark patterns

Lecturers

Pol van Aubel

- Networking & network security
  - Networking protocols
  - Secure VPN deployment
  - ...
- Security & privacy in critical infrastructure
  - Smart meters
  - Electric Vehicle charging infrastructure

Engelbert Hubbers

- Formal verification (using e.g. Coq)
- Logic; in particular propositional, predicate, and modal logic

Lecturers

Bram Westerbaan

- Group based cryptography
- Quantum algorithms/logic

fin