INF-744: Security and Privacy for IoT

Diego F. Aranha

Institute of Computing – University of Campinas

About myself

Prof. Diego F. Aranha, Ph.D. in Computer Science

`dfaranha@ic.unicamp.br`

15 years of academic/consulting experience in Computer Security

Building IC-1, Office 06 at IC/Unicamp

Research interests:

- Cryptographic Engineering
- Privacy-preserving computing
- Real-world security
- Electronic voting

Course syllabus

Objective

familiarize the students with fundamental concepts of security, cryptography and privacy and their applications in the design of secure and privacy-preserving systems in the IoT context.

Course syllabus

Objective

familiarize the students with fundamental concepts of security, cryptography and privacy and their applications in the design of secure and privacy-preserving systems in the IoT context.

In other words: Help prevent the IoT privacy/security nightmare.

Course syllabus

Objective

familiarize the students with fundamental concepts of security, cryptography and privacy and their applications in the design of secure and privacy-preserving systems in the IoT context.

In other words: Help prevent the IoT privacy/security nightmare.

Course topics:

1. Taxonomy of **attacks** and defense
2. Main **vulnerabilities** and *defensive programming*
3. Basic **cryptography**
4. Key and identity **management**
5. Cryptographic **protocols**
6. **Authentication** mechanisms
7. Side-channel analysis
8. **Privacy** techniques

Course syllabus

Bibliography

1. **Security:** Matt Bishop. *Introduction to Computer Security*, Addison-Wesley, 2004.
2. **Defensive programming:** Gary McGraw. *Software Security: Building Security In*, Addison-Wesley, 2006.
3. **Vulnerabilities:** Michael Howard, David LeBlanc, John Viega. *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*, McGraw Hill, 2009.
4. **Protocols:** William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson.
5. **Cryptography:** Christof Paar and Jan Pelzl. *Understanding cryptography*, Springer, 2014.
6. **Privacy and IoT security:** Niteh Dhanjani, *Abusing the Internet of Things.* OReilly, 2015.

Additionally: links and material for further reading (Moodle).

Course syllabus

Grading plan:

- N in-class and M programming assignments (graded individually).
- Let S be the set of grades assigned to tests and programming assignments.
- Final grade F is the average of X best grades from S, where:
    1. $X = |S| - 1$ if $|S| <= 5$.
    2. $X = |S| - 2$ if $|S| > 6$.
- Minimum grade for approval: **7.0**
- Minimum required attendance: **9** (75%)

Course syllabus

Course management:

- Slides will be made available on Moodle: `https://moodle.lab.ic.unicamp.br/moodle/course/view.php?id=187`
- Course discussions/questions on Moodle discussion forum
- Contact for other issues: `dfaranha@ic.unicamp.br`

Important: Please use prefix `[INF744]` to reduce e-mail latency.