REAL WORLD CRYPTO AND PRIVACY REFLECTION REPORT

I. About the Event

The summer school on "Real World Cryptog and Privacy" took place in Šibenik (Croatia), between June 11–15, 2018. This event is jointly organized by the Digital Security (DiS) group, Radboud University (The Netherlands), ETH Zurich Information Security and Privacy Center (Switzerland) and Faculty of Electrical Engineering and Computing, University of Zagreb (Croatia).

The school aims at bringing together Master/PhD students, academics and security experts from industry. The focus of the summer school is on:

- Cryptography for the Internet
- Recent developments in symmetric key cryptography
- Security proofs in cryptography
- Wireless security
- Crypto for systems security
- Software and hardware security
- Privacy enhancing technologies
- Blockchain security (special session)

The rest of this report will highlight some of the lectures held during this summer school.

II. Hardware-assisted Security: From Trust Anchors to Meltdown of Trust

This lecture was given by Professor Ahmad-Reza Sadeghi who represents Technische Universität Darmstadt & Intel Collaborative Research Institute for Collaborative & Resilient Autonomous Systems.

The lecture started with a historical overview of how hardware has been underpinning software and system security since the beginning. Subsequently, an overview of the currently deployed hardware security primitives was presented with imitation of each one.

For example Intel SGX are vulnerable to side channel attacks, ARMTrustZone requires a string trust in manufacturers, and PUFs came as an afterthought and are not scalable.

The talk then discussed the trusted computing paradigm, specifically how the Trusted Platform Module has been enabling trusted boot for devices. However, it is unable to ensure the integrity of the whole execution environment.

The lecture also discussed how run-time security is unsolved problem and that it is an arms race between attackers and defenders.

Finally, the speaker discussed some of the recently published research projects on Intel SGX side channel attacks.

III. Password-Based Cryptography: Strong Security from Weak Secrets

This lecture was given by Anja Lehmann from IBM Research – Zurich. The premise of this talk is that password authentication is not broken, but that we are using it wrong.

One part of the lecture focused on how a database server compromise is the most widespread password authentication attack vector. The speaker presented Pythia: as a mitigation to this issue. Pythia proposes to use a distributed password architecture, and it uses the following steps at a high level:

- Replace $Hash$ by a secure PRF , pwd
- Split secret key into n shares
- h = PRF , pwd computed distributed:
- Servers don't learn anything about pwd or h

IV. References

https://summerschool-croatia.cs.ru.nl/2018/