Euro S&P

Chris Carr

April-May 2017, Paris

1 Euro Security and Privacy Conference 2017

EuroS&P, is the 2$^{\text{nd}}$ IEEE European Symposium on Security and Privacy, the sister conference of IEEE Security and Privacy, which has been running since 1980, in the US.

This year the conference took place in Paris, at UPMC Campus Jussieu. The conference accepted 38 papers out of a total submission of 194, giving an acceptance rate of 19.6%.

The conference also hosted workshops co-organised with the Eurocrypt conference. These events took place on Saturday and Sunday (29-30 April).

Saturday

- FOQUS Frontiers Of QUantum Safe cryptography.
- MTP: Models and Tools for Security Analysis and Proofs.
- EuroUSEC European Workshop on Usable Security.
- S&B Security on Blockchains.
- TPT Tamarin-Prover Tutorial.
- cataCRYPT catastrophic events related to CRYPTography and security with their possible solutions.
- CrossFyre Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers.
- IMPS Innovations in Mobile Privacy and Security.
- S4CIP 2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection.

Sunday

- FOQUS Frontiers Of QUantum Safe cryptography.
- QsCl Quantum-safe Crypto for Industry (RISQ).

- SEMS Security for Embedded and Mobile Systems.
- wr0ng: Random Number Generation Done Right.
- TLS:DIV TLS 1.3: Design, Implementation, Verification.
- WCS Second Workshop on Communication Security.
- CFRG Crypto Forum Research Group.
- CrossFyre Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers.
- FewMul: Fewer Multiplications in Cryptography - From Theory to Applications.

1.1 Participation

For my part, I was a student volunteer for the conference. I had three duties throughout the conference, to help with the front desk and arrival of the attendees, provide assistance with the conference banquet and to help manage the Saturday event on Security and Blockchains.

1.2 Relevant and Interesting Talks

Of particular interest to my line of reaeasrch was the session on Applied Cryptography. Containing a talk:

Redactable Blockchain - or - Rewriting History in Bitcoin and Friends.

This talk was relevant to my research area, and was an interesting approach to one of the problems with 'blockchain' constructions.

On Thursday, Dan Boneh gave an interesting recap of how crytographic techniques have evolved over time, in a keynote talk entitled **Applied crypto: the good, the bad, and the future**.

The first SoK talk: **Fraud in Telephony Networks** was particularly interesting, as many were not aware of the scale of the problems presented by the speakers.

On the Friday, the talk **A Formal Security Analysis of the Signal Messaging Protocol** was also well received, especially considering the widespread adoption of the signal protocol in secure messaging applications.

Figure 1: COINS Students.