Real World Crypto 2019

Real World Crypto 2019 was organized January 9. - 11. 2019 in San Jose, USA. This was the eight year of the conference, starting at what would´ve been Alan Turing's 100th birthday in 2012. The conference aims to bring together cryptography researchers and developers implementing cryptography in real-world systems to strengthen the dialogue between these two communities. The program is published at https://rwc.iacr.org/2019/program.html.

The conference had sessions on Messaging Security, Cryptography and Politics, Secure Communications, Passwords, Crypto Usability, Enterprise Cryptography, Cryptographic Implementation, Cryptography Standardization, Cryptographic Hardware, Formal Verification, Advanced Cryptographic Primitives, and Cryptocurrency and Blockchains.

My research is in post-quantum cryptography, and the most interesting and relevant talk in the program was Martin Albrecht´s presentation titled "So how hard is solving LWE anyway?". This was a study of lattice-based cryptography, with particular focus on the candidates for the NIST standardization process for post quantum cryptography. Albrecht looked at how different methods can find short vectors in different lattices, how this can be used to break the proposed systems and, most importantly, the running time and memory consumption of such algorithms.

There was a lot of great talks in the program, and I can especially recommend to check out the recordings of the following talks:

- "Messaging Layer Security: the beginning" by Richard Barnes,
- "OPAQUE: Strong client-server password authentication for standardization" by Hugo Krawczyk,
- "Managing Keys and Teams with Keybase.io" by Max Kohn,
- "FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution" by Daniel Genkin and Yuval Yarom,
- "True2F: Backdoor-resistant authentication tokens" by Emma Dauterman,
- "Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars" by Lennert Wouters,
- "Deploying MPC for Social Good" by Lucy Qin, and
- "A Full CryptoCurrency Custody Solution Based on MPC and Threshold ECDSA" by Yehuda Lindell.

The Levchin Prize was established in 2015 by internet entrepreneur, Max Levchin. The prize honors significant contributions to real-world cryptography and celebrates recent advances that have had a major impact on the practice of cryptography and its use in real-world systems. Up to two awards will be given every year and each carries a cash prize of $10,000. Award recipients are announced at the Real World Cryptography Conference, and the winners of 2019 was Eric Rescorla and Mihir Bellare. Website: https://levchinprize.com.

Eric Rescorla is Chief Technology Officer at Mozilla Firefox, and got the prize for sustained contributions to the standardization of security protocols, most recently in the development and standardization of TLS 1.3. Mihir Bellare is a professor at UC San Diego, and got the prize

for outstanding contributions to the design and analysis of real-world cryptography, including the development of the random oracle model, modes-of-operation, HMAC, and formal models of key exchange.


*Figure 1: Meeting with Whitfield Diffie, one of the pioneers of public-key cryptography. Diffie and Martin Hellman's 1976 paper "New Directions in Cryptography" introduced a radically new method of distributing cryptographic keys.*

I had a great time at the conference, and I got to meet several prominent researchers over the three days. Thank you Coins, for giving me the chance to attend Real World Crypto 2019.

January 14, 2019, USA
Tjerand Silde
www.tjerandsilde.org