REPORT FROM REAL WORLD CRYPTO (RWC) 2023

IETF 116

Sofía Celi

- Reporting mainly on the most relevant talks for the IETF → bias of what I found most interesting
- Served as part of the PC
- Full program: https://rwc.iacr.org/2023/program.php
  - Videos: https://www.youtube.com/@TheIACR

Day 1

- *Crypto Agility and Post-Quantum Cryptography @ Google* by Stefan Kölbl Anvita Pandit, Rafael Misoczki and Sophie Schmieg:
  a. Key rotation -> distributed architecture problem
  b. Priorities:
     - encryption on transit
     - signatures, where public keys are hard to change
     - all asymmetric cryptography
     - all symmetric cryptography (less priority)
  c. Focusing on ATLS (https://cloud.google.com/static/docs/security/encryption-in-transit/application-layer-transport-security/resources/alts-whitepaper.pdf) using HRSS (https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms)
  d. Found stack-overflows due to bigger sizes of keys → moved to the heap

Day 1

- *TLS-Anvil: Adapting Combinatorial Testing for TLS Libraries by* Marcel Maehren, Philipp Nieting, Sven Hebrok, Robert Merget, Juraj Somorovsky and Jörg Schwenk
  a. TLS is a complex protocol
  b. TLS test suite for black box evaluation of clients and servers
  c. Based on mandatory RFC statements
- Aimed to provide a way to automatically test TLS libraries in accordance to RFC and know input vectors

Tool: https://tls-anvil.com/

Paper: https://www.usenix.org/conference/usenixsecurity22/presentation/maehren

Day 1

- *Careful with MAc-then-SIGn: A Computational Analysis of the EDHOC Lightweight Authenticated Key Exchange Protocol by* Felix Günther Marc Ilunga Tshibumbu Mukendi:
  a. Designing a secure communication protocol for constrained environments:
     - Low-powered devices support only a limited set of cryptographic primitives
     - IoT security protocols must incur minimal bandwidth, round-trip time, and power consumption overhead
  b. OSCORE protocol (RFC 8613): determine how to securely communicate once a session key is available
  c. Lightweight Authenticated Key Exchange (LAKE) working group: determine how to generate such session key:
     - Security analysis of EDHOC (“Ephemeral Diffie–Hellman Over COSE”)
       - Of interest: the MAc-then-SIGn approach
     - Authors invited future analysis

Paper: https://eprint.iacr.org/2022/1705.pdf

Day 1

- *WhatsApp End-to-End Encrypted Backups by Kevin Lewi*
  a. Backups should have the same security/privacy guarantees as e2e
  b. Protect with:
     - Master encryption key
     - Password-based:
       - Usage of the OPAQUE protocol for registration of password

Day 1

- *Why E2EE Cloud Storage is hard - Challenges, Attacks and Best Practices* by Matilda Backendal, Miro Haller and Kenny Paterson

Consumer cloud storage lacks privacy

Provider	Active users	E2EE
Google Drive	> 1 billion	✗
OneDrive	0.5 – 1 billion	✗
iCloud	> 850 million	✗
Dropbox	>700 million	✗

Sources:

Google Drive (2018): https://techcrunch.com/2018/07/25/google-drive-will-hit-a-billion-users-this-week/?guccounter=1

OneDrive (2015, 2022): https://www.computerworld.com/article/3003140/microsofts-onedrive-changes-follow-the-money.html, https://news.microsoft.com/bythenumbers/en/give

iCloud (2018): https://www.cnbc.com/2018/02/11/apple-could-sell-icloud-for-the-enterprise-barclays-says.html

Dropbox (2022): https://dropbox.gcs-web.com/news-releases/news-release-details/dropbox-announces-second-quarter-fiscal-2022-results

Day 1

- *Why E2EE Cloud Storage is hard - Challenges, Attacks and Best Practices* by Matilda Backendal, Miro Haller and Kenny Paterson:
  - Cloud Storage problems:
    - Key Management: data available from any device
    - Usage of passwords: easy to forget/leak
    - Sharing encrypted files: difficult to establish a trusted channel
  - Analysis of MEGA: 10+ million daily active users
    - RSA key recovery
    - File key recovery
    - Reasons: no AE, usage of AES-ECB

More details: https://mega-caveat.github.io/

Lesson from Day 1

- Post-quantum cryptography migration has started:
  - An organized, careful approach seems like the path ahead
- Attacks in practice are still found:
  - At implementation level
  - In *ad-hoc* cryptography design
- Beyond “e2e”:
  - Backups
  - Cloud storage:
    - Call for active effort to standardise a protocol

Day 2

- *Design, applied cryptography and humans* by Stephan Somogyi
- *Cryptography for Grassroots Organizing* by Leah Namisa Rosenbloom and Seny Kamara
- *Designing cryptography for small organizations* by Sofía Celi, Alex Davidson and Pete Snyder
  - Focus on designing cryptography/protocols/systems with the user in mind
  - Integrate user studies/design/sociological-anthropological research as part of it
  - Inclusive design for diverse people
  - Move away from the assumption of “we know better”, as we don’t
- Invitation to HRPC

Day 2

- *On the possibility of a backdoor in the Micali-Schnorr generator by* Hannah Davis, Matthew Green, Nadia Heninger, Keegan Ryan and Adam Suhl
  a. Suspected a backdoor on the Micali-Schnorr generator → similar to Dual EC DRBG
  b. Initial avenue of research
  c. Is it used in practice?

Paper: https://eprint.iacr.org/2023/440

Day 2

- *Three Lessons From Threema: Analysis of a Secure Messenger by* Kenneth G. Paterson, Matteo Scarlata and Kien Tuong Truong
  - Using modern, secure libraries for cryptographic primitives does not on its own lead to a secure protocol design: It is possible to misuse libraries such as NaCl and libsignal
  - Beware of cross-protocol interactions

Information: https://breakingthe3ma.app/

Day 2

- *Interoperability in E2EE Messaging by* Esha Ghosh, Paul Grubbs, Julia Len and Paul Rösler
  - Identity Interoperability and Discovery
  - Messaging Protocols
  - Abuse Prevention

More information: https://eprint.iacr.org/2023/386.pdf

Lesson from Day 2

- Rethink on who we design for, and how we design for them
- Backdoors seem to still be an avenue for research
- Attacks on practice:
  - Cross protocol attacks
- Interoperability on secure messaging is on its early stages
  - Lots of research and design is needed

Day 3

- *HACSPEC: a gateway to high-assurance cryptography* by Franziskus Kiefer, Karthikeyan Bhargavan, Bas Spitters and Manuel Barbosa
  a. Formal verification is evolving!
  b. Integrate it on the implementation workflow

More information: https://github.com/hacspec/hacspec

Day 3

- *Using ZK Proofs to Fight Disinformation* by Trisha Datta and Dan Boneh
  - Use zk to proof “content provenance”
  - Reaction to the The Coalition for Content Provenance and Authenticity (C2PA) proposal: https://c2pa.org/specifications/specifications/1.1/specs/C2PA_Specification.html

More information:
https://medium.com/@boneh/using-zk-proofs-to-fight-disinformation-17e7d57fe52f

Lesson from Day 3

- “Novel” cryptography is on the rise:
  - ZK, threshold…
  - Seems capable to solve challenging problems → more research and consideration is needed
- Formal verification is landing

THANK YOU!

@claucece