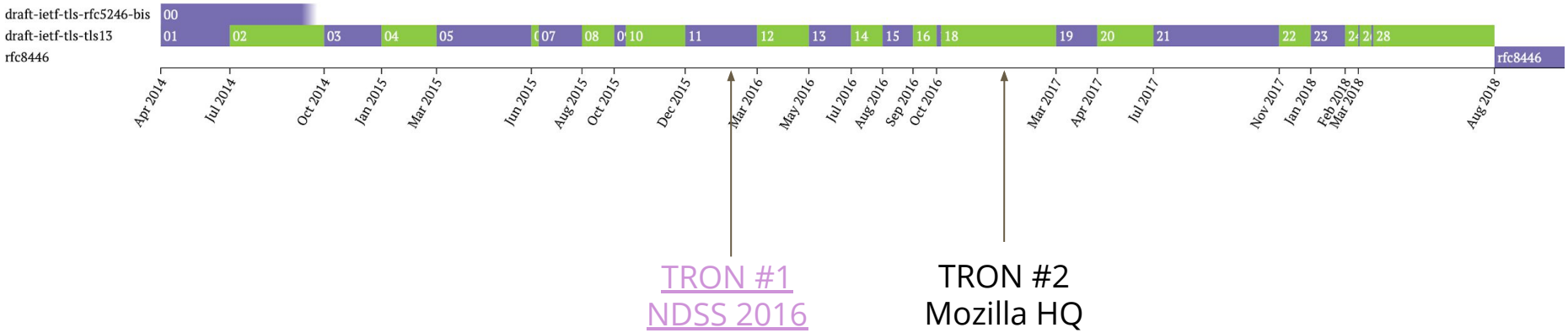
Privacy and Security Workshop
NDSS 2020
February 23, 2020

https://www.ndss-symposium.org/ndss-program/2020-program/quips-workshop/

TLS 1.3


draft-ietf-tls-rfc5246-bis
draft-ietf-tls-tls13
rfc8446
00
01
02
03
04
05
07
08
10
11
12
13
14
15
16
18
19
20
21
22
23
28
rfc8446
Apr 2014
Jul 2014
Oct 2014
Jan 2015
Mar 2015
Jun 2015
Aug 2015
Oct 2015
Dec 2015
Mar 2016
May 2016
Jul 2016
Aug 2016
Sep 2016
Oct 2016
Mar 2017
Apr 2017
Jul 2017
Nov 2017
Jan 2018
Feb 2018
Mar 2018
Aug 2018
TRON #1
NDSS 2016
TRON #2
Mozilla HQ

TLS Analysis

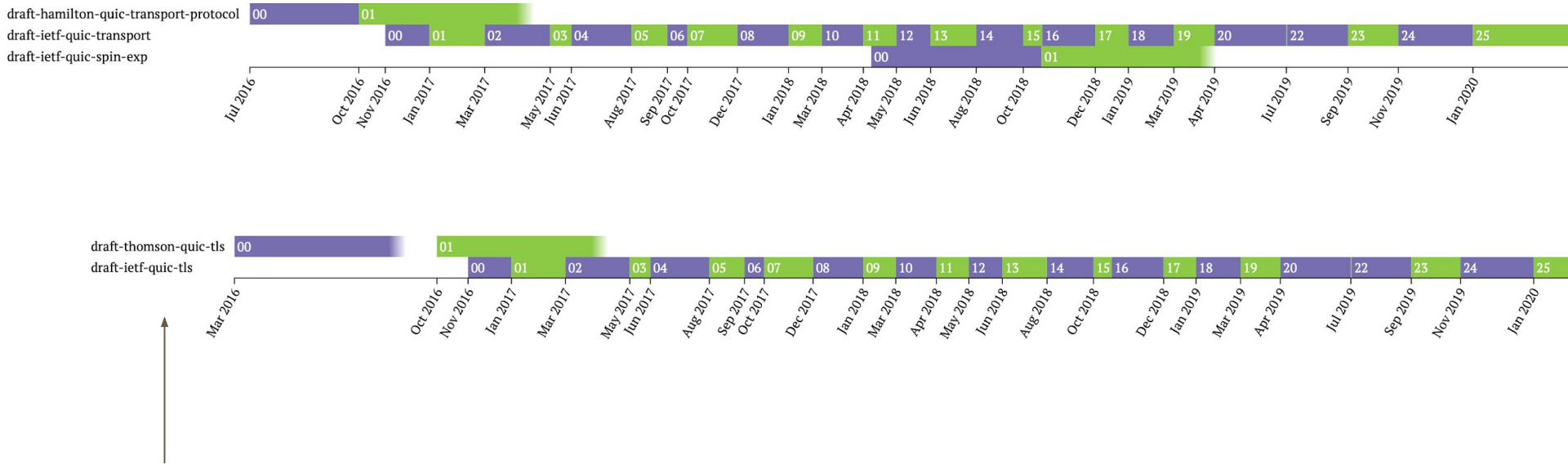
At least 15 highly cited papers focusing on the *core protocol*

Proofs in the symbolic and computational models

More research underway…

- Handshake privacy
- Hybrid key exchange models
- Semi-static key exchange and 0-RTT priming
- Safe external PSK usage

IETF QUIC



QUIC Crypto

IETF QUIC Analysis

Variety of papers covering different QUIC versions:

- Lychev, Robert, et al. "How secure and quick is QUIC? Provable security and performance analyses." *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015.
- Jager, Tibor, Jörg Schwenk, and Juraj Somorovsky. "On the security of TLS 1.3 and QUIC against weaknesses in PKCS# 1 v1. 5 encryption." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015.
- Fischlin, Marc, and Felix Günther. "Multi-stage key exchange and the case of Google's QUIC protocol." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014.
- Langley, Adam, et al. "The quic transport protocol: Design and internet-scale deployment." *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*. 2017.
- ...

How many of them apply to the current QUIC protocol version?

Why QUIPS? Why Now?

QUIC(v1) is a non-trivial extension to TLS nearing the end of standardization

To our knowledge, there has been no dedicated conference, workshop, or journal welcoming papers on the protocol

Before the RFC is minted...

1. Raise awareness to protocol design aspects and properties worthy of analysis
2. Give the academic community time to analyze!

Workshop Overview

Primary goals:

- Discuss QUIC's past, present, and future
- Analyze currently specified protocol
- Highlight possible issues or areas worth further analysis

Expected outcomes:

- Analysis results fed right back into QUICv1
- Report of workshop circulated to the QUIC WG

Agenda

Morning Sessions

- New peer-reviewed research paper presentations

Afternoon Sessions

- Previously published paper presentations and talks

Panel and Conclusion

- Answers for your burning questions!

Thanks to the PC!

Adam Langley	Google
Adrian Perrig	ETH Zürich
Antoine Delignat-Lavaud	Microsoft
Bryan Parno	Carnegie Mellon University
Cas Cremers	CISPA Helmholtz Center for Information Security
Christian Huitema	Private Octopus Inc.
Christopher Wood	Apple
Felix Günther	ETH Zürich
Martin Thomson	Mozilla
Subodh Iyengar	Facebook

A Couple Requests...

Note taker for each session?

Volunteers to help with the report upon workshop completion?