Not-So-Low Hanging Fruit
Security and Privacy Research Opportunities for IETF Protocols

Christopher A. Wood
Research Lead, Cloudflare

IETF 117 - Applied Networking Research Workshop 2023
Improper Forward Secrecy: How Diffie-Hellman Fails in Practice

David Adrian*, Karthikeyan Bhargavan*, Zakir Durumeric*, Pierrick Gaudry, Matthew Green
J. Alex Halderman*, Nadia Heninger, Drew Springall*, Emmanuel Thomé, Luke Valenta
Benjamin Vanderyse* Eric Wustrow* Santiago Zanella-Béguelin*, Paul Zimmermann

*INRIA Paris-Rocquencourt **INRIA Nancy-Grand Est, CNRS, and Université de Lorraine
\*Microsoft Research \*University of Pennsylvania \*Johns Hopkins \*University of Michigan
For additional materials and contact information, visit WeekiF.org.

The OPTLS Protocol and TLS 1.3
(extended abstract)
Hugo Krawczyk* Hoeteck Wee*
October 9, 2015

The QUIC Transport Protocol:
Design and Internet-Scale Deployment
Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan
Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind,
Joanna Kulik, Patrik Westin, Raman Yenteti, Robbie Shade, Ryan Hamilton, Victor Vasiliev,
Wan-Teh Chang, Zhongyi Shi
Google
quic-sigcomm@google.com
QUIC: A UDP-Based Multiplexed and Secure Transport

Using TLS to Secure QUIC
### Specifications

<table>
<thead>
<tr>
<th>quic-go</th>
<th>ngtcp2</th>
<th>quant</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Diagram" /></td>
<td><img src="image2.png" alt="Diagram" /></td>
<td><img src="image3.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>
HTTP version by requests share over time (Multiple browsers, Worldwide)

Worldwide - 2022-05-26 00:00:00 to 2023-04-30 01:00:00 (UTC)

https://blog.cloudflare.com/http3-usage-one-year-on/
Specifications at the IETF

Specifications transfer science to software (theory to practice)

Clear descriptions for target algorithm, protocol, or system

Basis for implementations and deployments

Targets for verification and analysis

Specifications encourage open collaboration and build communities
Software at the IETF

Software is a primary input and output of the IETF

  Rough consensus *and running code*

  Standards service interoperable deployments of protocols

Shipping software reveals new insights and unearths new challenges
Science at the IETF

Science is a valuable part of shipping IETF protocols

  Advances our understanding of problem and solution space

  Improves confidence in what we ship

Science has transitive effects on other parts of the process

  Progress creates opportunities for more research
Multiparty Computation
Multiparty Computation Overview

Multiparty Computation (MPC) is a technique for computing (arbitrary) functions over private inputs.

- Privacy-preserving measurement (PPM)
- Privacy-preserving ad-click attribution (IPA)

Specialized MPC protocols are being standardized and deployed today:

- Distributed Aggregation Protocol (draft-ietf-ppm-dap)
- Verifiable Distributed Aggregation Protocol (draft-irtf-cfrg-vdaf)
Are there more performant heavy hitter protocols?

How do we helpfully compose differential privacy with these protocols?
Is DAP correct?

Can we prove so with symbolic analysis?
Can we formally verify VDAF implementations?

Can we provide guidance for users of these protocols and libraries in practice?

Janus is an experimental implementation of the Distributed Aggregation Protocol (DAP) specification. Currently it supports VDAFs with trivial aggregation parameters only, e.g., Prio3. VDAFs with nontrivial aggregation parameters (e.g., Poplar) are not yet supported.

Janus is currently in active development.

Daphne

Daphne is a Rust implementation of the Distributed Aggregation Protocol (DAP) standard. DAP is under active development in the PPM working group of the IETF.
Other Research Opportunities

Anonymous credentials
- Post quantum cryptographic solutions
- Formal verification of existing implementations
- Deployable generic anonymous credentials

Zero-knowledge proof (systems)
- Building blocks for higher-level protocols (API models and reusable abstractions)
- Formally verified and reference implementations for experimentation
- New protocol embeddings
Questions?
Comments?
Not-So-Low Hanging Fruit
Security and Privacy Research Opportunities for IETF Protocols

Christopher A. Wood
Research Lead, Cloudflare

IETF 117 - Applied Networking Research Workshop 2023