CS408 Computer Networks Spring 2024
Homework 2

Kanat Özgen

March 2024

1 Title of the Session and the Speaker

Title of the session was "Post-Quantum Use In Protocols". The main speaker was Paul Hoffman. Hoffman is a network engineer mainly interested in security.

2 What Was the Session About

Session was mainly about the defense line against post-quantum era of payload security. When quantum computing technologies reach a point where breaking a password is no matter, more than several adjustments should be made to the technologies that revolve around secure connections, secure transmissions etc.

3 Material Coverage and Previous Discussions

3.1 What Did the Materials Cover

The document provides a comprehensive analysis of various aspects of hybrid signature schemes, including their design principles, security features, and potential advantages and disadvantages. Also, in the document, extensive information regarding PQC is present. The information in the PDF file includes explanations of why engineers need to be aware of and understand post-quantum cryptography, insights into key sizes, processing time differences between PQC algorithms and traditional ones, and recommendations for security/performance trade-offs in the context of PQC.

3.2 What Did the Group Discuss in Previous Meetings

They discussed the classification of design goals and security considerations for hybrid digital signature schemes. This includes aspects like proof composability, non-separability of component signatures, backward/forward compatibility, and simultaneous verification among others. They also discussed the impact of Cryptographically Relevant Quantum Computers (CRQCs) on current cryptographic systems and the need for transitioning to post-quantum algorithms to ensure long-term security. This includes understanding differences between Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEMs) and traditional key exchange mechanisms, as well as insights into expected key sizes and processing time differences. In IETF 118, name changes occured in many of the protocol names.

4 What Did the Engineers Talk About

4.1 Nomenclature

In previous IETF meetings, some encryption strategies were given a name. However, these names changed in the past two meetings. Also, there is an ongoing debate in the usage of terms such as "Composite" and "Hybrid" about where to use them etc. A British lady dominated this particular subject.

4.2 PQC Migration Use Cases

There has to be a migration step for the adoption of PQ encryption strategies. These migration steps must be systematically approached.

4.3 Hash-based Signatures

A decision-tree like structure (There was a debate going on as to what to call this data structure) that has one-time-use keys as leaf nodes. Divide the time in epochs, and for each epoch, have one key. Do not ever reuse a key. Manage the state of used keys, which is a very hard subject. The division of time in epochs is also a big problem because UNIX time and XMLDate types are not very much aligned and a solution is yet to be found.

4.4 Composite and Parallel Signatures

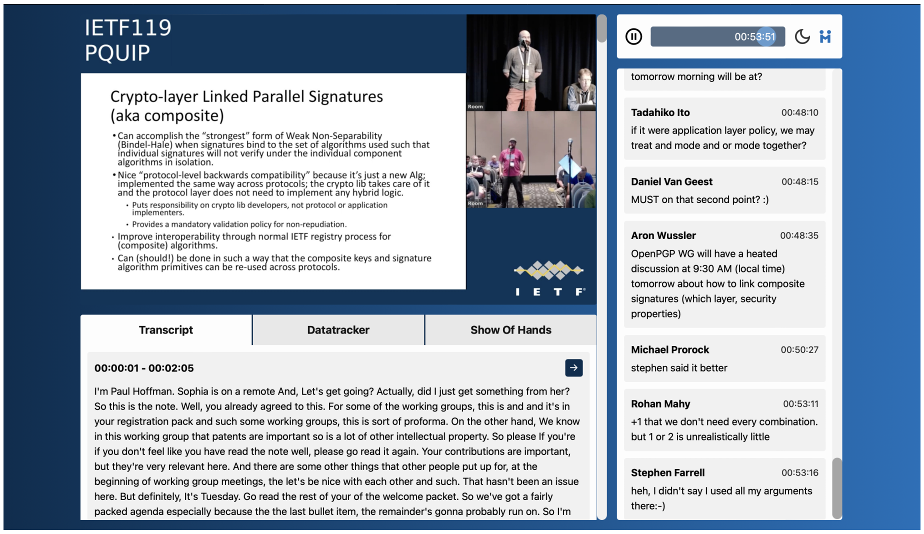
This was the main talking point of the whole session. There are parallel and composite encryption models. Parallel encryption models mainly encapsulate the aggregate usage of both PQ and T-type encryption models. There are OR-type parallelizations and AND level parallelizations. Also there exists composite approaches where OpenPGP and CMS are the main hybrid signature types.

5 What Did You Learn in the Context of Computer Networks?

The parallelization schemes mainly take place in the application layer of the TCP/IP protocol. The JSON payload sent with an HTTP request of the Application layer will have multiple signatures alongside with the actual payload of the JSON object. By this way, in OR-type models, modifications to the already-existing protocol infrastucture will be much more easier.

6 Proof of Attendance to an IETF Meeting

Here is a screenshot taken from the Meetecho session of the PQUIP meeting in IETF 119 Brisbane:



IETF119
PQUIP

Crypto-layer Linked Parallel Signatures (aka composite)

- Can accomplish the "strongest" form of Weak Non-Separability (Bindel-Hale) when signatures bind to the set of algorithms used such that individual signatures will not verify under the individual component algorithms in isolation.
- Nice "protocol-level backwards compatibility" because it's just a new Alg; implemented the same way across protocols; the crypto lib takes care of it and the protocol layer does not need to implement any hybrid logic.
  - Puts responsibility on crypto lib developers, not protocol or application implementers.
  - Provides a mandatory validation policy for non-repudiation.
- Improve interoperability through normal IETF registry process for (composite) algorithms.
- Can (should!) be done in such a way that the composite keys and signature algorithm primitives can be re-used across protocols.

00:00:01 - 00:02:05

I'm Paul Hoffman. Sophia is on a remote And, Let's get going? Actually, did I just get something from her? So this is the note. Well, you already agreed to this. For some of the working groups, this is and and it's in your registration pack and such some working groups, this is sort of proforma. On the other hand, We know in this working group that patents are important so is a lot of other intellectual property. So please If you're if you don't feel like you have read the note well, please go read it again. Your contributions are important, but they're very relevant here. And there are some other things that other people put up for, at the beginning of working group meetings, the let's be nice with each other and such. That hasn't been an issue here. But definitely, It's Tuesday. Go read the rest of your of the welcome packet. So we've got a fairly packed agenda especially because the the last bullet item, the remainder's gonna probably run on. So I'm

tomorrow morning will be at?

Tadahiko Ito 00:48:10
if it were application layer policy, we may treat and mode and or mode together?

Daniel Van Geest 00:48:15
MUST on that second point? :)

Aron Wussler 00:48:35
OpenPGP WG will have a heated discussion at 9:30 AM (local time) tomorrow about how to link composite signatures (which layer, security properties)

Michael Prorock 00:50:27
stephen said it better

Rohan Mahy 00:53:11
+1 that we don't need every combination. but 1 or 2 is unrealistically little

Stephen Farrell 00:53:16
heh, I didn't say I used all my arguments there:-)