Title: Formal Analysis of Quantum Resistant Network Protocol Proposals

Ed Zieglar

Problem Statement

Recent developments in quantum computer research demonstrate that a cryptographically relevant quantum computer is a possibility. Although the advent of such a machine could be years from now and likely unannounced if developed by a nation state actor, the existence of such a machine threatens all our data that traverses the network. In anticipation of the development of such a quantum computer, standards bodies have begun proposing quantum resistant modification to existing standards to mitigate the threat.

Standards bodies, such as the IETF, have also realized that more care should be put into the development of security protocols to prevent the release of vulnerable specifications. Toward that end, the IETF has been encouraging the submission of formal analysis and proofs of the security properties of proposed protocols. Unfortunately, the protocol designers are often not knowledgeable in the approaches or tools for formal analysis and rely on outside groups to perform the analysis of their protocols. To that end, this project is intended to provide formal analysis to verify the security properties of the proposed quantum resistant modifications to existing protocols.

Proposed Approach

Choose a recently proposed quantum resistant protocol modification and perform an analysis of the security properties of the protocol. There have been recent requests for an analysis of RFC 8773 so there would be particular interest in the results, although other protocols are also in need of analysis. The analysis can be performed with any number of cryptographic protocol analysis tools with which the students may be familiar. We tend to use the Cryptographic Protocol Shapes Analyzer (CPSA), so for students that are not already familiar with a tool, training can be provided in CPSA to the students. The objective of the analysis would be to verify the security properties of the protocol specification or identify any vulnerabilities and propose verified fixes to the specification.

Areas of Research: Network Security, Quantum Resistance, Formal Analysis

Student Participant Background Needed

This project is focused on the verification of the security of proposed internet security standards. As such, the students should have an understanding of the following basic concepts:

- A core understanding of network protocols and network operation
- An understanding of network security concepts and network attacks
- Familiarity with programming concepts. Although the students will not be writing programs, the input to many of the tools has a resemblance to many programming languages.
- Some familiarity with the mathematical proofs and notations in first order logic.

Resources

Literature and resources available for pre-project preparation include:

- IETF RFCs (There is current interest in RFC 8773 being analyzed. This will require familiarity with the TLS 1.3 RFCs)
- There are published formal analysis of different protocols available. If choosing to analyze RFC 8773, there exist TLS 1.3 published analyses performed with both Tamarin and ProVerif.
- Recent analysis of the Session Binding Proxy protocol and FIDO UAF registration and authentication protocols with CPSA have been submitted for publication and are available upon request.

References to various tools that could be used are the following. Note that we use CPSA and have the most expertise in that tool readily available, but if students are familiar with another tool, that is acceptable as well

1. CPSA can be found at: https://hackage.haskell.org/package/cpsa or https://github.com/mitre/cpsa
2. Maude-NPA can be found at: http://maude.cs.uiuc.edu/tools/Maude-NPA/
3. Tamarin Prover can be found at: https://tamarin-prover.github.io
4. ProVerif can be found at: https://bblanche.gitlabpages.inria.fr/proverif/
5. Example report of a formal analysis of a protocol with CPSA can be found at: https://arxiv.org/abs/2003.07421

Potential Cybersecurity Benefit

We are reliant on the security standards published by the standards bodies. These bodies are made up of participants from around the world creating those standards. Some of those participants have differing views on what security protocols should provide. Verification of the properties that the protocols actually provide is advantageous to understanding which standards should be adopted to provide required security and to eliminate vulnerabilities that may have been overlooked by the developers.