From: Smith-Tone, Daniel (Fed)
To: Sonmez Turan, Meltem (Fed)
Subject: Talk
Date: Monday, May 16, 2016 12:03:04 PM

Speaker: Oscar Garcia Morchon

Title: Efficient Quantum-Resistant Trust Infrastructure based on HIMMO

Abstract:

Secure Internet communications face conflicting demands: advances in (quantum) computers require stronger, quantum-resistant algorithms, while at the same time the Internet of Things demands better-performing protocols; and finally, communication links usually depend on a single root-of-trust, e.g., a certification authority, a single point-of-failure that is too big of a risk for future systems.

This paper proposes a hybrid infrastructure that combines a quantum-resistant HIMMO key pre-distribution scheme based on multiple Trusted Third Parties with public-key cryptography to address these problems. During operation, any pair of devices can use HIMMO key material and public-keys to establish a secure link, and public-keys are then certified by multiple TTPs. The solution is resilient to the capture of individual roots of trust, without affecting performance, while public keys can provide features such as forward secrecy. Combining HIMMO identities with public-keys enables secure certification of public keys and distribution of HIMMO key material from multiple TTPs, without requiring an out-of-band channel. The infrastructure can be tuned to fit Internet of Things scenarios benefiting from an efficient, non-interactive and authenticated key exchange, or to fit use cases where the use of multiple TTPs provides privacy safe-guards when lawful interception is required.

As proof-of-concept we show how TLS can benefit from these ideas with minimal extensions, while exhibiting good security features and performance compared with solutions based on public-key cryptography only.

Here is a link to an eprint that interested attendees may want to read:
http://eprint.iacr.org/2016/410.pdf

This is entirely made up. It could be the case that he talks about Mickey Mouse. I actually have no clue.

Cheers,
Daniel