From: Mouha, Nicky W. (IntlAssoc)
To: ntcw2019
Subject: TC-forum e-mail
Date: Thursday, February 28, 2019 2:17:33 PM

Hi all,

Below is an e-mail that I'm planning to send to later today to tc-forum, as we discussed this morning. Let me know if you have any feedback!

PS: It can be a good idea to check the spelling of the NTCW website: I see "theroshld" instead of "threshold"...

Regards,
Nicky

Dear subscribers of the NIST Threshold Crypto forum,

Registration closes on **March 4th** for the NIST Threshold Cryptography Workshop 2019, to be held at NIST, Gaithersburg, Md. on March 11-12, 2019. The full program is available here: https://csrc.nist.gov/Events/2019/NTCW19 (#NTCW2019).

We're happy to let you know that the titles and abstracts for the keynote talks are now available.

Keynote 1: **Threshold Cryptography: Ready for Prime Time?** (Hugo Krawczyk, IBM Research)

The trend in trust decentralization together with the ever increasing value of digital assets (cryptocurrencies, blockchains, mega data repositories, key (mis)management, intellectual property, privacy, etc.) and the need to protect these assets for secrecy and availability, make threshold cryptography a most relevant technology whose time has come. We need to see more targeted applications as well as software platforms on which to build solutions that take into account real-world considerations such as asynchronous networks, support for diversified architectures, hardware enclaves, and more. Additionally, we need to refresh the set of techniques supporting threshold cryptography with advances in areas such as multi-party computation, quantum-resistant primitives, and blockchain-inspired consensus protocols. In addition to arguing these points, the talk will discuss some recent applications of threshold cryptography in the domain of key and password management, blockchain, and how threshold cryptography can be relevant to the #metoo movement.

Keynote 2: **Challenges for Multisignature and Threshold Signature Implementation in a**

Bitcoin Context (Andrew Poelstra, Blockstream)

Bitcoin, started in 2009, is a digital currency in which all activity is publicly verifiable. Coins are controlled by spending policies expressed in Bitcoin Script, a simple stack-based programming language which supports hash preimage challenges and digital signatures. Included in Bitcoin Script is a basic form of threshold ECDSA signature: a list of public keys and a threshold is specified; the coins can then be moved if threshold-many valid ECDSA signatures are provided in sequence.

This threshold scheme is inefficient in terms of both signature size and verification time (both linear in the threshold size), which are the two most important considerations for cryptosystems designed for inclusion on blockchains. Being explicitly specified, they also represent a fungibility loss as threshold-controlled coins are visibly distinct from non-threshold-controlled coins. However, they achieve several practical goals which have proved difficult to preserve in more efficient threshold schemes: they are noninteractive; they require no persistent state during signing; they work in the plain public-key model and require no interactive key setup; their security follows immediately from the security of the underlying ECDSA scheme even when signing counterparties are considered to be adversarial.

In this talk we describe our work in developing a multisignature scheme for Bitcoin, called MuSig, which supports an extension to threshold signatures, over the last several years. We describe how consideration of both practical use cases and formal security models guided the evolution of our goals, and the unexpected tradeoffs that we found ourselves forced to make.

Regards,
Nicky
On behalf of the Threshold Cryptography Team