Compact Asymmetric Authentication using Hash-based Signatures

David McGrew mcgrew@cisco.com

Emerging Technologies and Applications: Smart Objects, Internet of Things, Software Signing

Cryptographic Requirements: Compact Digital Signature Implementations

Abstract:
Hash-based signatures are amenable to extremely compact implementations, and their performance is competitive with other digital signature technologies. This compactness is valuable for software and firmware authentication, as well as entity authentication. In order to authenticate system software, such as a bootloader, an operating system kernel, or a device driver, it is necessary to have signature validation function implemented in the hardware, BIOS, FPGA, or firmware that loads and runs that software.
In many systems it is essential for these cryptographic functions to be small, so that they can be accommodated in the software-loading system. The compactness of OTS implementations is also useful in constrained environments in which entity authentication is needed, such as device authentication for smart objects. There has been a resurgence in interest in hash-based signatures in recent years, because of their "post quantum" security: unlike RSA, DSA, and ECDSA, they can be secure even if a quantum computer is built. In this presentation, we describe some constrained environments that perform software and firmware authentication, then we review several hash-based signature designs, including the foundational work of Lamport, Winternitz, Merkle as well as more recent optimizations, and analyze implementation size, performance, and security for different parameter and hash function choices. We compare to other signature technologies, and show that hash-based signatures are well suited to constrained environments.

Submission to the Workshop on Cryptography for Emerging Technologies and Applications