UNIVERSITY OF SOUTH FLORIDA

Defense of a Master's Thesis

Efficient Forward-Secure and Compact Signatures
for the Internet of Things (IoT)
by

Efe Ulas Akay Seyitoglu

For the MSCS degree in Computer Science and Engineering

In the modern Internet of Things (IoT) applications, the system entities collect security-sensitive information that must be cryptographically protected. In particular, authentication and integrity, as foundational security services, are essential for any IoT applications. Digital signatures provide both authentication and integrity to these applications. Nevertheless, once an IoT device is compromised, its signature private key is leaked to an adversary. Forward-secure digital signatures mitigate the impact of such key compromises by incorporating a key-evolving mechanism into the authentication process. However, existing forward-secure signatures suffer from large signature/key sizes, heavy computational overhead, and some prominent variants that can only sign a limited number of messages. Hence, there is a critical need for forward-secure and compact digital signatures that can be used to authenticate large amounts of critical information.

In this work, we proposed two forward-secure signatures with signature and partial public key aggregation capabilities that we refer to as $\text{CORE}^{\text{K}}_{\text{Base}}$ and CORE_{MMM}. Our first scheme, to the best of our knowledge, is the first K-time forward-secure and aggregate signature scheme with a public-key aggregation feature. The idea is to use a hash-chain mechanism to evolve the keys and pre-compute the aggregated public key. For each message, we compute its signature and aggregate it. $\text{CORE}^{\text{K}}_{\text{Base}}$ offers compact public keys as well as compact signatures with low verification overhead. We fully implemented $\text{CORE}^{\text{K}}_{\text{Base}}$ in commodity hardware and tested for various performance metrics. We also compared $\text{CORE}^{\text{K}}_{\text{Base}}$ with its most efficient counterparts . For instance, $\text{CORE}^{\text{K}}_{\text{Base}}$ has 180x faster signature verification compared to its most verification-efficient counterpart, it also has 16.5x more compact public-keys compared to the most public-key compact counterpart. Our second scheme CORE_{MMM}, is a practically unbounded forward-secure signature scheme that leverages $\text{CORE}^{\text{K}}_{\text{Base}}$. Our use of $\text{CORE}^{\text{K}}_{\text{Base}}$ is central to the design of CORE_{MMM} because we crafted $\text{CORE}^{\text{K}}_{\text{Base}}$ to optimize the performance of unbounded signing capability under the generic MMM transformation. To the best of our knowledge, this specific design led to the most efficient compromise-resilient and compact signature which we refer to as CORE_{MMM}. We also compared the performance of CORE_{MMM} with its state-of-art alternatives. Our analysis shows that CORE_{MMM} outperforms its state-of-art counterparts in most performance metrics. Some notable examples include small public keys (only 32 Bytes), more than two magnitudes more efficient key updates, compact signatures, and a magnitude smaller private keys compared to its most efficient counterparts for each metric.

Friday, February 7, 2020
2:30pm
ENB337

THE PUBLIC IS INVITED

Examining Committee

Attila Altay Yavuz, Ph.D., Major Professor
Jay Ligatti, Ph.D.
Mehran Mozaffari Kermani, Ph.D.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.