GridStat Middleware Communication Framework: Management Security and Trust

K-Time Signature Deployment: A Practical Framework

Kelsey Cairns, Carl Hauser

GOALS

High-Level

- Provide fast authentication for high-rate, low-latency sensor data streams.

Focused

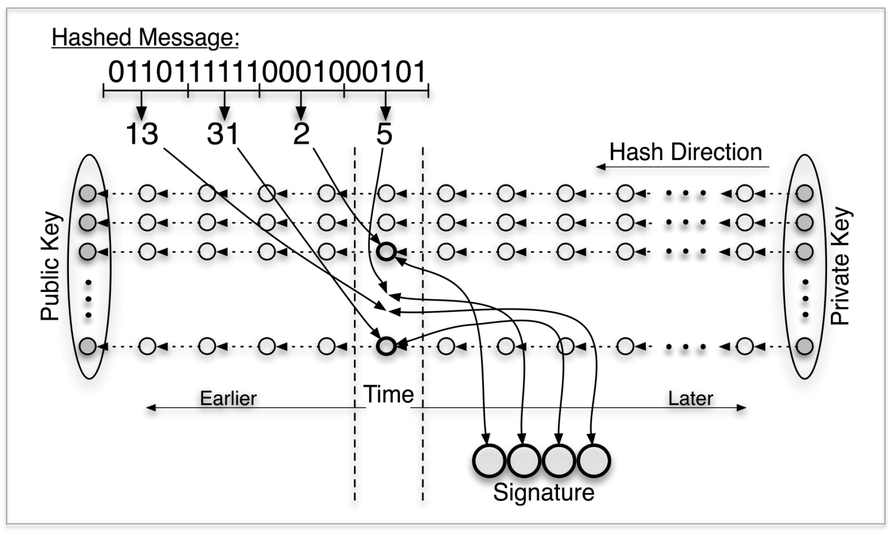
- Create a deployment framework for data authentication using k-time signatures.
  - Pre-compute and distribute future key material in a continuous stream.
  - Efficiently transmit key material independently of message stream.
- Build framework for TV-OTS on GridStat.
- Validate through testing with DETERLab testbed.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Data authentication for Smart Grid applications ideally supports the following features:
  - Low latency.
  - Secure multicast.
  - Low key distribution overhead.
  - Message independence.
- Current protocols do not satisfy these requirements.
- Our previous work shows TV-OTS has these features:
  - Low-latency signature generation and verification.
  - Flexibility to adjust security and performance.
  - Robust against attacks (dictionary, DoS, dropped packet, replay).

TV-OTS Overview

- Time divided into fixed-length epochs.
- Senders maintain a set of secret hash chains.
- Signatures are created with the HORS signature scheme, using the set of i^{th} hash chain secrets during epoch i.
  - Messages hashed into multiple short bit strings (indices).
  - Generated indices specify secrets to include in signature.
  - Timestamp also included in signature.
- Signature verification.
  - Packet freshness verified.
  - Indices generated from message to determine expected index of each included secret's chain.
  - Each secret verified by hashing to recreate publicly known value.
  - Verified for the epoch of the signature timestamp.



Current Challenges

- Large amounts of key material (hash chain secrets) require pre-computation.
  - Can be performed out of band.
- Public keys for new hash chains must be received before old chains are exhausted.

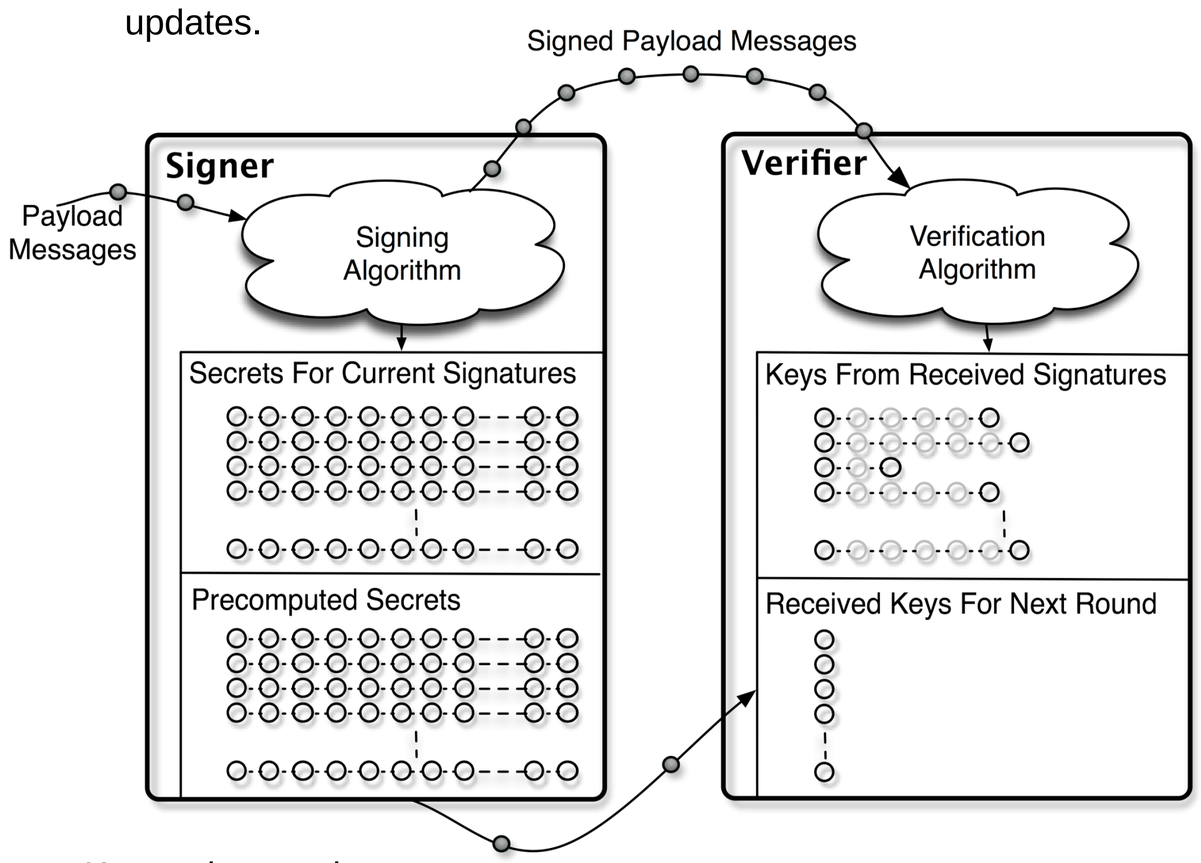
RESEARCH PLAN

- Design and develop deployment framework for TV-OTS.
  - Timing of transmitted key material must allow seamless transitions from each hash chain to the next.
  - Should be robust even without delivery guarantees.
  - Potentially distribute keys to late-joining receivers.
- Implement as part of GridStat.
- Deploy in DETERLab for robustness testing.

RESEARCH RESULTS

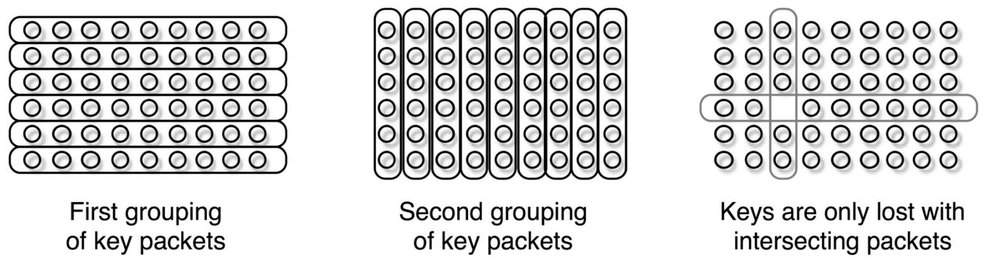
Design Overview

- Separate key and data transmission.
- Senders compute future public keys while signing with current secrets.
- Key update messages much less frequent than payload messages.
  - Allows traditional public key authentication (e.g., RSA) for key updates.



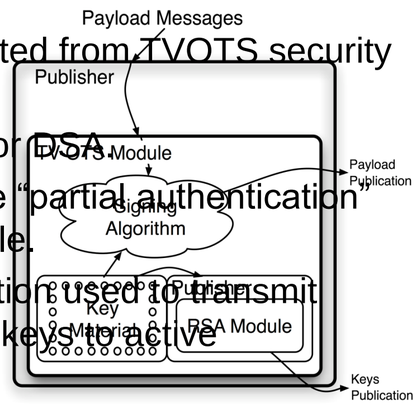
- Key update packets carry keys in small groups.
- Redundancy strategies protect against loss of keys during transit:
  - Option 1: Maximal overlap: small probability of many lost keys.
  - Option 2: Minimal overlap: high probability of a few lost keys.

Minimal Overlap Strategy Example



Implementation Using GridStat

- Key publication initiated from TVOTS security module.
  - Signed with RSA or DSA.
- Subscribers may use "partial authentication" if keys are unavailable.
- Periodic communication used to transmit current intermediate keys to active subscribers.



BROADER IMPACT

- Addresses the framework problem faced by all k-time signature schemes.
- Fast authentication, applicable to a large class of big data applications.

INTERACTION WITH OTHER PROJECTS

- Continuing investigation of TV-OTS, originally a TCIP project.
- Implemented as part of GridStat.
- Leverages GridStat's deployment in DETERLab.

FUTURE EFFORTS

- Complete implementation and testing.
- Compare HORS signatures to others in the same family.
- Investigate potential real-world interest.

References:

[1] Kelsey Cairns; Carl Hauser; Thoshitha Gamage, "Flexible Data Authentication Evaluated for the Smart Grid," IEEE SmartGridComm 2013, October 2013

[2] Kelsey Cairns; Thoshitha Gamage; Carl Hauser, "Efficient Targeted Key Subset Retrieval in Fractal Hash Sequences," ACM CCS 2013, November 2013

[3] Qiyan Wang; Himanshu Khurana; Ying Huang; Klara Nahrstedt, "Time Valid One-Time Signatures for Time-Critical Multicast Data Authentication," IEEE InfoCom 2009, April 2009

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T