TCIPG

GridStat Middleware Communication Framework: Management Security and Trust

Flexible Data Authentication Evaluated for the Smart Grid

Kelsey Cairns, Carl Hauser, and Thoshitha Gamage

GOALS

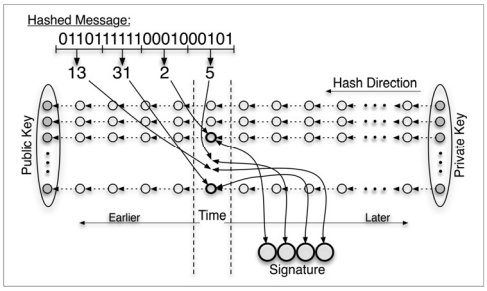
- Evaluate Time-Valid One-Time Signatures (TV-OTS) data authentication protocol with respect to smart grid applications.
  - Consider the specific needs of smart grid applications.
  - Theoretically evaluate the security of TV-OTS signatures.
  - Implement TV-OTS for latency testing.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Data authentication for smart grid applications ideally supports the following features:
  - Low latency.
  - Multicast.
  - Low key distribution overhead.
  - Message independence.
- Current protocols do not satisfy those requirements.
- TV-OTS has these features, and more:
  - Flexibility to adjust security and performance.
  - Robust against attacks (Dictionary, DoS, Drop Packet, Replay).

TV-OTS Overview

- Time divided into fixed-length epochs.
- Signatures created with HORS using different keys in each epoch.
  - Large indexed pool of available secret keys.
  - Messages hashed into multiple short bit strings (indices).
  - Generated indices specify keys to include in signature.
  - Time stamp also included in signature.
- Signature verification.
  - Indices generated from message to determine expected index of each included key.
  - Each key is verified by hashing to recreate publicly known value.
  - Keys verified for the epoch of the signature timestamp and the expected key index.



- Hash chains supply new keys for each epoch.
  - New secret keys verified by previously exposed keys.
- Key distribution overhead incurred only when chains are initialized.

RESEARCH PLAN

- Formulate security analysis against brute-force attacks in two cases:
  - Attacker forges the signature to a specific given message.
  - Attacker finds a message for which a signature can be forged.
- Implement TV-OTS in GridStat.
- Use security analysis to guide parameter choices for latency testing.
- Perform latency tests on TV-OTS authenticated data streams.

Adjustable Parameters:

- N – Size of key pool / Number of hash chains
- n – Length of hash chain
- k – Number of keys carried in each signature
- r – Number of messages sent per epoch

For security analysis:

- x – Number of adversarial hash guesses per epoch

RESEARCH RESULTS

Security Against Brute Force Attacks

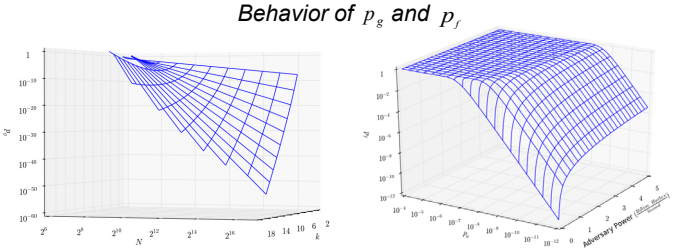
- Probability p_g of forging a given message involves:
  - Probability P_{k_g} that k_g keys are required for signature.
  - Probability p_{k_g} that all k_g required keys have been exposed.

$$p_{k_g} = \left(\frac{rk}{N}\right)^{k_g} \qquad P_{k_g} = \frac{\binom{n}{k_g}\binom{k-1}{k_g-1}}{\binom{k+n-1}{n-1}} \qquad p_g = \sum_{k_g=1}^{k} P_{k_g} \times p_{k_g}$$

- Probability p_f of finding any message involves:
  - Number of guesses attacker is capable of attempting (x).
  - Probability of guess's being correct (p_g).

$$p_f = 1-(1-p_g)^x$$

Behavior of p_g and p_f



Latency Testing

- Message rate fixed at 30 messages / second.
- Assumed adversary capable of 2 billion hashes / second.
- Hash chain length set at 8192, managed with *Fractal Hash Traversal.*
- Latency potentially improved by *Targeted Fractal Hash Traversal.*

N	k	Epoch (*s*)	Lifetime (*h:mm*)	Latency (*ms*)	p_g	p_f
1024	13	0.25	0:34	4.39	5.3e-14	2.6e-5
		1	2:16	1.87	3.6e-6	≈ 1
2048	14	0.5	1:08	3.93	1.4e-14	1.4e-5
		1	2:16	2.72	2.3e-10	.37
4096	13	1	2:16	3.99	5.3e-14	1e-4
		1.25	2:50	3.22	3.1e-12	.0077
8192	12	1	2:16	5.5	5.2e-17	≈ 0
		3	4:33	3.05	1.2e-13	8.5e-4
16384	11	1	2:16	6.98	1.3e-20	≈ 0
		4	9:06	2.1	2.1e-13	.0017

BROADER IMPACT

- Clarifies the effect of TV-OTS parameter selection on security, latency, and storage and communication overhead.
- Potential multicast data authentication solution.

INTERACTION WITH OTHER PROJECTS

- Implemented as a GridStat security module.
  - Accessible to other GridStat-based projects.

FUTURE EFFORTS

- Determine parameter choices based on risk analysis.
- Deploy testing in the DETER testbed environment.

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 Hahrstedt, "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