Building Dynamic Remote Attestation Framework

Wenjuan Xu (UNC Charlotte) **Gail-Joon Ahn (**Arizona State University) **Hongxin Hu (**Arizona State University)
Xinwen Zhang (Samsung Information Systems America) **Jean-Pierre Seiffert** (Technical University of Berlin)

UNCCHARLOTTE

ARIZONA STATE UNIVERSITY

Motivation

❖ Attesting a system dynamically changing is critical for the distributed environment. Two main barriers of dynamically attestation exist

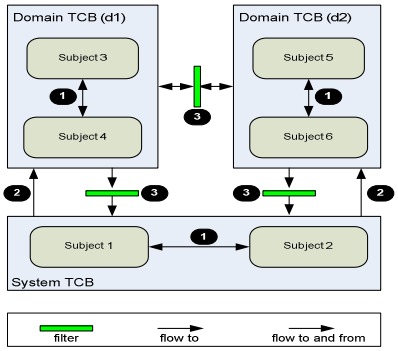
- ➢ *Efficiency requirement:* Due to the frequency of system changes and the volume of system state information, it is necessary to have an efficient way for attesting a system.
- ➢ *Effectiveness requirement:* It is necessary to have an effective way for presenting the attestation result and accommodating such results while resolving any identified security violations.

Aim

❖ Propose an approach for describing the system integrity requirements.
❖ Propose a dynamic attestation framework, which can efficiently attest the system against the proposed approach.
❖ Adopt a graph-based method for analyzing the security policy, based on which a technique for prioritizing the violation is required.

Method

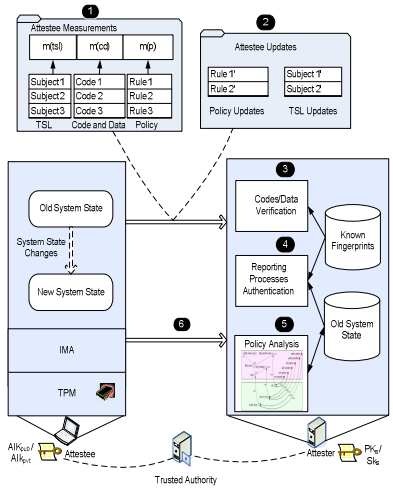
❖ Domain-Based Isolation



- ➢ System TCB is composed of a set of subjects and objects which are responsible or related to the reference monitor
- ➢ Domain TCB is composed of a set of subjects and objects in an information domain which has the same level of security.

- ➢ Domain-based isolation information flow principles:
  - ❑ Information flow is allowed within System TCB or Domain TCB
  - ❑ Information flow is allowed within System TCB or Domain TCB
  - ❑ TCB Information can flow from a domain TCB to another domain TCB or system TCB through Filter.

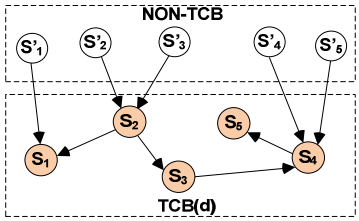
❖ Dynamic Remote Attestation Framework



- ➢ Step 1: The attestee measures the information including TSL, codes and data and policy and send to the attester
- ➢ Step 2 : The attestee generates the policy and TSL updates information and sends to attester
- ➢ Step 3: The attester verifies the measured information of the attestee
- ➢ Step 4: The attester verifies the reporting processes of the attester which is for the attestee information measurement and updates generation.
- ➢ Step 5: The attester analyzes the updated security policy of the attestee
- ➢ Step 6: The attester generates the attestation result and sends to the attestee.

❖ Policy Violation Analysis

- ➢ A policy violation graph



- ➢ Ranking policy violation graph
  - ❑ Ranking Subjects in TCB(d)
  - ❑ Ranking Direct Violation Path

Subject	SubjectRank
S_1	0.28
S_2	0.4
S_3	0.08
S_4	0.432
S_5	0.3456

Path	PathRank
$<S'_1, S_1>$	0.28
$<S'_2, S_2>$	0.8104
$<S'_3, S_2>$	0.8104
$<S'_4, S_4>$	0.6048
$<S'_5, S_4>$	0.6048

Results

❖ Attestee configuration:
- ➢ SELinux is configured on the attestee platform which is a Lenovo ThinkPad X61 with Dual , Atmel TPM
- ➢ IMA is installed on the attestee for measuring the information on the attestee

❖ Attestation Implementation
- ➢ Our attestation is realized based on a graph-based methodology.

❖ Performance evaluation:
- ➢ Our performance evaluation is mainly based on the system policy changes

Change	Dynamic Attestation		
Size	attestee	attester	Overhead
No change	0.23	0	0.23
-0.002MB (Reduction)	0.12	0.94	1.06
-0.019MB (Reduction)	0.09	0.91	1.00
-0.024MB (Reduction)	0.06	0.90	0.96
0.012MB (Addition)	0.38	0.96	1.34
0.026MB (Addition)	0.60	1.07	1.67

Attestation Performance For Dynamic Method

Change	Static Attestation		
Size	attestee	attester	Overhead
No change	14.76	90.13	104.89
-0.002MB (Reduction)	14.76	90.11	104.87
-0.019MB (Reduction)	14.74	89.97	104.34
-0.024MB (Reduction)	14.74	89.89	104.23
0.012MB (Addition)	14.77	90.19	104.96
0.026MB (Addition)	14.78	90.33	105.11

Attestation Performance For Static Method

Conclusion

❖ We have presented a dynamic remote attestation framework for efficiently attesting a target system
❖ We have adopted a graph-based methodology to represent integrity violations in an intuitive way with the ranking scheme.
❖ Our results showed that our dynamic approach can dramatically reduce the overhead compared to static approach

❖ References:

- ➢ **Wenjuan Xu**, Mohammed Shehab and Gail-Joon Ahn, "Visualization Based Policy Analysis: Case Study in SELinux," In Proceedings of 13th ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, USA, June 11-12, 2008
- ➢ **Wenjuan Xu**, Xinwen Zhang and Gail-Joon Ahn, "Toward System Integrity Protection with Graph-Based Policy Analysis," Data and Applications Security XXIII, 23rd Annual IFIP WG 11.3 Working Conference, Montreal, Canada, July 12-15, 2009. Proceedings

Acknowledgements

The work was partially supported by the grants from National Science Foundation (NSF-IIS-0242393) and Department of Energy Early Career Principal Investigator Award (DE-FG02-03ER25565).