ArmoredSoftware: Trust in the cloud

Annual Demonstration

Dr. Perry Alexander, Dr. Andrew Gill, Dr. Prasad Kulkarni,
Adam Petz, Paul Kline, Justin Dawson, Jason Gevargizian,
Leon Searl, Edward Komp

Information and Telecommunication Technology Center
Electrical Engineering and Computer Science
The University of Kansas
palexand@ku.edu,andygill@ku.edu,prasadk@ku.edu

January 15, 2015

KU INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

Outline

Introduction and Project Goals
- Big Picture
- Design Refinements

Prototype demonstration and discussion
- Refine big picture to current demo
- Protocol Execution
- Appraisal
- Measurement
- Communication
- Demonstration

Short term goals and milestones

Questions and guidance

Program Goal

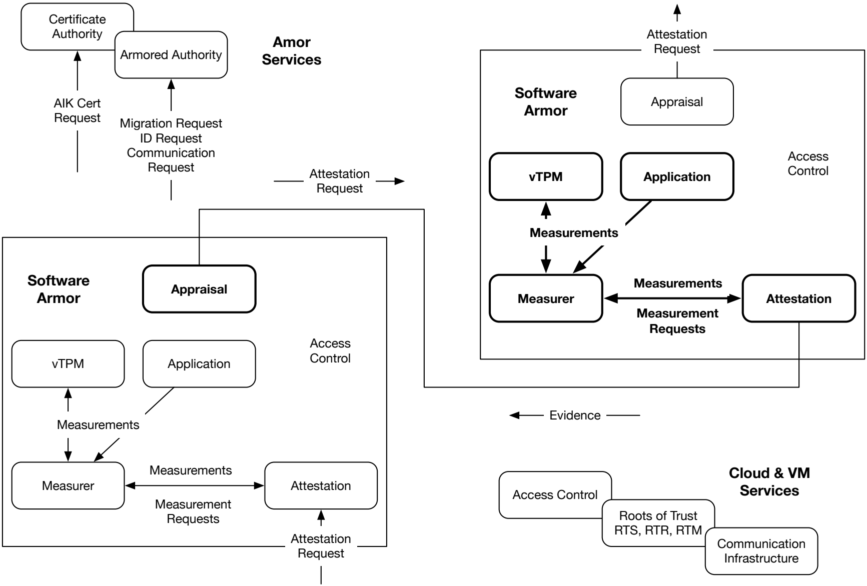
Trust in the Cloud

Provide new capabilities that help establish and maintain trustworthy cloud-based application deployment

New Capabilities

- Establish trust among cloud components
  - trust among cohorts of processes
  - trust among processes and environment
- Promote informed decision making
  - data confidentiality can be confirmed
  - execution and data integrity can be confirmed
- Autonomous run-time response and reconfiguration
  - responds to attack, failure, reconfiguration, and repair
  - response varies based on measurement
- Lightweight integration with existing cloud
  - targeting Xen, OpenStack, and Linux
  - user-space measurement and attestation

High-Level Architecture



Design Refinements

Demonstration Protocol

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

What We Are Demonstrating

3-4 Slides on Attestation Protocol Execution

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

1-2 Slides on Appraisal

3-4 Slides on Measurement

2-3 Slides on Communication Mechanisms

KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER The University of Kansas

Step Through Demonstration

Goals and Milestones for 2015

- Push to the cloud
- Establish roots of trust and trust argument
- Executable protocol representation and protocol semantics
- Operational, integrated vTPM prototype
- Name Server / Certificate Authority prototype
- More capable measurement
- Downloadable demonstration

Questions and Guidance

- What problems are interesting?
- What problem would be a nice attention grabber?
- What should we be watching and integrating with?

References

[1] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. Principles of remote attestation. *International Journal of Information Security*, 10(2):63–81, June 2011.

[2] V. Haldar, D. Chandra, and M. Franz. Semantic remote attestation – a virtual machine directed approach to trusted computing. In *Proceedings of the Third Virtual Machine Research and Technology Symposium*, San Jose, CA, May 2004.

KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas