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
- Implementation

Prototype demonstration and discussion

- Refine big picture to current demo
- Protocol Execution
- Appraisal
- Measurement
- Communication
- Demonstration

Short term goals and milestones

Questions and guidance

KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

Program Goal

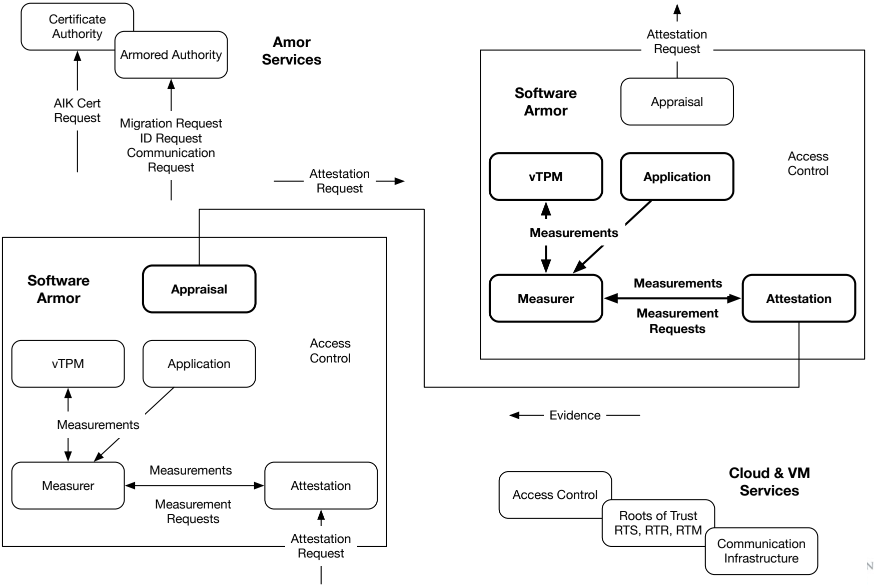
Trust in the Cloud

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 TXT, Xen, Linux, and OpenStack infrastructure
  - user-space measurement and attestation

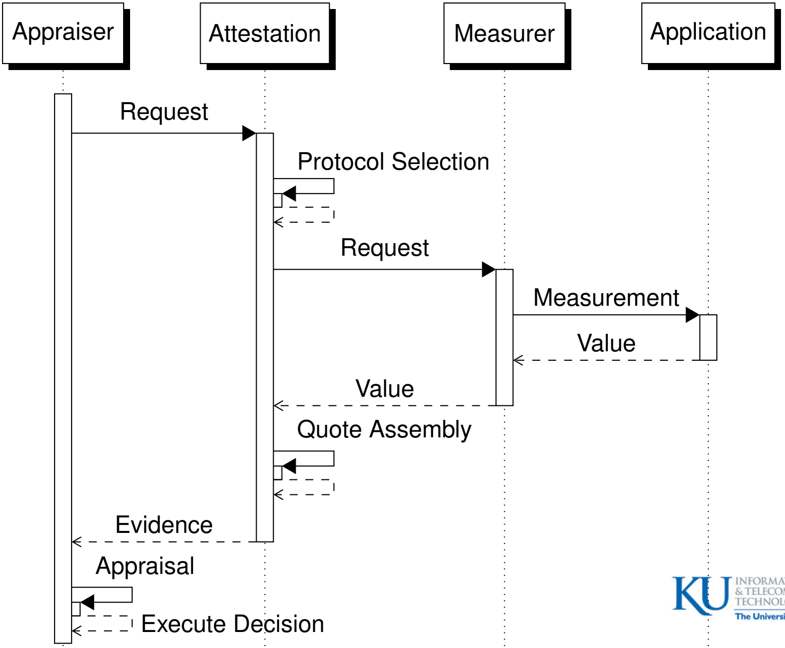
High-Level Architecture



Implementation Decisions

- Standard delivery platform
  - Xen+XSM VM infrastructure
  - OpenStack cloud infrastructure
  - Fedora, HotSpot JVM, GHC
- Standard communication mechanisms
  - JSON structures for all exchanged data
  - *vchan* for on-platform communication
  - TCP/IP for off-platform communication
- Trusted Computing Group standards compliant
  - Trusted Platform Module (TPM) 1.2
  - TCG vTPM in principle
- Executable protocol representation
  - protocol fragments as first-class structures
  - strand space formal semantics

CA-Based Attestation Protocol

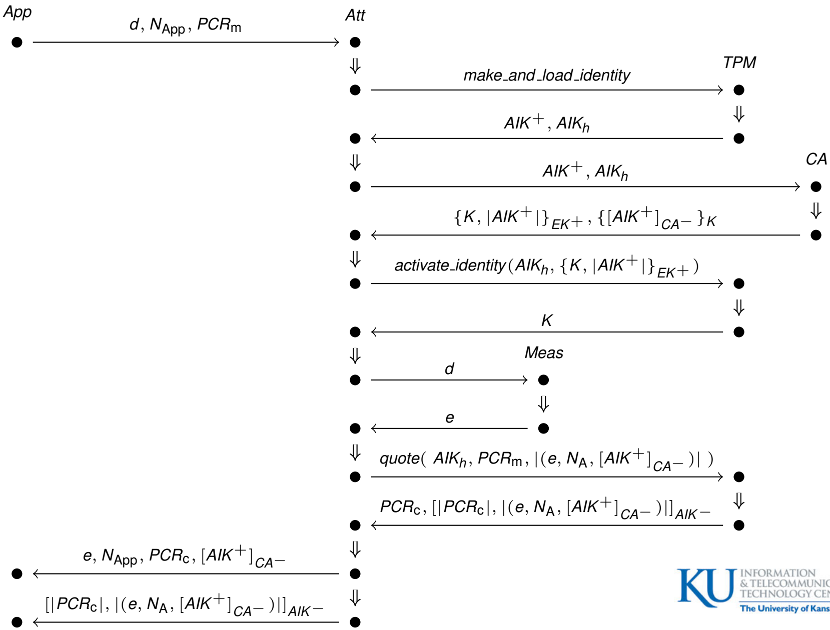


KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER The University of Kansas

What We Are Demonstrating

3-4 Slides on Attestation Protocol Execution

Strand Space Diagram



App

Att

$d, N_{\mathrm{App}}, PCR_{\mathrm{m}}$

TPM

$\mathit{make\_and\_load\_identity}$

AIK^{+}, AIK_{h}

CA

AIK^{+}, AIK_{h}

$\{K, |AIK^{+}|\}_{EK+}, \{[AIK^{+}]_{CA-}\}_{K}$

$\mathit{activate\_identity}(AIK_{h}, \{K, |AIK^{+}|\}_{EK+})$

K

Meas

d

e

$\mathit{quote}(\ AIK_{h}, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA-})|\ )$

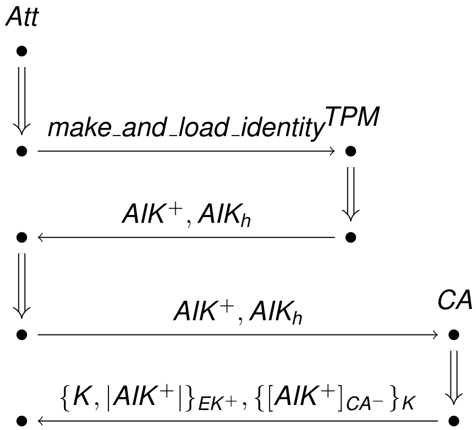
$PCR_{\mathrm{c}}, [|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA-})|]_{AIK-}$

$e, N_{\mathrm{App}}, PCR_{\mathrm{c}}, [AIK^{+}]_{CA-}$

$[|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA-})|]_{AIK-}$

Generating and Certifying an AIK

- Request a new *AIK* from TPM (optional)
- Receive public *AIK* and hash
- Request *AIK* signed by CA (*AIK* cert)
- Receive *AIK* cert encrypted with session key *K*
- Receive *K* encrypted with private *EK*



Att

TPM

CA

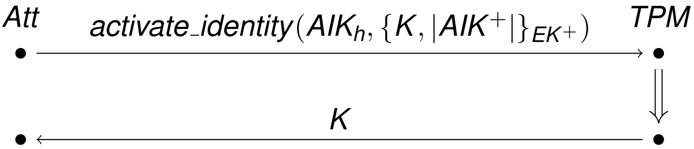
make_and_load_identity

AIK^{+}, AIK_{h}

AIK^{+}, AIK_{h}

$\{K, |AIK^{+}|\}_{EK^{+}}, \{[AIK^{+}]_{CA^{-}}\}_{K}$

Activating the AIK



Att

TPM

$\mathit{activate\_identity}(\mathit{AIK}_h, \{K, |\mathit{AIK}^+|\}_{\mathit{EK}^+})$

K

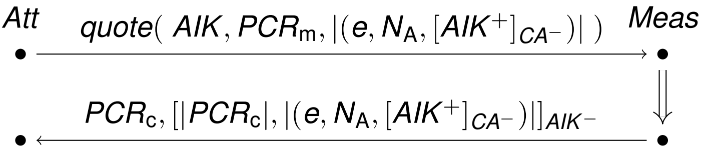
- Request TPM decryption of the *AIK* cert
- Receive *K* used to decrypt signed public *AIK*
- Only TPM can gain access to *K*
- Only TPM can obtain signed, public *AIK*
- Oddly, No manipulation of the *AIK* in this “activation” process

Measurement

$$\begin{tikzcd}
\overset{Att}{\bullet} \arrow[rrrr, "d"] & & & & \overset{Meas}{\bullet} \arrow[d, Rightarrow] \\
\bullet & & & & \bullet \arrow[llll, "e"']
\end{tikzcd}$$

- Request information from measurer
- Receive evidence *e* from measurer
- *d* is abstract allowing protocol reuse
- Most protocols make many requests of the measurer

Generating a Quote



Att

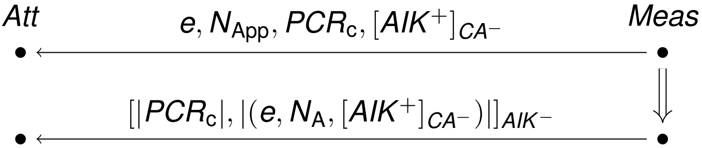
Meas

$quote(\; AIK, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})| \;)$

$PCR_{\mathrm{c}}, [|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}$

- Request a quote from the TPM
  - *AIK* identifies the signing *AIK*
  - PCR_m identifies desired PCRs
  - $|(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|$ guarantees integrity of returned evidence
- Receive quote from TPM
  - PCR_{c} is PCR composite built from requested PCRs
  - $[|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}$ is the signed quote

Appraisal



Att

Meas

$e, N_{\text{App}}, PCR_{\text{c}}, [AIK^{+}]_{CA^{-}}$

$[|PCR_{\text{c}}|, |(e, N_{\text{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}$

- Receive quote from the attestation manager
- Receive evidence from the attestation manager
- Evaluate evidence and quote

1-2 Slides on Appraisal

3-4 Slides on Measurement

2-3 Slides on Communication Mechanisms

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