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
- Attestation Protocol Execution
- Appraisal
- Measurement
- Communication

Short term goals and milestones

Questions and guidance

Program Goal

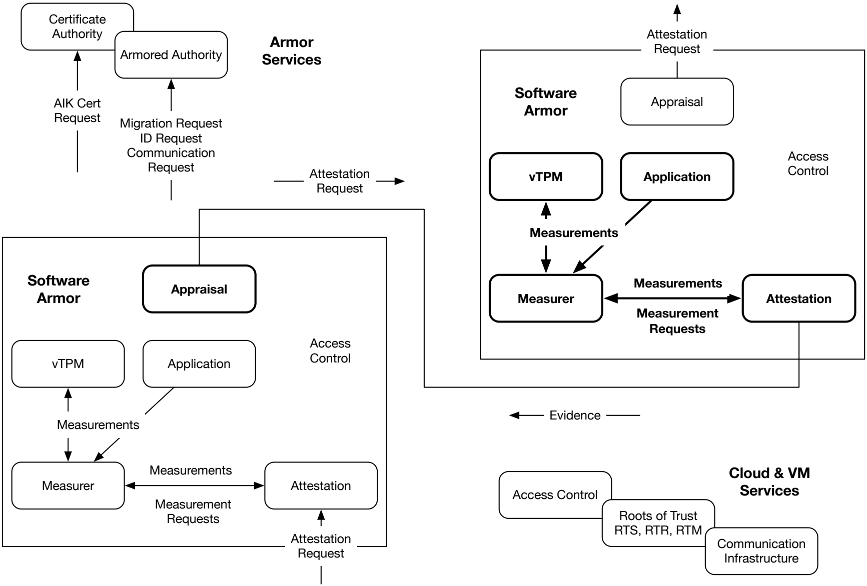
Trust in the Cloud

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

High-Level Architecture



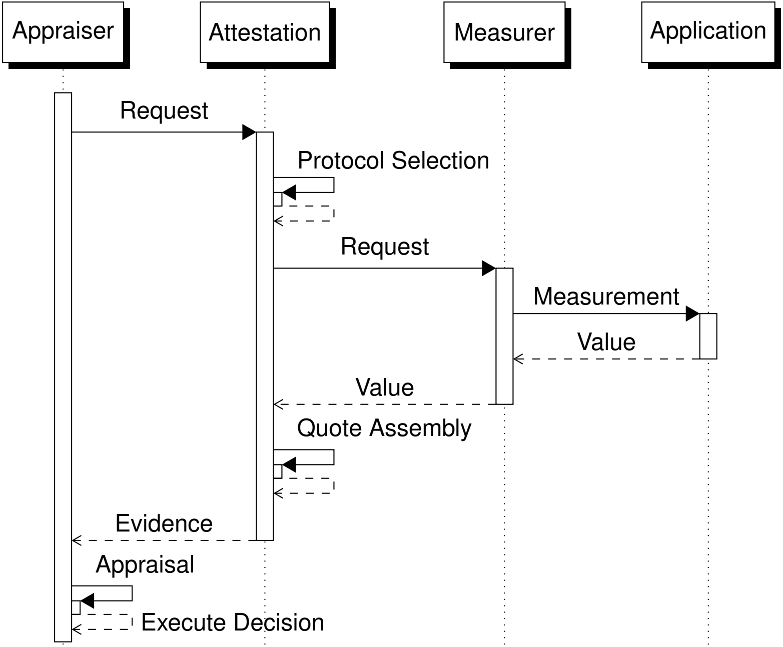
Implementation Decisions

- 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

What We Are Demonstrating

- Execution of a CA-based Attestation Protocol
  - Attestation request
  - Protocol execution
  - Evidence appraisal
- Major architectural subsystems
  - Appraiser
  - Attestation Manager
  - Measurer
  - Instrumented JVM
  - vTPM and Certificate Authority
- Anomaly Detection
  - Bad signatures and PCRs
  - Bad CA certificates
  - Bad quotes and AIKs
  - Bad measurements

Abstract CA-Based Attestation Protocol



Message List Representation

$App \to Att : d, N_{\mathrm{App}}, PCR_{\mathrm{m}}$ on C_{AppAtt}

$Att \to TPM : make\_and\_load\_identity$ on C_{AttTPM}

$TPM \to Att : AIK^{+}, AIK_{h}$ on C_{TPMAtt}

$Att \to CA : Att, AIK^{+}$ on C_{AttCA}

$CA \to Att : \{K, |AIK|\}_{EK^{+}}, \{[AIK^{+}]_{CA^{-}}\}_{K^{+}}$ on C_{CAAtt}

$Att \to TPM : activate\_identity(AIK_{h}, |AIK|)$ on C_{AttTPM}

$TPM \to Att : K$ on C_{TPMAtt}

$Att \to Meas : d$ on $C_{AttMeas}$

$Meas \to Att : e$ on $C_{MeasAtt}$

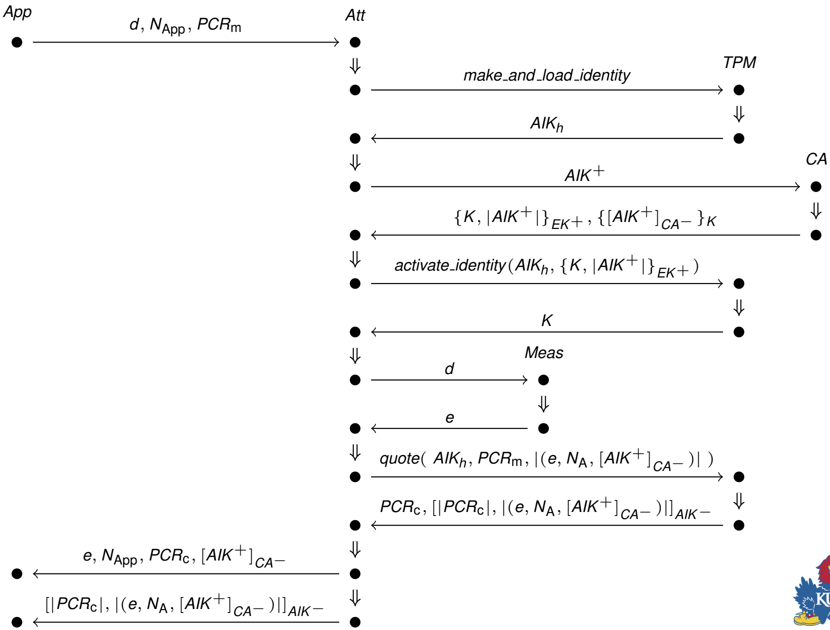
$Att \to TPM : quote(\ AIK_{\mathrm{h}}, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|\ )$ on C_{AttTPM}

$TPM \to Att : PCR_{\mathrm{c}}, [|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}$ on C_{TPMAtt}

$Att \to App : e, N_{\mathrm{App}}, PCR_{\mathrm{c}}, [AIK^{+}]_{CA^{-}}$ on C_{AttApp}

$Att \to App : [|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}$ on C_{AttApp}

Strand Space Diagram Representation



App

Att

TPM

CA

Meas

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

make_and_load_identity

AIK_h

AIK^+

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

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

K

d

e

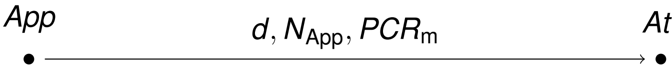
$quote(\ AIK_h, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, [AIK^+]_{CA-})|\ )$

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

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

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

Attestation Request



App

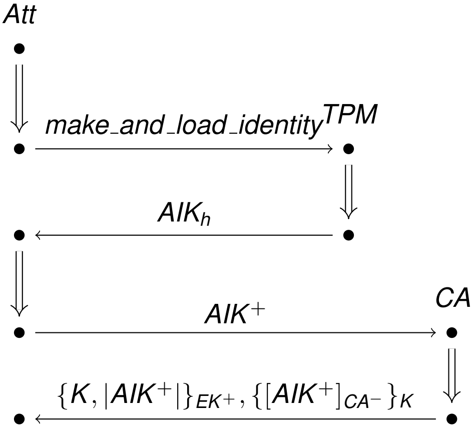
$d, N_{\mathrm{App}}, PCR_{\mathrm{m}}$

Att

- Initiate with an attestation request
  - *d* abstractly defines desired evidence
  - N_{App} is the appraiser’s nonce
  - PCR_{m} selects PCRs
- Attestation agent selects and executes protocol based on request

Generating and Certifying an AIK

- Request a new *AIK* from TPM (optional)
- Receive *AIK* handle
- Request AIK^+ signed by CA (*AIK* cert)
- Receive *AIK* cert encrypted with session key *K*
- Receive *K* encrypted with public *EK*



Att

TPM

CA

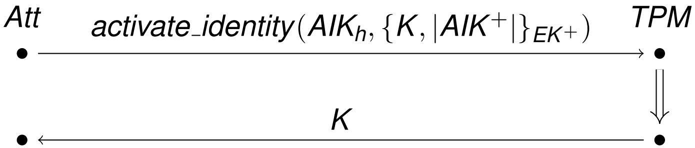
make_and_load_identity

AIK_h

AIK^+

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

Activating the AIK



Att

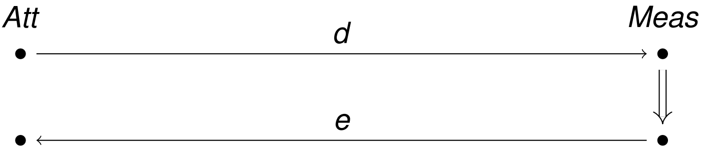
$activate\_identity(AIK_h, \{K, |AIK^+|\}_{EK^+})$

TPM

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



- 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

$$\begin{tikzcd}
\overset{Att}{\bullet} \arrow[rr, "quote(\ AIK\,, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|\ )"] & & \overset{Meas}{\bullet} \arrow[d, Rightarrow] \\
\bullet & & \bullet \arrow[ll, "PCR_{\mathrm{c}}, [|PCR_{\mathrm{c}}|, |(e, N_{\mathrm{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}"']
\end{tikzcd}$$

- 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

$$\begin{tikzcd}[column sep=huge]
\overset{\mathit{Att}}{\bullet} & \overset{\mathit{Meas}}{\bullet} \arrow[l, "{e, N_{\text{App}}, PCR_{\text{c}}, [AIK^{+}]_{CA^{-}}}"'] \arrow[d, Rightarrow] \\
\bullet & \bullet \arrow[l, "{[|PCR_{\text{c}}|, |(e, N_{\text{A}}, [AIK^{+}]_{CA^{-}})|]_{AIK^{-}}}"']
\end{tikzcd}$$

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

3-4 Slides on Attestation Protocol Execution

1-2 Slides on Appraisal

3-4 Slides on Measurement

2-3 Slides on Communication Mechanisms

CA communication

Shared notion of AIKCertRequest, AIKCert, and CAResponse JSON structures.

Attester

- creates an AIKCertRequest (containing attester ID, AIK) and converts to JSON
- JSON sent as POST request to CA running as web server

Certificate Authority

- POST body bytes → UTF8 → JSON → AIKCertRequest
- looks up TPM_PUBKEY associated with ID in sql database
- AIKCert ≈ AIK signed with CA_{-1}
- generates key K and encrypts with TPM_PUBKEY
- AIKCert encrypted with K
- both wrapped in a CAResponse, converted to JSON and sent as response.

CA communication continued

Properties

- CA only responds to receiving an $AIKCertRequest_{JSON}$
- The CACert can *only* be decrypted by knowing K (and therefore TPM_PRIVATEKEY)

Appraiser Knowledge after receiving Cert:

- signature on AIK ensures it was CA who generated signature

  +
- only an entity knowing TPM_PRIVATEKEY could decrypt and send me the CACert

  =
- Attester is using a registered TPM

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