ArmoredSoftware

User-Space Remote Attestation

Dr. Perry Alexander[1] Dr. Andrew Gill[1] Dr. Prasad Kulkarni[1]
Adam Petz[1] Paul Kline[1] Justin Dawson[1]
Jason Gevargizian[1] Leon Searl[1] Edward Komp[1]
Edward Bishop[2] Ciro Pinto-Coelho[2]

[1]Information and Telecommunication Technology Center
Electrical Engineering and Computer Science
The University of Kansas

[2]Southern Cross Engineering

May 1, 2015

Clouds and Trust

- The promises of “the cloud” are substantial
  - reduced hardware and software costs
  - reduced resource consumption
  - improved availability and reliability
- The promises of “the cloud” complicate assurance
  - not under the desk
  - ambiguous and changing runtime environment
  - unknown and unknowable actors in the same environment
- Is trust possible in “the cloud” environment?
  - unambiguous identification
  - confirmation of uninhibited execution
  - direct or trusted indirect observation of good behavior

Trust in the Cloud

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

- 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

Delivery Platform

Open source, standards compliant

- Lightweight integration with existing cloud infrastructure
  - OpenStack cloud infrastructure
  - Xen+XSM VM infrastructure
  - Fedora, HotSpot JVM, GHC
- Trusted Computing Group standards compliant
  - Trusted Platform Module 1.2
  - TCG vTPM (in principle)
  - Trusted OS infrastructure
- Standard communication mechanisms
  - JSON structures for all exchanged data
  - *vchan* for on-platform communication
  - TCP/IP for off-platform communication

New Technologies

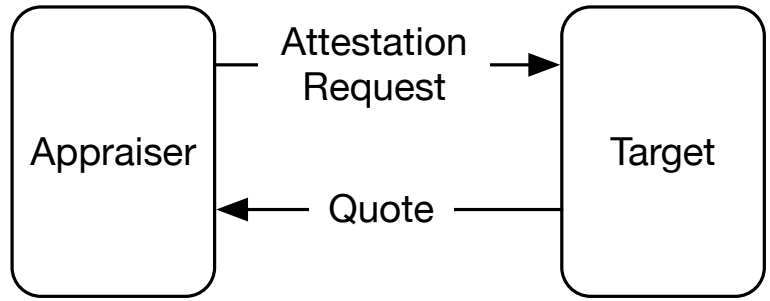
- Trustworthy protocol execution
  - executable protocol representation
  - protocol execution generates evidence of trustworthiness
  - highly focused protocols
  - strand space formal semantics
- Application specific measurement
  - managed and traditional execution environments
  - compile-time assistance for measurer synthesis
  - specialized measurement bundled with applications
- Attestation driven cloud application and data management
  - health monitoring
  - problem mitigation
  - application migration
  - access control

Trusted Platform Module

- Provides and Protects Roots of Trust
  - Storage Root Key (SRK) - root of trust for storage
  - Endorsement Key (EK) - root of trust for reporting
- Quote generation
  - high integrity quotes - ($\{|RS|\}_{AIK^-}$, SML, $\{|n, PCRComp|\}_{AIK^-}$)
  - high integrity evidence - ($\langle E, n \rangle$, $\{|\,|\langle E, n \rangle|, PCR|\}_{AIK^-}$
- Sealing data to state
  - $\{D, PCR\}_{K^+}$ will not decrypt unless PCR = current PCR
  - data is safe even in the presence of malicious machine
- Binding data to TPMs and machines
  - ($\{K^-\}_{SRK^+}$,K) - $\{D\}_{K^+}$ cannot be decrypted unless SRK^- is installed
  - ($\{J^-\}_{K^+}$,J) - $\{D\}_{J^+}$ cannot be decrypted unless K^- and SRK^- are installed

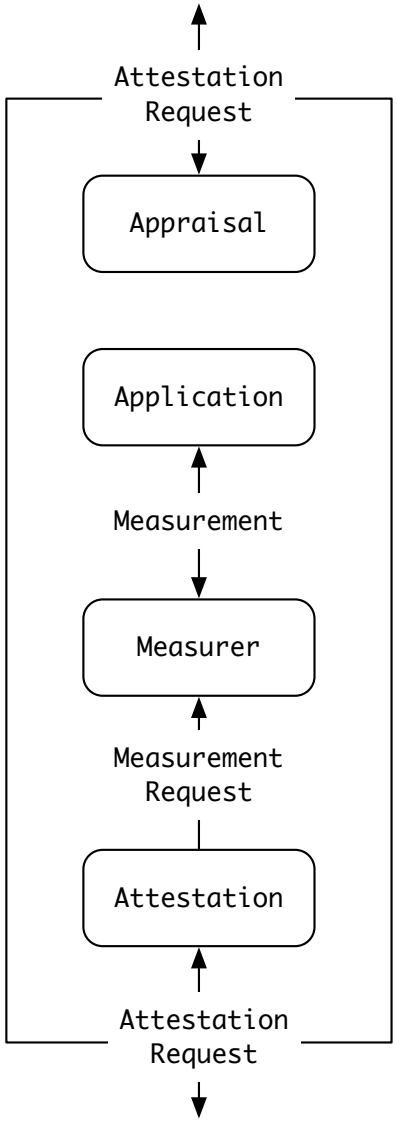
Semantic Remote Attestation

- Appraiser requests a quote
  - specifies needed information
  - provides a nonce
- Target gathers evidence
  - measures application
  - gathers evidence of trust
- Target generates quote
  - measurements and evidence
  - original nonce
  - cryptographic signature
- Appraiser assesses quote
  - good application behavior
  - infrastructure trustworthiness

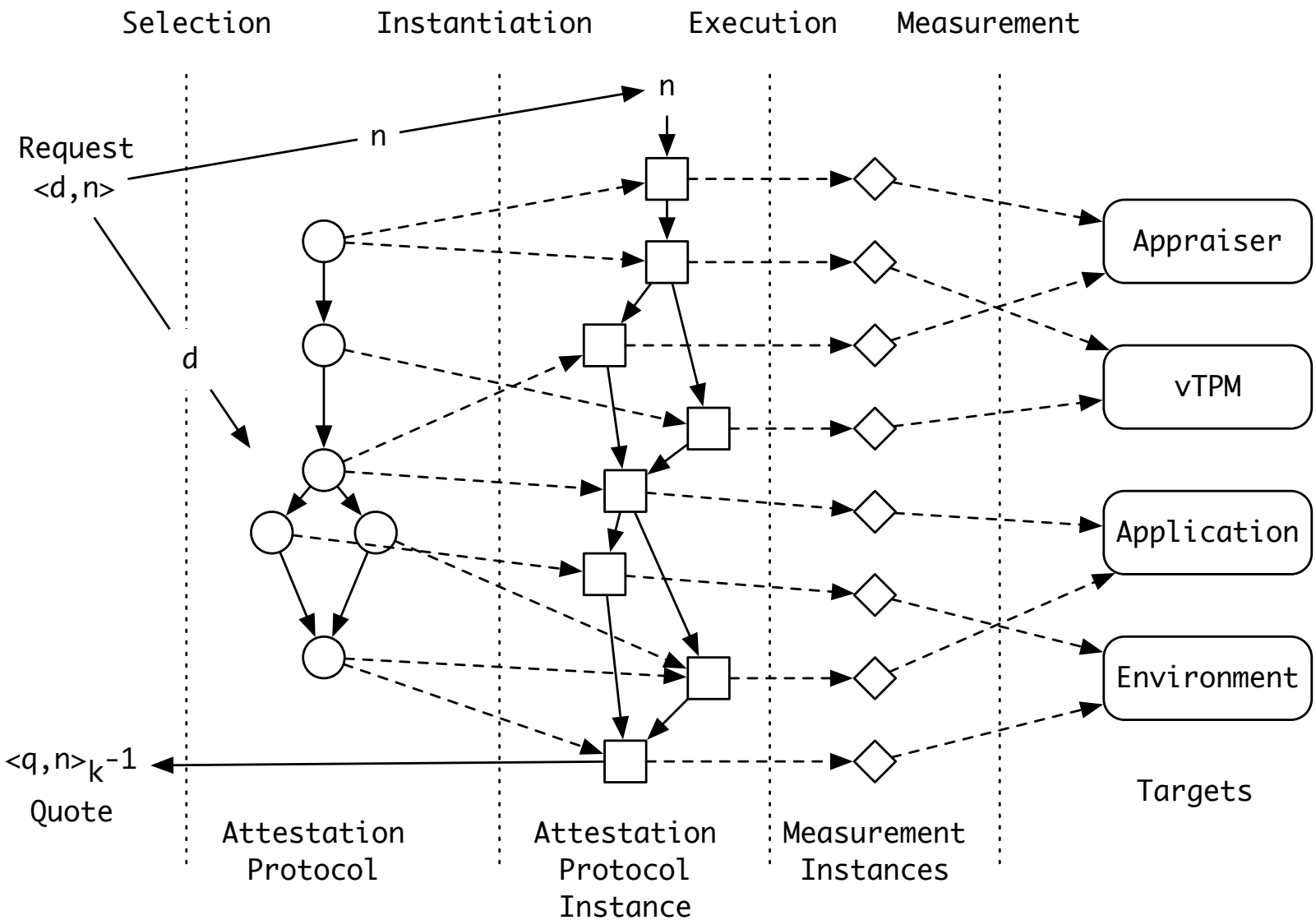


Armored Application Architecture

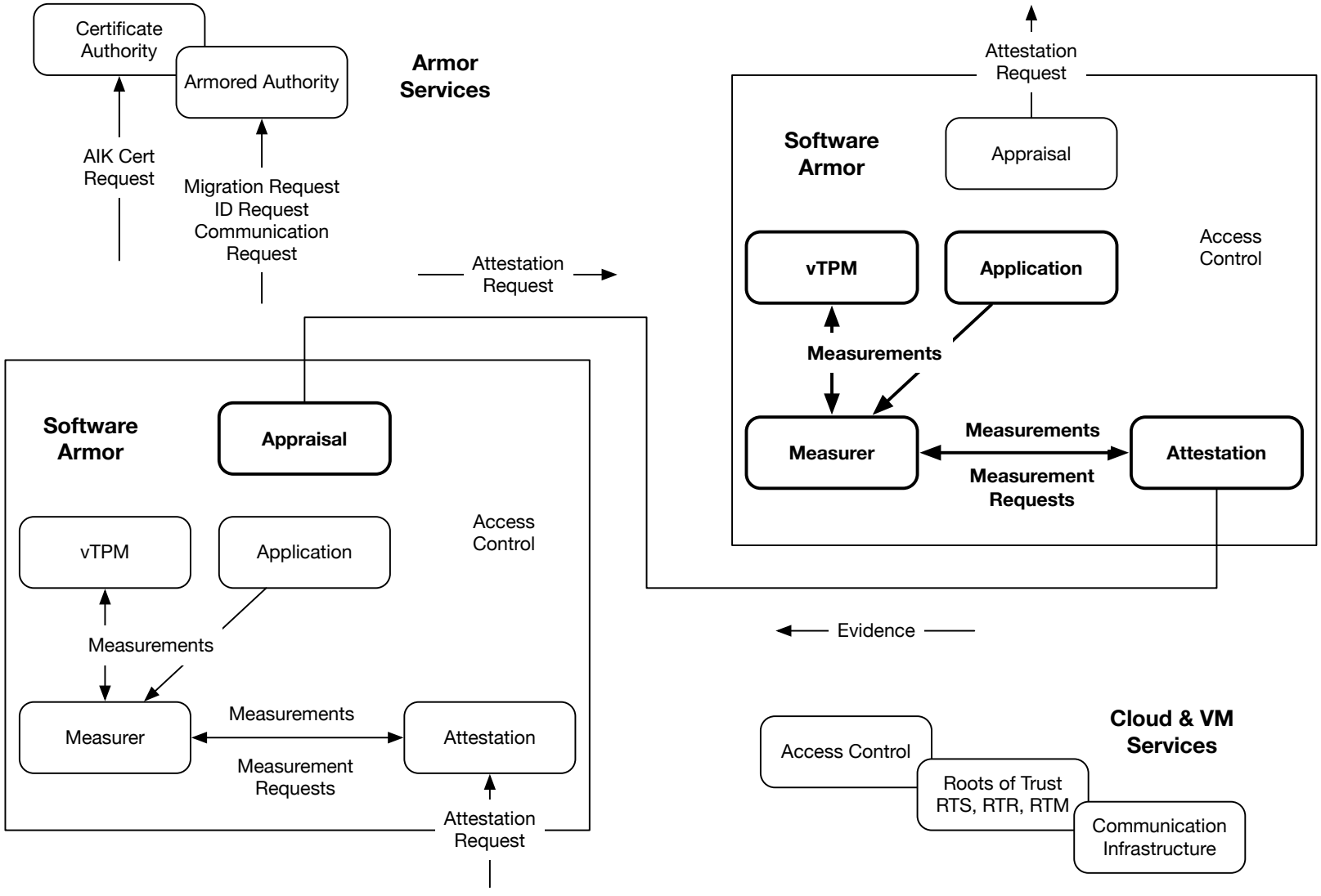
- Focus is user-space applications
- Assesses the cloud infrastructure and environment
- Attests to the state of its application
- High-assurance, lightweight infrastructure
- Influenced by the *Trusted Research Platform* and *Principles of Remote Attestation*



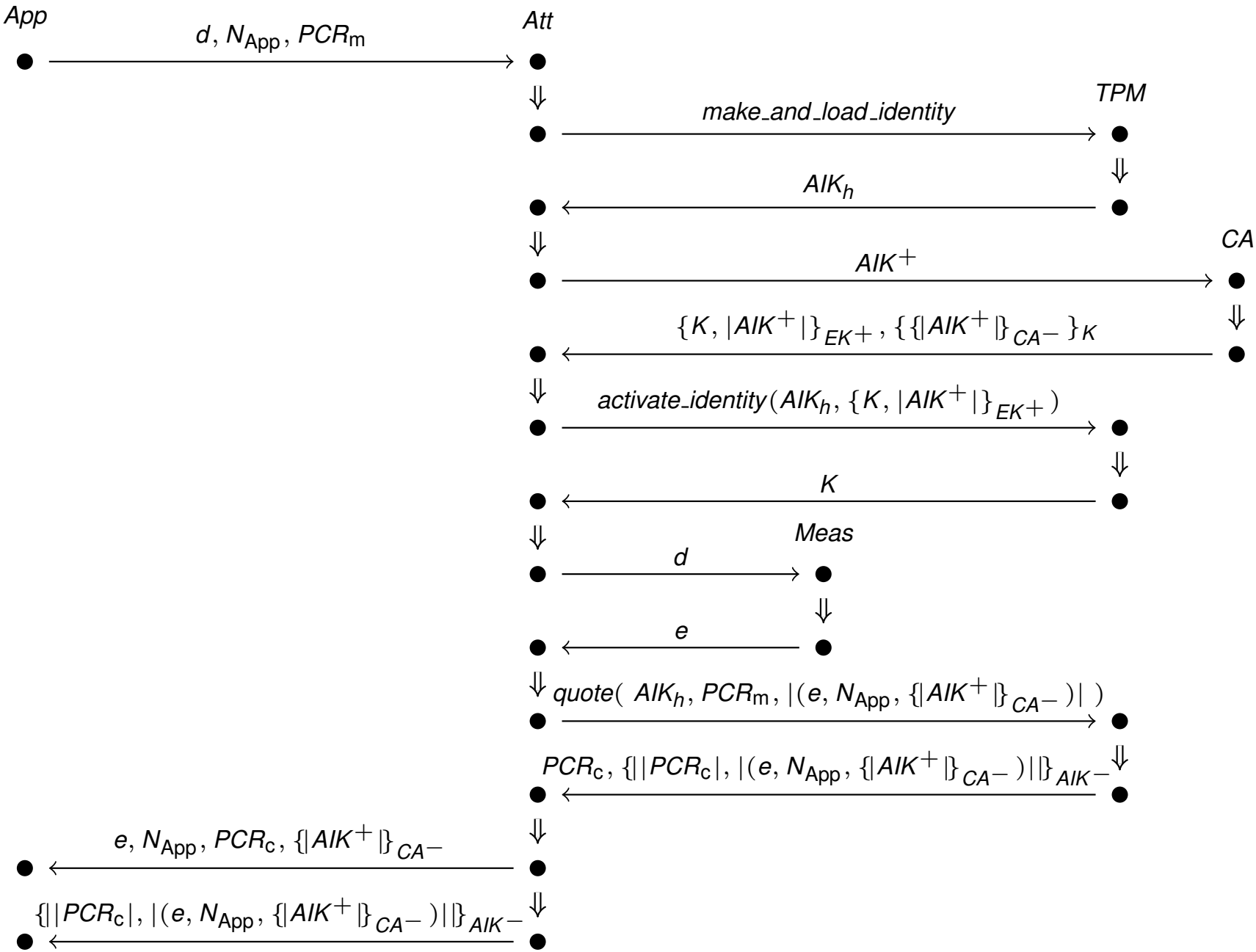
Measurement and Attestation



System-Level Architecture



Privacy CA Attestation



Negotiation

Protocol

```
do { send t $ r;
     q <- receive t;
     e <- case {p:q | policy?(p)} of
            ∅ : None
            p : send t $ choose(p)
          end;
     case e of
       Some v : appraise(v)
       None : None
     end
}
```

Proposals

$$\{\langle E_0, P_0\rangle, \langle E_1, P_1\rangle, \ldots, \langle E_n, P_n\rangle\}$$

Single Realm Attestation

Protocol

```
do { id <- getVCID;
     sig <- getSigFileEvidence;
     src <- getSigFileSrc;
     e <- createEvidence(id,sig,src);
     returnEvidence(e)
}
```

Evidence

$$\langle (id, sig, src), \{||(id, sig, src)|, PCRComp_0||\}_{AIK_0^-} \rangle$$

Protocol

```
do { id <- getVCID;
     sig <- getSigFileEvidence;
     src <- getSigFileSrc;
     srcEvidence <- send src $ r;
     e <- createEvidence(id,sig,src,srcEvidence)
     returnEvidence(e)
}
```

Evidence

$$b = \langle (e), \{||e|, PCRComp_1\|\}_{AIK_1^-} \rangle$$

$$\langle (id, sig, src, b), \{||(id, sig, src, b)|, PCRComp_0\|\}_{AIK_0^-} \rangle$$

Current Status

Completed four demonstrations culminating in running an attestation protocol in response to an attestation request.

- Attestation and Appraisal development
  - CA-Based attestation protocol execution example
  - integration with Berlios TPM 1.2 emulator
  - simple dynamic appraisal of attestation results
- Measurement development
  - on demand Java program measurement
  - HotSpot-based Java VM run time measurements
  - standard mechanism for extending measurement capabilities
- Communication infrastructure
  - vchan, TCP/IP and socket communication infrastructure
  - language-based interface with TPM 1.2
  - JSON-based data exchange formats
  - initial certificate authority API

Goals and Milestones for 2015

Increased functionality and robustness

- Push to the cloud
  - integration with OpenStack
  - migration across Xen instances
  - vTPM function migration
- Establish roots-of-trust and trust argument
  - measured launch and remeasurement of ArmoredSoftware
  - establish trust in the Xen/OpenStack infrastructure
- Executable protocol representation and protocol semantics
  - richer protocol collection
  - evidence of proper execution
  - protocol-centered appraisal
- Operational, integrated vTPM prototype
  - integration with TPM 1.2
  - find and integrate, not build (we hope)

Goals and Milestones for 2015

- More robust communication and system services
  - Armor Authority prototype
  - Certificate Authority integration
  - communications management
- More capable measurement
  - compiler directed measurement
  - continuous measurement of trends
- More interesting download-able demonstration
  - sponsor-defined problem
  - more realistic attacker model

References

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

Fábrega, F. J. T., Herzog, J. C., and Guttman, J. D. (1999). Strand spaces: Proving security protocols correct. *Journal of computer security*, 7(2):191–230.

Haldar, V., Chandra, D., and Franz, M. (2004). 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.

Ryan, M. (2009). Introduction to the tpm 1.2. Draft Report.