

# ArmoredSoftware: Trusting the Cloud Commons

Dr. Perry Alexander, Dr. Andy Gill, Dr. Prasad Kulkarni

ITTC - The University of Kansas

Ed Bishop, Ciro Pinto-Coelho

Southern Cross Engineering



# Background Projects

- Trusted Research Platform (DoD with Galois)
  - modeling SVP architecture and access control
  - capturing system design
- Verified TPM (Battelle)
  - verified substantial TPM 1.2 subset
  - verified simple attestation and migration protocols
- Verified vTPM (DoD with Kestrel)
  - verifying SVP vTPM infrastructure
  - capturing SVP vTPM system design
- ACHILLES (DARPA with Adventium Labs)
  - imagining malice in embedded systems
  - assessing and appraising runtime environment and applications



# 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



# How Might ArmoredSoftware Help?

- Estimating likelihood of client software or host system compromise
- Appraising cloud applications without sacrificing anonymity or performance
- Guiding migration from untrusted to trusted infrastructure
- Implementing mission specific appraisal monitoring multiple applications
- Aggregating trust information from cloud components to enhance decision making
- Providing architectural support ensuring long-term cloud-based resource availability



# Ultimate Goal

Provide new capabilities that help overcome barriers to cloud acceptance by industry and government, specifically DoD

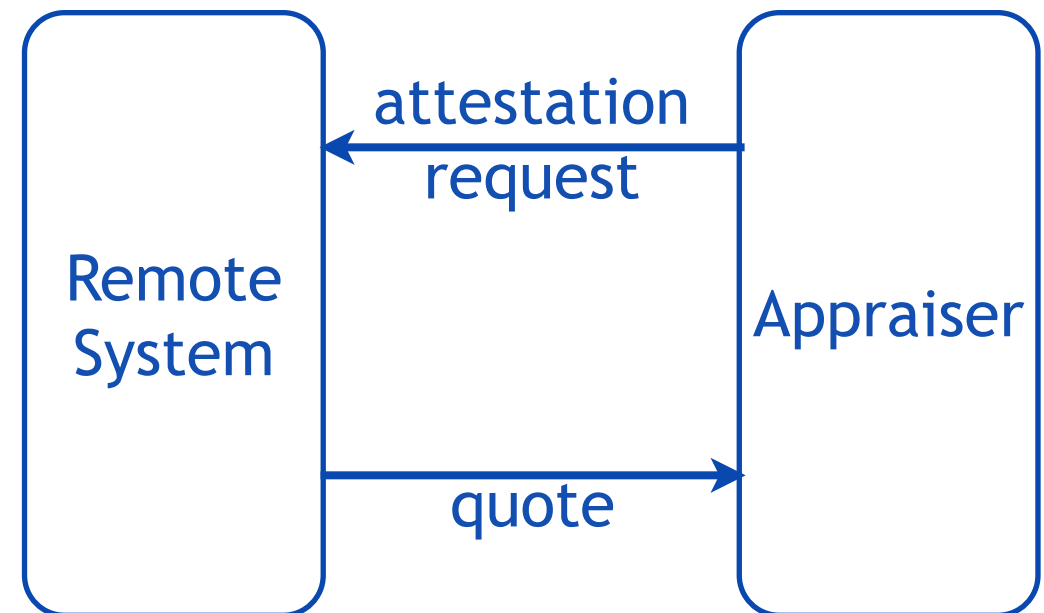


# ArmoredSoftware Features

- Establishes trust among cloud components
  - trust among cohorts of processes
  - trust among processes and environment
- Promotes 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

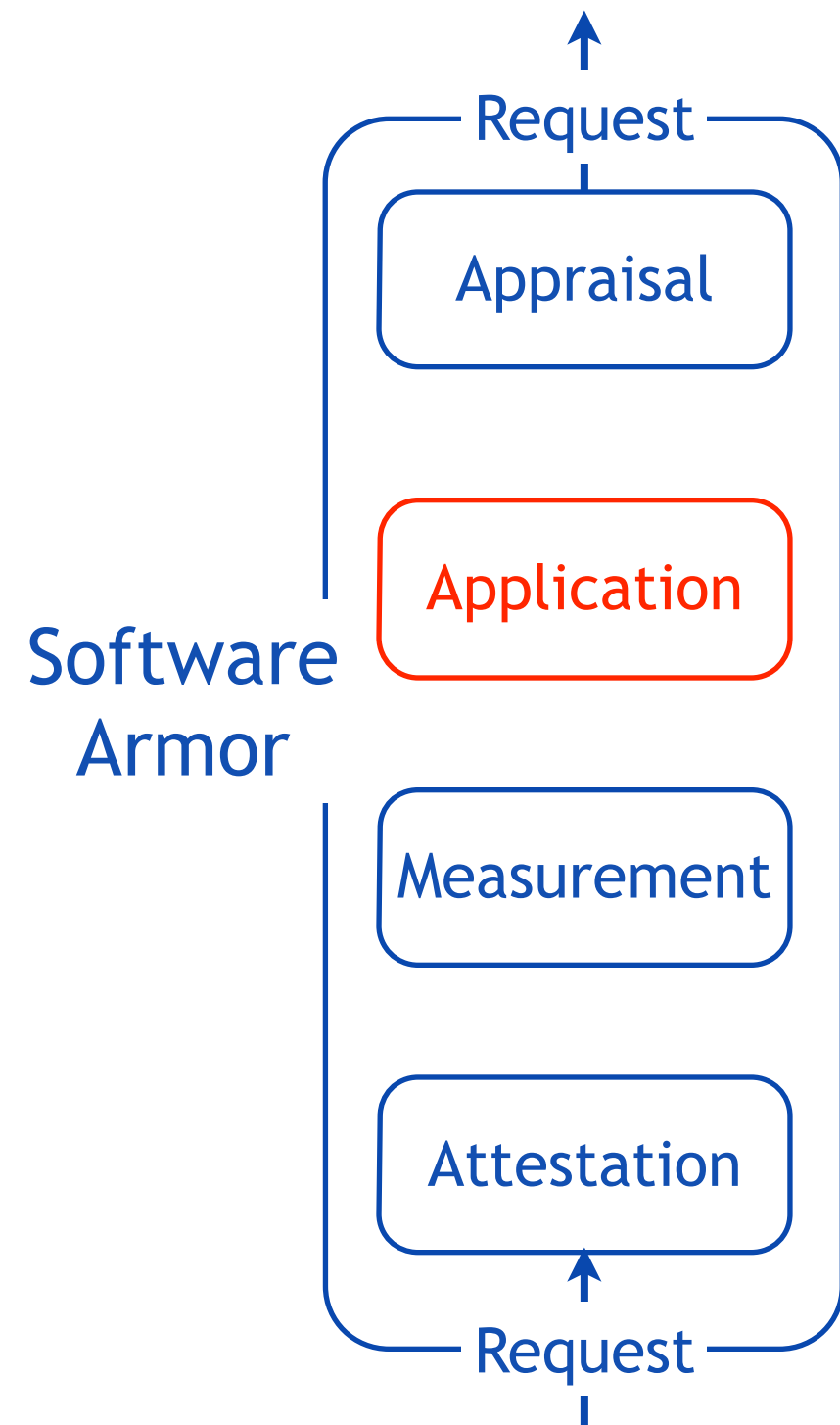
# Based on Remote Attestation

- Appraiser requests a quote
  - specifies what information is needed
  - includes a nonce for freshness
- Remote system gathers evidence
  - measures executing software
  - gathers historical evidence
- Remote system generates quote
  - evidence describing system
  - the original nonce
  - cryptographic signature
- Appraiser assesses quote
  - correct boot process
  - correct parts
  - evidence integrity and identity



# Armor Component Architecture

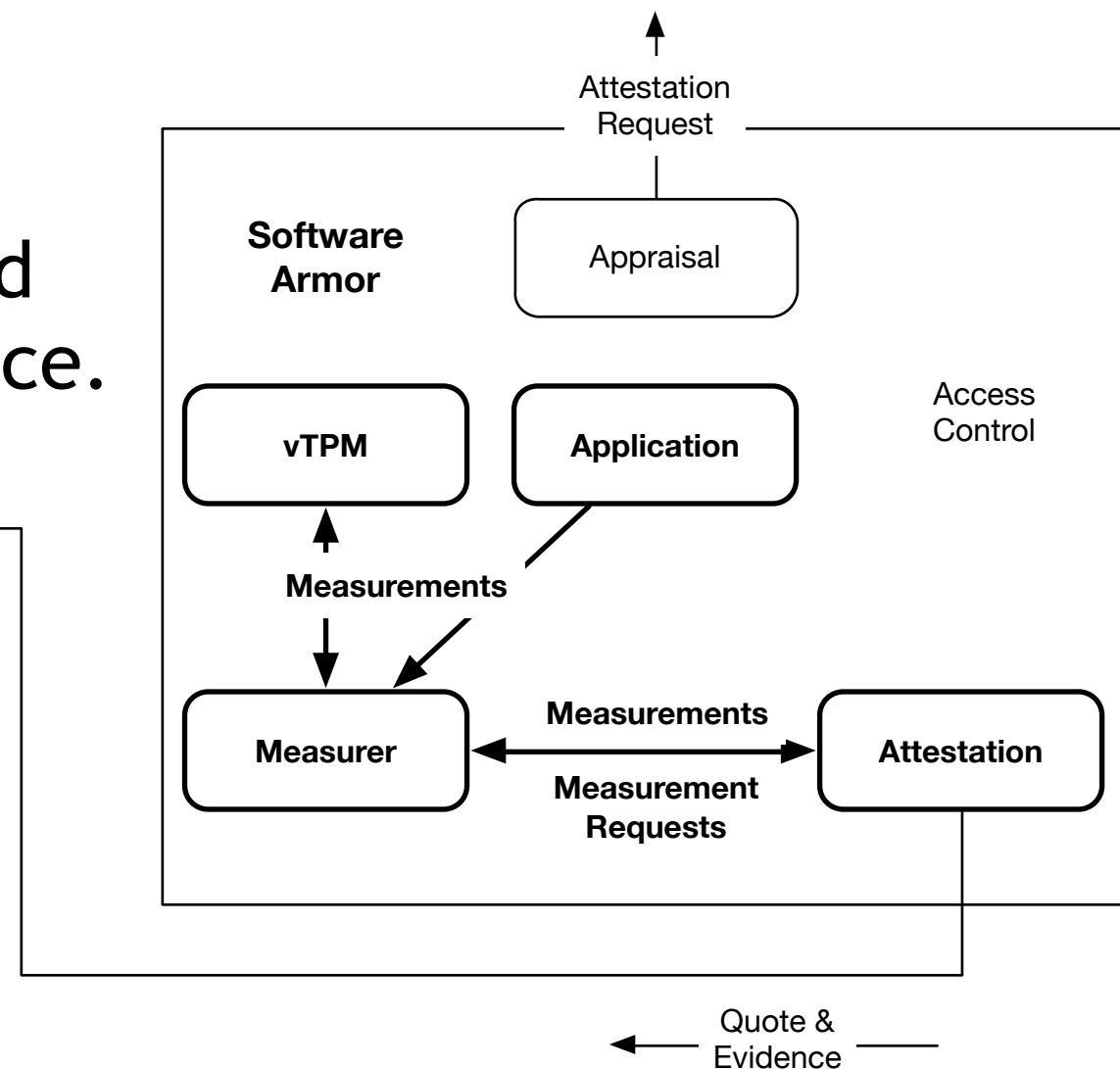
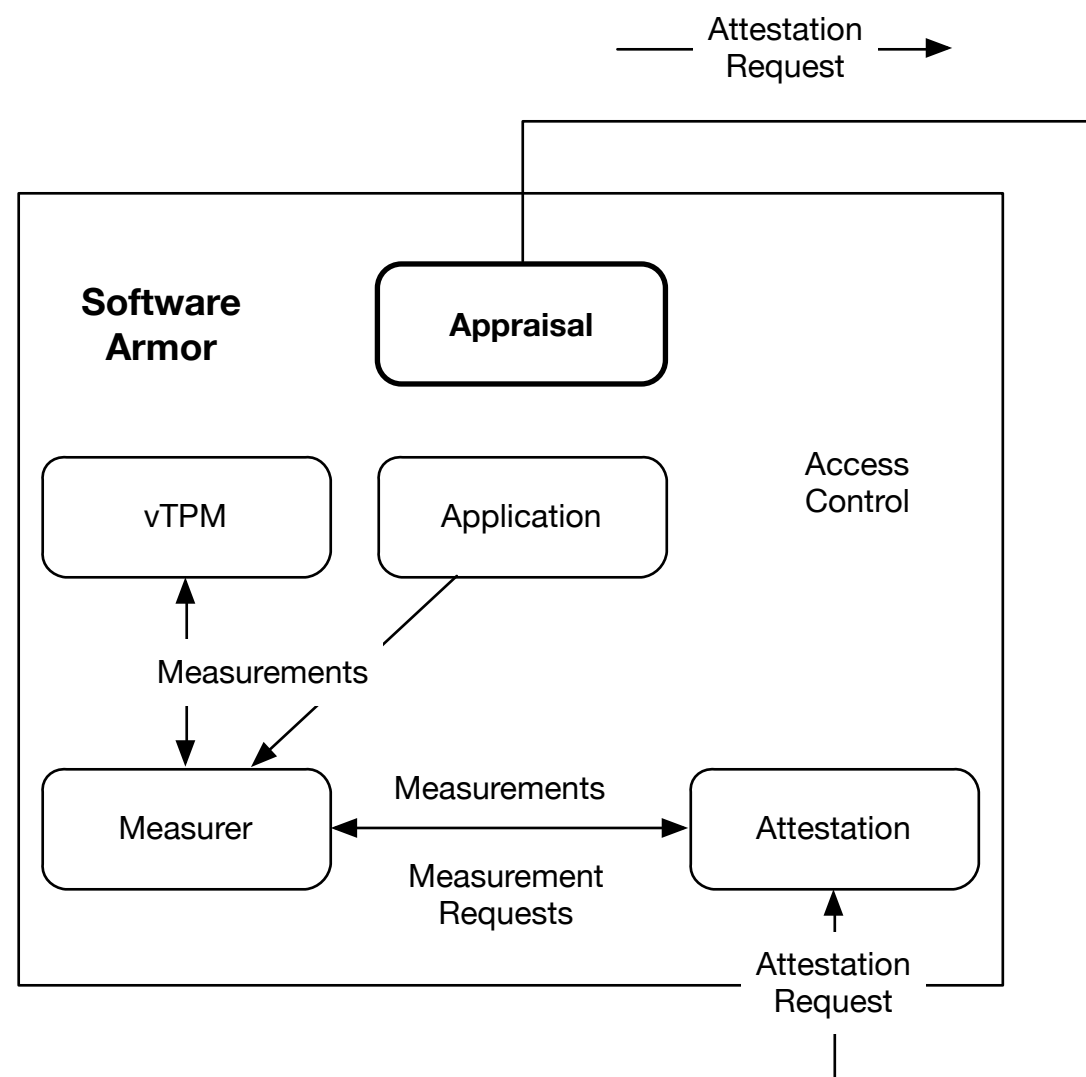
- Focused on user-space applications
- Protects the application from the cloud infrastructure and environment
- Provides attestations to cloud infrastructure and environment
- High-assurance, lightweight infrastructure
- Influenced by the *Trusted Research Platform* and *Principles of Remote*





# Attestation in ArmoredSoftware

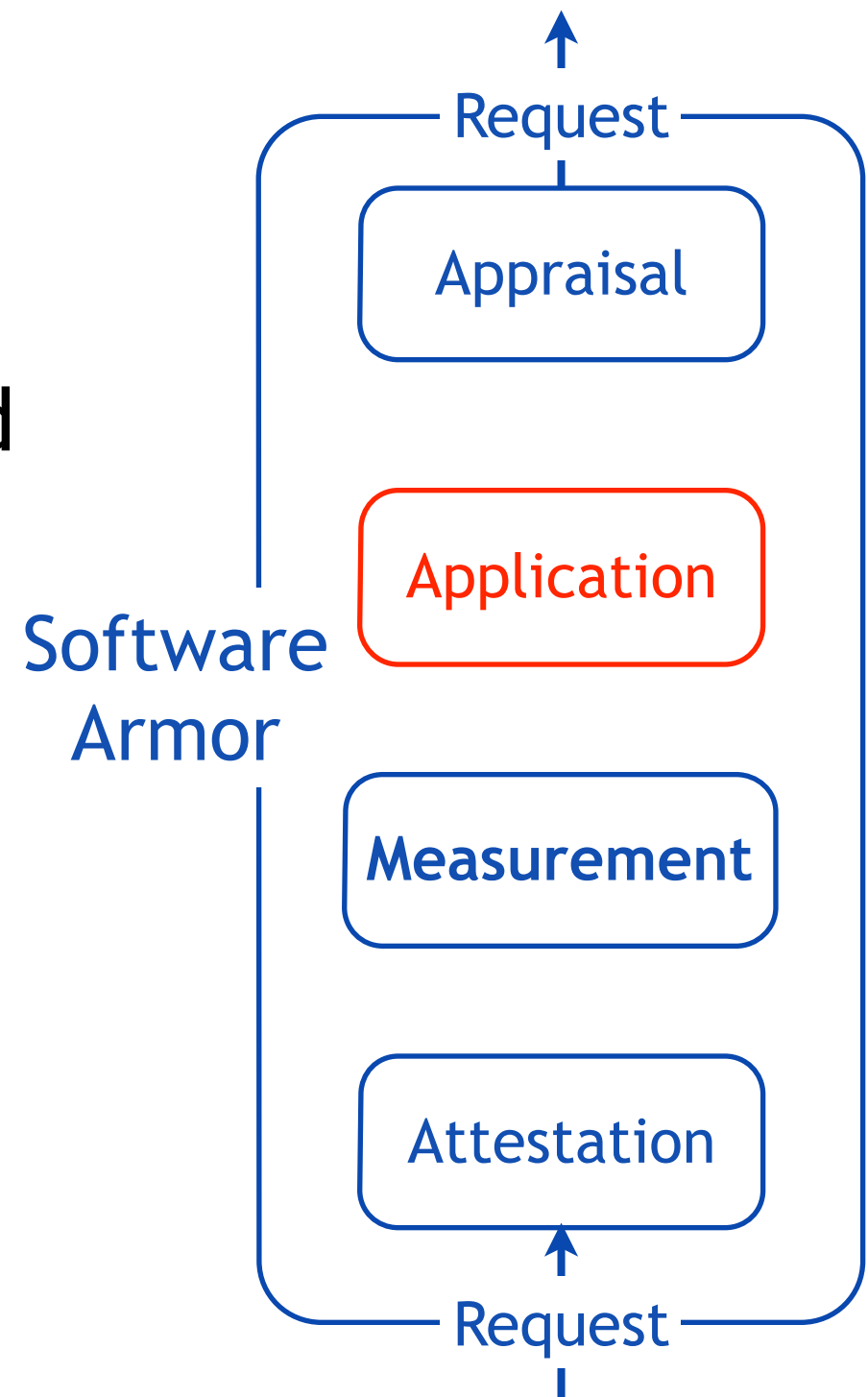
An *appraiser* requests an attestation from a target and assesses trustworthiness based on received quote and evidence.



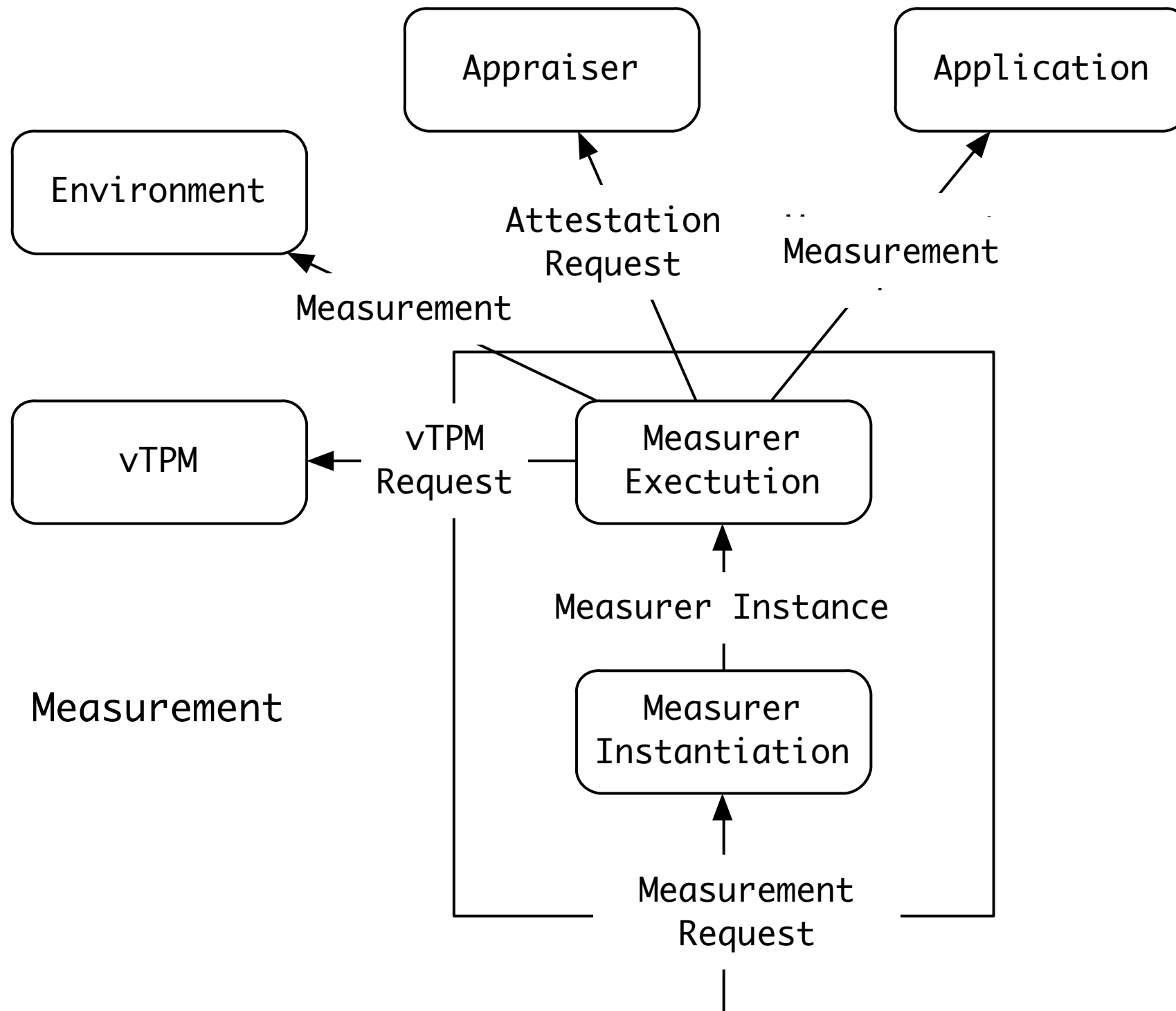
A *target* responds to an attestation request by gathering evidence, generating a cryptographic quote, and returning quote and evidence.

# Measurement

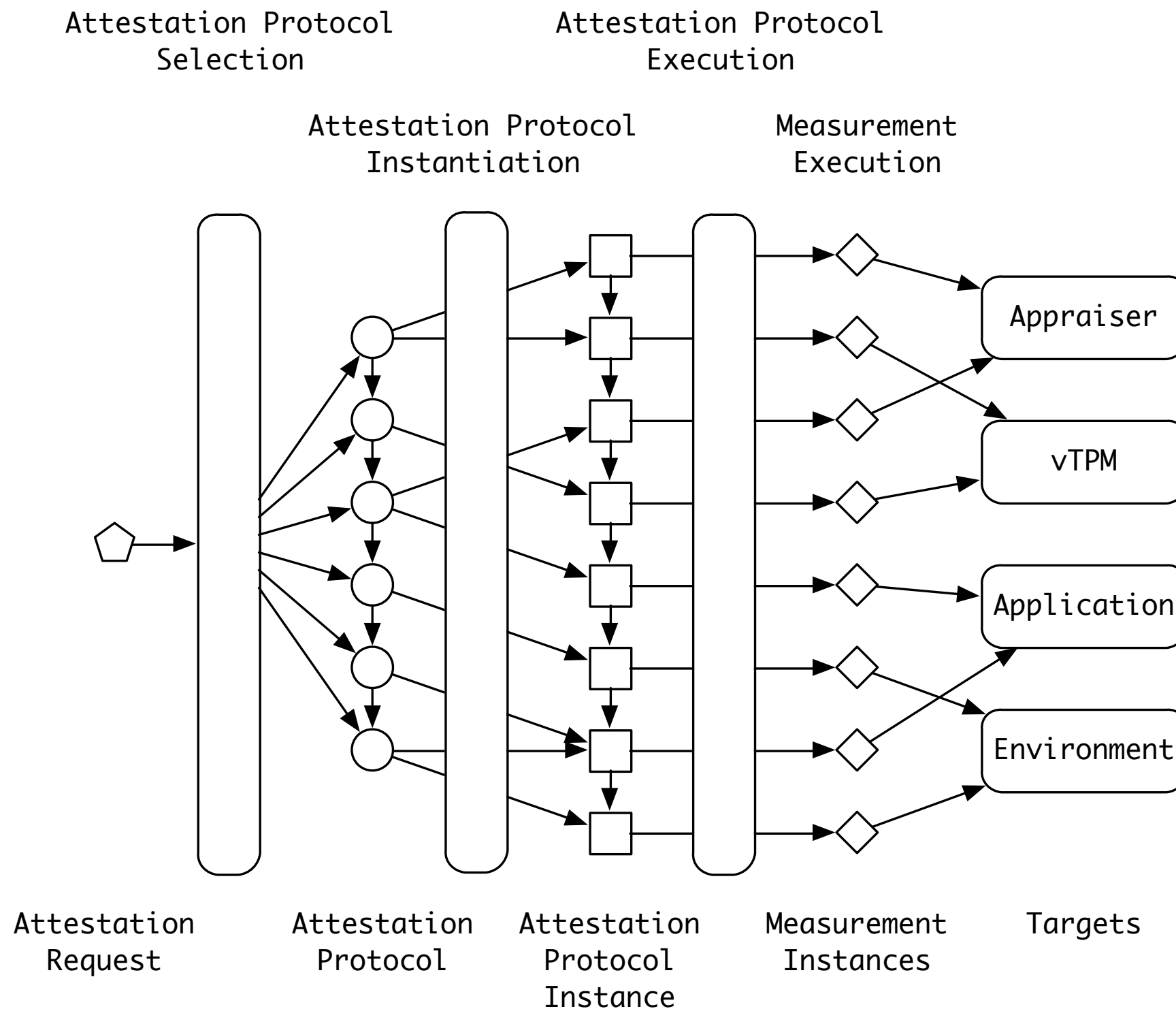
- Gathers information
  - Configuration and boot information
  - Runtime information
- Armor measures and is measured
  - measures itself and its application for others
  - requests measurements from environment
- Target classes include:
  - Hosted languages (Java)
  - Compiled code (C,C++)
  - Operational environment



# Measurement

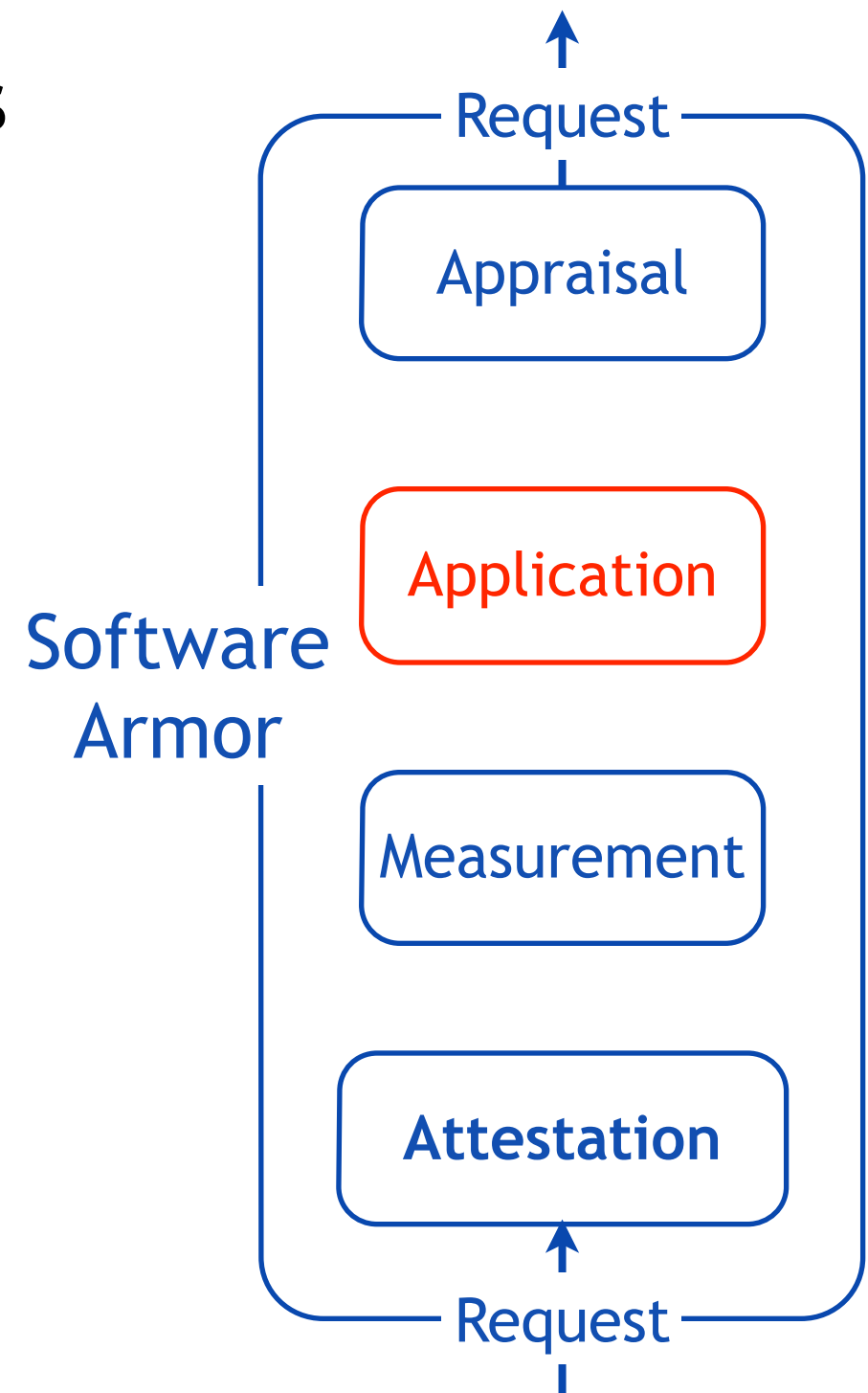


# Detecting Evidence of Malice

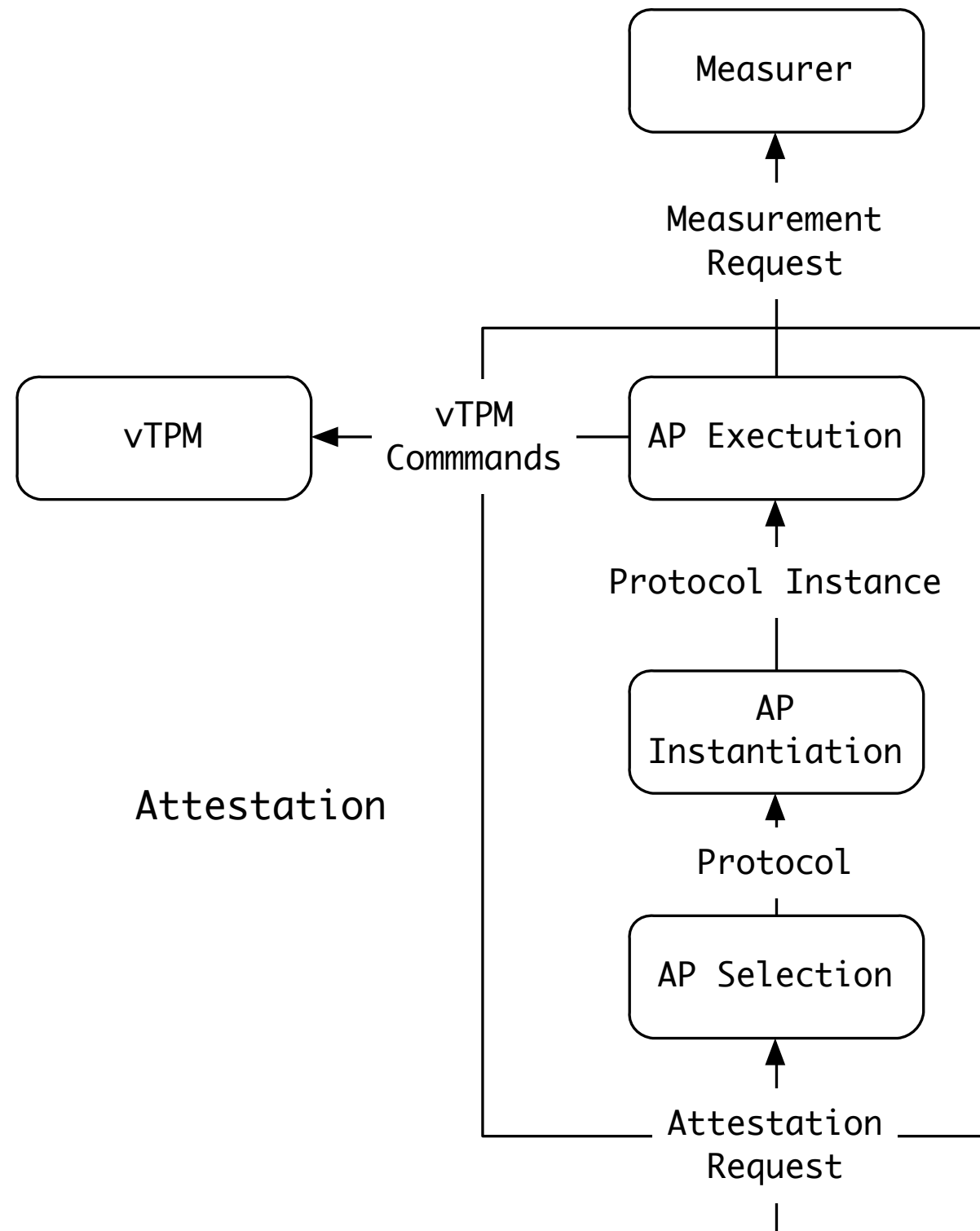


# Attestation

- Responds to attestation requests
  - receives attestation requests
  - obtains measurement information
  - high-integrity response
- Armor reports on its state
  - application boot and runtime state
  - armor boot and runtime state
- Protocols implement responses
  - invokes measurement
  - vTPM provides assurance
  - vTPM manages measurements
  - complex interactions among Armor elements and environment

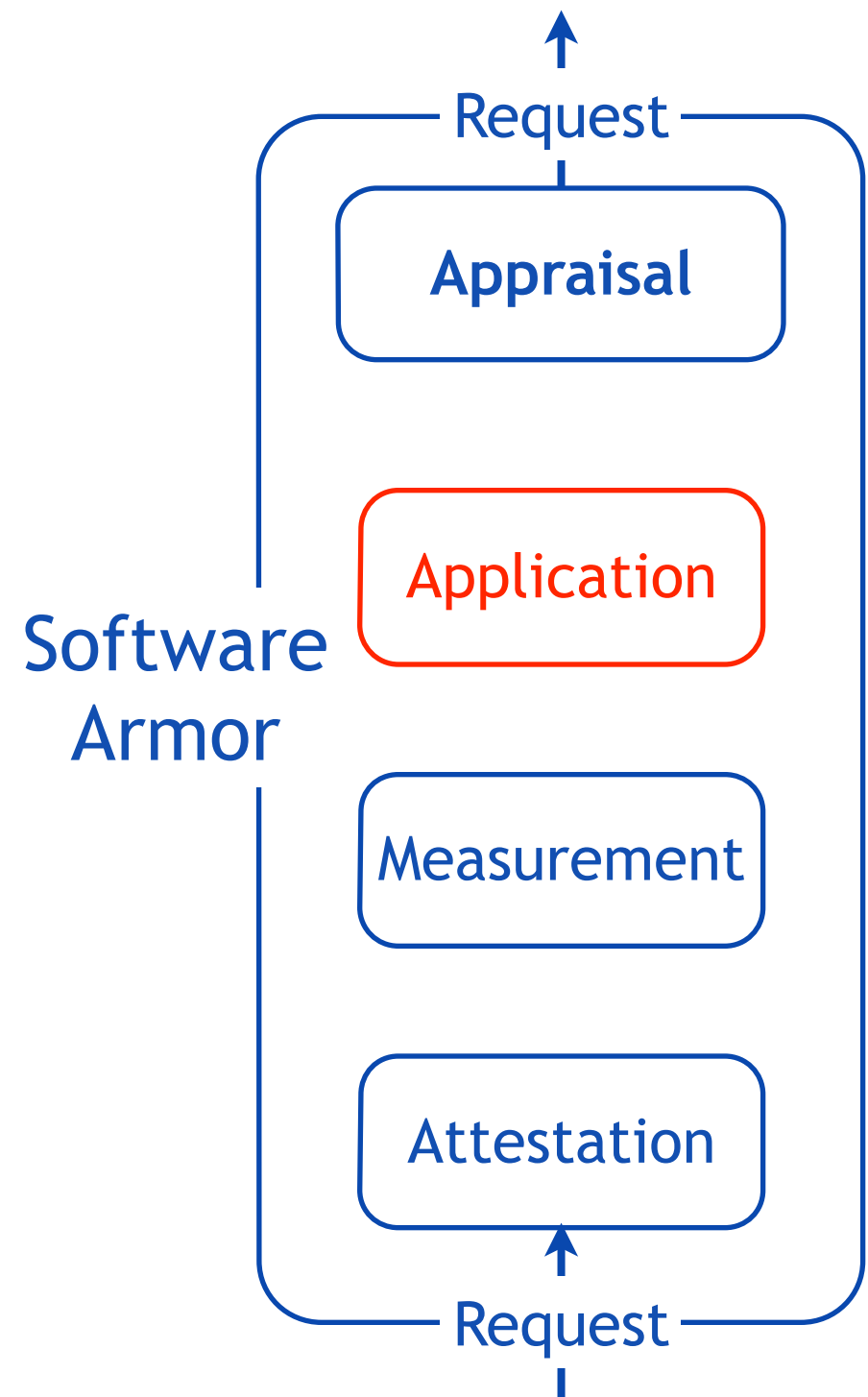


# Attestation



# Appraisal

- Assesses environment
  - sends attestation requests
  - determines measurement integrity
  - calculates salient properties
- Armor appraises its environment
  - requests information
  - assesses information
  - determines response as appropriate
- Responses include
  - information reporting
  - migration
  - reconfiguration in the current environment



# TPM Inside

- 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 -  $(\{|RS|\}_{AIK}^{-1}, SML, \{|n, PCR_{0-m}|\}_{AIK}^{-1})$
  - high integrity evidence -  $(\langle E, n \rangle, \{|#E, PCR, n|\}_{AIK}^{-1})$
- Sealing data to state
  - $\{D, PCR\}_K$  will not decrypt unless PCRs = current PCRs
  - data is safe even in the presence of malicious machine
- Binding data to TPMs and machines
  - $(\{K^{-1}\}_{SRK}, K) - \{D\}_K$  cannot be decrypted unless SRK is installed
  - $(\{J^{-1}\}_K, J) - \{D\}_j$  cannot be decrypted unless K and SRK are installed





# vTPM & Trust Infrastructure

- Focus on light and mobile
  - easy migration among cloud infrastructure
  - lightweight, minimal implementation
  - decentralized, lightweight construction
- Abstract DSL for Trust
  - specifies high-level (v)TPM-based protocols
  - abstracts communication details and components
  - interpretable and verifiable with precise semantics
- Appropriately verified core infrastructure
  - vTPM ecosystem including creation and management
  - protocol execution across VMs
- Moving towards automated synthesis



# Research & Development Plan

- Develop measurement capabilities
  - hosted languages measurers (Java)
  - traditional languages measurers (C, C++)
  - environment measurers (Xen, OS)
- Develop attestation capabilities
  - attestation protocols
  - protocol instantiation
- Develop appraisal framework
  - flexible, user configurable appraisal protocols
  - establishment of Armor trustworthiness
- Develop lightweight, mobile vTPM infrastructure
  - vTPM management with support for mobile roots of trust
  - appropriately strong argument for correctness



# Research & Development Plan

- Automated synthesis and verification
  - DSL for protocol specification
  - synthesis of executable components
  - artifact verification across components
- Demonstrations
  - initially simple demonstration applications demonstrating
  - cloud-based “big data” environment demonstration
  - federated trust demonstrations
  - *demonstrations as discovered/directed*
- Scale up and roll out
  - full integration with Xen, OpenStack, Linux
  - installation management and packaging



# Current Status

- Experimental environment up and running
  - eight node development cloud - Xen, OpenStack
  - five node experimental cloud - Xen, OpenStack
- Simple measurement prototyping
  - gathering information from hosted language execution
  - triggered by external attestation agent
- Inter-VM communication techniques established
  - using Cloud Haskell on industry standard mechanisms
  - TCP/IP based communication and shared page communication
  - integrating XSM into development infrastructure
- Planning initial demonstrations Fall 2014



# Outreach

- Talking with potential commercial users
  - Cisco - OpenStack integration
  - Google - Trust infrastructure
  - BATS - Trust infrastructure
- Application examples
  - cloud-based data enclave
  - migration from danger
  - what are good use cases for secure cloud?
- Contacts
  - Perry Alexander - alex@ittc.ku.edu
  - website - <http://armoredsoftware.github.io>
  - sources - <http://github.com/armoredsoftware>



# References

- G Coker, J Guttman, P Loscocco, A Herzog, J Millen, J Ramsdell, A Segall, J Sheehy, B Sniffen, “Principles of Remote Attestation” in *International Journal of Information Security*, 2012
- TRP Research Team, *TRP Design White Paper - Version 0.1.9*, available upon request
- P Barham, B Dragovic, K Fraser, S Hand, T Harris, A Ho, R Neugebauer, I Pragg, A Warfield, “Xen and the Art of Virtualization”, *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP'03)*, Boldon Landing, NY, 2013
- V Haldar, D Chandra and M Franz, “Semantic remote attestation: a virtual machine directed approach to trusted computing,” *Proceedings of the 3rd Conference on Virtual Machine Research and Technology Symposium*, USENIX Association, 2004
- A Martin, *The Ten-Page Introduction to Trusted Computing*, 2008, <<http://www.cs.ox.ac.uk/files/1873/RR-08-11.PDF>>



# People

- Institutions
  - KU Information and Telecommunication Technology Center
  - Southern Cross Engineering
- KU People
  - Dr. Perry Alexander, PI
  - Dr. Prasad Kulkarni, Dr. Andy Gill, Co-PI
  - Leon Searl, Technical Staff
  - Justin Dawson, Jason Gevargizian, Adam Petz, Paul Kline, students
- Southern Cross Engineering People
  - Edward Bishop, Ciro-Coelho

