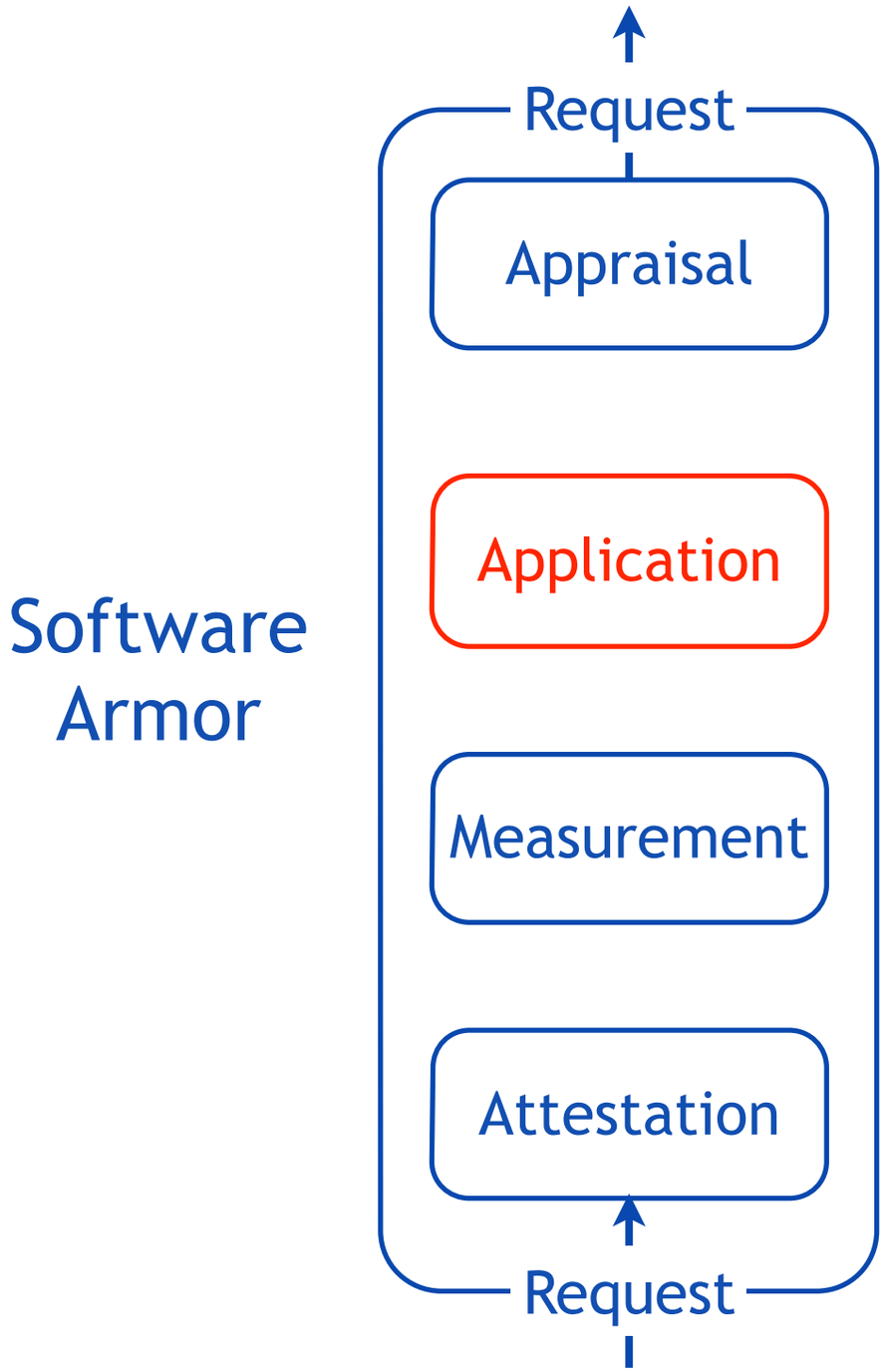
KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

ArmoredSoftware

Capability Overview

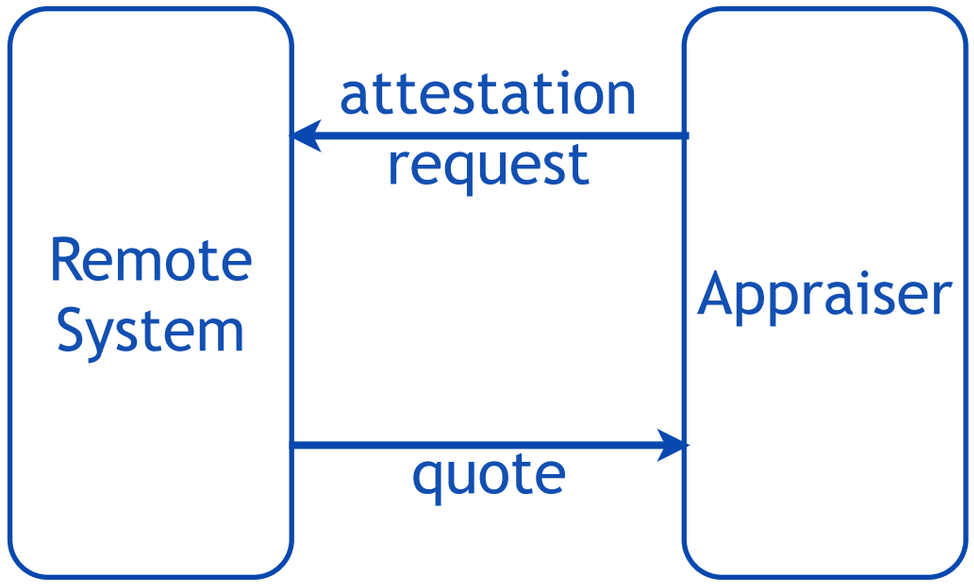
ArmoredSoftware

- Architectural *armor* that enables cloud software to assess and protect itself from its environment
- Supports evaluating *trustworthiness* of cloud based computational environments, resources, and processes
- Deployed in *common cloud environments* with minimal impact on application performance



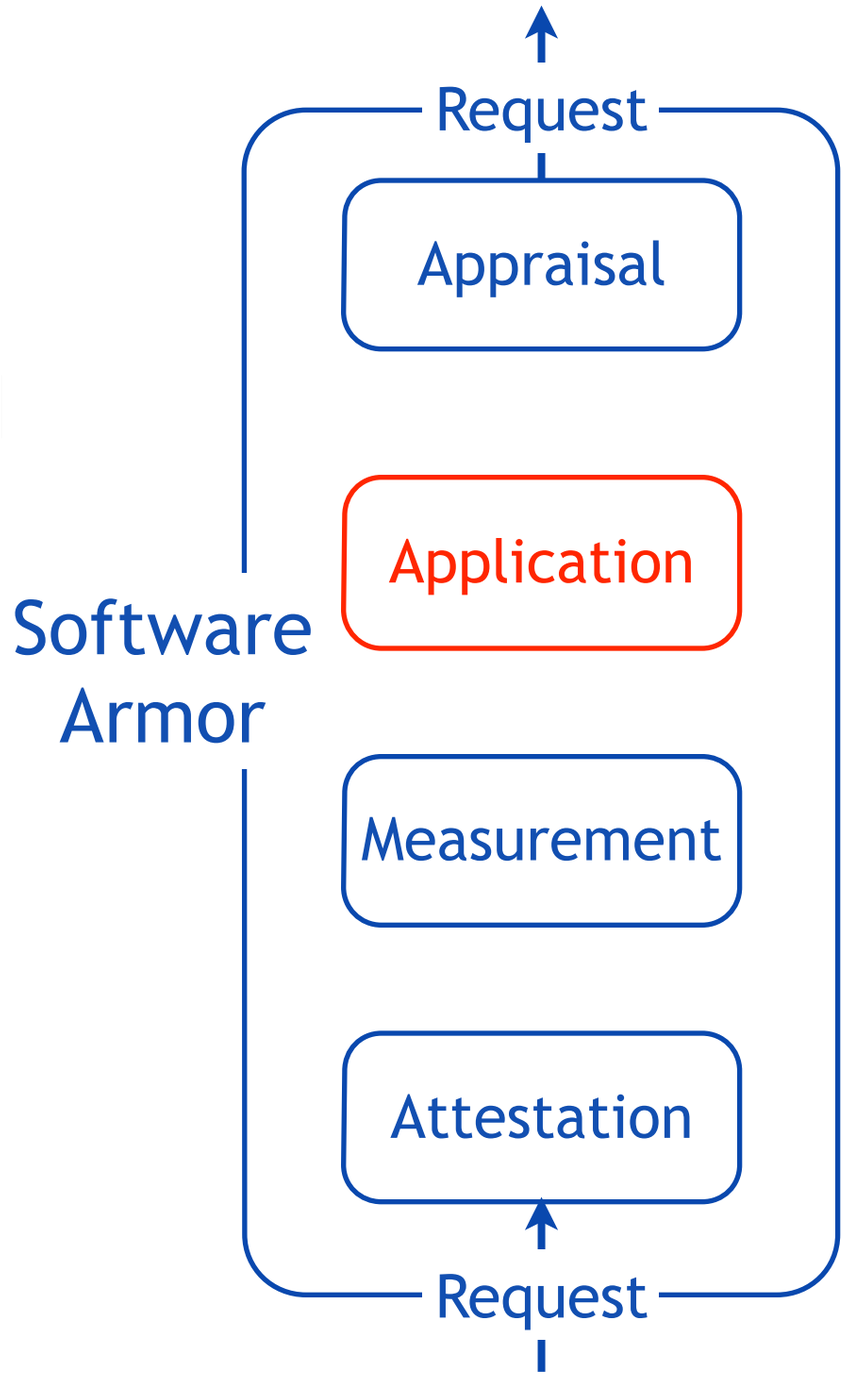
Mechanism

- Appraiser requests quite
  - 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



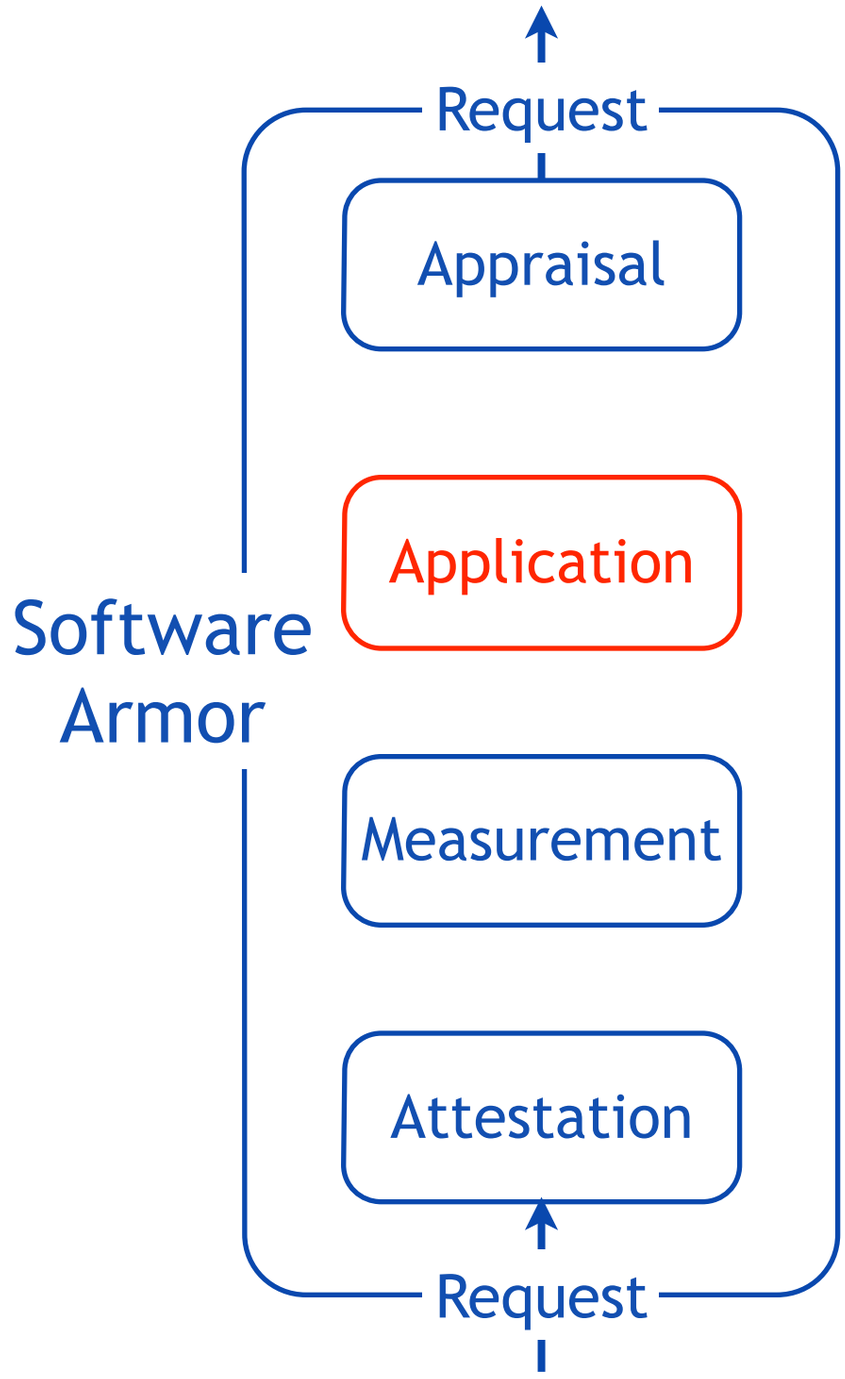
Measurement

- 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



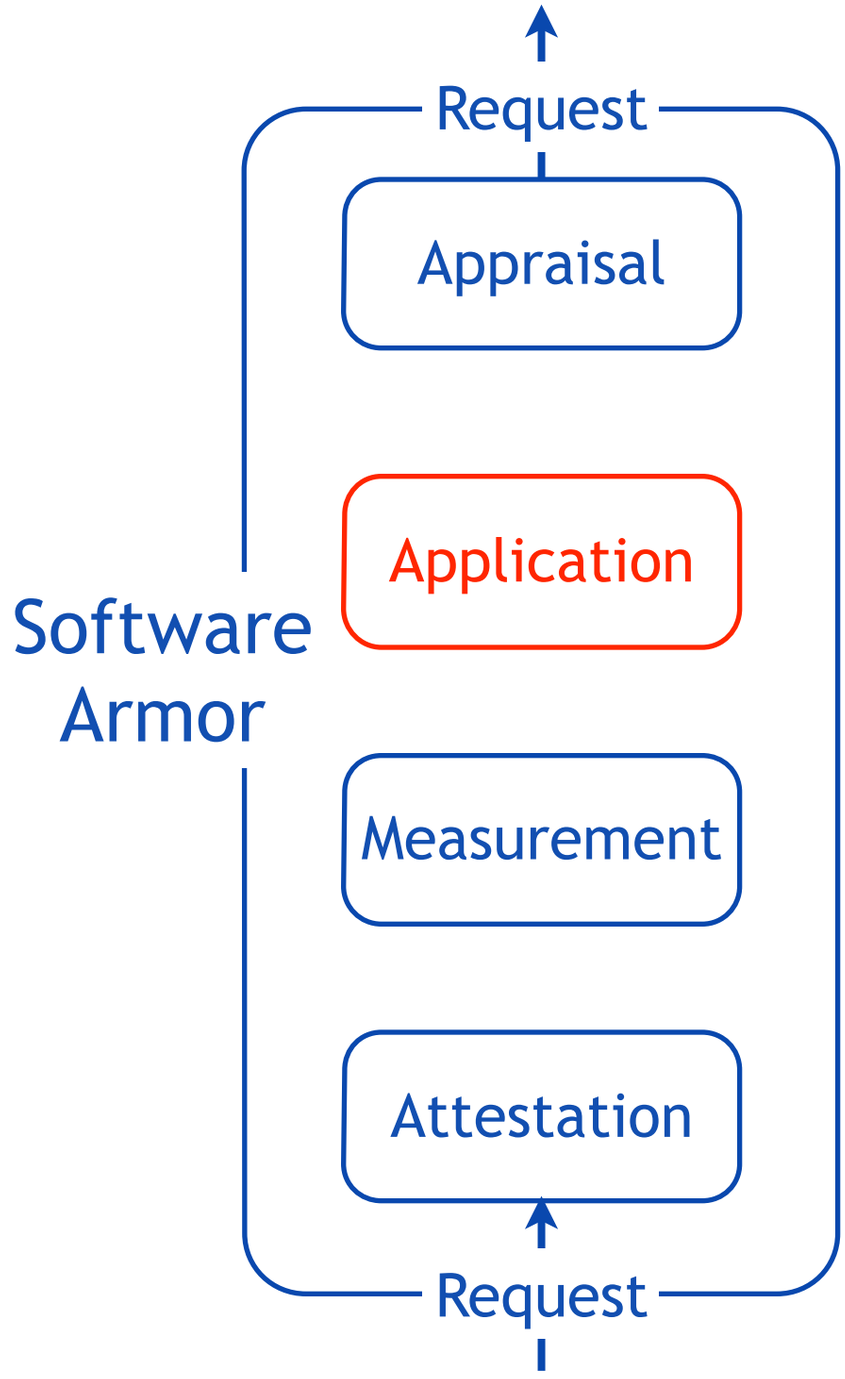
Attestation

- Attests to system state
  - receives attestation requests
  - obtains measurement information
  - high-integrity response
- Armor attests to 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



Appraisal

- Assesses environment
  - sends attestation requests
  - determines measurement integrity
  - determines target properties
- Armor appraises its environment
  - requests information from environment
  - assesses information
  - determines response as appropriate
- Responses include
  - simple information reporting
  - migration to another environment
  - reconfiguration in the current environment



TPM and vTPM

- 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, $\{|n,PCR_{0\text{-}m}|\}_{AIK^{-1}}$)
  - high integrity evidence - (<E,n>, $\{|\#E,PCR,n|\}_{AIK^{-1}}$)
- 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

Features

- Establishes trust among components
  - trust among cohorts of processes
  - trust among processes and environment
- Promotes informed decision making
  - cloud processes are first-class entities
  - 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 discoveries
- Operates in traditional cloud environments
  - Xen virtualization environment
  - OpenStack cloud environment