Can you trust me?
An introduction to the TPM

Dr. Perry Alexander
Director, Information and Telecommunication Technology Center
Professor, Electrical Engineering and Computer Science
The University of Kansas
(alex@ittc.ku.edu)

KU THE UNIVERSITY OF KANSAS

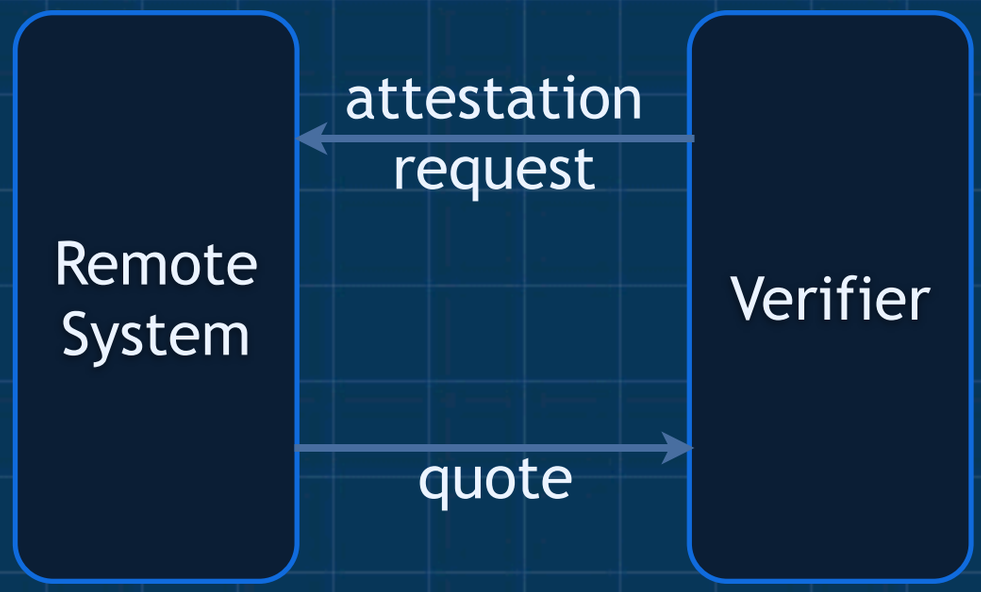
Overview

- Remote and Self Attestation
  - establishing trust in a remote system
  - establishing trust in the local system
- The Trusted Platform Module
  - PCRs and PCR Extension
  - SRK and chaining keys
- Using the TPM
  - generating quotes for remote attestation
  - sealing data to system state
- Odds and ends
  - the TPM controversy
  - information assurance and KU

KU THE UNIVERSITY OF KANSAS

Remote Attestation

- An attestation request is made
  - indicates what information is needed
  - includes a nonce to ensure freshness
- Measurements are gathered
  - hashes and extended hashes
  - LKIM and other dynamic approaches
- A quote is generated
  - includes evidence describing the system
  - includes the original nonce
  - signed by the attester
- A trust determination is made
  - safe, correct boot process
  - correct software and data
  - can the evaluated system be trusted?

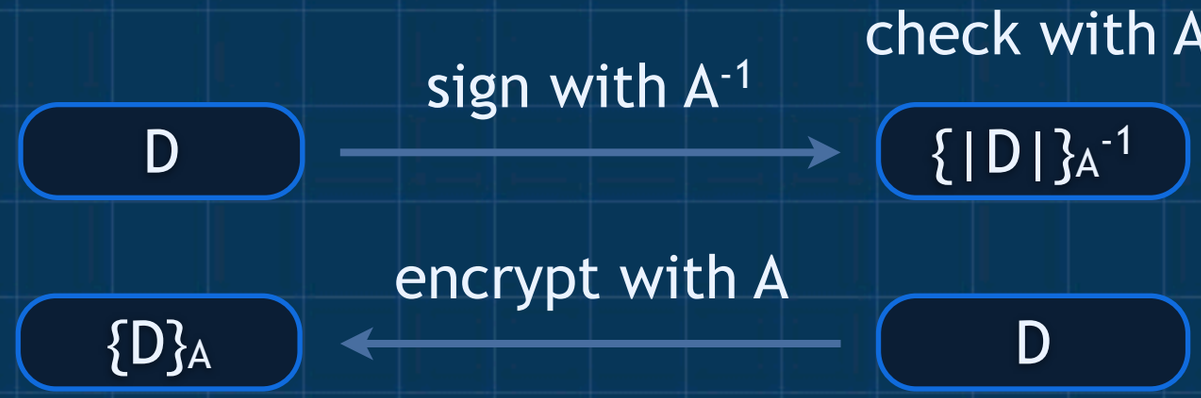


KU THE UNIVERSITY OF KANSAS

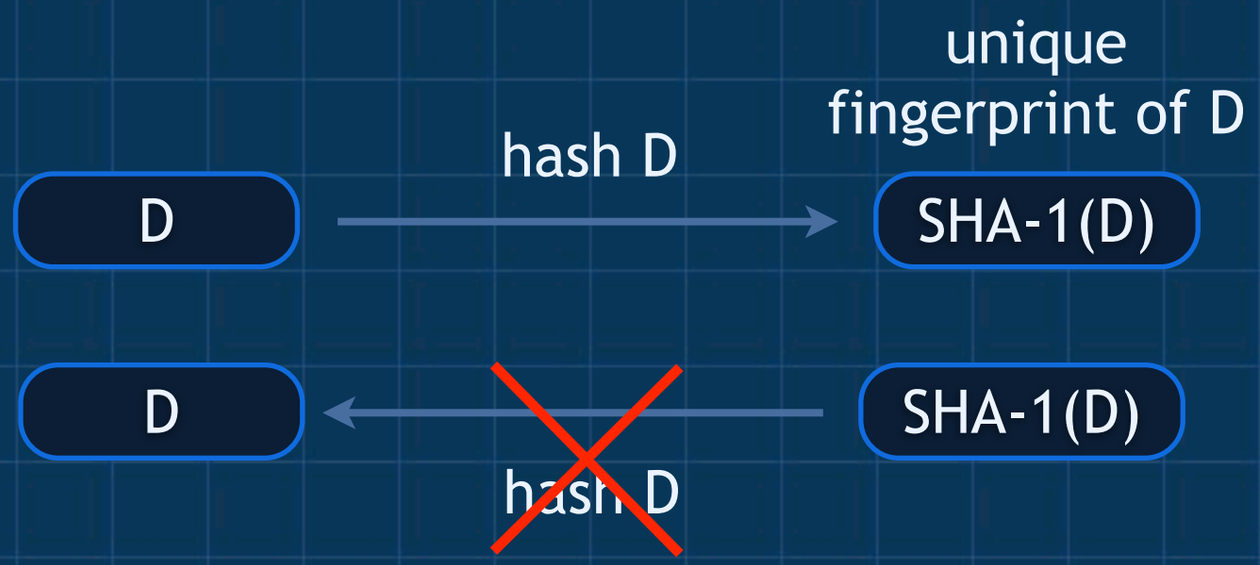
Preliminaries

(A, A^{-1}) - asymmetric key pair

A^{-1} - Private or signing key A - Public or encryption key



decrypt with A^{-1}



KU THE UNIVERSITY OF KANSAS

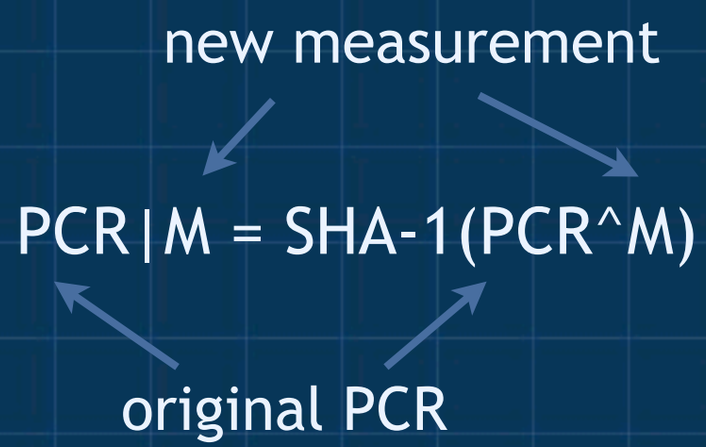
Trusted Platform Module (TPM)

- Non-volatile memory (NV)
  - Endorsement Key (EK) uniquely identifying the TPM
  - Storage Root Key (SRK) for wrapping asymmetric keys
- Volatile Memory
  - Platform Configuration Registers (PCR) for storing measurements
  - Attestation Identity Key (AIK) for individual attestations
- Cryptographic Engine
  - SHA-1 functionality for generating PCR contents
  - DSA cryptographic functionality for signatures, sealing, and encryption
  - Random number and asymmetric key generators for nonces and keys
- Unique instance “soldered onto” each motherboard
  - EK is established by the factory and cannot be reset
  - establishes a unique identifier for each computer system

KU THE UNIVERSITY OF KANSAS

Process Configuration Registers

- PCRs contain measurements
  - SHA-1 hashes of images and data
  - may be more sophisticated
- Stored in volatile RAM
  - minimum of 12, 120-bit registers
  - contain SHA-1 hashes
- PCRs are extended rather than set
  - SHA-1 of the PCR concatenated with a new measurement
  - captures the new value, original value, and order
- Records the state of a system and trajectory of states
  - used in attestation to evaluate system state
  - used to seal secrets to system state

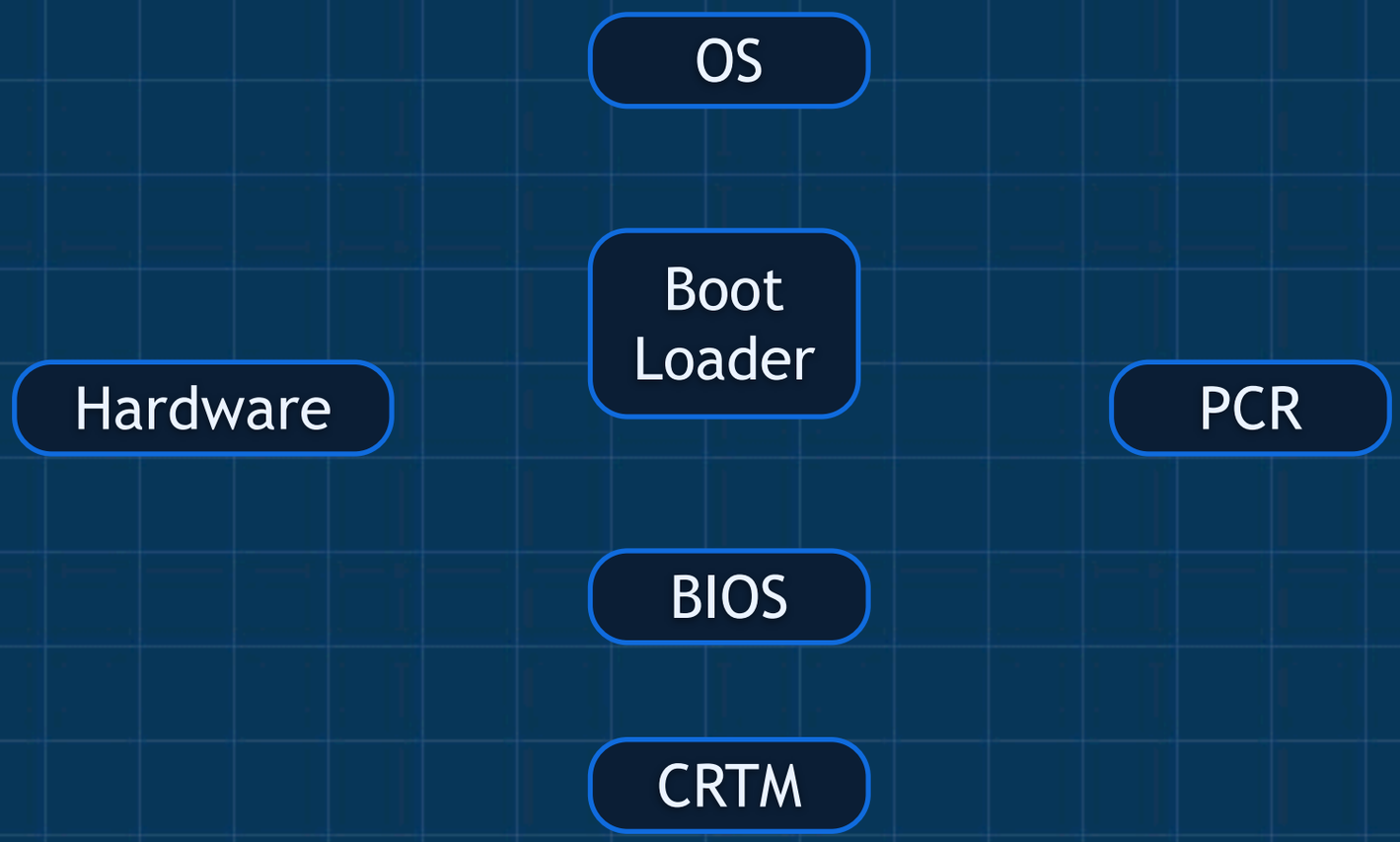


order matters!

PCR|M ≠ M|PCR

KU THE UNIVERSITY OF KANSAS

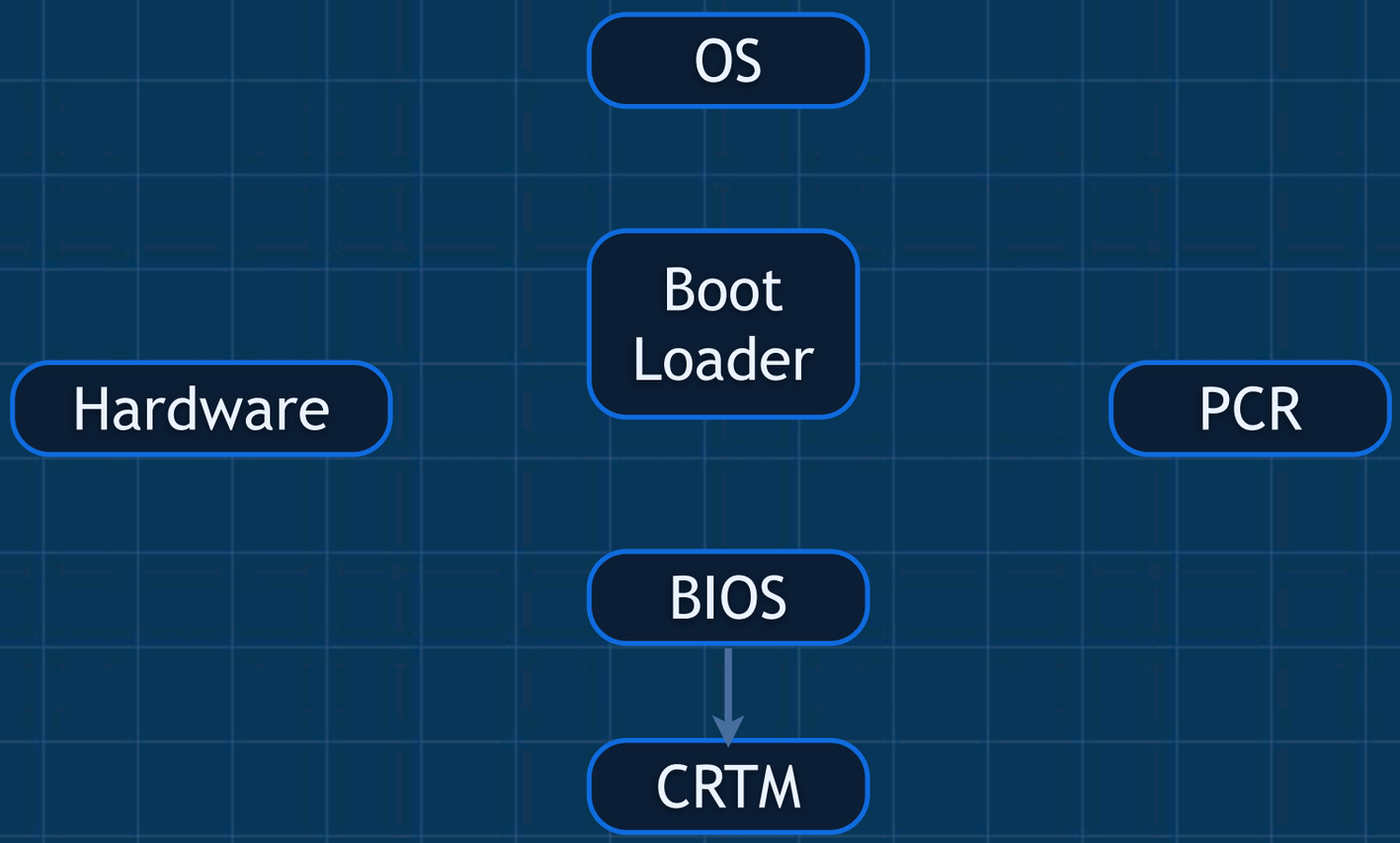
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the “bottom turtle”

KU THE UNIVERSITY OF KANSAS

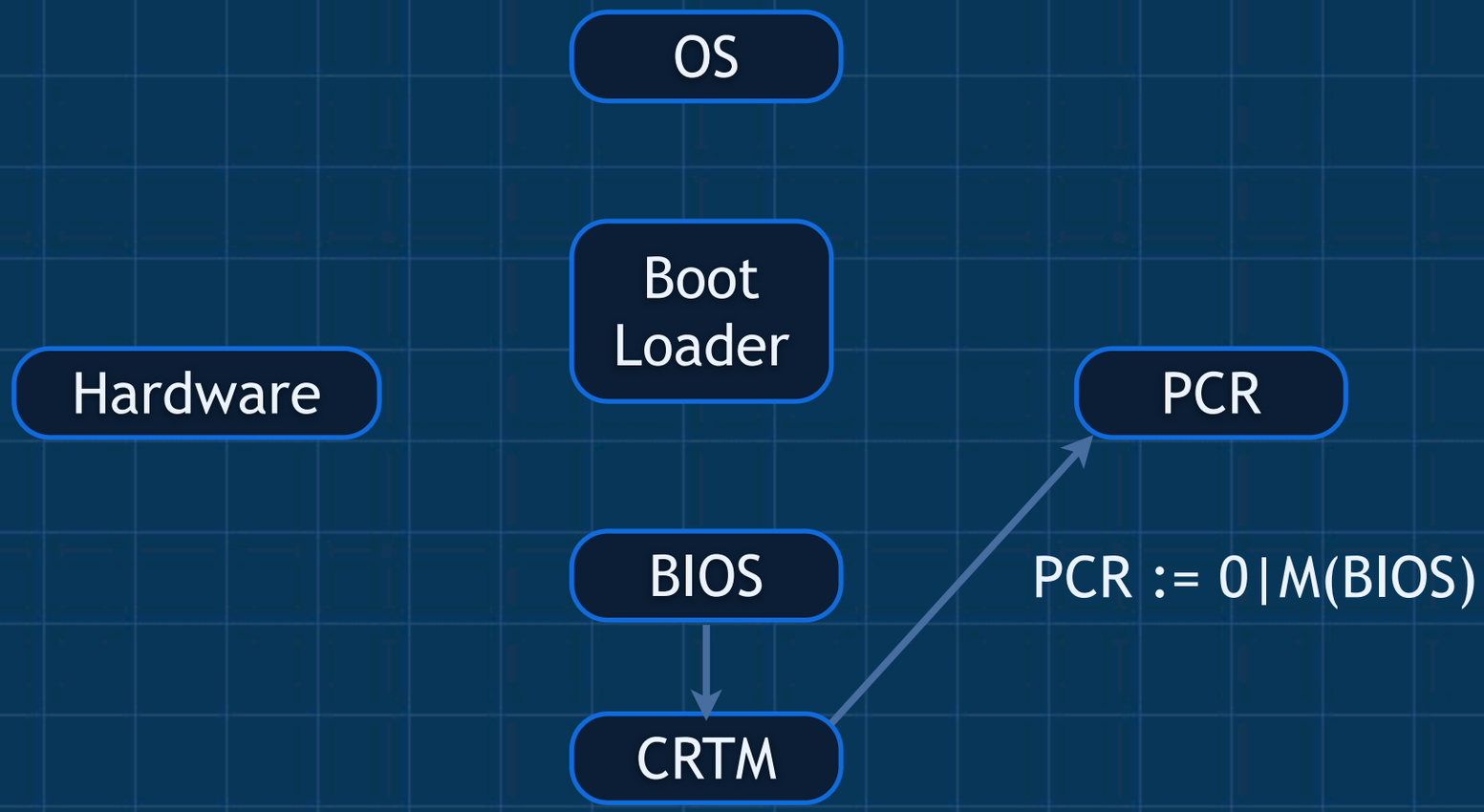
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the “bottom turtle”

KU THE UNIVERSITY OF KANSAS

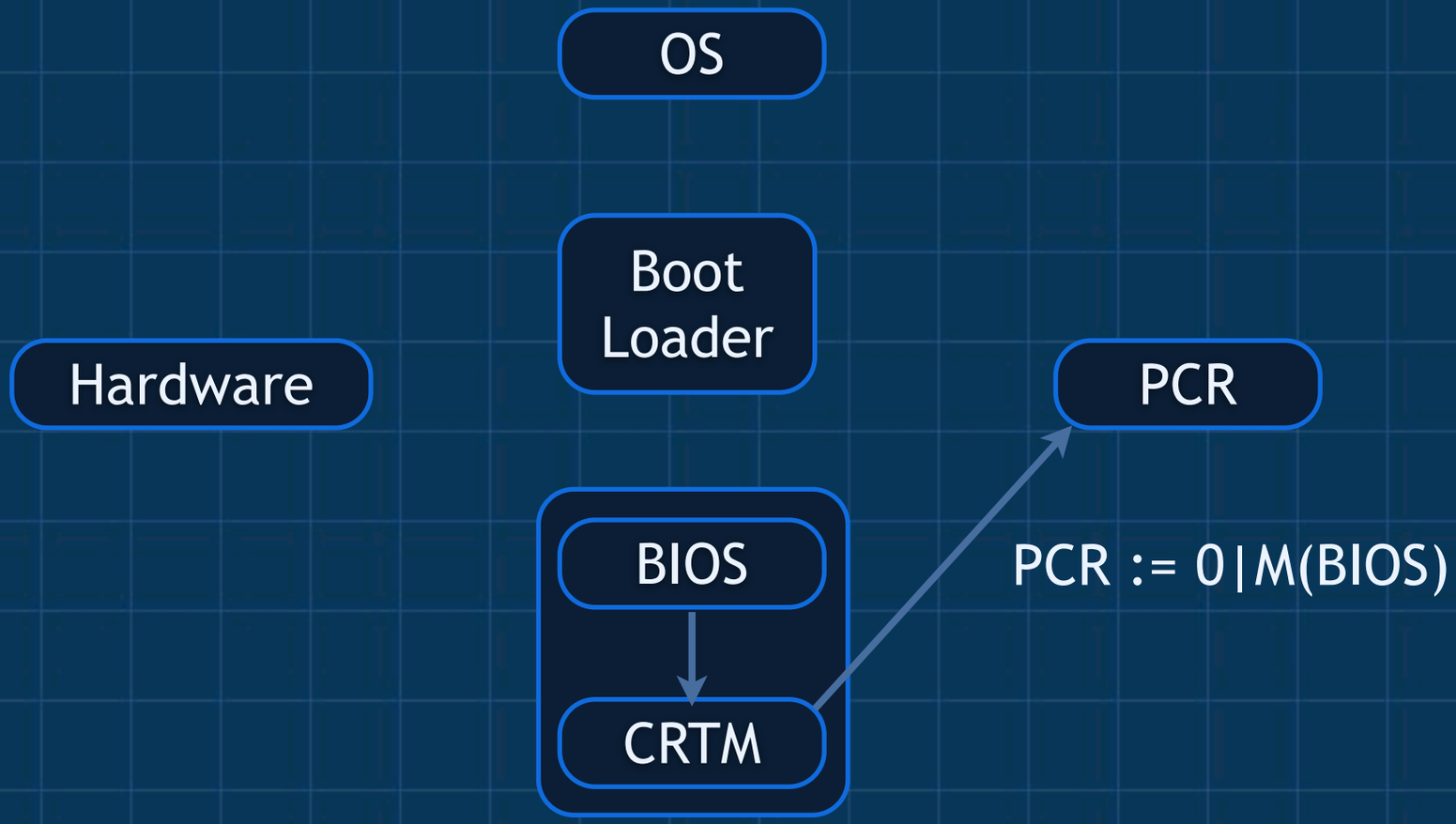
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

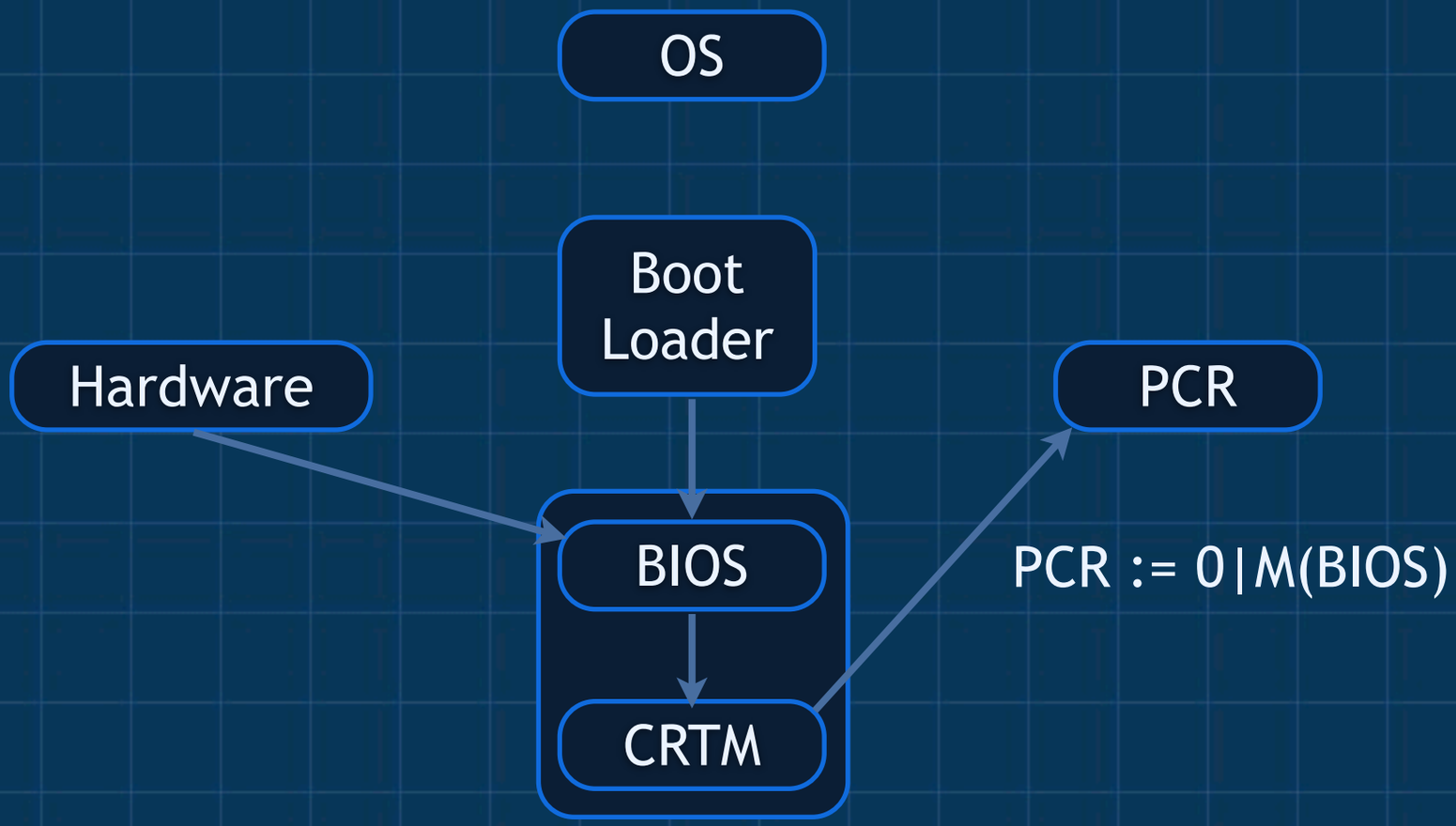
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

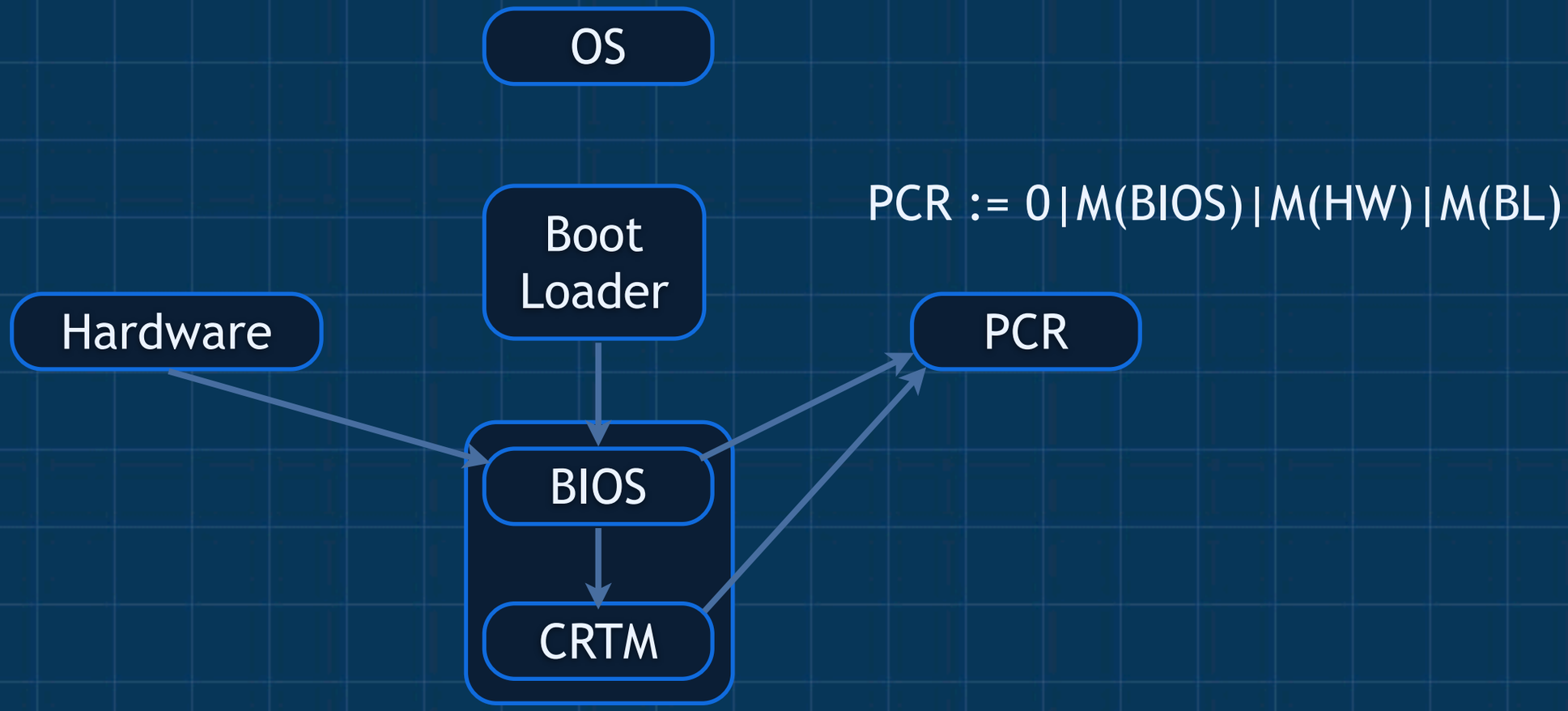
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

Measuring Boot to PCRs

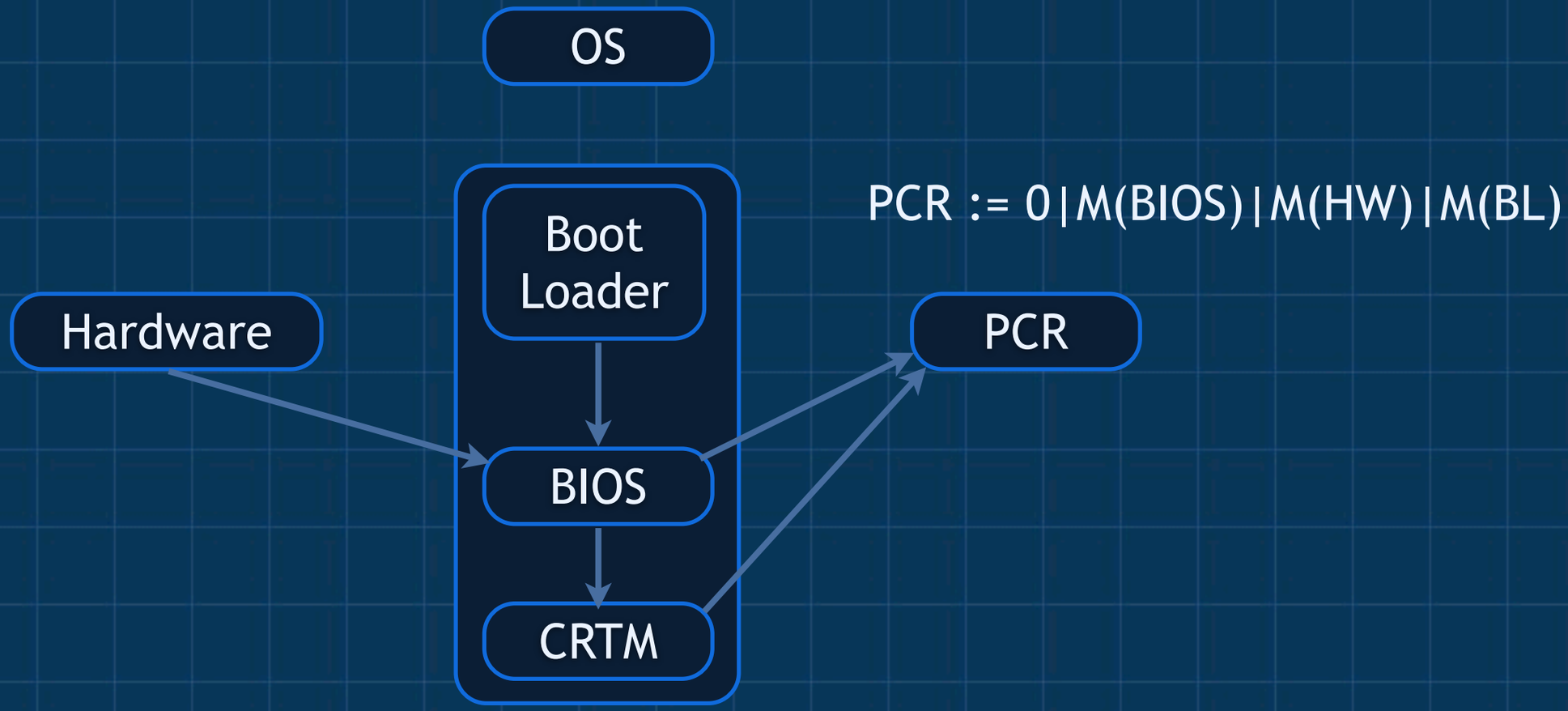


PCR := 0|M(BIOS)|M(HW)|M(BL)

Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

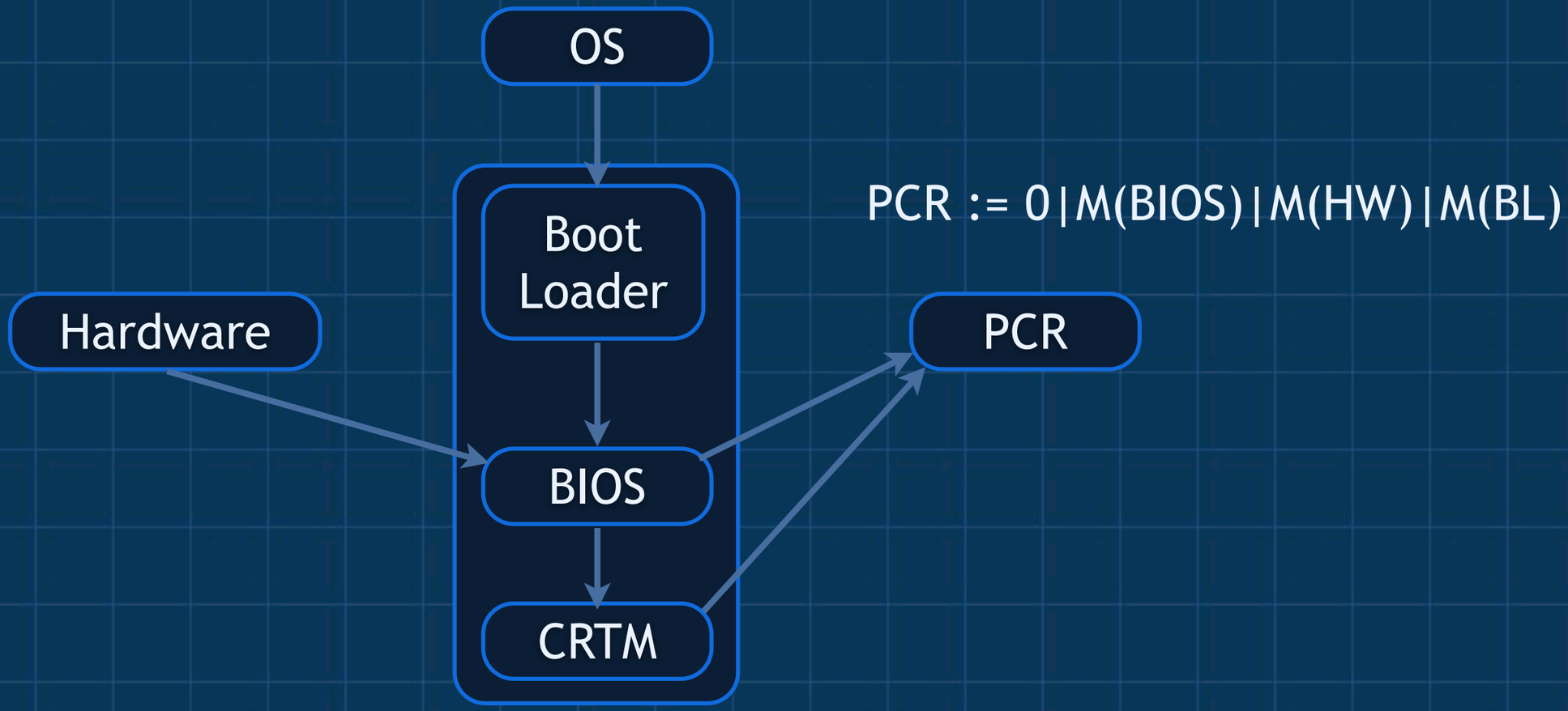
Measuring Boot to PCRs



Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

Measuring Boot to PCRs

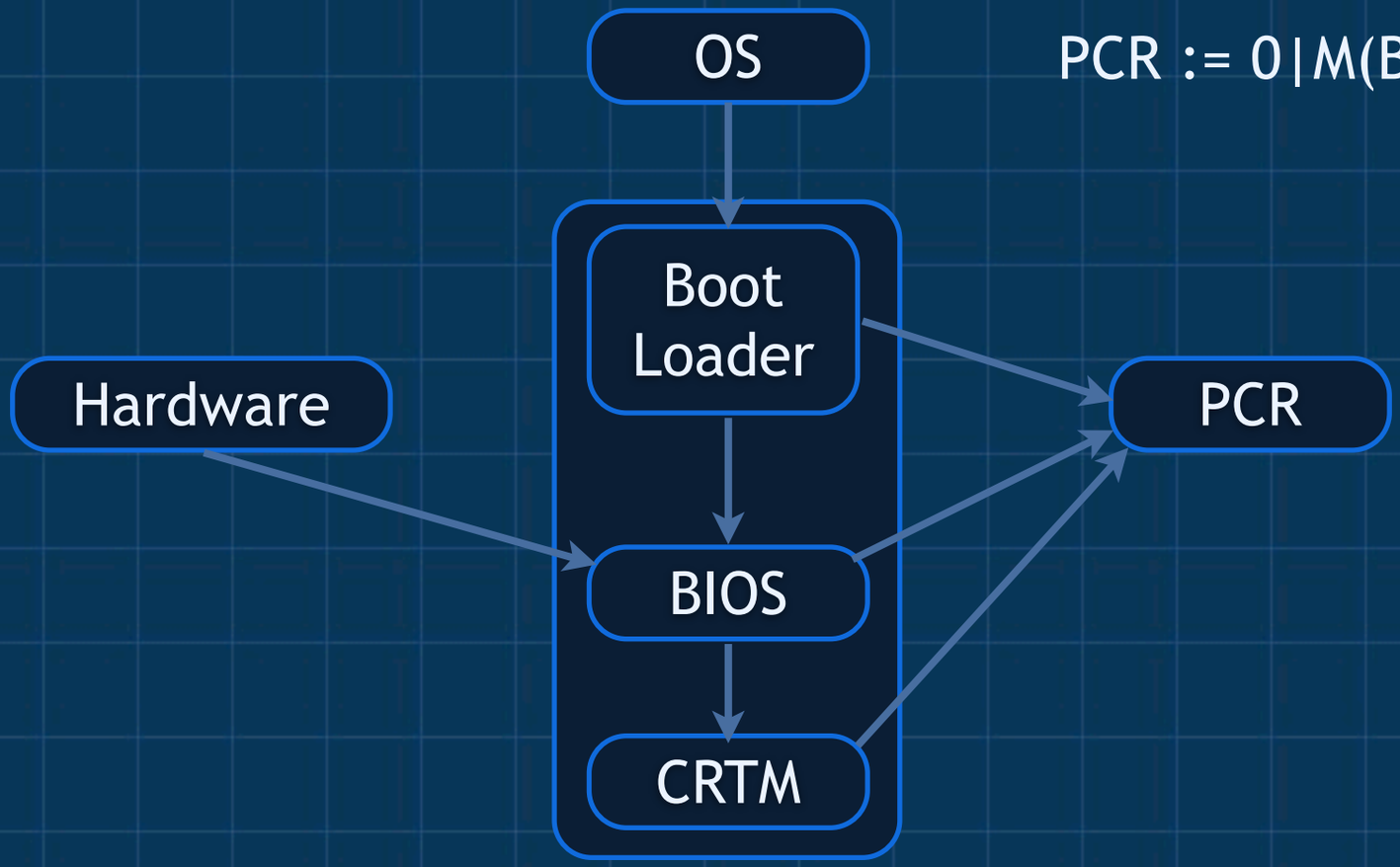


PCR := 0|M(BIOS)|M(HW)|M(BL)

Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

Measuring Boot to PCRs

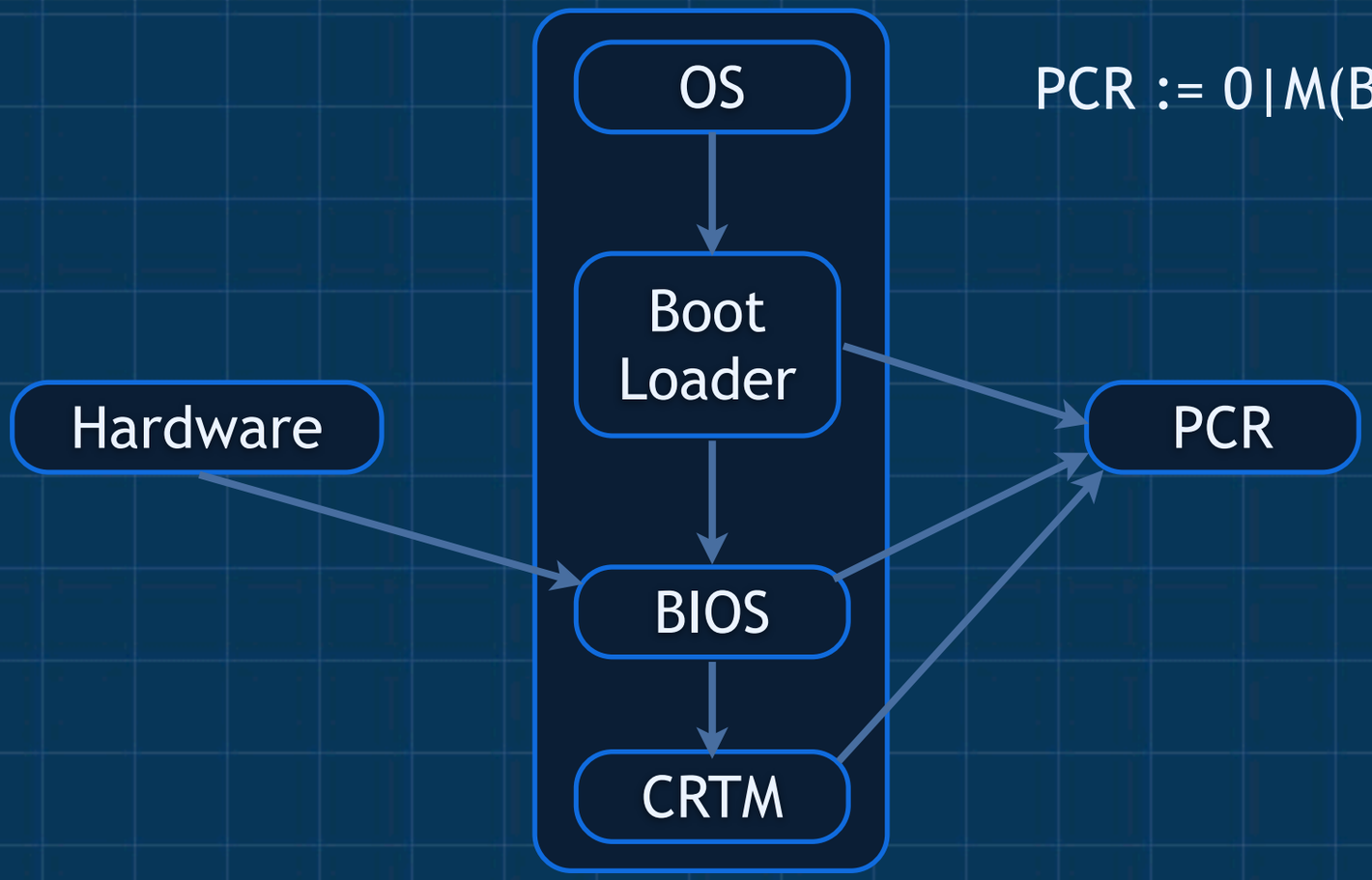


PCR := 0|M(BIOS)|M(HW)|M(BL)|M(OS)

Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

Measuring Boot to PCRs



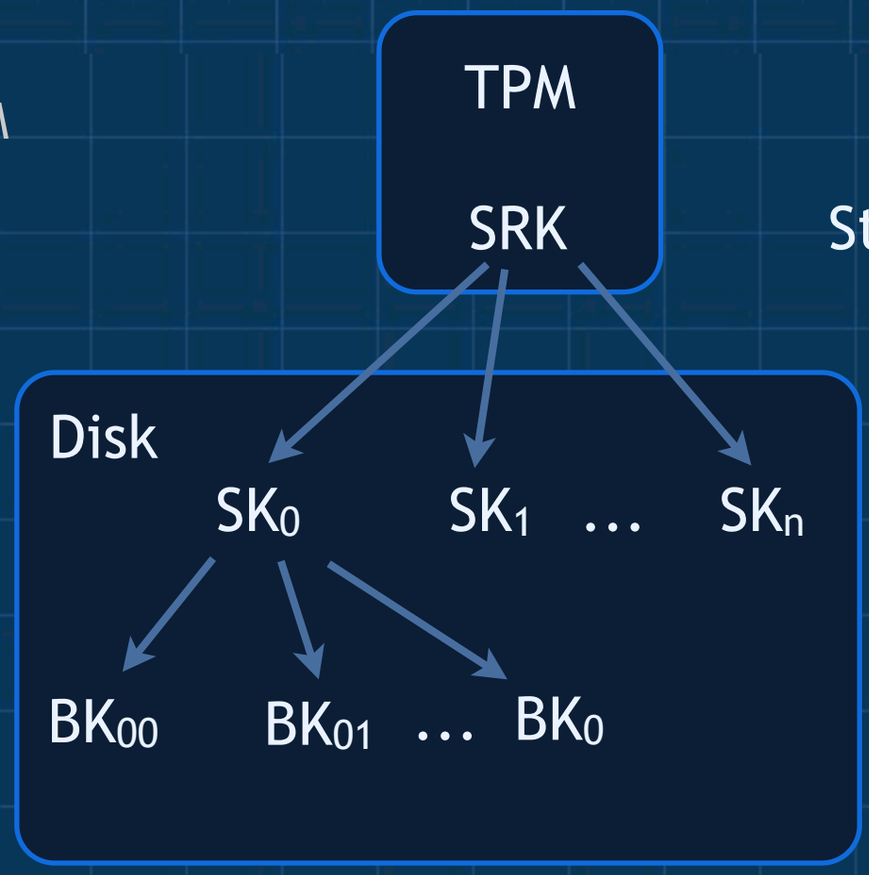
PCR := 0|M(BIOS)|M(HW)|M(BL)|M(OS)

Core Root of Trust for Measurement
place to stand for the "bottom turtle"

KU THE UNIVERSITY OF KANSAS

Keys and Data

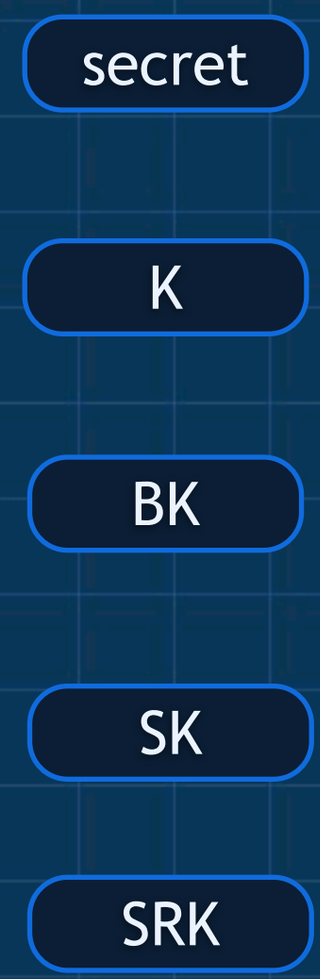
- Storage Root Key Pair (SRK)
  - generated by TPM when “owned”
  - private key stored in TPM non-volatile RAM
  - public key encrypts storage keys on disk
- Storage Keys
  - wrapped key - $(\{SK^{-1}\}_{SRK}, SK)$
  - exclusively used to encrypt keys
- Binding Keys
  - wrapped key - $(\{BK^{-1}\}_{SK}, BK)$
  - used to encrypt keys and small data
- Migratable vs Non-Migratable
  - migratable keys move to other TPMs (SK)
  - non-migratable keys must be used on their generating TPM (SRK)
  - non-migratable keys tie secrets to specific TPM



THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM

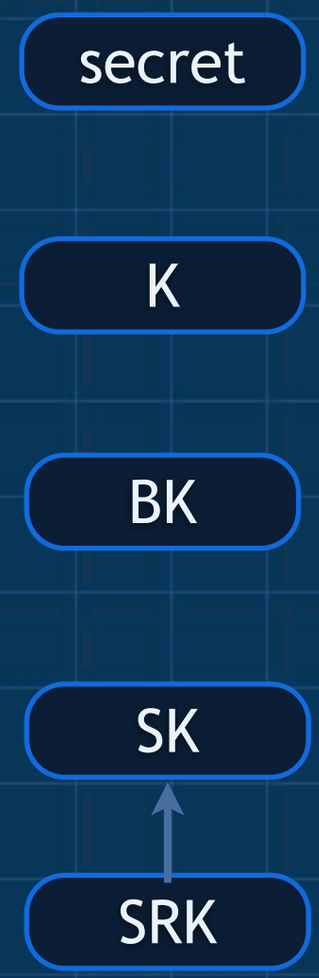


Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM

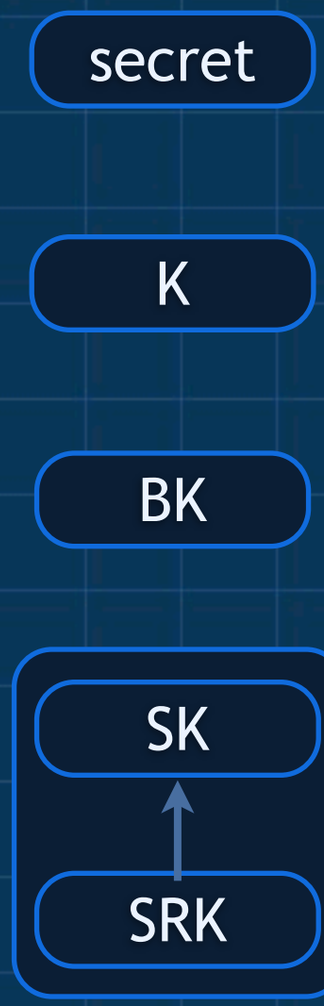


Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM



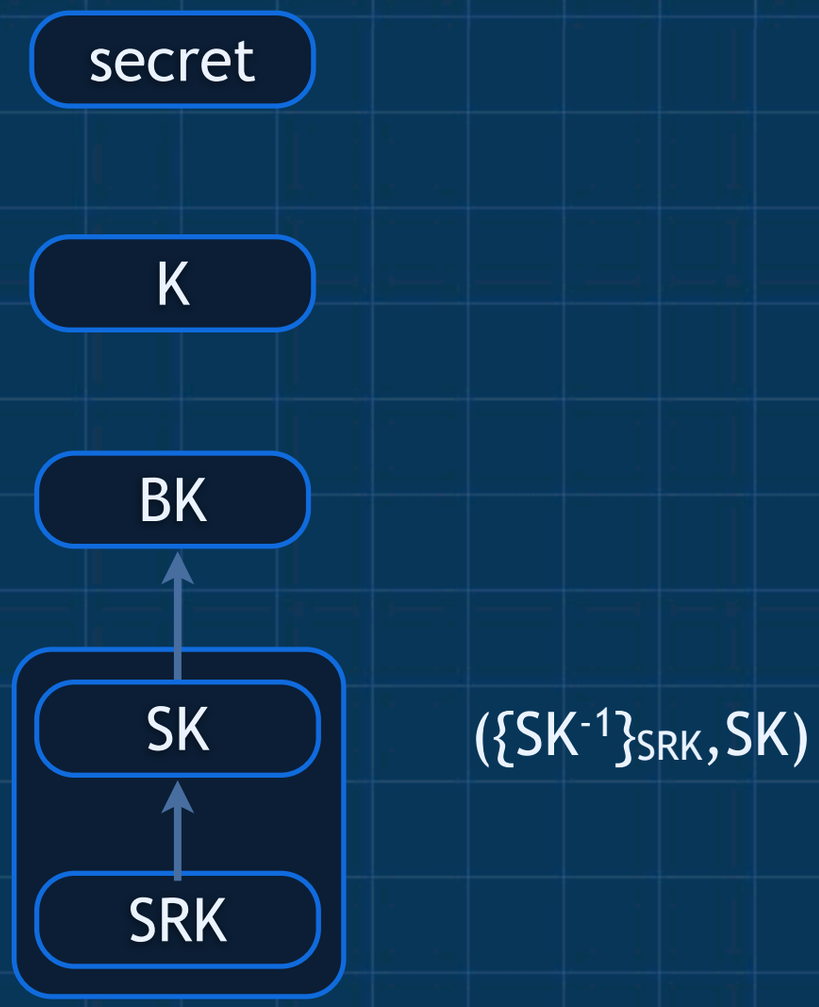
$(\{SK^{-1}\}_{SRK}, SK)$

Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM



KU THE UNIVERSITY OF KANSAS

Protecting Secrets

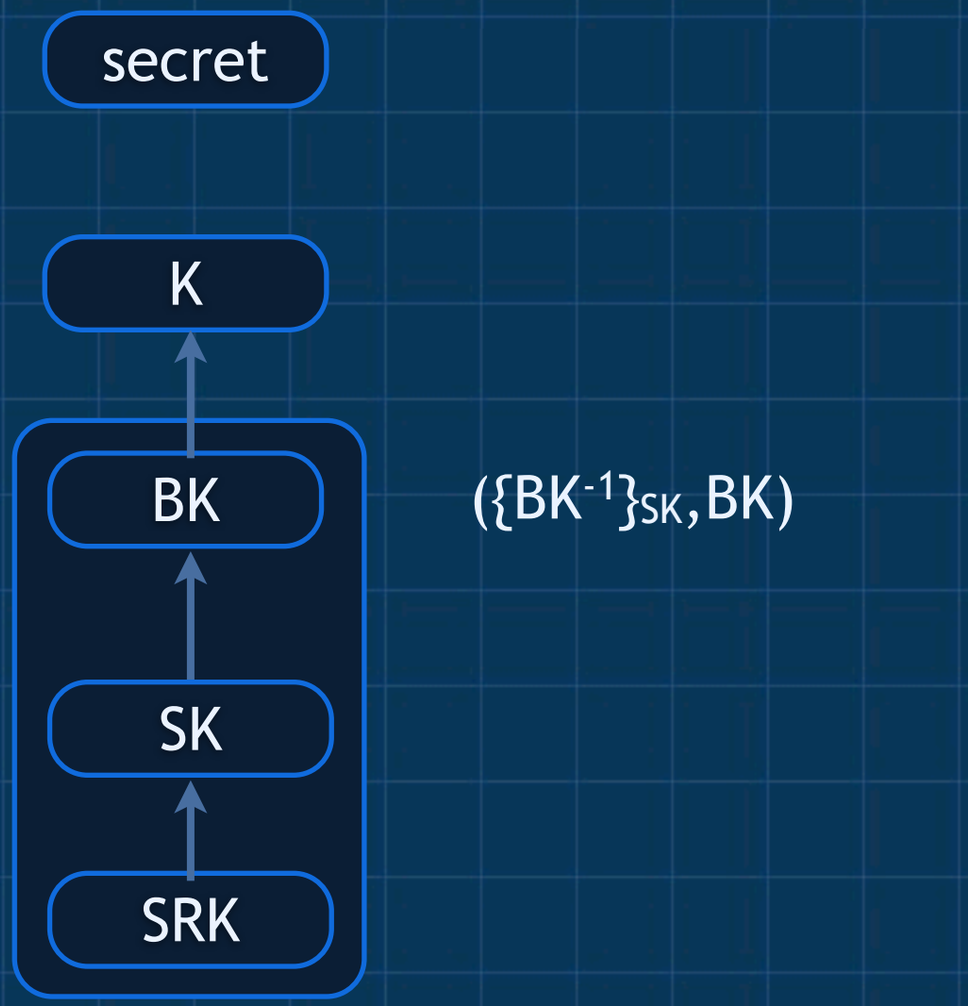
- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM

Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM

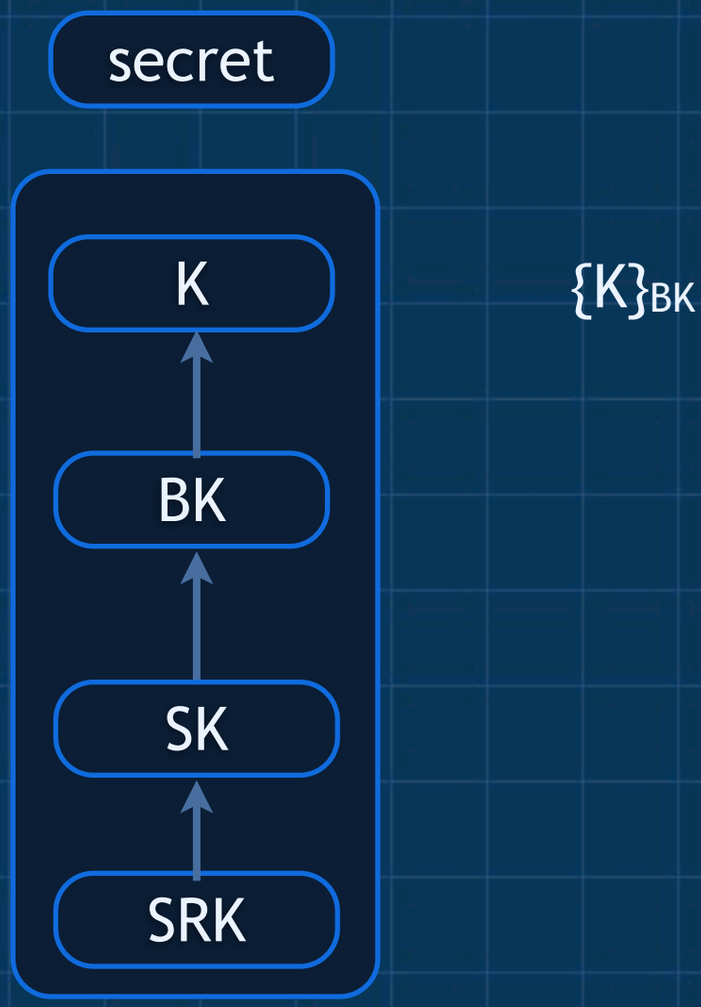


Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM

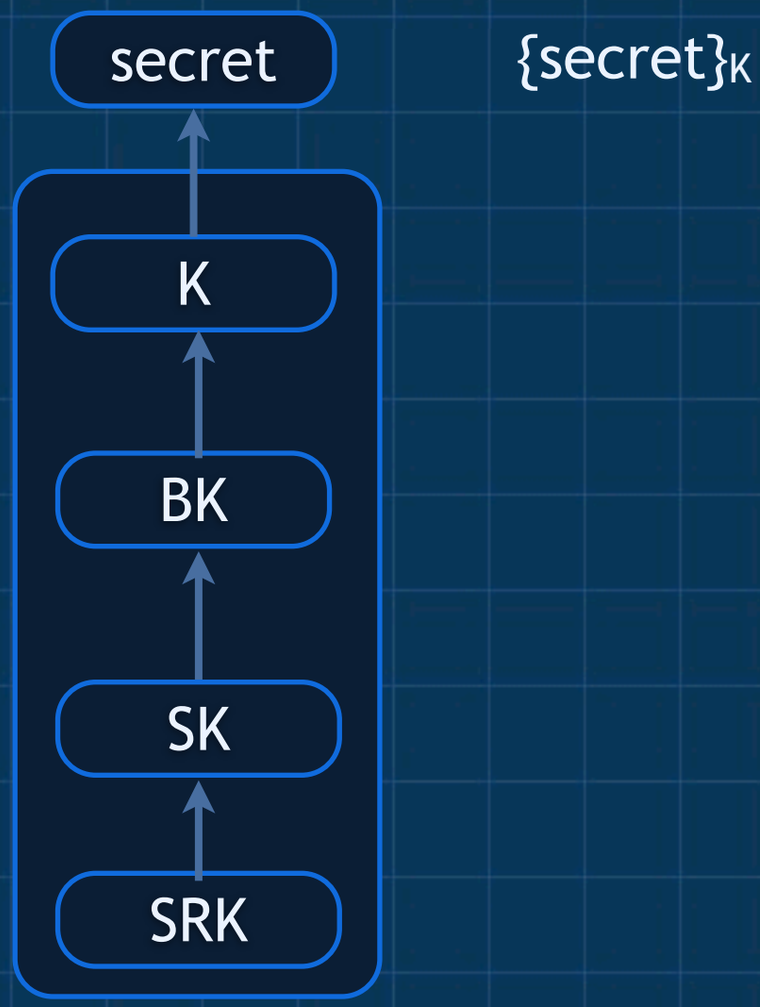


Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Protecting Secrets

- Symmetric key K encrypts a secret outside TPM
  - TPM is not a bulk encryptor
- Encrypt K with public key of BK
  - $\{K\}_{BK}$ is stored with the secret - enveloping
- Decrypt K to access secrets:
  - SK installed in the TPM, SRK^{-1} decrypts SK^{-1},
  - BK installed in the TPM, SK^{-1} decrypts BK^{-1}
  - BK^{-1} decrypts K, K decrypts secret
- Chain is broken if
  - Any key is corrupted or illegal
  - The the original SRK^{-1} is not available in the TPM
  - SRK^{-1} cannot be obtained from the TPM



$\{secret\}_K$

Root of Trust for Storage

KU THE UNIVERSITY OF KANSAS

Can you trust me?

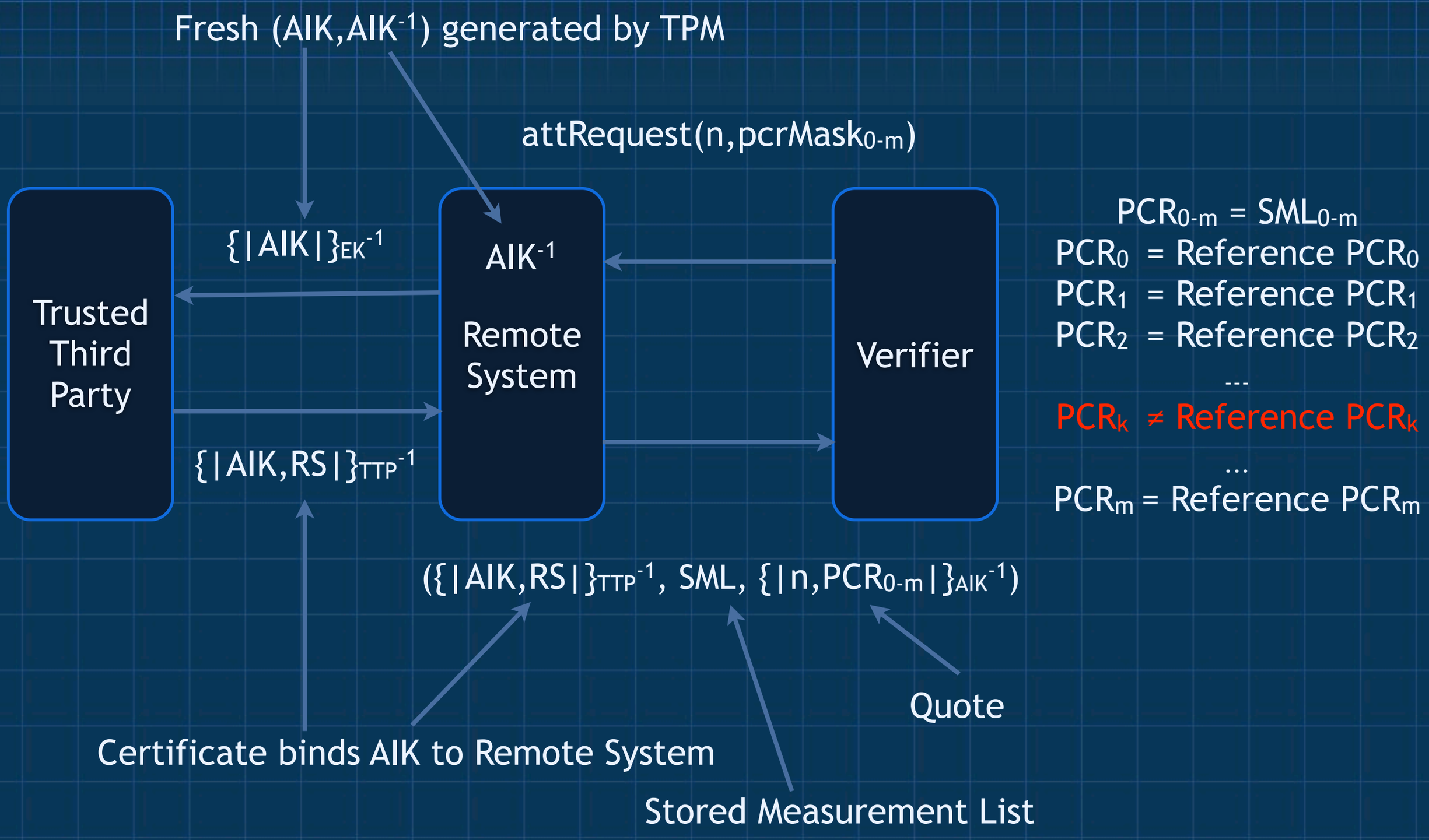
Remote Attestation

- Receive attestation request
  - PCR IDs and nonce
- Collect specified PCRs and nonce
  - concatenate PCR values
  - adding nonce prevents replay
- Sign and return as quote attesting to system state
- Check cryptographic properties
  - signature check ensures integrity
  - signature check ensures authenticity
  - nonce ensures freshness
  - “zero knowledge” of target

Sealing Secrets

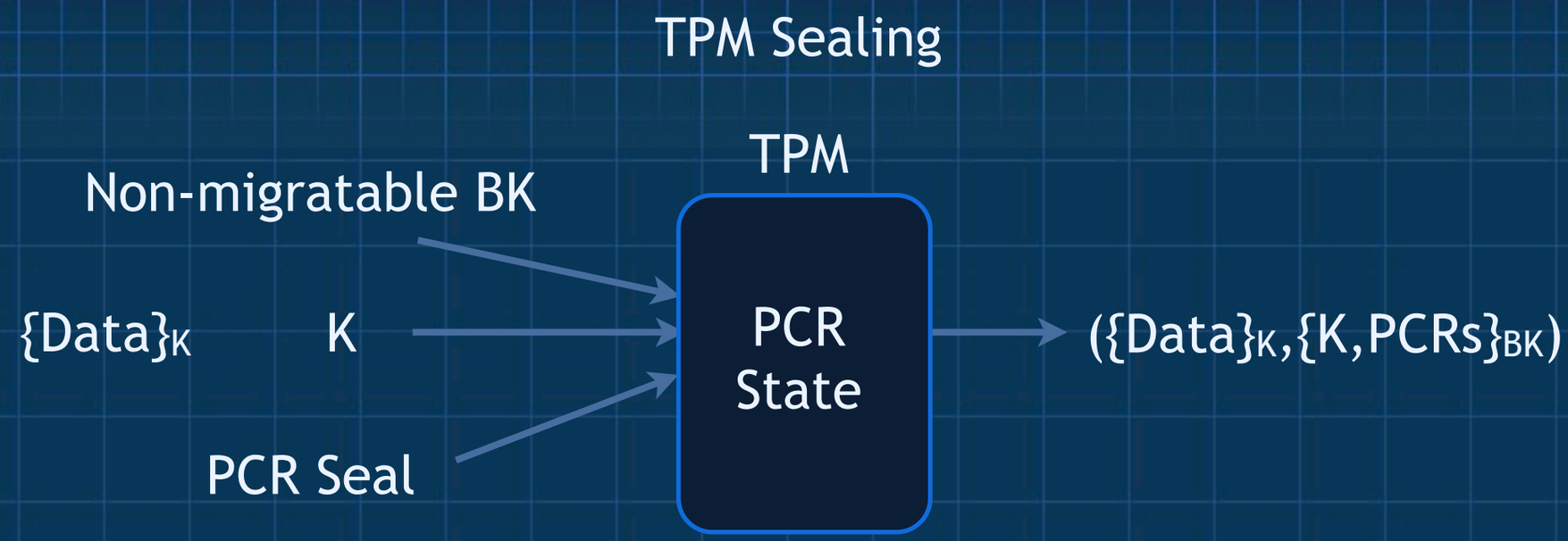
- Encrypt data blob with symmetric key
  - TPM is not a bulk encryptor
  - envelope the symmetric key
- Seal symmetric key with PCRs
  - use SRK->SK->BK->K stack
  - include selected PCRs from TPM with encrypted K
- Unseal key with TPM
  - install key stack using SRK as base
  - will not decrypt if PCR seal does not match TPM state
  - secrets can be protected even in unauthorized system state

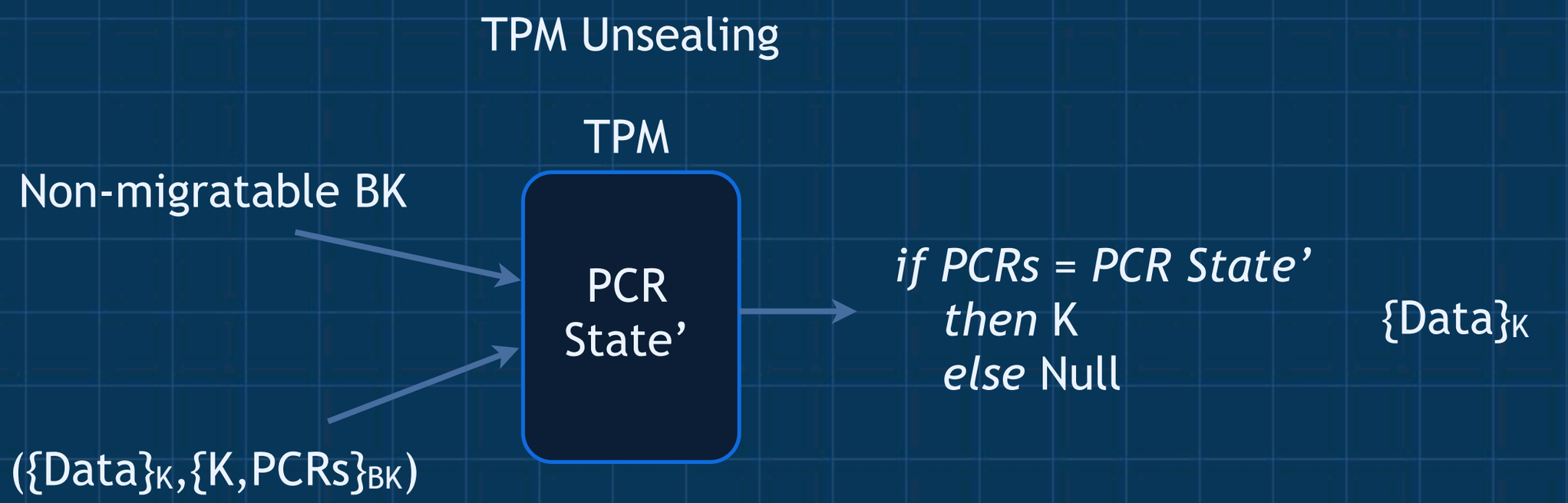
Attestation Protocol



THE UNIVERSITY OF KANSAS

Sealing Data to State





THE UNIVERSITY OF KANSAS

On to bigger things...

- Virtual Trusted Platform Module (vTPM)
  - like virtual memory, makes the TPM bigger
  - allows migration in virtual machine environments
- Software roots of trust
  - TPM requires hardware CRTM
  - software or virtual CRTM requires no hardware modifications
- More sophisticated run-time measurements
  - Linux Kernel Integrity Measurement (LIKM)
  - CoPilot, NFORCE, TripWire
  - hashing process components at run-time
  - re-measurement
- Aggregate trust
  - trusting things made from other trusted things
  - establishing collections external verifiers

KU THE UNIVERSITY OF KANSAS

What's the Controversy?

- The TPM uniquely identifies a machine
  - No more anonymity on the network
  - No more spoofing identities on the network
- The TPM can seal data to a machine
  - Programs and media can be locked to an individual machine
  - Personal data can be locked to an individual machine
- The TPM can track and deliver system state descriptions
  - No more communicating with a hacked system
  - No more communicating with a compromised system
- The TPM *is not* a DRM device
  - No more than AES or SHA-1 are DRM algorithms
  - In all likelihood there is one in your enterprise PC

KU THE UNIVERSITY OF KANSAS

The ITTC Information Assurance Laboratory

- An NSA/DHS Center of Excellence in Information Assurance Education
  - 5 year designation based on education, research and implementation
- Research
  - the ITTC IA Laboratory is 5 researchers spanning several disciplines
  - remote attestation and establishment of trust
  - system-level security and assurance
  - information aggregation in social networks
  - network security and resiliency
- Education
  - MSIT in Information Security (Edwards Campus)
  - MS and PhD emphasis in Information Assurance (Lawrence Campus)
  - education outreach to other regional institutions
- Implementation
  - KU Information Security Officer
  - EECS and ITTC Security Officers

KU THE UNIVERSITY OF KANSAS

Summary

- Remote and Self Attestation
  - establishing trust in a remote system
  - establishing trust in the local system
- The Trusted Platform Module
  - PCRs and PCR Extension
  - SRK and chaining keys
- Using the TPM
  - generating quotes for remote attestation
  - sealing data to system state
- Odds and ends
  - the TPM controversy
  - information assurance and KU

KU THE UNIVERSITY OF KANSAS