March 8, 2021
Zero Trust

- Today
  - Lab 2 Info
  - Zero Trust Computing
  - Trusted Platform Modules
  - Trusted Execution Environments
  - Network Enclaves
- Assignments
  - Project
    - Outline: Due Monday, Mar 29
  - Lab 2
    - Due Monday, Apr 5

Zero Trust Architectures

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

- Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.
- Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

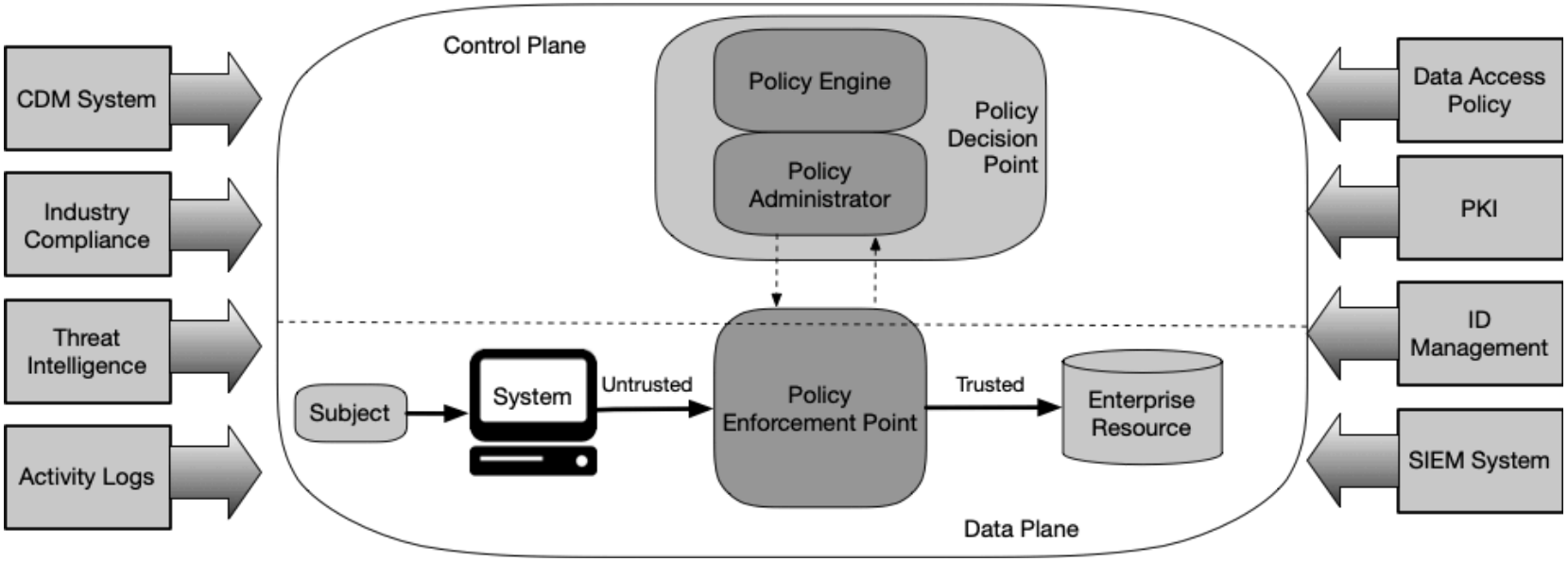
Tenets of Zero Trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

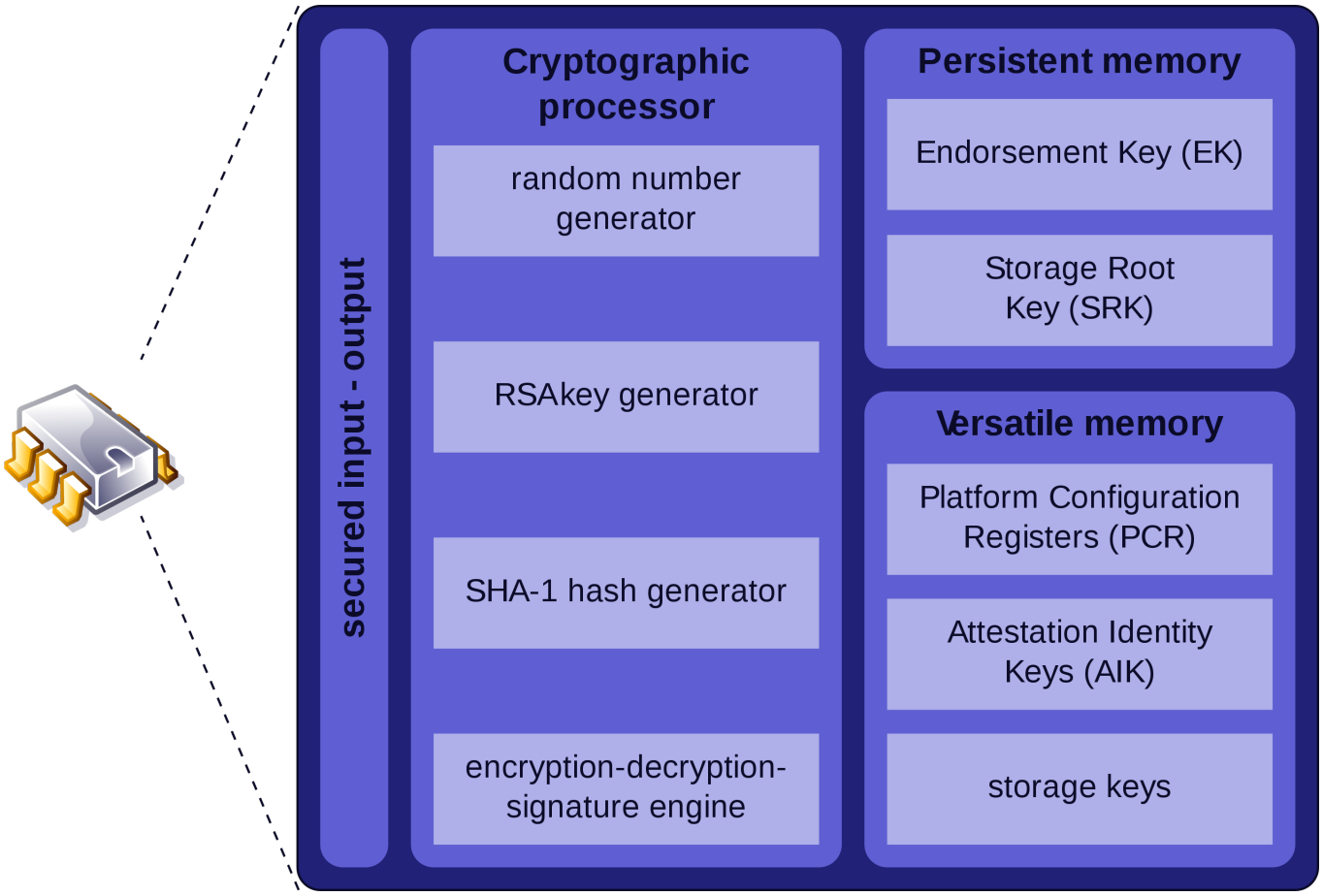
Tenets of Zero Trust

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Components of ZTA



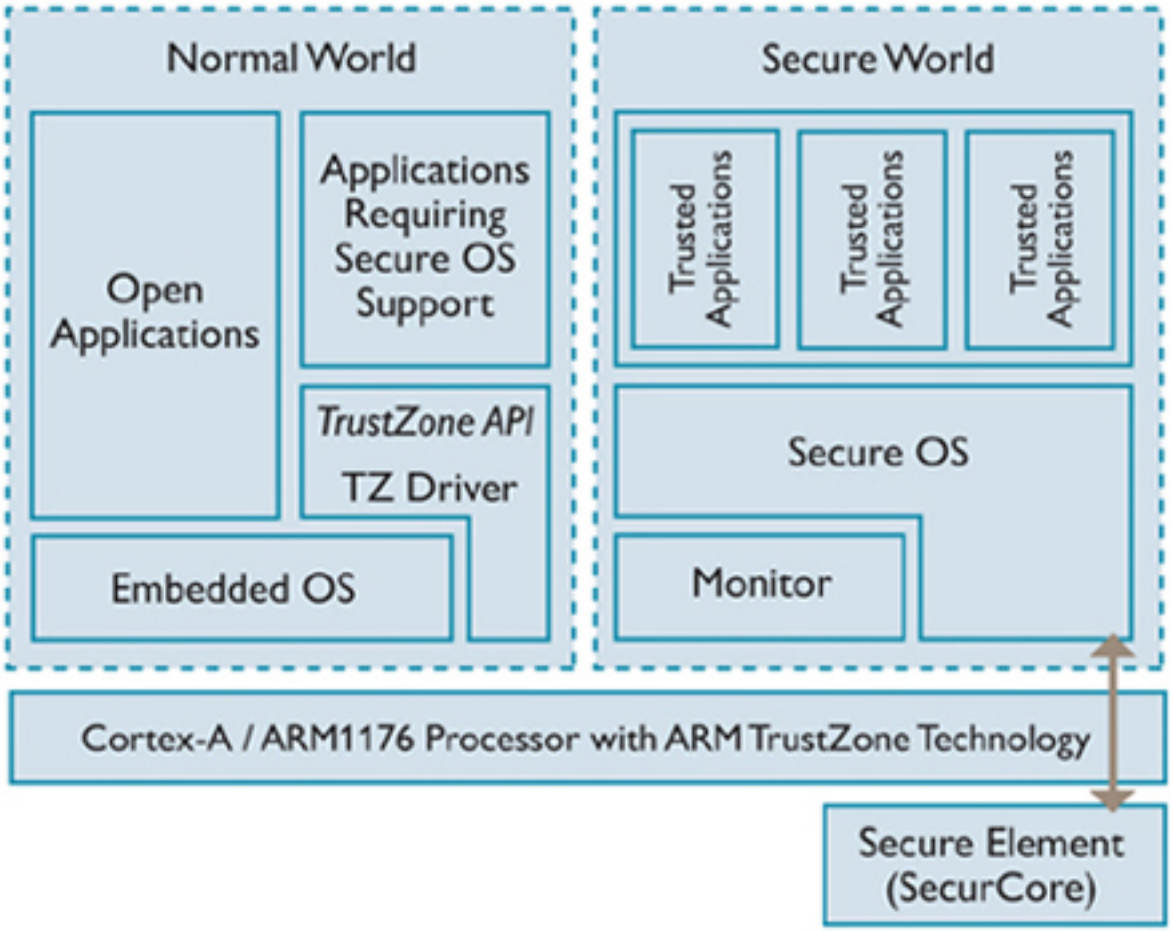
Trusted Platform Modules



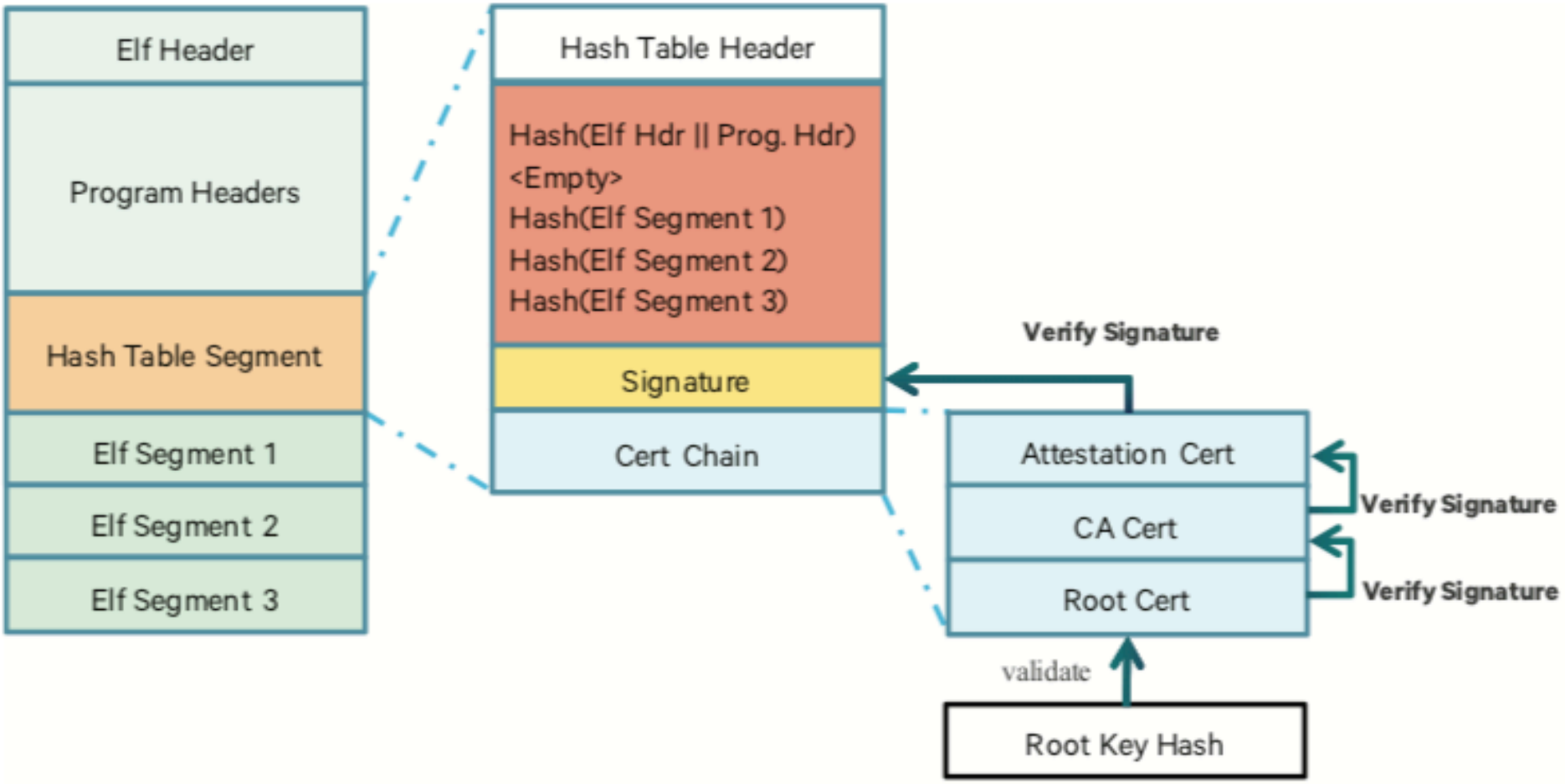
Intel Trusted Execution Technology

- Trusted Execution engine
- Components
  - Processor
  - Chipset
  - Keyboard and Mouse
  - Graphics
  - TPM
- VT Virtualization Extensions

ARM TrustZone



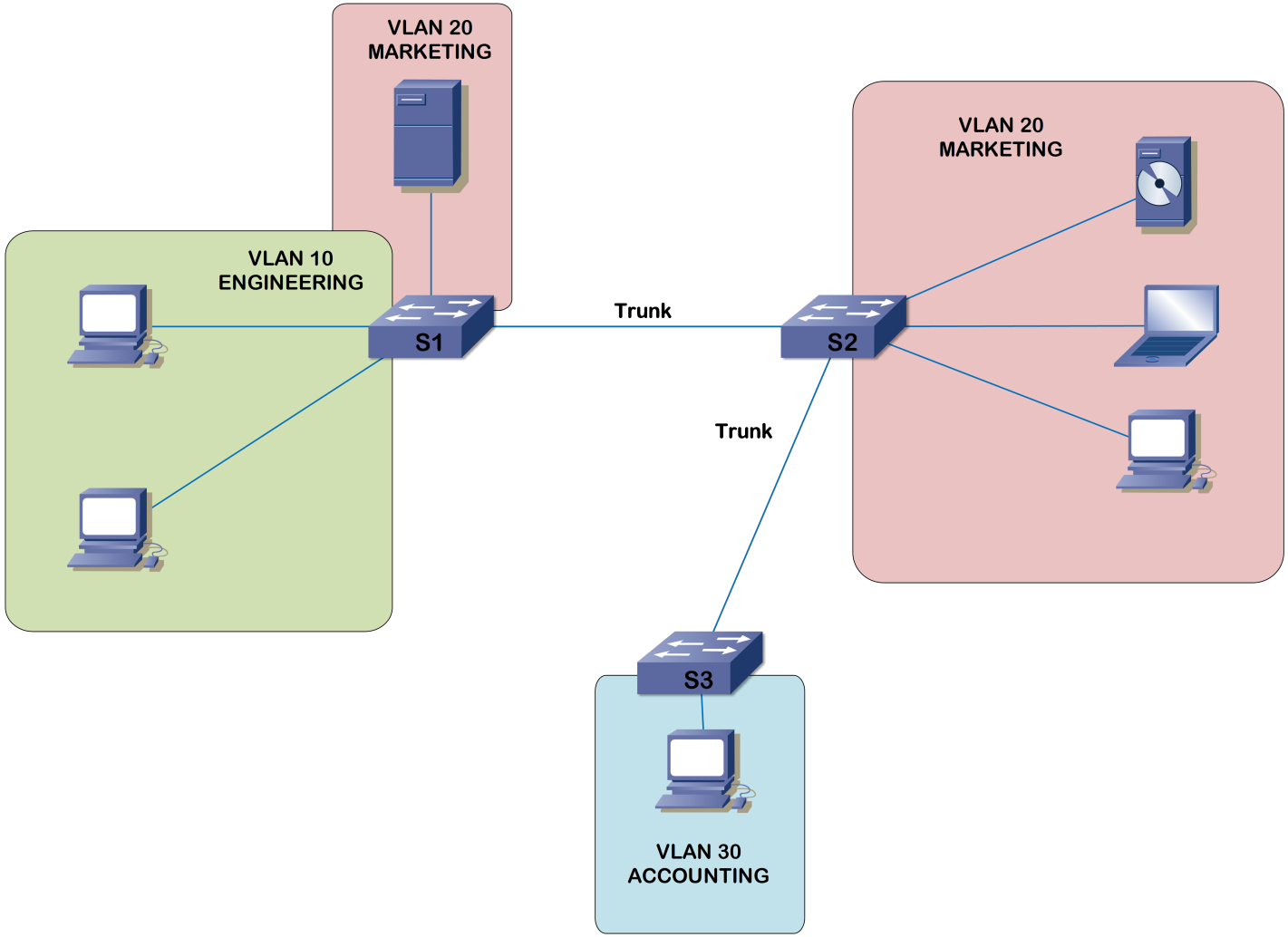
TrustZone Chain of Trust



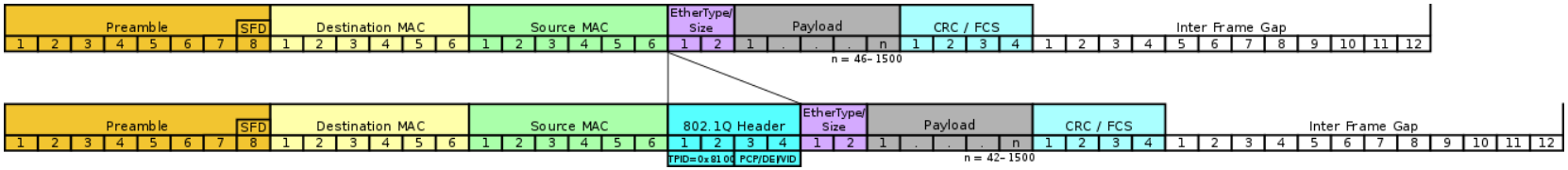
Network Enclaves

- Limit access to a portion of a network
- Mechanisms
  - Firewalls
  - VLANS
  - VPNs
- Challenges?

VLANS


VLAN 20
MARKETING
VLAN 10
ENGINEERING
S1
Trunk
S2
VLAN 20
MARKETING
Trunk
S3
VLAN 30
ACCOUNTING

L2 Frame format for IEEE 802.1Q



- TPID – Tag Protocol Identifier (Always 0x8100)
- TCI – Tag Control Information
  - 3 Bits – Priority code
  - 1 bit – Drop eligible
  - 12 bits – VLAN id