SDC 20

BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

Trustworthy Storage - Expectations and Realities

Eric Hibbard, CISSP, CITP, CISA
PrivSec Consulting LLC

About the Speaker

Eric Hibbard, CISSP-ISSAP, ISSMP, ISSEP, CIPT, CISA, CCSK

Security/Privacy Professional
eric.Hibbard@gmail.com

Chair, SNIA Security Technical Work Group
Chair, INCITS TC CS1 Cyber Security
Chair, IEEE Computer Society, Cybersecurity & Privacy Standards Committee (CPSC)
Co-Chair, Cloud Security Alliance (CSA) – International Standardization Council (ISC)
Member, American Bar Association – Science & Technology (SciTech) Law Council
Member, American Bar Association – Cybersecurity Legal Task Force
Co-Chair, American Bar Association – SciTech Law – Internet of Things (IoT) Committee
ISO Editor: ISO/IEC 27040, ISO/IEC 27050 (multi-part), ISO/IEC 17788, ISO/IEC 22123 (multi-part), ISO/IEC 20648
IEEE Editor: IEEE Std 1619 (XTS-AES)

Abstract

As security capabilities are added to storage technologies, storage-based systems and solutions can serve as a last line of defense in an organization's defense in depth strategy. While these storage security developments are important, the threat landscape continues to change in negative ways, so new responses are needed. Models such as zero trust and trustworthiness have emerged as potential approaches for dealing with the near-ubiquitous threats. In essence, trust nothing, verify everything, and design for failures. Easy enough to state, but the reality is fraught with many challenges.

This session highlights important storage security elements that can serve as building blocks for these models. In addition, the concepts behind zero trust and trustworthiness are explored with an eye to storage, both traditional and cloud based. Lastly, the drivers (e.g., regulations) for adopting these new models and the standards/specifications that outline what is necessary will be discussed.

Agenda

- Trustworthiness Overview
- Zero Trust Overview
- Securing Storage

Trustworthiness

Trustworthiness Defined

Trustworthiness corresponds to the ability to meet stakeholders' expectations in a verifiable way.

NOTE 1: Depending on the context or sector, and also on the specific product or service, data, and technology used, different characteristics apply and need verification to ensure stakeholders expectations are met.

NOTE 2: Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability, and accuracy.

NOTE 3: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

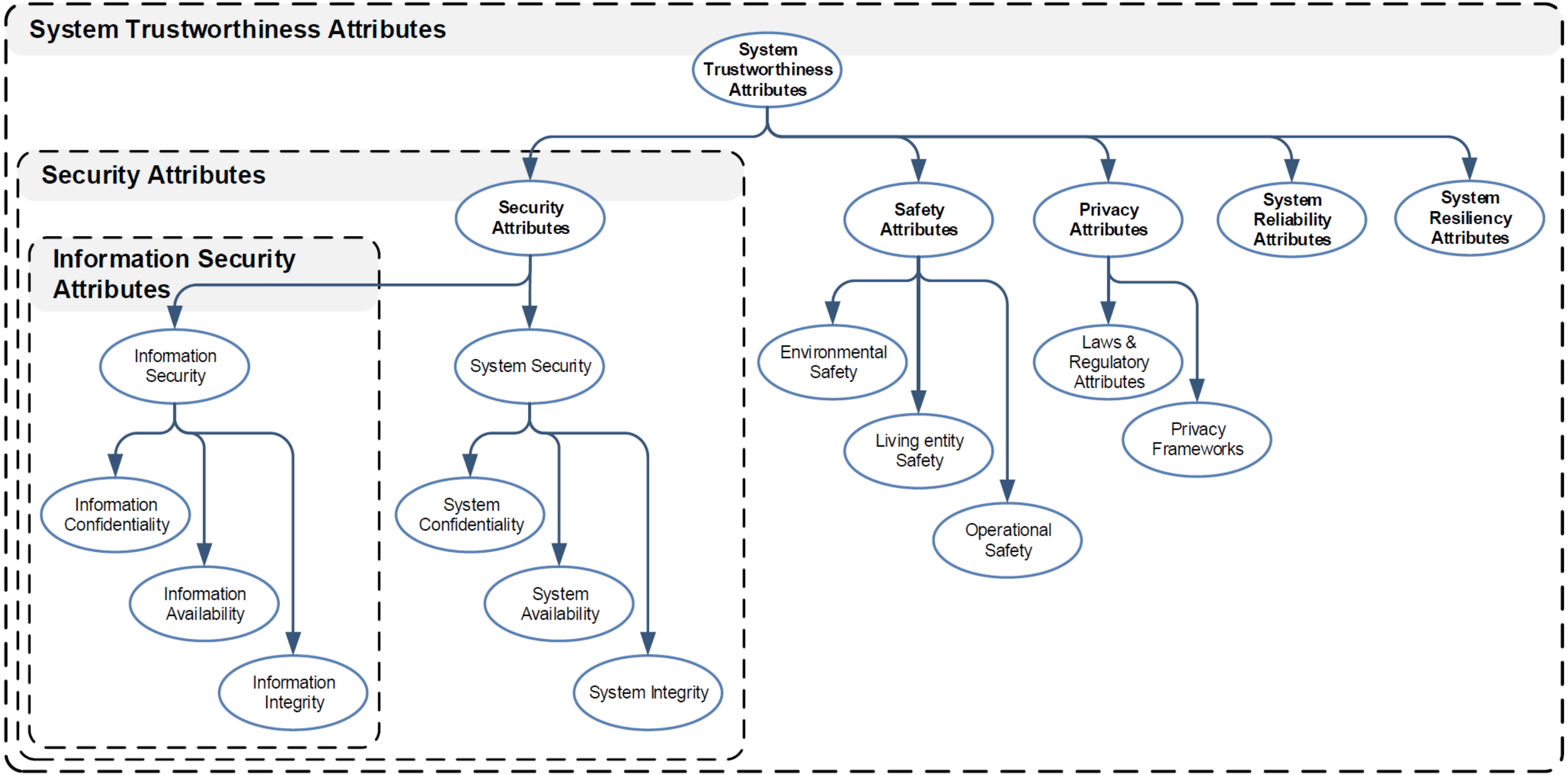
Key Elements of Trustworthiness

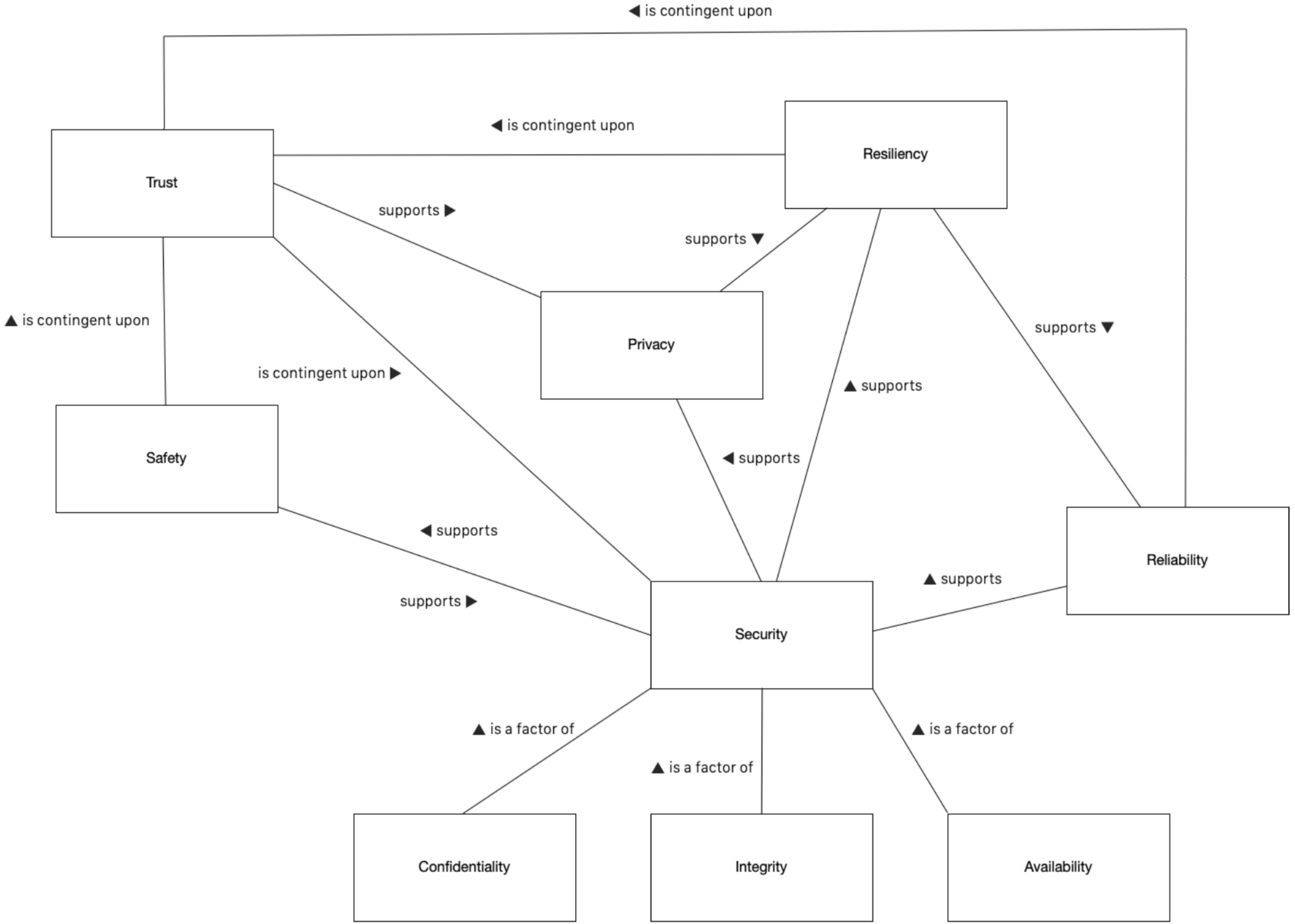
- Safety
  - Prevention of unacceptable risk of physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment
  - Consists of environmental safety, living entity safety, and operational safety
- Security
  - Consists of information integrity, system integrity, information availability, system availability, information confidentiality, and system confidentiality
- Privacy
  - Consists of privacy frameworks, law and regulations

Key Elements of Trustworthiness (cont.)

- Resilience
  - Property of a system that behaves in a manner to avoid, absorb and manage dynamic adversarial conditions while completing the assigned missions, and reconstitute the operational capabilities after causalities
- Reliability
  - Set of conditions under which the system is tested to demonstrate that the functions perform for a specified period of time

System Trustworthiness Attributes Overview




◀ is contingent upon
◀ is contingent upon
Resiliency
Trust
supports ▶
supports ▼
▲ is contingent upon
Privacy
supports ▼
is contingent upon ▶
▲ supports
Safety
◀ supports
◀ supports
Reliability
▲ supports
supports ▶
Security
▲ is a factor of
▲ is a factor of
▲ is a factor of
Confidentiality
Integrity
Availability

Processes to promote trustworthiness

- Configuration management for information assets
- Configuration management for physical assets
- Reproducible build process
- Reproducible distribution and deployment process
- Secure development process
- Secure response process
- Incident response process
- Systems management and security management processes
- Supply chain processes to promote authenticity and integrity
- Follow international and industry standards, best practices
- Evaluation by accredited laboratories

Protections needed for trustworthiness

- Protection from
  - Unauthorized disclosure
  - Modification
  - Temporary or permanent loss
  - Loss of confidence in the information asset
  - “Interference”, i.e., the lack of isolation from others (when desired)

Controlling capabilities for trustworthiness

- Control over error reporting and diagnostics
- Control over real-time protection capabilities
- Control over key escrow capabilities
- Ability to add, remove, replace, augment selected features

Zero Trust (ZT)

Zero Trust Defined

- *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. [NIST SP 800-207]

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

Tenets of Zero Trust (cont.)

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.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets

Tenets of Zero Trust (cont.)

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

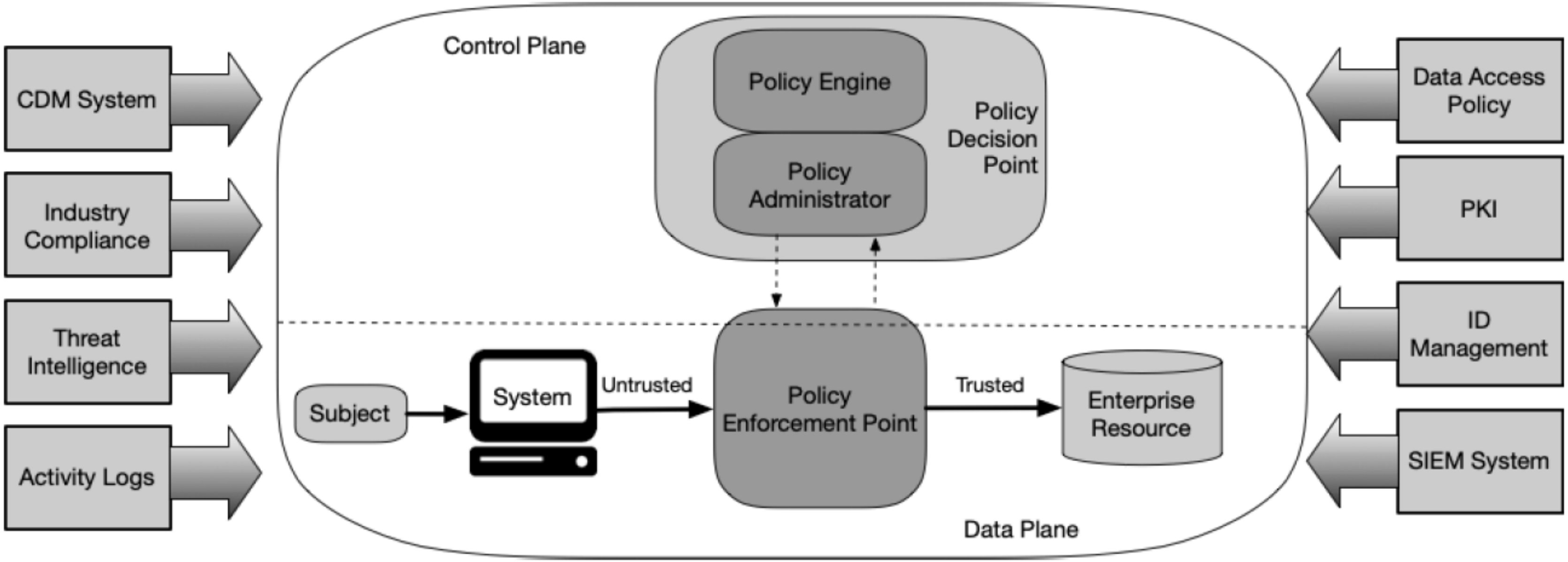
Zero Trust View of a Network

1. The entire enterprise private network is not considered an implicit trust zone
2. Devices on the network may not be owned or configurable by the enterprise
3. No resource is inherently trusted
4. Not all enterprise resources are on enterprise-owned infrastructure

Zero Trust View of a Network (cont.)

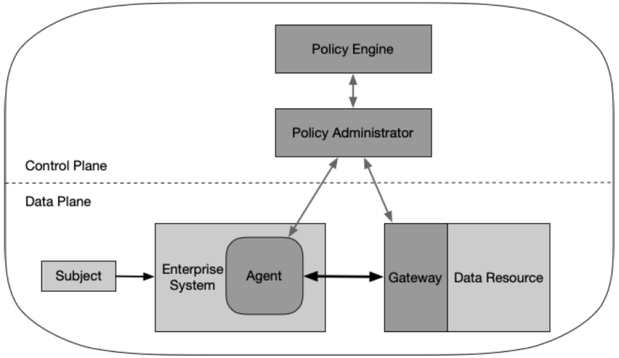
5. Remote enterprise subjects and assets cannot fully trust their local network connection
6. Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture

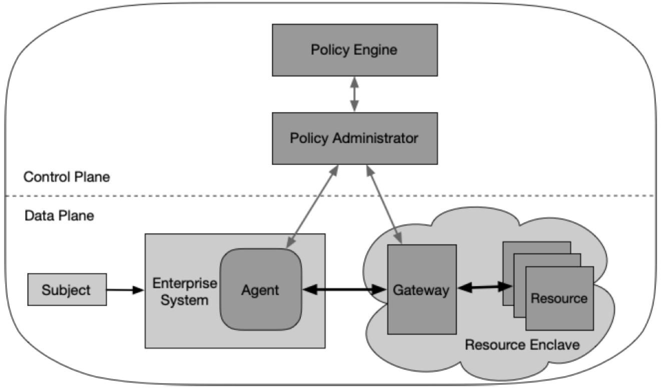
Core Zero Trust Logical Components

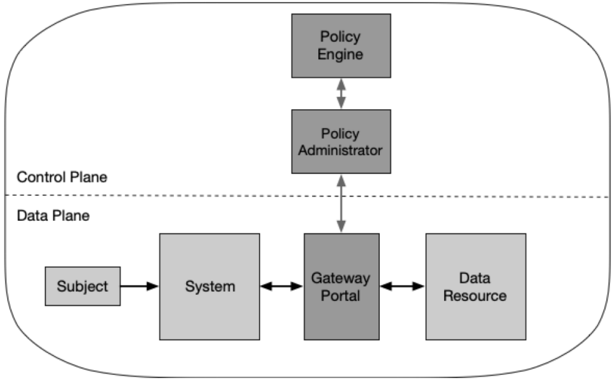


Policy Engine receives real-time input from external sources.

ZT Deployment Models







Implications and Challenges

Threat Landscape Impacts Storage

- Privacy regulations have redefined “data breaches” such that storage systems are affected
- Attacks (ransomware) are targeting enterprise IT for massive ransoms; storage is being caught up in the mess
- Deperimeterization of enterprise networks mean that all IT must participate in defense
- Eliminating data on storage media can be difficult, but necessary to encourage reuse of resources

Contemporary Storage Security

- Systems/network security (hardening)
- Securing storage management
- Securing data access
- Encryption and key management
- Media sanitization
- Leveraging security infrastructures/services (LDAP, syslog, etc.)

Advanced Storage Security

- Storage Link Encryption
- Secure autonomous data movement
- Secure Multi-tenancy
- Long-term Retention and Preservation
- Software defined ****
- Cloud Storage (hybrid)

Security capabilities for trustworthiness

- Ecosystem hardening
- Identity Access Management (IAM) / Federation
- Dynamic Access Control with Constraints
- Tamper-proof
- Isolation and sandboxing
- Realtime protection from malware
- Exploit protection
- Monitoring for regular operations
- Monitoring for forensic purposes

Final Thoughts

- Adversaries are changing their attacks at a rapid pace; defenders must be nimble
- Data is today’s currency, which places storage in the line of fire
- Emerging technologies (5G, IoT, AI, etc.) likely to impose new requirements and dependencies on storage

Thank You

Please take a moment to rate this session.

Your feedback matters to us.