DSci526:
Secure Systems Administration

Zero Trust
Case Studies

Prof. Clifford Neuman

Lecture 13
21 April 2021
Online

Announcement

- Today's Lecture April 21st Lecture
  - Wednesday 21 April
  - 10:30AM to 1:50PM
  - Same Zoom Link

Agenda

1030-1130 Zero Trust Computing
1130-1200 Case Studies
1200-1210 Break
1210-1330 Case Studies continued
1315-1330 General Discussion and Reports Group Projects
1330-1350 Breakout Groups

DSci526:
Secure Systems Administration

Zero Trust

Prof. Clifford Neuman

Lecture 13
21 April 2021
Online

Trust No-One

Zero-trust is not a specific technology, rather it is a justified application of paranoia, i.e that you cannot implicitly trust users, devices, or processes acting on behalf of users.

- You must reverify decisions on which access is based.
  - E.g. access to a network segment does not mean a device or packet is authorized, just because it made it past a firewall.
    - Authentication and access control to be applied on each access.
    - Plain-old network protection domains is not enough.
- Assume nothing

But in practice, we all trust something

Administering Zero Trust

- User Administration – Identity Management
  - Centralized administration – (trusted)
- Configuration Management
  - Devices
    - Assessing system health (you are trusting this)
    - Admission
    - Authentication / Attestation – (trust points)
  - Software – Trusted Computing – Attestation
- Network Administration
- SOC / SIEM
- Fine Grained Access Control
  - Least Privilege (least trust)

NIST 800-207

- A zero trust architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level. Many organizations already have elements of a ZTA in their enterprise infrastructure today. Organizations should seek to incrementally implement zero trust principles, process changes, and technology solutions that protect their data assets and business functions by use case.

NIST 800-207: Basics

- Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges (e.g., read, write, delete) needed to perform the mission.

NIST 800-207

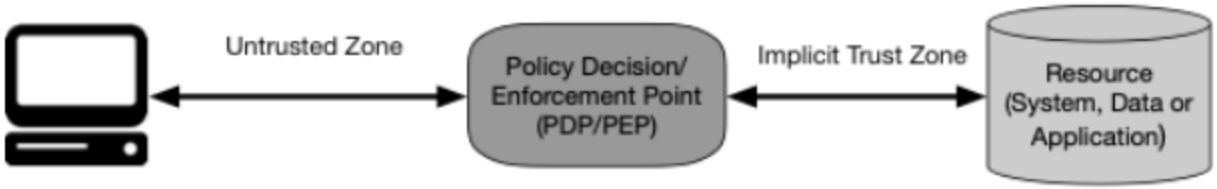

Figure 1: Zero Trust Access

NIST 800-207: Basics

- The definition focuses on the goal of preventing unauthorized access to data and services coupled with making the access control enforcement as granular as possible. That is, authorized and approved subjects (combination of user, application (or service), and device) can access the data to the exclusion of all other subjects (i.e., attackers).
- To lessen uncertainties, the focus is on authentication, authorization, and shrinking implicit trust zones while maintaining availability and minimizing temporal delays in authentication mechanisms. Access rules are made as granular as possible to enforce least privileges needed to perform the action in the request.
- The “implicit trust zone” represents an area where all the entities are trusted to at least the level of the last PDP/PEP gateway.The PDP/PEP applies a set of controls so that all traffic beyond the PEP has a common level of trust. The PDP/PEP cannot apply additional policies beyond its location in the flow of traffic. To allow the PDP/PEP to be as specific as possible, the implicit trust zone must be as small as possible.

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.
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.

NIST 800-207

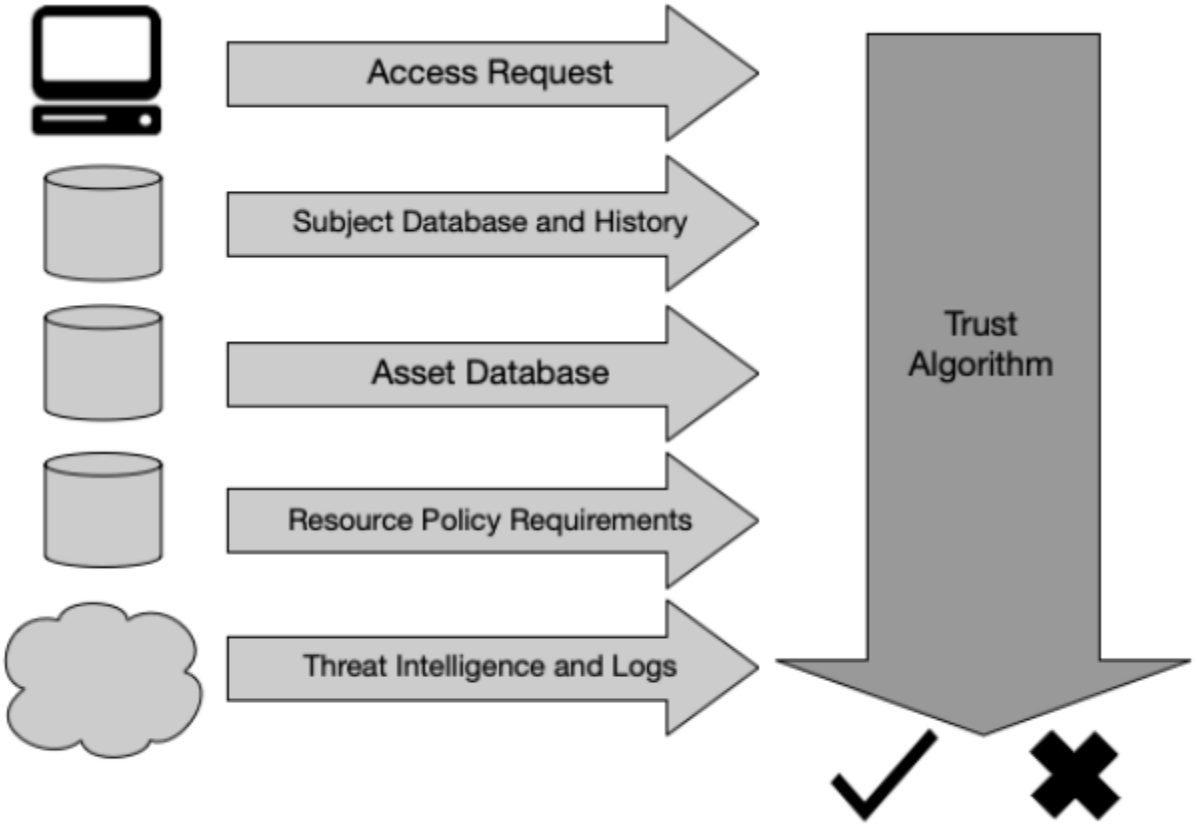

Figure 7: Trust Algorithm Input

NIST 800-207

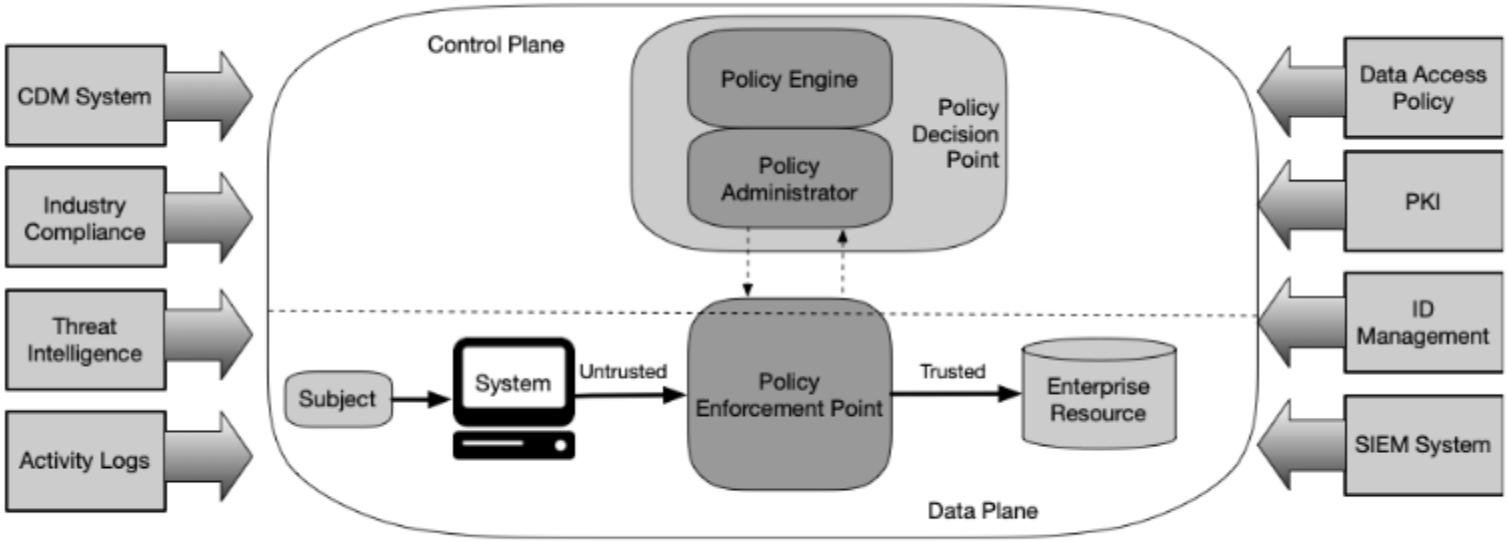

Figure 2: Core Zero Trust Logical Components

Network Non-Assumptions

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

Policy Engine Variations (NIST calls this Trust Algorithm)

- Criteria vs Scoring
  - Deterministic
  - Probabilistic
- Singular vs Contextual
  - Individual
  - Based on history and other state
    - "This also means that the PE must be informed of user behavior by the PA (and PEPs) "

Remaining Threats

- Subversion of ZTA Decision Process
- Denial-of-Service or Network Disruption
- Stolen Credentials/Insider Threat
- Visibility on the Network
- Storage of System and Network Information
- Use of Non-person Entities (NPE) in ZTA Administration

DSci526:
Secure Systems Administration

Case Studies in Administration

Prof. Clifford Neuman

Lecture 12
14 April 2021
Online

Assigned Reading For Today

- Please skim and read the introduction and relevant sections (the ones labeled FY 2018 Inspector General FISMA Report) from:
  - FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK STAFF REPORT PERMANENT SUBCOMMITTEE ON INVESTIGATIONS UNITED STATES SENATE
  - We will use this as the basis of discussion of case studies of unsecure system administration.
  - Please think about which aspects of secure system administration as covered in this class were not properly applied, and what should be done instead.

Summary of Report

Report shows failures at eight US agencies in following cyber-security protocols

- US Senate report finds appallingly bad cyber-security practices at eight US government agencies.
  - ZDNet – June 26 2019
  - Catalin Cimpanu for Zero Day

Highly Concerning Issues in IG report

- Agencies historically failed to comply with cybersecurity standards.
- Protection of PII.
- Comprehensive list of IT assets.
- Remediation of cyber vulnerabilities.
- Authority to operate.
  - The IGs identified multiple agencies that failed to ensure systems had valid authorities to operate. These included DHS, DOT, HUD, USDA, HHS, and Education.
- Overreliance on legacy systems.

Elements of Administration

- Risk Assessment – Security Requirements
- Containment Architecture
- Configuration Management
- Network Managements
- Pen-testing / Red-teaming
- SIEM
- Response Planning
- Accreditation and Acceptance Testing

Homeland Security

- Lack of Valid Authorities to Operate. This review revealed that 48 unclassified and 16 national security systems did not have valid authority to operate.211 These authorities are usually granted by DHS for a period of three years.212 For the systems lacking a valid authority, it means that an "official management decision given by a senior organizational official to authorize the operation of a system and explicitly accept the risk to organizational operations" was not granted.
- Use of Unsupported Systems. The IG found that DHS continued to use unsupported operating systems creating the possibility that "known or new vulnerabilities [could] be exploited on operating systems for which vendors no longer provide service patches or technical support."216 For example, the IG determined that several DHS components still used Windows Server 2003—for which Microsoft stopped providing updates in 2015.217 These components included DHS Headquarters, Coast Guard, and Secret Service.218
- Failure to Remediate Vulnerabilities. During its review, the IG determined that DHS "did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems."221

State Department

- Failure to Remediate Vulnerabilities. The Department does not currently have the ability to scan their networks to detect rouge devices.275
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Among the specific issues noted was the State Department's failure to maintain an accurate and complete IT systems inventory.277
- Failure to Provide for the Adequate Protection of PII. Although State is aware that its systems are the constant target of cyber adversaries, in September 2018 hostile actors "gained access to the Department's unclassified email system and exposed PII of Department employees."283

Department of Transportation

- Lack of Valid Authorities to Operate.
- Use of Unsupported Systems.
- Failure to Remediate Vulnerabilities.
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory.
- Failure to Provide for the Adequate Protection of PII.
  - From a network access standpoint, DOT also has yet to require the use of personal identity verification ("PIV") cards to login to all agency computers.352 PIV card use strengthens network access security by requiring "a computer system user to authenticate his or her identity by at least two unique factors."353
- The DOT IG's FY 2018 review also documented that the Department's Respond controls "are insufficient."357 In 2017, the IG found 10 unresolved security incidents "that were over 90 days old" five of which involved PII.358

Housing and Urban Development

- Lack of Valid Authorities to Operate.
- Use of Unsupported Systems.
- Failure to Remediate Vulnerabilities.
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory.
- Failure to Provide for the Adequate Protection of PII.
  - HUD currently lacks a defined "process to identify and inventory all of its PII and thus [cannot] review and remove unnecessary PII collections on a regular basis."416 As a result, the IG discovered that some records were retained in violation of National Archives and Records Administration requirements.417

Department of Agriculture

- Lack of Valid Authorities to Operate.
- Use of Unsupported Systems.
- Failure to Remediate Vulnerabilities.
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory.
- Failure to Provide for the Adequate Protection of PII.
  - RMA determined that USDA has yet to finalize a data protection and privacy policy to protect PII.480Without a final policy, the "decentralized governance of PII throughout the Department" will continue.481 This decentralization is problematic because of the PII maintained by the Department. The Department informed the Subcommittee that since RMA's audit, it has implemented Microsoft Data Loss Prevention technology that "notifies employees when they are sending PII outside of USDA."482

Health and Human Services inc

Centers for Medicare and Medicaid Services ("CMS") Marketplace Consumer Record ("MCR") system

- Lack of Valid Authorities to Operate.
- Use of Unsupported Systems.
  - HHS's Medicare Enrollment system is an example of a legacy system.543 In light of the antiquated nature of system, HHS now has a difficult time finding people who know how to work with this system.544
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory
  - Although HHS has instituted a process for compiling an IT asset inventory, the Department failed to ensure that some hardware assets "connected to the network are subject to the monitoring processes defined within the organization's information security continuous monitoring strategy."546
- Failure to Provide for the Adequate Protection of PII.
  - In October 2018, a breach of Healthcare.gov compromised the confidential records of roughly 75,000 consumers.549 The breach itself involved a system "used by agents and brokers as part of the insurance program," and exposed PII such as credit information.550

Department of Education

- Lack of Valid Authorities to Operate.
- Use of Unsupported Systems.
- Failure to Remediate Vulnerabilities.
  - The IG found that FSA "was not consistently applying software patches and security updates to its systems and information technology solutions."591 As part of this failure, FSA failed to apply critical patch and security updates.
- Failure to Provide for the Adequate Protection of PII.
  - This task is especially difficult at Education because departmental access to PII is highly decentralized.595 This decentralization is a result of the Department's reliance on contractors and college and university access to student financial aid information.596
- The IG determined that the Department failed to consistently ensure that agency websites were configured to use secure internet connections.603 Out of 60 systems identified by the IG, only a third were "configured to use a trusted internet connection or managed trusted internet protocol services" as required by DHS and OMB.604

Social Security Administration

- Use of Unsupported Systems.
- Moreover, the IG found that SSA consolidated all regional office DDS case processing systems into a single authority to operate, creating the risk that SSA "did not appropriately document system boundaries."654
- Failure to Remediate Vulnerabilities.
- Failure to Compile an Accurate and Comprehensive IT Asset Inventory.
  - SSA also failed to implement an "inventory of related hardware and software components at a level of granularity necessary for tracking and reporting to management."658 SSA's inventory did not include all of its information systems pursuant to NIST standards.659
- Failure to Provide for the Adequate Protection of PII.
  - Nation state cyber-attackers frequently target SSA because of the substantial quantities of PII it maintains.663 This fact further underscores the importance of SSA efforts to better protect sensitive information in its custody.664 The most troubling findings in the latest SSA FISMA audit were the weaknesses identified in identity and access management.

Other Major Breaches

- Equifax
- Capital One
- Solar Winds
- Microsoft Exchange Emails

DSci526:
Secure Systems Administration

Second Group Project
Third Week Discussion

Prof. Clifford Neuman

Lecture 12
14 April 2021
Online

Wrapping up Project Two

- It is time to wrap up exercise Two. By Monday 26 April - each group should prepare a report describing:
  - User documentation for their application (high level)
  - Their network and server architecture (what servers are on what VM's and how they are interconnected)
  - A risk assessment/vulnerability analysis enumerating the risks, explaining the mitigation of those risks, and listing those threats that are not defended against (i.e. where you accept the risks).
  - A description of the steps taken for pen testing of your system.
  - On Wednesday 28 April, your team will have 25 minutes to present this summary to the entire class (this time, no withholding of information from the other team)
  - This week and next, basic 5 minute presentation, and Break Out Groups.
- We will use time in the final lecture to demonstrate the operation of your systems.
  - Please prepare a list of tests (with appropriate scripts) that you believe should be run against your system, and the other team's system, and send me that list of tests by Monday 26 April.

Teams for Second Group Project

- Team One
  - Shagun Bhatia
  - Anthony Cassar
  - Sarahzin Chowdhury
  - Tejas Kumar Pandey
  - Pratyush Prakhar
  - Christopher Samayoa
  - Louis Uuh
  - Ayush Ambastha
  - Jason Ghetian
  - Abhishek Tatti
  - MaryLiza Walker
  - Hanzhou Zhang
- Team Two
  - Azzam Alsaeed
  - Marco Gomez
  - Alejandro Najera
  - Doug Platt
  - Carol Varkey
  - Yang Xue
  - Aditya Goindi
  - Malavika Prabhakar
  - Dwayne Robinson
  - Amarbir Singh
  - Shanice Williams

Second Exercise - Criminal Enterprises

- Chosen because of differences in the high-level principles.
  - Not because I expect you to implement these kinds of systems in your future endeavors.
  - But you may be called upon to break some of these systems if later employed by government organizations.
- Your organization must:
  - Accept Bitcoin as payment (not really, but it must accept something that stands in for bitcoin)
  - Manage an inventory of stolen account identifiers with passwords
    - Enable the sale of collection of such information in exchange for your stand-in for bitcoin
    - Control access to such information
  - Prevent collection of evidence or intelligence by third parties.
  - Note, do not deal in any illegal goods, but use dummy information to stand in for such goods. Also, do not use terms associated with such illegal goods or information in communications, make up new names for this dummy information.