/*---------perfect is the enemy of good enough-------------*/

(or, Zero Trust Networks)

/*---------first things first------------*/

Problem

Solution

/*---------dramatic opener------------*/

"The millions of dollars that people are spending, all the hype and the sexy marketing and the AI and the anomaly-behavioral… whatever buzzword you want to use, it's a bunch of smoke and mirrors, and I won't call it useless, but it's on the periphery of the issue when people still aren't

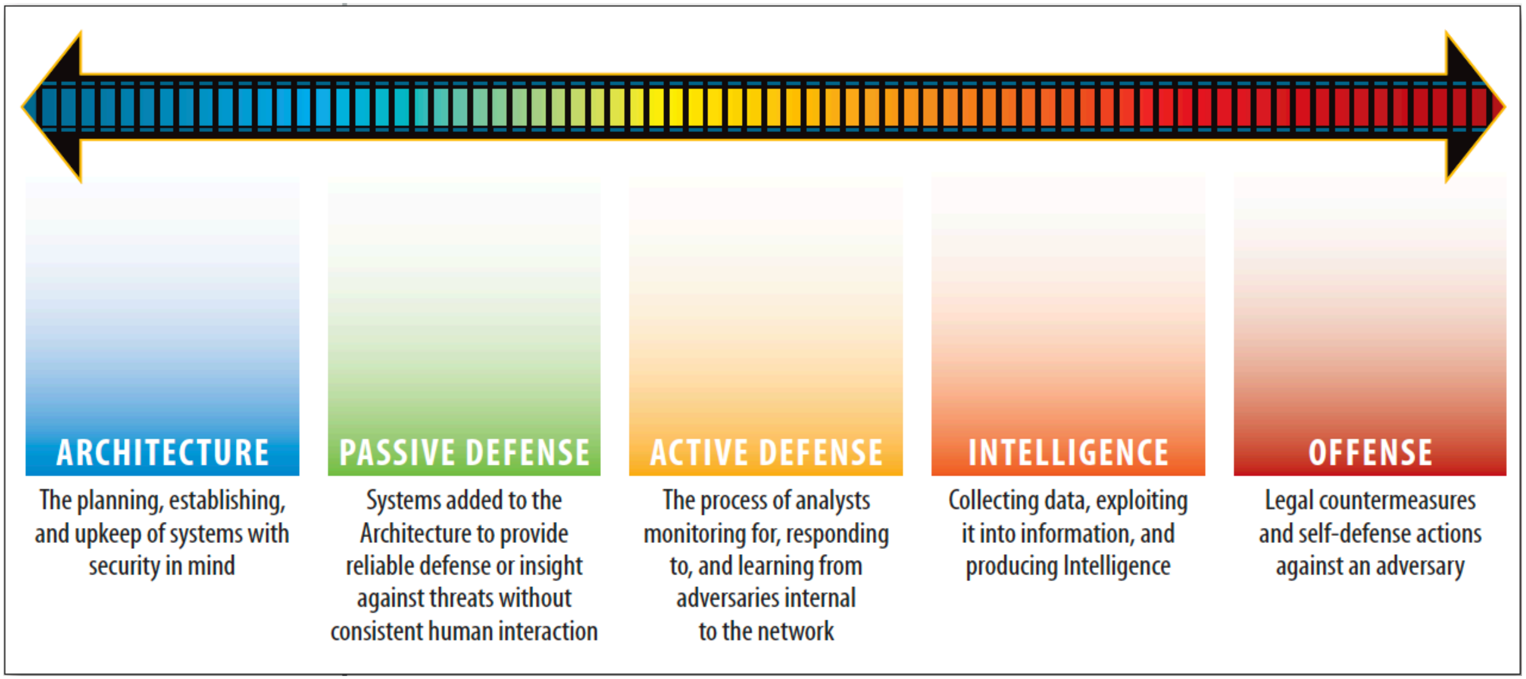
doing the basics."

Tenable CEO Amit Yoran
RSA 2019

/*---------traditional networking-----------*/

- It’s not always who you think
- Facilitates the Insider Threat
- Multiple entry points. (Cloud?)
- Security is allow all, or deny all

/*---------the sliding scale of cybersecurity-----------*/



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

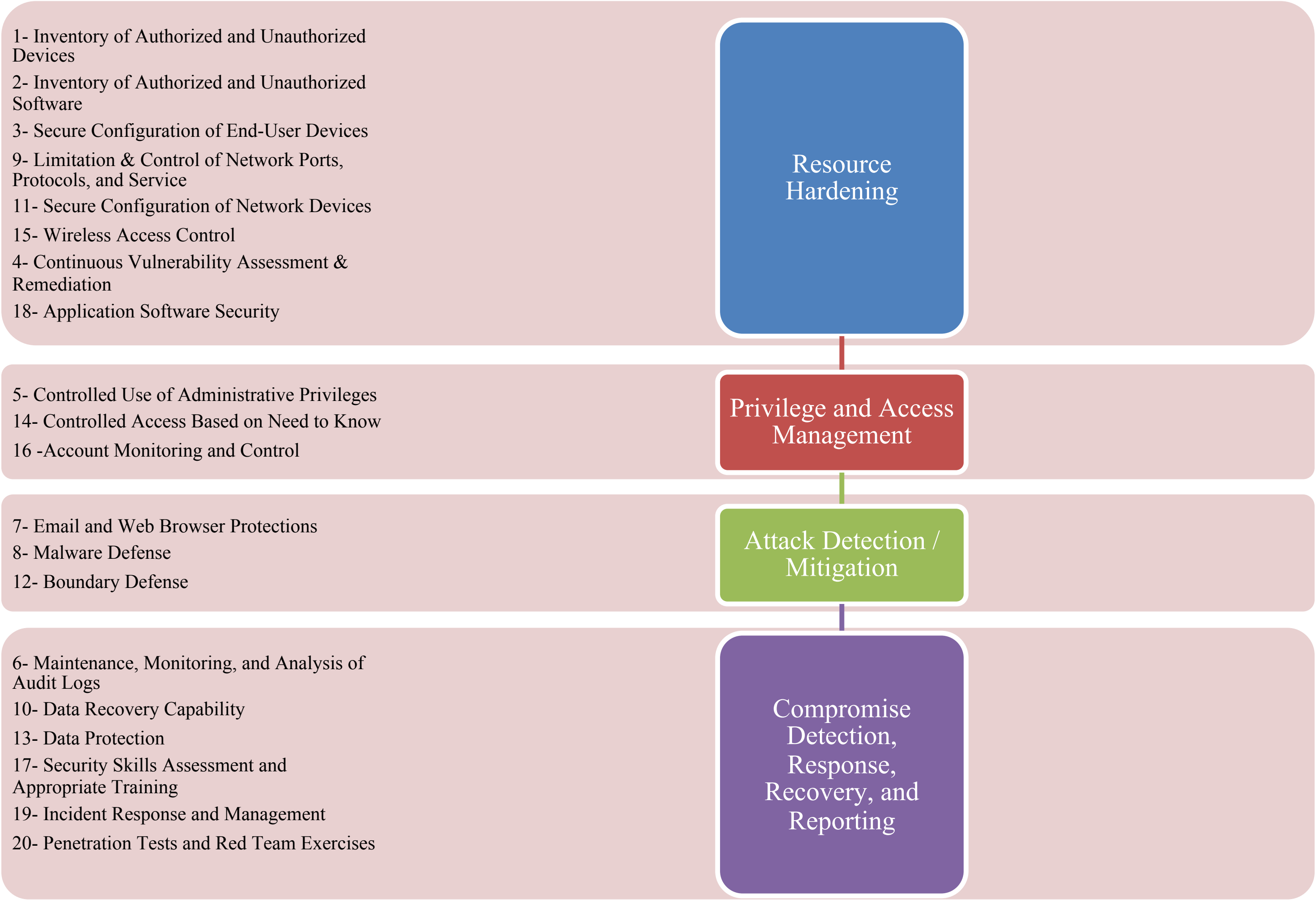
Legal countermeasures and self-defense actions against an adversary

/*--------the solution-----------*/

Do the basics

- Flat Networks fail catastrophically
  - (Eric Conrad SANS)
- Reconfigure what you already have
- No need to buy shiny new tools (usually)
- Define system group
  - Servers
  - Normal clients
  - IT clients
- Block the following apps in normal clients using Windows firewalls
  - e.g. psexec, Powershell, WMIC, etc.
- Configure logging (sysmon)
- Restrict workstation to workstation communications (VLAN)

/*--------begin with the fundamentals-----------*/



1- Inventory of Authorized and Unauthorized Devices

2- Inventory of Authorized and Unauthorized Software

3- Secure Configuration of End-User Devices

9- Limitation & Control of Network Ports, Protocols, and Service

11- Secure Configuration of Network Devices

15- Wireless Access Control

4- Continuous Vulnerability Assessment & Remediation

18- Application Software Security

Resource Hardening

5- Controlled Use of Administrative Privileges

14- Controlled Access Based on Need to Know

16 -Account Monitoring and Control

Privilege and Access Management

7- Email and Web Browser Protections

8- Malware Defense

12- Boundary Defense

Attack Detection / Mitigation

6- Maintenance, Monitoring, and Analysis of Audit Logs

10- Data Recovery Capability

13- Data Protection

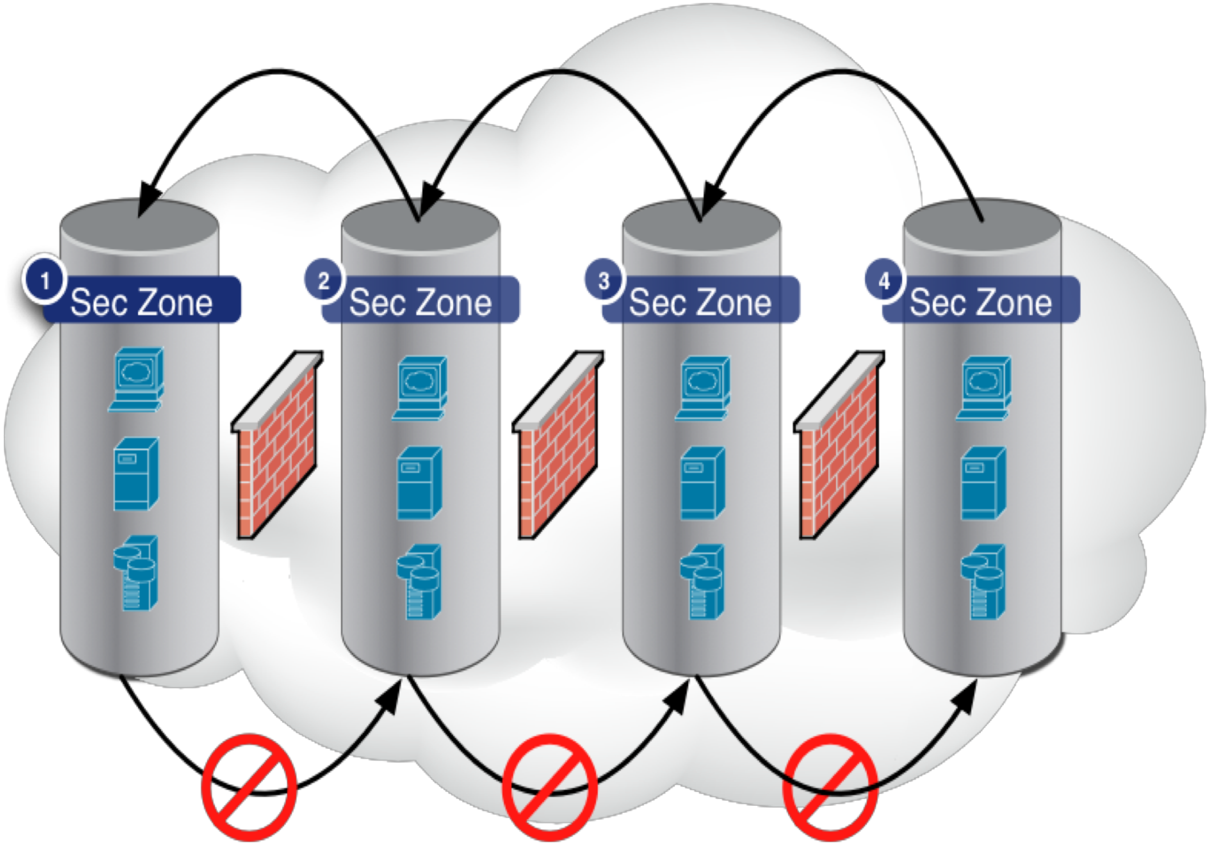
17- Security Skills Assessment and Appropriate Training

19- Incident Response and Management

20- Penetration Tests and Red Team Exercises

Compromise Detection, Response, Recovery, and Reporting

/*---------network segmentation (vlan)------------*/



/*---------zero trust (one size does not fit all)------------*/

- User Access (username/password)
- Machine Access (IP Address)

Does not guarantee access to asset

- Access is based on identity (Network Agent)

- Encrypted and digitally signed communications

(Mutual TLS) Like the Internet

/*--

The goal ***ISN’T: Defend against ALL threats***

The goal ***IS: Defend against most common internal threats***

--*/

- Given enough time and resources, any attack will be successful
- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.
- Automation is critical
- Leverage Existing Technology

/*---------managing trust ------------*/

- RFC 3552 the Internet Threat Model
- The Internet environment has a fairly well understood threat model
- Assume that the attacker has nearly complete control of the communications channel over which the end-systems communicate
- This means that the attacker can read any PDU (Protocol Data Unit) on the network and undetectably remove, change, or inject forged packets onto the wire
- This includes being able to generate packets that appear to be from a trusted machine
- The Internet provides no assurance that packets which claim to be from that system in fact are

/*---------some best practices-----------*/

- 1st - Harden systems proactively against compromised peers
- 2nd - Facilitate detection of those compromises
- 3rd - Detection is aided by scanning devices and behavioral analysis of the activity from each device
- 4th - Mitigation of endpoint compromise is achieved by:
  - Frequent ***upgrades*** to software on devices
  - Frequent and automated ***credential rotation***
  - Frequent ***device rotation***

/*---------all zero trust networks rely on pki-----------*/

- Strong Authentication
- Mutual TLS (X.509 bi-directional)
- Certificate Rotation
- Certificate Revocation

Hashicorp Consul
Client pushes Certificate Signing Request (CSR)
Generates Key Pair
Can act as CA
Push Short TTL certs (<72 hours

- Devices
- Users
- Applications

Trust variance and invalidation - CRITICAL

/*---------private vs public pki-----------*/

Private PKI is preferred in a ZT implementation

- Private is cheaper
- Hard to FULLY trust third party CAs
- The Public CA might not have an API - hard to automate
- Key management is . . . Well, key!

The importance of Secrets management cannot be over stated

/*---------about trust------------*/

- Least privilege
  - Elevate late
  - Drop early
- Variable (not binary) Trust (compute a trust score)
- Prompt for password, second factor auth, or out of band confirmation
- Privilege is dynamic – few static policies
- No privilege creep
- Temporal
- Geographical
- Behavioral
- Control/Data Plane (CP/DP)

/*---------a network agent is:------------*/

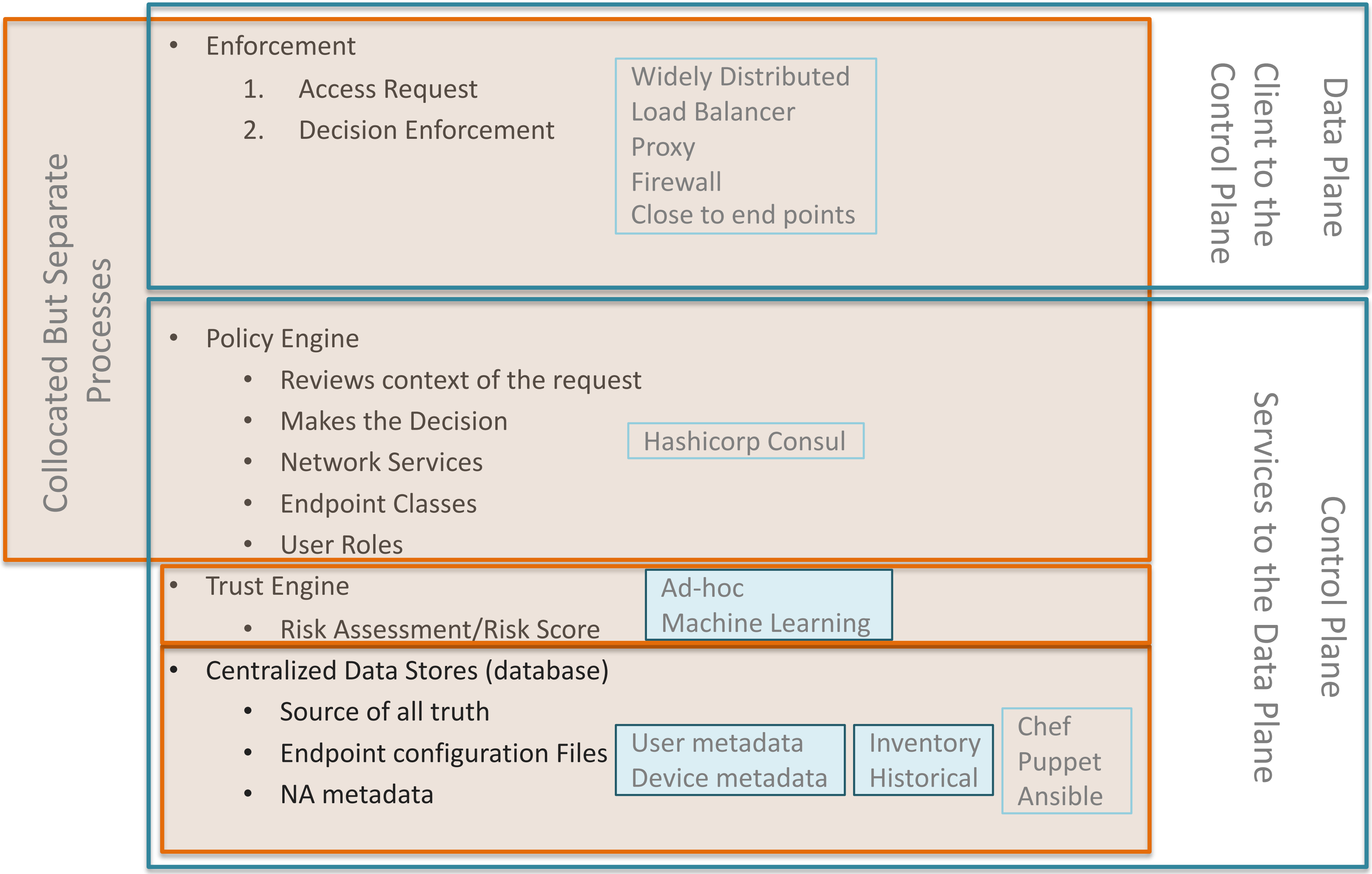
  - Critical to ZT realization
  - Ephemeral
  - User
  - Application (services)
  - Device/Location

What about SSO?

- Volatility
- Network Agent (NA) purpose
  - AuthZ NOT AuthN
  - Revoke AuthZ first then revoke creds
- NA details reside in CP
  - CP enforces AuthZ based on NA
- No NA standards yet
- NA used for AuthZ decisions

/*-------the architecture components that ensure authz--------*/

Ensure AuthZ



Collocated But Separate Processes

- Enforcement
  1. Access Request
  2. Decision Enforcement

Widely Distributed
Load Balancer
Proxy
Firewall
Close to end points

Data Plane

Client to the Control Plane

- Policy Engine
  - Reviews context of the request
  - Makes the Decision
  - Network Services
  - Endpoint Classes
  - User Roles

Hashicorp Consul

- Trust Engine
  - Risk Assessment/Risk Score

Ad-hoc
Machine Learning

- Centralized Data Stores (database)
  - Source of all truth
  - Endpoint configuration Files
  - NA metadata

User metadata
Device metadata

Inventory
Historical

Chef
Puppet
Ansible

Control Plane

Services to the Data Plane

/*---------trusted device inventory database-----------*/

- Configuration Management Database (CMDB) (e.g. Puppet, Chef)
- Hashicorp Consul (dynamic state and service discovery tool)

- Metadata
  - Device Type
  - Role
    - Client workstation
    - Webserver
    - FTP server
  - IP address
- Authentication

Restrict Write Access
For metadata in
CMDB

Least Privilege

/*---------user identity ≠ device identity-----------*/

- User Identity
  - Informal – Weak When risk is low Online Persona
  - Authoritative - Stronger When risk is high Passport or DL

- Credentials
  - Can be lost or stolen Need a mechanism to recover

  - Bootstrapping User registration/creation in-person
  - Updating

- Identity storage (target for attack) Segment over several distributed DBs Exposed via API

  - LDAP (Active Directory)
  - Organizational Employee system

Integrated/Automated

Which one is the authoritative source?

User experience is critical to ZT acceptance

/*---------user identity ≠ device identity-----------*/

User AuthN

- Validating identity
- Annoying for users
- Too many AuthN requests breeds discontent
    - (increases the likelihood of insider threat)
- Find a balance

More sensitive resource

Stronger AuthN method

What you know
What you have
What you are
Where you are
How you behave

Passwords
One-time codes
Push notifications (NOT SMS)
Tokens (Most secure)

Hashicorp Vault
For secrets mgt

Group AuthN

- Multi-person rules for highly sensitive data

Cloudflare Red October

- Train users to report suspicious activity

See Something
Say Something

Over reporting is good
No shame for lost devices
Give thanks for false alarms

- Leverage user access and application use logs

Baseline of user behavior

Better trust scores

Revoke tokens when trust levels erode or fluctuate

/*---------trusting the code-----------*/

- Trusted Application Pipeline

  Similar to Supply chain security

  Trusted people
  Trusted app
  Trusted infrastructure
  App is monitored for trusted behavior

  - Securely code

    Review the code
    Hash the code
    Sign the code
    Secure the repo

    Version Control

  - Securely build

    Does what it should do
    Does not do what it shouldn’t

    Trusted Input
    Trusted output
    All the right processes

  - Securely distribute

    Integrity
    Authenticity

    Hash
    Sign

  - Securely execute

    Inventory software

    Hashicorp Consul

- Human attention – scarce but critical resource
  - Where to put the human in the loop

    Limit human involvement for security

/*---------trusting the code-----------*/

- Monitor running instances

- Trust degrades when vulnerabilities are discovered

Netsh (windows Firewall)

Application security hygiene

- Secure coding practices

Saltzer and Schroeder 1975

- Deploy apps in isolation

Limit access to resources

SELinux
AppArmor
BSD jail
Virtualize
Containerize
Apple App sandbox
Windows Isolated Applications

- Monitor aggressively

Fuzzing
SQL scanning
Network port scan
Vulnerability scanning

Afl-fuzz
Sqlmap
Nmap
Nessus

- Secrets management enables frequent rotation of creds

The importance of Secrets management cannot be over stated

/*---------trusting the traffic----------*/

- Zero trust networks require
  - Encryption
  - Authentication

- First packet problem – servers

First packet unauthenticated

Pre-authentication
A UDP packet (no responses)
with signed data.

Single Packet Authorization (SPA)

Only for solving the first-packet problem

Attackers won't get a response

Firewall Knock Operator (fwknop)

GnuPG

AES

- Encrypt all traffic

- Modern authentication systems large surface area for attacks

Hide services behind SPA

/*---------encrypting the traffic-----------*/

- TLS
  Resides around OSI Layer 5 and 6 and is most common
- IKE and IPsec
  Resides around OSI Layer 3 and 4

Server to server
Legacy software benefits

No IPsec on AWS
Few public hotspots

IPsec inside the datacenter where Network Address Translation is absent

- Mutually authenticated TLS (turnkey solution these days)
  - Client/server interactions
  - Heterogeneous environments

- Packet filtering capabilities deployed throughout the network
  - Host-based
    Iptables
    Windows Firewall service
  - Bookended
    Apply policy at TX and RX of packet
    Programmatic implementation
  - Intermediary
    The network fabric applies firewall rules
    Dynamically program the network.
    Results in software defined network

/*--------putting it together----------*/

- ZT is an architectural ideal
- Transition over time
- Decentralized Access control

Chef or LDAP

- Authentication Proxies to cover incompatible systems
- Begin with server<->server comms
- Define network policy
- Deploy in test network first
- Collect logs/metrics for inspection
- Ensure desired behavior
- Slowly roll out the policy in production

/*---------attacking it----------*/

- Architecture mitigates some attacks
  - Identity theft
  - DDoS
  - Endpoint enumeration
  - ZT guarantees confidentiality not privacy. Packet payloads are encrypted.
  - Untrusted computing platform
  - Social engineering
  - Physical coercion
  - Invalidating actions once trusted
- Others can only be detected
- Reality – Every system can be compromised
- Advanced threats – efficient and accurate detection
- Zero-trust model needs to replace the perimeter model

Conclusion