Creating Infinite Possibilities.

SCTE
a subsidiary of CableLabs

Zero Trust Security Architecture For The Enterprise

Christopher Zarcone

Distinguished Engineer
Comcast
(856) 638-4116 – Christopher_Zarcone@cable.comcast.com

SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

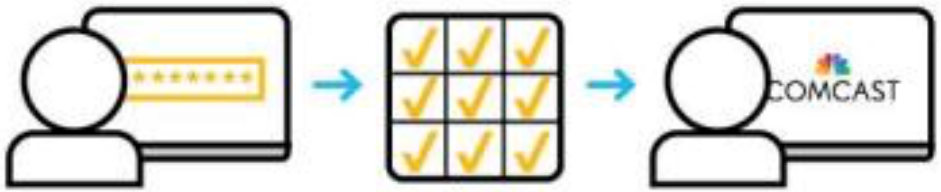
2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

Agenda

- Introduction
- Background on Zero Trust Architecture
- History of Zero Trust at Comcast
- Guiding Principles
- Security Domains
- Program Governance
- Lessons Learned
- Future Work
- Service Provider Considerations
- Conclusions

Background on Zero Trust Architecture

- Zero Trust Architecture (ZTA) is an information security model based on the principle of **Never Trust, Always Verify**
- Concept has existed for decades; popularized in 2010 by Forrester Research
- ZTA argues that:
  - All computer networks are untrusted by default. Therefore:
  - All **Users** and **Devices** on computer networks are untrusted by default
  - Users/Devices must establish trust before access to **Resources** is granted
- Users and Devices establish trust through:
  - Strong authentication (MFA, cryptography)
  - Compliance
  - Context (Continuous Risk Assessment)



- Do NOT use networks as trust factors for Users and Devices!

ZTA Frameworks & Approaches

- Adopting ZTA can require considerable effort and attention to detail:
  - ZTA cuts across many different policy and technology domains
  - For most organizations, ZTA is a multi-year journey
- Several notable ZTA frameworks have been published to assist. Examples:
  - **BeyondCorp** – Series of six influential whitepapers published by Google
    - Defines five overarching design objectives
  - **NIST** – Special Publication 800-207
    - Outlines seven core “tenets”
- Two practical approaches:
  - Adopt a ZTA framework completely
  - Borrow elements of various ZTA frameworks that make sense for your organization

History of ZTA at Comcast

- Started our Journey in 2019
  - Developed the business case for ZTA
    - Response to increasing number of industry breaches, zero-day incidents, ransomware, etc.
    - Identified as best alternative to the ”Castle and Moat” perimeter architecture
  - Developed overall structure of the program, guiding principles, governance
- 2020 and COVID-19
  - Shifted some employees to remote work, further diminishing the perimeter model
  - Emphasized the relevance of ZTA
- 2021 to Present
  - Accelerated our program – we’re making good progress!

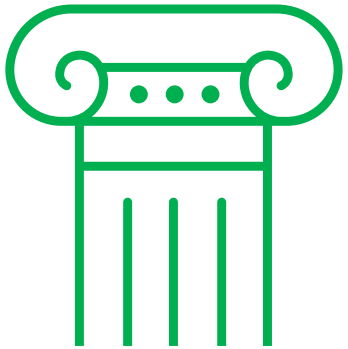
Guiding Principles

- ZTA assumes that every security principal (User, Device) is a threat until verified:
  - Regardless of network location (internal and external)
- Also assume that incidents can and will occur:
  - Despite our best efforts and sound information security practices
  - Mainly due to Zero-Day exploits (remember Log4j?) and other unforeseen factors
- These assumptions give rise to two guiding principles of our ZTA:

1. **Never Trust, Always Verify.** Users and Devices must establish trust before obtaining access to Resources.
2. **Prepare To Be Breached.** Our networks, systems, and applications must be designed to limit the impact of incidents.

Security Domains (Part I)

- We applied the guiding principles across three broad security domains:
  - **Security Hygiene**
  - **Network Microsegmentation**
  - **Application Access**
- **Security Hygiene** concerns the security posture of our main ZTA principals (Users, Devices, and Resources)
- We defined five focus areas, or **Pillars**:
  - User Identity & Access Management
  - Resource Identity & Access Management
  - Asset Ownership
  - Device Identity & Management
  - Visibility & Hardening

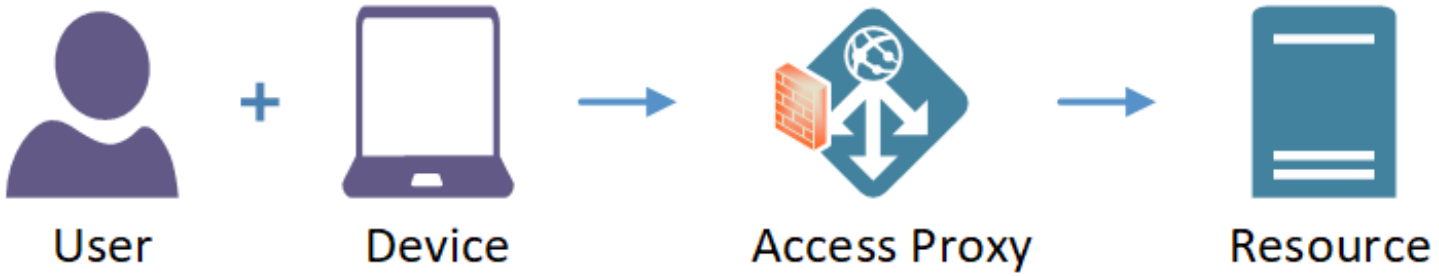


Security Domains (Part II)

- **Microsegmentation** focuses on partitioning the network environment into smaller, workload-specific enclaves.
  - Good analogy comes from the shipbuilding industry: compartmentalization
  - Compartments limit damage to a subsection of the ship, instead of the whole ship
  - Apply the same philosophy to network architecture – segment (compartment) the network down to individual workloads, applications, etc.
  - (Relatively) easy to do in virtualized environments

Security Domains (Part III)

- **Application Access** governs how Resources are exposed to Users and Devices, regardless of their physical or logical network locations.
  - Many ZTAs suggest the use of **Identity-Aware Proxies**, or **Access Proxies**, to mediate access between Users/Devices and Resources
  - Web-based alternatives to VPN, NAC and other edge controls
  - Enforces the security requirements of VPN, NAC, etc. without protocol overhead, tunnelling, etc. and makes for a simple, all-browser-based user experience



Governance

- Any effort as large as ZTA requires significant governance and project management
  - Our ZTA was championed by our EVP & Chief Information Security Officer
  - A dedicated project management office, staffed with full-time project management, was assigned to support the overall ZTA program
  - Product, Program & Architecture leaders were nominated to guide the effort
  - Executive, Product and Program leaders were assigned to the Hygiene Pillars
  - An executive leadership committee was established to provide guidance on a quarterly basis
  - A steering committee was established to provide stakeholder direction between the organizations contributing DevOps resources to the program
- Also requires significant engagement and outreach with stakeholders
  - BISOs & our Business Units, Portfolio & Cybersecurity Leads across the company, our Cybersecurity Guild, Employee Resource Groups, etc.

Lessons Learned

- Engagement – Important to get key stakeholders involved early:
  - Office of the CIO, Workforce IT, Network Engineering, Procurement, Finance, Human Resources, Corporate Communications
- Cloud First – Initiated our ZTA journey with a priority on new cloud deployments
  - Flexibility, agility, ease of implementing some controls (like microsegmentation)
- Buy vs. Build – There are (an emerging number) of commercial products and services in the ZTA space. It is also possible to build your own tools and/or leverage open source
  - We ultimately pursued a combination of both
- Business Partner Collaboration – Understanding the needs of our internal customers
  - Different business units, different geographic divisions, etc.
- Application Owner Collaboration – Applications are not uniform widgets
  - Can require varying degrees of assistance onboarding applications to ZTA

Future Work

- Continue on our multi-year journey
  - We're making good progress!
- Refine our real-time risk assessment of Users and Devices (context)
  - More telemetry from more sources of truth (MDM, EDR, SIEM, etc.)
  - Include Resource-level risk assessment where possible
- Extend our Microsegmentation strategy
  - Especially across non-cloud environments
- Extend our Access Proxy footprint
  - Both on-premises networks as well as off-premise

Service Provider Considerations

- In many ways, ZTA for Multi-System Operators and Internet Service Providers is not fundamentally different than other organizations
- Arguably, the cable industry has been practicing ZTA on access networks for years
- Consider DOCSIS 3.0 Security Specification, which dates to 2006. Its stated goals:
    1. To provide cable modem (CM) users with data privacy across the cable network;
    2. To prevent unauthorized users from gaining access to the network's services
- That's ZTA!
- Providers have also long applied significant security controls to protect infrastructure:
    - Centralized AAA, administrative MFA, RBAC, ACLs, etc.
- Providers should treat their enterprise networks as akin to their access networks:
    - Strongly authenticate all devices on enterprise networks
    - Harden enterprise network infrastructure with access network-level controls

Conclusions

- ZTA represents a fundamental shift away from traditional approaches to information and network security
  - Before, ”internal” networks were safe places, walled off from external threats by ”the firewall”
  - Now, we are in a state of constant vigilance, where networks do not provide the assurance they once did
- ZTA recognizes this reality and proposes an alternative approach where Users and Devices must establish trust before gaining access to resources
  - Trust must be established with confidence (e.g. strong authentication)
  - Network location is not to be used as an authenticator or trust factor
- ZTA is a practical, pragmatic approach that can be realized with current technologies
- Start your ZTA journey today!

Creating Infinite Possibilities.

Thank You!

Christopher Zarcone

Distinguished Engineer
Comcast
(856) 638-4116 – Christopher_Zarcone@cable.comcast.com