BS Network Operations & Security
Western Governors University
Graduation Date: 12/20/2019

Zero Trust Network Security

Lawrence Coulter Mentor: Bryan Boatright, IT-B

"Are you on the list?"

IT & Communications Services
IT Security (IT-B)
Network Security Perimeter

What?

More traditional approaches tended to automatically trust connections that come from inside the network perimeter. Under traditional approaches, if the device is connected to the center's network, it has access to the everything on the network.

The **Zero Trust** approach to network security involves not automatically trusting **anything**. The device has to be **whitelisted** to gain access to the network.

NASA is ultimately taking this to the application (software) level, meaning a device that wants to use licensed software needs to be explicitly authorized to do so. This could save the agency millions in fines and avoids the introduction of malicious software.

Why?

The number of ways a user could inflict damage to the *confidentiality*, *integrity*, and/or *availability* of the network is almost innumerable once they have a foot in the door. They could use that basic level of access to:

- Transmit sensitive data outside the secure perimeter
- Download malware (intentionally or inadvertently)
- Gain access to restricted files through privilege escalation and steal, modify, or delete them.

Under a **Zero Trust** approach a device has to have been approved before gaining any kind of access to the network. If the device has been approved but engages in foul play anyway, it is much easier to track down the offending device and remediate that situation.

When?

NAC (Network Access Control) Portion:

4th Quarter, FY 2019	Authentication credentials assigned to devices
4th Quarter, FY 2019	New NASA Visitor Network Is Turned Up.
4th Quarter, FY 2019	NAC Enforcement Activities Begin In Earnest.
3rd Quarter, FY 2020	NASA Target For NAC Enforcement Completion.

Future iterations should bring the Agency closer to a true **Zero Trust** model.

Analogies:

Traditional Network Connection: A public building – once you're inside you can go pretty much anywhere.
Network Connection w/ Password: All you have to do to enter the speakeasy is know the right password to give to the doorman and then you can go anywhere.
Network Access Control: A royal wedding – if you're not on the guest list, you aren't getting in and if you're press you're limited to a certain area.
Zero Trust: A sensitive research facility – even if your badge gets you in the building, it won't let you in every room.

Network Access Control (NAC):

This is the initial stage on the long road to a **zero trust** environment. Regardless of how a user accesses the network, the architecture will check if the device is allowed on the network at all, and if so, which portion of the network may be accessed. If NAC would give you access to a room, Zero Trust restricts your access to the drawer and cabinets in the room, and watch you while you're accessing them.

In this way, different devices are placed in the appropriate environments and limited in what they can access. For example, devices that belong to visitors, the personal devices of NASA employees and contractors, and untrusted devices can be connected directly to the Internet and be kept far away from NASA's internal network.

Previous Experience:

Service Desk (Tech Support) -> Overnight Service Provisioner and "First Responder"
Socket Telecom – Regional ISP, Telephone, and IPTV provider
Desktop Support Technician -> Network/VOIP Lead
Sinclair Research – Preclinical Research Facility (AALAC, GLP, SEND, FDA)

Current Tasks:

- Configuring equipment in the IT Security lab to enable testing of IPv6 security solutions in advance of wider deployment.
- Establishing secure configurations on IT Security lab equipment.
- Explored government compliant options for sanitizing systems prior to being excessed.
- Securely excessing surplus HDDs.