SEGMENTATION IS NOT ENOUGH

GETTING IOT OFF THE ISLAND OF ZERO TRUST

ABSTRACT

Network segmentation has been a common recommendation in the security community for years. Done correctly, it can minimize the attacker's ability to move laterally throughout a network, to inflict more damage on a system, or to consume network resources in an availability attack. In practice, however enterprises rarely take the step of fully segmenting their networks in accordance with organizational policies and, if they do take this step, they don't monitor the segments for policy violations.

The zero-trust security model is designed to take the segmentation model a step beyond, forcing authentication and authorization between devices, users, networks and applications from end to end. The rapid adoption of IoT not only exacerbates the need to monitor the network segments, but also the need to have a broader context of the whole system in order to make zero trust models applicable for secure IoT adoption.

MAIN TAKEAWAY

This talk describes the failings of the zero trust model when considering the pace of IoT adoption and identifies how understanding the IoT *system context* can improve the efficacy of zero-trust architecture implementations.

QUICK REFRESHER: MANAGING RISK

In general, there are a few ways to manage risk: it can be ignored, deferred, transferred, mitigated or fully assumed. In many situations, the most advantageous approach to managing risk is to defer it or transfer it and the least preferable approach is to assume it outright. In all cases, the risk must be identified and quantified in order to assume as little risk as possible to gain the biggest benefit.

The modern enterprise network should be architected with the same considerations for risk. It must be flexible, resilient, and responsive like a living, breathing thing. Retaining these qualities, while still minimizing risk makes the zero-trust model especially compelling.

WHAT IS ZERO TRUST?

A 'Zero Trust' network architectures take the approach that nothing on the network—not the users, not the devices, not the applications--should be trusted until they can be authenticated and authorized. Sometimes this authorization is temporal, such as what one would find with the use of a one-time password or guest access for a one time visitor. Effective implementation of zero trust requires development and implementation of trust zones on the network; articulation of rules for each trust zone; assignment of roles and permissions to devices, users and applications; the ability to identify violations to the trust model and; the ability to automatically enforce the "rules" if any of those entities violates the trust model. Essentially, zero-trust is meant to ensure that these entities have the just the right amount of access they need to perform the functions they need to perform when they need to perform them. No

additional access or permission is granted beyond this.

The term 'zero-trust' is relatively new, however the practice of deferring the risk from these entities is relatively old hat. In practice, this would look a lot like network segmentation through VLANs, but with additional controls placed around what users, devices and applications are allowed to be on those specific VLANs and when.

ADVANTAGES

When implemented fully, a zero-trust architecture aims to tackle confidentiality, integrity and availability challenges at every level in the stack:

- Zero-trust makes lateral movement through a network extremely difficult because the attacker would have to exploit the right user with the right device with the appropriate level of network access to move into more privileged trust zones.
- Since a key paradigm of zero-trust also assumes confidential communications *between* devices and applications, eavesdropping and man-in-the-middle attacks become much more difficult to execute.
- Denial of Service attacks become much less effective since zero-trust severely limits access to other trust zones.

DISADVANTAGES

"Zero trust" is a model and, as such, is subject to the limitations of the real world:

- Zero trust assumes that the organization has done the pre-work to develop a true threat model for their enterprise. Without having a clear understanding of what is at stake everything ends up with the same trust level: critical.
- Most organizations don't know what they have or who is supposed to have access to it. In 2017 Pwnie Express conducted a survey of 868 IT Security professionals as part of their annual Internet of Evil Things Report. 66 percent of respondents stated that they did not know how many connected devices were coming into their organizations. Zero trust doesn't work if you don't know what you have (or what you're supposed to have)
- Can be complicated and time consuming to fully implement throughout an enterprise. For large (greater than 1,000 employees) organizations, the challenge is to gain buy-in from potentially dozens of business units; for small organizations, the challenge is to carve out the time necessary to build and implement the solution while managing other projects and responsibilities. The result is a half-baked implementation, riddled with exceptions to policy.

THE RISE OF THE MACHINES

By 2020 there will be 20 billion connected devices in the world. Nearly one-quarter of them will be deployed in businesses, as integral parts of critical systems intended to optimize operations, increase profits, and provide competitive differentiation. In 2016 alone, 52 percent of global enterprises had or were planning to utilize Internet of Things (IoT) solutions to move their business forward.

Simply having more devices aren't a problem. The issue is that these devices enter the enterprise riddled with vulnerabilities which, if exploited can have

direct impact on the integrity of critical systems.

In preparing for the onslaught of these devices, CISOs, administrators, architects and engineers have relied on security approaches which are designed to minimize the impact of exploitation by keeping IoT devices segmented off in network purgatory, where they remain, untouched and unmonitored while they act as beachheads for malware and botnets. In keeping these devices in perpetual quarantine they, and the overarching systems they are part of, unreliable and unstable.

CHALLENGES TO ZERO TRUST FROM IOT

The pace of IoT adoption in the enterprise makes effective implementation of zero-trust architectures especially challenging for the following reasons:

- Scale: the sheer number of connected things means that developing trust zones by device becomes a tedious, manual exercise
- Diversity: unlike commodity hardware like laptops and desktops, IoT systems are often made up of general purpose hardware (e.g. a Raspberry Pi) running specialized software. The common network scanner will only see the Raspberry Pi without the context of the device's *intent*
- Upgrades and maintenance may require breaking the trust
- Can't just add agents or look at traffic to identify when something's wrong—maybe it's supposed to be doing that
- Older, previously isolated networks and systems are being retro-fitted to interconnect with other business systems to promote efficiencies in productivity and revenue. These older systems tend to be extremely sensitive and latency intolerant, such that any kind of intrusive security scans, agents or certificate requirements could render the system inoperable.

THE IMPORTANCE OF SYSTEM CONTEXT FOR ZERO TRUST

The reason why IoT is so promising is because it can provide insights, efficiencies and access to data that can give organizations an advantage over their peers. Commonly, security only considers the individual devices themselves, not the larger system in which these devices operate. There may be thousands of individual devices in a system, but they will collectively operate as part of a unified process or function.

A key component of building system context is to assess the common relationships between devices and determine whether or not they are appropriate based upon user-defined policies and previous behaviors observed. As a simple example, drones are often paired with a controller component. Should that relationship be broken or changed in an unusual way, that would be considered a violation of the trust.

CONCLUSION

Zero-trust architectures *can* be successfully implemented, though IoT can pose a challenge to the security model. To be effective in identifying, assessing and controlling the risk posed by the rapid adoption of IoT, zero-trust architectures implementations must take into account the whole device, its intent and the system in which it operates.

ABOUT THE AUTHOR

Yolonda Smith is the Director of Product Management at Pwnie Express, responsible for development & execution of Pwnie's product strategy and roadmap. Yolonda is focused on providing security professionals the visibility and control to identify, characterize and neutralize threats to their wired and wireless assets. A security professional herself, she spent 8 years in the United States Air Force as a Cyberspace Operations Officer with duties and responsibilities varying from Mission Commander, Advanced Network Operations where her team developed & orchestrated the first DoD Cyber Hunting missions to Flight Commander, Cyber Defense Capabilities Development where her team developed the first and only malware neutralization tool for Predator Drones.