NOVEMBER 2021

The Application of Zero Trust to Legacy Systems & Operational Technologies

Don Maclean, ICIT Fellow
Chief Cyber Security Technologist, DLT

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

ICIT's Bright Minds Q&A Series

The Application of Zero Trust to Legacy Systems and Operational Technologies

With Don Maclean, ICIT Fellow and Chief Cyber Security Technologist, DLT

November 2021

About This ICIT Bright Mind Q&A:

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations.

Zero Trust is a model that promises the security in environments in which the "network perimeter" is an obsolete concept. In this ICIT Bright Minds Q&A, Don Maclean, ICIT Fellow and and Chief Cyber Security Technologist, DLT, explains the challenges and benefits of applying Zero Trust paradigms to legacy and operational technology systems.

About this Bright Mind:

As Chief Cybersecurity Technologist for DLT, Don Maclean formulates and executes cybersecurity portfolio strategy, speaks and writes on security topics, and socializes his company's cybersecurity portfolio. Don has nearly 30 years' experience working with U.S. Federal agencies. Before joining DLT in 2015, Don managed security programs for numerous U.S. Federal agencies, including DOJ, DOL, FAA, FBI, and the Treasury Department. This experience allowed him to observe the strengths and limitations of traditional cybersecurity defenses, leading to his interest in innovative technologies such as those featured in this article. In addition to his CISSP, PMP, CEH, and CCSK certificates, Don holds a B.A. in Music from Oberlin, an M.S. in Information Security from Brandeis Rabb School, and is a recipient of the FedScoop 50 award for industry leadership. An avid musician, Don organizes a concert for charity every year, and has been known to compete in chess and Shogi (Japanese chess) tournaments, both in person and online.

About ICIT:

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

ICIT:

What are the challenges of securing operational technologies and legacy systems? Are there any unique challenges to each?

Maclean:

Government systems frequently use outdated or old technology, funding for modernization is challenging to obtain, and institutional knowledge resides with contracting staff who may no longer be available on the contract. Operational systems ("OT") often require 100% uptime, greatly complicating patching, updates, and the installation of security software.

ICIT:

What are the benefits of adopting Zero Trust frameworks for Operational Technology & Legacy Systems? Are there any potential downsides?

Maclean:

If a Zero Trust program facilitates modernization, it would be a definite plus for eliminating or updating legacy systems. Currently, disruptive attacks (commonly called "ransomware") are growing in severity and frequency. Zero Trust assumes that breaches have or will occur and emphasizes detection and rapid response. These principles are important in IT environments, but rapid-response is absolutely essential for OT, where uptime is critical. The downside of Zero Trust is its "boil-the-ocean" approach. Even minor changes are difficult to deploy in OT environments. The major changes necessary for Zero Trust could prove too ambitious to be practical.

ICIT:

Is Zero Trust adoption more important with the IT-OT convergence and the integration of legacy systems with modern networked systems?

Maclean:

Zero Trust recognizes the disappearance of a network perimeter. The convergence of OT and IT accelerates the dissolution of a perimeter, making Zero Trust even more important for protecting converged environments.

ICIT:

What are the barriers to Zero Trust adoption?

Maclean:

The barriers to Zero Trust are:

1. Culture change - Zero Trust entails a fundamental shift in thinking about cybersecurity.
2. Cost – Zero Trust is comprehensive, long-term, and costly
3. Metrics - Progress and improvement are difficult to measure quantitatively, especially in the monetary terms senior management will want to see.

ICIT:

Are there any final thoughts on which you would like to conclude?

Maclean:

"Zero Trust" has become a bit of a buzzword, giving rise to detractors and nay-sayers. While some of their criticism is warranted, alternative approaches are hard to find. Clearly, our approach to cybersecurity is not working; news reports about hacks and intrusions abound. A new approach is necessary, and while Zero Trust may have its weaknesses, it appears to be the best bet at the moment.
