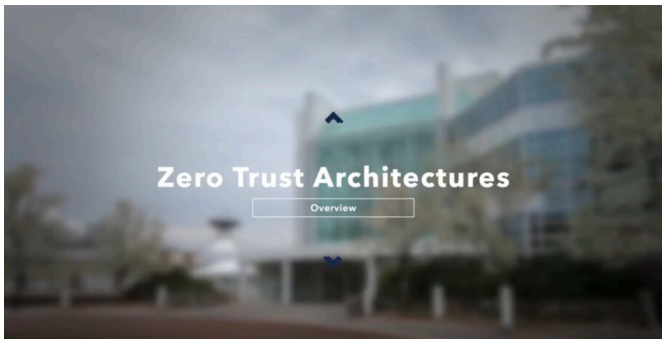
Zero-trust architecture may hold the answer to cybersecurity insider threats

18 May 2022, by Nathan Parde



MIT Lincoln Laboratory recently completed a study on zero-trust architectures, a cybersecurity approach in which users must prove their authenticity each time they access a network application or data. Credit: MIT Lincoln Laboratory

For years, organizations have taken a defensive "castle-and-moat" approach to cybersecurity, seeking to secure the perimeters of their networks to block out any malicious actors. Individuals with the right credentials were assumed to be trustworthy and allowed access to a network's systems and data without having to reauthorize themselves at each access attempt. However, organizations today increasingly store data in the cloud and allow employees to connect to the network remotely, both of which create vulnerabilities to this traditional approach. A more secure future may require a "zero-trust architecture," in which users must prove their authenticity each time they access a network application or data.

In May 2021, President Joe Biden's Executive Order on Improving the Nation's Cybersecurity outlined a goal for federal agencies to implement zero-trust security. Since then, MIT Lincoln Laboratory has been performing a study on zero-trust architectures, with the goals of reviewing their implementation in government and industry, identifying technical gaps and opportunities, and developing a set of recommendations for the United States' approach to a zero-trust system.

The study team's first step was to define the term "zero trust" and understand the misperceptions in the field surrounding the concept. Some of these misperceptions suggest that a zero-trust architecture requires entirely new equipment to implement, or that it makes systems so "locked down" they're not usable.

"Part of the reason why there is a lot of confusion about what zero trust is, is because it takes what the cybersecurity world has known about for many years and applies it in a different way," says Jeffrey Gottschalk, the assistant head of Lincoln Laboratory's Cyber Security and Information Sciences Division and study's co-lead. "It is a paradigm shift in terms of how to think about security, but holistically, it takes a lot of things that we already know how to do—such as multi-factor authentication, encryption, and software-defined networking—and combines them in different ways."

Recent high-profile cybersecurity incidents—such as those involving the National Security Agency, the U.S. Office of Personnel Management, Colonial Pipeline, SolarWinds, and Sony Pictures—highlight the vulnerability of systems and the need to rethink cybersecurity approaches.

The study team reviewed recent, impactful cybersecurity incidents to identify which security principles were most responsible for the scale and impact of the attack. "We noticed that while a number of these attacks exploited previously unknown implementation vulnerabilities (also known as 'zero-days'), the vast majority actually were due to the exploitation of operational security principles," says Christopher Roeser, study co-lead and the assistant head of the Homeland Protection and Air Traffic Control Division, "that is, the gaining of individuals' credentials, and the movement within

a well-connected network that allows users to gather a significant amount of information or have very widespread effects."

In other words, the malicious actor had "breached the moat" and effectively became an insider.

Zero-trust security principles could protect against this type of insider threat by treating every component, service, and user of a system as continuously exposed to and potentially compromised by a malicious actor. A user's identity is verified each time that they request to access a new resource, and every access is mediated, logged, and analyzed. It's like putting trip wires all over the inside of a network system, says Gottschalk. "So, when an adversary trips over that trip wire, you'll get a signal and can validate that signal and see what's going on."

In practice, a zero-trust approach could look like replacing a single-sign-on system, which lets users sign in just once for access to multiple applications, with a cloud-based identity that is known and verified. "Today, a lot of organizations have different ways that people authenticate and log onto systems, and many of those have been aggregated for expediency into single-sign-on capabilities, just to make it easier for people to log onto their systems. But we envision a future state that embraces zero trust, where identity verification is enabled by cloud-based identity that's portable and ubiquitous, and very secure itself."

While conducting their study, the team spoke to approximately 10 companies and government organizations that have adopted zero-trust implementations—either through cloud services, in-house management, or a combination of both. They found the hybrid approach to be a good model for government organizations to adopt. They also found that the implementation could take from three to five years. "We talked to organizations that have actually done implementations of zero trust, and all of them have indicated that significant organizational commitment and change was required to be able to implement them," Gottschalk says.

But a key takeaway from the study is that there isn't a one-size-fits-all approach to zero trust. "It's why we think that having test-bed and pilot efforts are going to be very important to balance out zero-trust security with the mission needs of those systems," Gottschalk says. The team also recognizes the importance of conducting ongoing research and development beyond initial zero-trust implementations, to continue to address evolving threats.

Lincoln Laboratory will present further findings from the study at its upcoming Cyber Technology for National Security conference, which will be held June 28–29. The conference will also offer a short course for attendees to learn more about the benefits and implementations of zero-trust architectures.

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology