Cybersecurity at
MIT Sloan

Cybersecurity at MIT Sloan
Zero Trust Networks and Industrial Control Systems

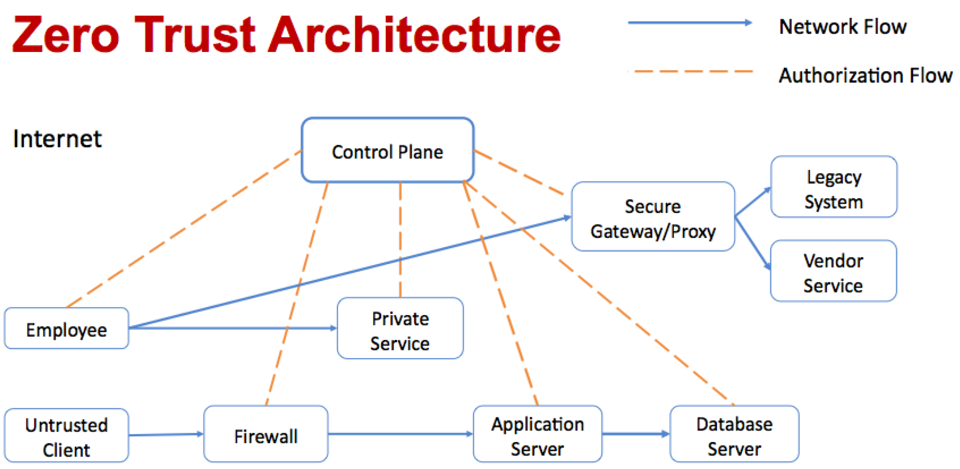
Cybersecurity at MIT Sloan brings thought leaders from industry, academia and government together with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

A zero trust defense architecture fills the gaps left by traditional perimeter defense, and can help defend against threats that haven't been seen before

Industrial Control System Cyber Defense

Some of the worst cyber attacks in recent memory targeted industrial control systems: in 2015, as a result of spear phishing, the Ukranian electric grid attack and the German Steel Mill attack both resulted in massive physical and financial damage. In the case of industrial control systems, traditional "perimeter defense" doesn't cut it. Sophisticated hackers can access an ICS from a corporate network, often in spite of network segmentation and firewalls.

CAMS researchers are working to apply a "zero trust architecture" to ICS cyber defense systems to prevent such attacks. This kind of setup includes an authorization system that is separate from the network flow and provides additional checks to ensure that malicious users are not able to sneak in by impersonating authorized users. An authorization control plane keeps data stores, which include an inventory of users, devices, and applications, as well as authorization records, network flows, and environment/deployment specific records. These allow the control plane to use more information to verify identity. A trust engine performs risk analysis and generates a "trust score" that is used to make authentication decisions. The engine bases its decision on factors such as historical activity, time, and location, adding levels of context-based security and control. If an authorization request is considered risky, the system will require additional forms of verification to ensure strong authentication.



IMPACT:

With traditional perimeter defense architecture, policies must be constantly updated. Over time, more users are granted access, increasing network vulnerability. It creates a single point of failure for ICS defense. As an alternative, zero trust architecture provides greater protection against cyber attacks. With zero trust architecture, even if an attacker gains some credentials to access the system, authentication controls would protect the most critical physical systems.

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletters. For more information, visit https://ic3.mit.edu or contact:

Dr. Stuart Madnick • Professor and Director • smadnick@mit.edu
Dr. Michael Siegel • Director • msiegel@mit.edu
Dr. Keri Pearlson • Executive Director • kerip@mit.edu