Life Sciences Cybersecurity Executive Roundtable
Detecting Wireless Eavesdroppers
December 9, 2020

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual winter roundtable. Following introductions, participants engaged in a discussion surrounding supply chain cyber and auditing. Following the hot topics discussion, CAMS Researcher Jun Huang shared research and led a discussion about detecting wireless eavesdroppers.

Hot Topics Session

The hot topics discussion revolved around 3rd party risk within organizations. The group discussed how auditors are frequently pushing to find out what organizations are doing in regards to self-auditing. One attendee said that his company manages the process internally, creating more assessments every year for outside vendors. One thing many companies are noticing as their security protocols mature is that managing and processing these controls demands a magnitude of resources. With a limited security budget, tighter auditing for the more crucial vendors may take importance. To properly allocate resources, one life sciences company in attendance preferred to scrutinize clinical trial vendors more thoroughly than marketing vendors. By putting more resources into the highest risk vendors, such as using more questionnaires and scorecards, organizations can assume a proportionate level of risk.

Another angle to approach internal auditing is that recently a growing abundance of critical service providers for other parties will provide compliance reports. Finding providers who offer these reports can establish a line of trust pre-contract. Companies can discuss with these 3rd party providers and get good traction while determining a service contract. As a smaller company, it may be difficult to predict how much pushback from vendors will occur. One attendee stressed that even as a small company of 1,500 people, they are generally accepted as a vendor if they are able to align their wording, timing, and communication.

CAMS Research Presentation: Ear Fisher

Eavesdropping is a fundamental threat to the security and privacy of wireless networks because hackers can steal information or change the way a device functions. To date, wireless eavesdroppers have gone unnoticed because they do not alter or transmit signals. This research presents a system for detecting wireless eavesdroppers in a way that can differentiate them from legitimate receivers. EarFisher achieves this by simulating wireless eavesdroppers using bait network traffic, and then capturing eavesdroppers' responses by sensing and analyzing the memory in the device.

Extensive experiments show that EarFisher accurately detects wireless eavesdroppers even under poor signal conditions, and is resilient to the interference of system memory workloads, high volumes of normal network traffic, and the memory EMRs emitted by coexisting devices. A device to detect these eavesdroppers can be an essential building block of a secure network. To learn more about this research, click here to view the research brief on the CAMS website: https://bit.ly/3smQr0G

About Cybersecurity at MIT Sloan

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

For more information, visit https://cams.mit.edu