Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan
EarFisher: Detecting Wireless Eavesdroppers by Stimulating and Sensing Memory EMR

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 System that can Detect Wireless eavesdroppers and Differentiate them from Legitimate Receivers

Eavesdropping is a fundamental threat to the security and privacy of wireless networks. To date, wireless eavesdroppers have gone unnoticed because they do not alter or transmit signals. This research presents EarFisher- the first system that can detect wireless eavesdroppers. 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.

EarFisher accurately detects wireless eavesdroppers even under poor signal conditions and is resilient to the interference of system memory workloads, high traffic volumes, and the memory EMRs emitted by coexisting devices

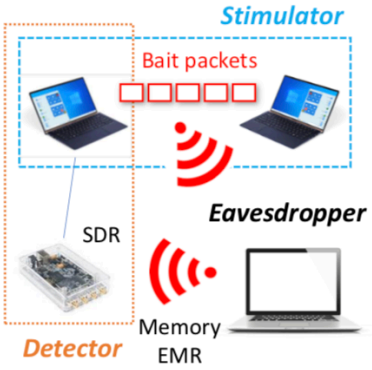

Figure 5: EarFisher architecture.

Design Overview

As illustrated here, EarFisher consists of a stimulator and a detector. It is designed as a standalone system to detect eavesdroppers in a wireless network without the cooperation of other network nodes. The stimulator is a wireless network of two cooperative nodes, which exchange packets to generate stimuli. The detector senses memory EMR using a software define radio, which is hosted by one of the simulator nodes and is synchronized with the wireless NIC to monitor the variations of memory EMRs under traffic stimuli.

Detection

At a high level, the stimulator of EarFisher consists of two cooperative devices, which exchange packets to generate stimulus traffic. To detect eavesdroppers in a specific wireless network, the bait packets should be transmitted on the same frequency channel. In case the network to protect is operated on multiple channels, the stimulator can hop across channels to inject baits. The principle of this presented design is broadly applicable to other types of wireless networks.

Possible Limitations

By EarFisher's detection methodology, any device that digests others' packets in CPU EMR memory systems will be convicted of eavesdropping. Because is nearly impossible to differentiate benign or malicious use of other's packets, all software radios will be identified as eavesdroppers as long as they transfer baseband signals.

IMPACT: EarFisher allows wireless eavesdroppers to be detected by stimulating and sensing memory EMRs. EarFisher provides an important block for building secure wireless networks.

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 newsletter. For more information visit cams.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