Fingerprinting the Internet of Things

February 9 2022, by Madison Brewer

A woman in the background with her digital fingerprint and an unlocked IoT device. Credit: Carnegie Mellon University

The Internet of Things (IoT) refers to the growing number and type of devices that are connected to the internet. IoT devices range from Amazon Alexa and Google Home to bluetooth coffee makers and toothbrushes. Unlike cell phones and computers, these IoT devices may not have robust security. Hackers can infiltrate a network through a weaker device to access private information on devices with better security.

Creating security for IoT devices is challenging because they must be physically small (to fit in the device) and require relatively low power (to avoid draining the device). Usually, these devices are also not capable of performing complex computations. Carnegie Mellon University researchers at the Energy-Efficient Circuits and Systems (EECS) Lab from the Department of Electrical and Computer Engineering are inventing new ways to meet these challenges. In two recently published papers, Assistant Professor Vanessa Chen and her Ph.D. students Yuyi Shen and Jiachen Xu explored using variations from the manufacturing process for more robust security.

Within a network, the devices—also called nodes—already trust one another; that is, they openly communicate by sending and receiving signals. If a foreign device tried to interact with a node, the network would ignore it. One way that hackers gain access to networks is by impersonating a trusted node. Thus creating security measures must involve a robust process for verifying the identity of any device attempting to communicate.

"The typical approach for implementing a wireless security system is through some kind of cryptographic mechanism, which requires computational power that some IoT devices have trouble supporting," Shen said. "The focus of our research is on one specific form of low power security mechanism called radio frequency fingerprinting."

Radio frequency fingerprinting (RFF) refers to a method of identifying devices by exploiting hardware variations that arise despite the precision used during the manufacturing process. These variations result in unique features in the radio waves the device transmits. After signal processing, these features can be used to identify a specific device.

One way to make RFF harder for hackers to identify, and thus mimic, is to change the fingerprint's features. This is a non-trivial task, especially given the fact that the RFFs result from unintentional manufacturing deviations. One of the researchers' papers looked at using power amplifiers to change a device's signal features.

"Usually, each device will have fixed hardware characteristics that might change with the environment or slowly over time," Xu said. "But this power amplifier is capable of reconfiguring itself to generate various radio frequency fingerprints in one device, preventing people attacking the device from mimicking the hardware characteristics."

This work used a convolutional neural network (CNN) to process and classify signal transmissions. The researchers found that the CNN was able to accurately classify incoming signals as safe or unsafe by evaluating the RFF within the processed signal.

The other paper was a proof-of-concept investigation into using Bayesian neural networks (BNN) to identify and classify the RFFs. A BNN relies on Bayesian statistics, which accounts for uncertainties in its predictions. Unlike traditional neural networks, for any given input, the BNN will not produce the same output every time. Like the CNN, they found that the BNN was able to complete these tasks quickly and accurately. They also found that a lightweight neural network could be used, meaning the BNN did not require too much computational power.

Both papers show promising results for using RFF as security measures for IoT devices. Next, the researchers are planning to create hardware that would enable the use of radio frequency fingerprinting in small, low power devices that would be used in outer space. Keeping IoT devices safe is necessary for keeping networks—and therefore sensitive information—out of reach of hackers.

Provided by Carnegie Mellon University Electrical and Computer Engineering

Citation: Fingerprinting the Internet of Things (2022, February 9) retrieved 25 April 2024 from https://techxplore.com/news/2022-02-fingerprinting-internet.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.