New privacy threat combines device identification with biometric information

April 29 2020

Credit: CC0 Public Domain

A study by computer scientists at the University of Liverpool has revealed a new privacy threat from devices such as smartphones, smart doorbells and voice assistants that allows cyber attackers to access and

combine device identification and biometric information.

Over a one month period, computer scientists collected and analysed over 30,000 biometric samples from over 50 users and over 100,000 different device IDs, to find that identity leakages from different devices allow cyber attackers to correlate device IDs and biometric information to profile users in both cyber and physical domains, posing a significant online privacy and security threat.

Using the samples, computer scientists were able to de-anonymize over 70% device IDs (e.g. smartphone MAC addresses) and harvest the biometric information (facial images or voices) of device users with 94% accuracy.

Although single modal identity leakage—the leakage of information from one source or device—is well studied, this is the first time a new privacy issue of cross-modal identity leakage has been observed revealing an unprecedented threat in environments with multiple different sensors.

With the `Internet of Things' becoming an increasing reality devices such as smartphones, smart thermostats, smart lightbulbs, speakers and virtual assistants are far more common. In addition, there are Increasingly rich sets of sensors in smart buildings and on smart devices. For example, a smart doorbell today can be outfitted with more than 9 different sensors (e.g. cameras, microphones, WiFi etc).

This, however, spawns an increased opportunity for many multi-modal sensing scenarios that can be maliciously leveraged by cyber attackers.

Dr. Chris Xiaoxuan Lu, with the University of Liverpool's Department of Computer Science who led the study, said: "This is an important new study which confirms the concern presented by numerous IoT devices

and unveils a compound identity leak from the combined side channels between human biometrics and device identities.

"Technically, we present a data-driven attack vector that robustly associates physical biometrics with device IDs under substantial sensing noise and observation disturbances.

"These findings have wider implications for policy makers in IT laws and for IoT manufacturers who need to look into this new privacy threat in their products.

"To date there is not good enough countermeasures against such new attacks and all possible mitigation will inevitably undermine user experience of IoT devices."

The research team is now working with the IT law researchers to scope out new policies for IoT manufacturers. Meanwhile on the technology side, they are also investigating how to effectively detect hidden electronic devices (e.g., spy cameras and microphones) with consumer smartphones."

More information: Nowhere to Hide: Cross-modal Identity Leakage between Biometrics and Devices. DOI: 10.1145/3366423.3380108 , arxiv.org/abs/2001.08211

Provided by University of Liverpool