C28 Is Your Home Secretly a Confidential Informant for the Police? The Potential of Smart Home Devices to Serve as Evidence in Criminal Cases

Jason Lewis, PhD, University of the Virgin Islands, Dept of Computer & Computational Sciences, No 2 John Brewers Bay, Saint Thomas, VI 00802; Arl Polydore, University of the Virgin Islands, No 2 John Brewers Bay, College of Science and Mathematics, Saint Thomas, VI 00802; Lawrence White, University of the Virgin Islands, No 2 John Brewers Bay, College of Science and Mathematics, Saint Thomas, VI 00802; Jair Smith, University of the Virgin Islands, No 2 John Brewers Bay, College of Science and Mathematics, Saint Thomas, VI 00802; K'Mari McClean, University of the Virgin Islands, No 2 John Brewers Bay, College of Science and Mathematics, Saint Thomas, VI 00802; and Roberto Tirado, University of the Virgin Islands, No 2 John Brewers Bay, College of Science and Mathematics, Saint Thomas, VI 00802*

After attending this presentation, attendees will better understand what data of evidential value is contained on various smart home devices as well as techniques to forensically acquire the data.

This presentation will impact the forensic science community by providing the techniques to acquire data of forensic value from various smart home devices.

We are living in a society where more and more of the items that we come into contact with each day are connected to the internet. This phenomenon has powered an entire technological industry known as the Internet of Things (or IoT). Nowhere can this idea be better exemplified then in the modern home. As recently as ten years ago, the average home would have been lucky to have one device connected to the internet, namely the home Personal computer (PC). Now we are seeing a diverse range of devices in the modern home that are also connected to the internet (from the light switch to the kitchen sink and everything in-between). This has given rise to the new smart home, where these devices are constantly monitoring activity and trying to help make people's daily lives easier.

This explosion in internet-connected devices (and the terabytes of data that comes with them) brings an interesting question to the forefront for law enforcement: Can these smart devices act as eyes and ears for the police and help solve modern crimes? It is already known that the Amazon® Echo™ must be continually listening to every spoken word in order to be at our beck and call, but does this mean that it can also record the voice of the home intruder, and if so, can that voice be easily recovered *without* the help of Amazon®?

The goal of this study was to determine the forensic value of several common smart home devices and the techniques to acquire the relevant data from these devices. The research focused on the Amazon® Echo™ and Google® Home Smart Hubs™, the D-Link® 965 Wi-Fi Video Security Camera, the Logitech® Logi Circle Wireless HD Video Security Camera with 2-Way Talk, and the August® Smart Lock. This study determined what data was stored locally on these devices versus stored in the Cloud and explored techniques to extract that data.

Smart Home, Smart Devices, Internet of Things

*Presenting Author