<CFS>

Short abstract (c.25 words): Forensics readiness is the missing link in the Internet of Things development. This paper sheds light on this issue and elaborates on cyber forensics practitioners, device manufacturers and legal authorities role to cover this gap.

Long abstract (c.120 words): Every new device we create, every sensor we deploy, every byte we synchronize to other locations will at some point come under scrutiny in the course of investigations and legal matters. Yet no reliable forensics applications nor digital forensics guidance exists to retrieve the data from IoT devices in the event of a cyber event, an active investigation or a litigation request. The digital forensics of internet of things (IoT) technologies is the missing conversation in our headlong rush to the promise of connecting every device on the planet. This paper discuss about issues and importance of further development in this field and elaborates on how forensics practitioners, device manufacturers and legal authorities could share the efforts and minimise this gap.

Digital Forensics: The Missing Piece of the Internet of Things Promise

Steve Watson, VTO Labs, Seattle, WA / Denver, CO / Washington, D.C, steve.watson@vtolabs.com
Ali Dehghantanha, School of Computing, Science and Engineering, University of Salford, Manchester, UK, a.dehghantanha@salford.ac.uk

As technology advances at a blinding pace, the promise of new gadgets to enhance every facet of our lives tempts every consumer and organization. From the ease of automation, control and monitoring of the most mundane aspects of our lives to advanced lifesaving and monitoring capabilities; our world is changing daily.

No longer does one need to remember to water the house plants, feed the dog, or return home to see if the garage door was closed. At the same time advanced technologies from our mobile and connected devices can perform a hospital grade EKG (electrocardiogram) from a remote location and forward the data to our doctors before we arrive at the hospital. The industry focus on these new technologies is on compatibility and ubiquity across devices and experiences. The industry has begun to grapple with securing these new devices both from intrusion and control [1,2].

However a massive gaping hole exists in our industry planning and execution on the topic of internet of things. Every new device we create, every sensor we deploy, every byte we synchronize to other locations will at some point come under scrutiny in the course of investigations and legal matters [3]. The very principle that we must 'secure' the devices [4] implies that we will be able to accurately determine IF the devices have been compromised.

Yet no reliable forensics applications nor digital forensics guidance exists to retrieve the data from IoT devices in the event of a cyber event, an active investigation or a litigation request. Not only does guidance not exist, industry does not know what data is captured in most instances, what other devices the data lands on or if the data is readable and accessible if it could be retrieved.

The digital forensics of internet of things (IoT) technologies is the missing conversation in our headlong rush to the promise of connecting every device on the planet.

The digital forensics of embedded technologies

Internet of Things, wearables, drones, 3D printers even emerging medical devices have a common overlooked thread – all of these new technologies are making use of embedded technologies in their product designs. The concept of connecting devices to the internet by adding network capability is simply an expansion of the embedded technology platforms that have existed for quite some time.

With the rapid growth and expansion of these new network connect technology platforms, one area of science is struggling to keep pace. Digital forensics is the branch of forensic science concerned with the recovery and investigation of data found on digital devices. As these new and updated platforms based on embedded technologies emerge, the industry and practitioners struggle to develop the tools and procedures to keep pace with the technology.

Embedded technologies are electronics or computing systems with specific functions that may exist as part of a larger platform. An embedded technology design includes some or all of the following components: a PCB (printed circuit board), microcontroller, RAM, flash memory, and networking capabilities (e.g. Bluetooth, WiFi, GSM). In the case of modern embedded technologies designs, the larger platform may include other wireless connected devices and centralized storage systems (e.g. wearable device connected to smartphone, synchronizing to the cloud).

The Internet-enabled refrigerators and kitchen appliances are great examples of a new embedded technology device which is not a full computer in the traditional form factor we have grown accustomed to, yet the devices enough technology inside for it to talk to a network, receive commands and send statuses. When you call your investigation team to ask them was this internet-enabled refrigerator the source of infection on your network, they will likely look with blank stares as they try to figure out how to get started examining the device.

Is there data with evidentiary value within these new technology devices? Does it exist on the device or across a network connection retrieving and storing the information?

Why are embedded technologies more challenging?

The challenge for digital forensic practitioners is that industry tools and capabilities have historically been focused on traditional computer operating systems or magnetic media. The industry development of mobile forensic tools has made great inroads into a specific area of embedded technologies (mobile phone technology). Yet mobile forensic vendors are even feeling the strain of new device types, encryption capabilities and the evolution of mobile operating systems into new embedded devices like wearable's and automobiles.

The digital forensic complexity for embedded technologies centers around three issues: (1) the onboard data storage is not accessible via traditional digital forensics methods, (2) the cumulative dataset may exist in multiple locations and (3) even if the data can be acquired it may not be readable or accessible with existing tools. Examples of embedded technology areas which are challenging for forensics investigation are wearables, drones, prototyping microcontrollers, medical devices, sensor networks, home automation, Internet of Things, vehicles, 3D printers, connected appliances, security systems, access control systems, mobile phones, and sensor network technologies.

Inaccessibility via traditional digital forensics methods

Most embedded device examples contain onboard flash to run a pared down operating system or real-time application executables. As the devices do not have traditional hard drives (magnetic or solid state) that can be removed and are not running full computer operating systems, new techniques must be created to retrieve the data. In the instance where the embedded device is using a modified mobile operating system, some mobile forensic tools may assist in acquisition of the data or parsing the data into useable formats. If the embedded device is running a real-time application, decompiling the acquired application may be required to understand what the application is doing and where the data is being saved. Advance data recovery techniques are required when perform data acquisitions off of embedded devices. Analysis of the network traffic from the device can provide clues to what the device is doing and where the data may be landing.

Cumulative dataset may exist in multiple locations

Since the embedded devices may have limited flash memory storage, it is common for the device to be connected to another device for expanded network capability and offline storage. These alternate storage locations may have expanded data from what exists on the device included a longer historical timeline, configuration information, even user information identifying further sources which may hold additional data (e.g. internet storage aka the cloud).

Acquired data may not be readable or accessible with existing tools

If data can be retrieved from the wearable device, it may be that the data is encrypted or stored in a non-standard data format for which a viewer does not yet exist. Extensive data parsing or conversion may be required to derive meaningful content from the data retrieved off of the device. This challenge is not new to those working in the area of mobile device forensics as the technology has evolved very quickly in recent years.

The internet-enabled toaster would be affected by each of these challenges. None of the industry tools would support the toaster for digital forensics today. Data about the commands that were sent to the toaster could reside on the toaster, the connected devices or even a remote cloud account. Even if the data could be acquired from the flash memory on the device, it is highly likely that the existing digital forensic tools in your toolbox will not know how to interpret the data.

Why are Internet of Things devices of interest to digital forensics?

It is not a far leap to imagine wearable technologies being used as corroborating evidence that a person may have been asleep or exercising at the precise time an event was occurring. What happens when someone's IoT home automation system is disabled by a suspect to gain entry into a home? Or embedded sensor technology in the new IoT cities captures 100's of additional data points at the precise scene of a crime? How will we know when an edge node IoT device is compromised over an uncommon network protocol, gaining a foothold into an existing network? In these instances, digital forensics practitioners will be called upon to retrieve data that may exist on these devices.

As we look ahead to a world of expanding ubiquitous computing, the challenge grows in this space. We don't hear numbers of end nodes diminishing in the future but expanding at rates faster than we have encountered to date. If these devices are more vulnerable on networks because of immature security capabilities, we can be assured that investigations will be needed to understand what role these devices played in a breach.

Concluding Remarks

So far, it might be clear that embedded technology forensics should be escalated to senior digital forensic practitioners experienced in challenging devices. Practitioners experienced with mobile phone forensics including JTAG and chip-off or general practitioners experienced in damaged devices may have relevant experience to complete acquisitions. Techniques used to parse data from hard drives and mobile device images may be successful on data acquired from embedded technologies. Consider the other locations where the embedded device may be located. In some instances, it may be easier to acquire the necessary data from the connected devices than the primary embedded device.

Moreover, Legal authorities should understand that digital forensic capabilities in these new emerging technologies are not on pace with digital forensics of traditional computer technologies. Digital forensics researchers and practitioners are working hard to identify tools, techniques and capabilities to enhance the digital forensics capabilities against these new technology platforms. In some instances, recovery of data from some of these new technologies may not be possible or if it is possible, the data may not be readable. Digital forensic community seeks your patience as we are working through these new challenging areas.

Device manufacturers should consider that at some point in the future, data off of their new devices may very well be requested in a legal matter. Device manufacturers should consider at the outset how data may be extracted from the device or a position statement if the data is known to be inaccessible once retrieved. This guidance could be maintained internally to assist your legal teams in responding to subpoenas or requests for data when the needs arise.

With the forecasted growth in IoT device development, the challenge for those securing and investigating these embedded technology devices will continue to grow as well.

About the author

Mr. Steve Watson is the founder of VTO Labs, a firm focused on the most challenging areas of data preservation, data recovery and digital forensics. With nearly two decades of experience in information technology, information security, and investigations, he is also an active digital forensic researcher working in the areas of data recovery from emerging technologies and damaged devices. When he's not destroying devices for damaged devices research or taking apart the new technologies we see on the internet, he supports clients in the areas of data recovery for litigation and investigations. Watson sits on two Federal committees related to digital forensics and is pursuing a PhD in Digital Forensics.

Dr. Ali Dehghan Tanha (www.alid.info; AliD@AliD.info) is a Marie-Curie International Incoming Fellow in Cyber Forensics and has served for many years in a variety of research and industrial positions. Other than Ph.D in Cyber Security he holds many professional certificates such as GREM, CISM, CISSP, and CCFP. He has served as an expert witness, cyber forensics analysts and malware researcher with leading players in Cyber-Security and E-Commerce.

References

1. Liu, C. Securing networks in the Internet of Things era. *Comput. Fraud Secur.* 2015**,** 13–16 (2015).
2. Daryabar, F., Dehghantanha, A., Udzir, N. I. & bin Shamsuddin, S. Towards secure model for SCADA systems. in *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* 60–64 (IEEE, 2012). doi:10.1109/CyberSec.2012.6246111
3. Oriwoh, E., Jazani, D., Epiphaniou, G. & Sant, P. Internet of Things Forensics: Challenges and Approaches. in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* 608–615 (ICST, 2013). doi:10.4108/icst.collaboratecom.2013.254159
4. Tankard, C. The security issues of the Internet of Things. *Comput. Fraud Secur.* 2015**,** 11–14 (2015).