SWGDE Technical Notes on Internet of Things (IoT) Devices

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Table of Contents

1. Purpose

The purpose of this document is not to define, but to provide a general awareness of devices that comprise the “Internet of Things” (IoT), including their function, use, the potential to contain data of interest and the methods of data storage. The intended audience is personnel collecting evidence and digital forensics practitioners that will be acquiring and analyzing data from the devices being collected.

2. Scope

IoT devices are designed for consumer and industrial use; however, this document focuses on consumer devices for personal and residential use.

The ideas, concepts and technical aspects about these devices are strictly related to what is available at the time of this document. There may be additional features or capabilities developed in the future that could alter the collection, preservation, acquisition and analysis. Although some varieties of the devices/items being discussed in this document would not be considered IoT (e.g., most shoes are not IoT, most magnetic card readers, etc.) there are some that may have characteristics that would qualify them as IoT.

3. Definition

Currently, there is no single widely accepted industry definition for IoT. For the purposes of this document, we will focus on IoT being a system of interrelated computing devices, mechanical and digital machines or objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. These devices are not limited to a particular type of data storage medium or format. For additional information about the different perspectives of IoT, see NIST Special Publication 1900-202, *Cyber-Physical Systems and Internet of Things* [1].

4. Identification of IoT Devices

A variety of IoT devices are currently available and the market is rapidly expanding. The usage and capabilities of most devices are identifiable by the manufacturer’s marketing or user materials, and by conducting online research. However, some IoT devices may not be easily identifiable by their external appearance or markings. IoT devices have various functions and capabilities, and for the purpose of identification these devices can be separated into several classes, or groups of devices. The following is not meant to be an all-inclusive or comprehensive list, but provides information related to the various classes of devices to give investigators an idea of what to look for.

4.1. Classes/Groups

a. Wearables – Wearable technology (also called wearable gadgets) is a category of technology devices that can be worn by a consumer.
   i. Watches
   ii. Shoes
   iii. CPAP machines
   iv. Hearing-Aids
   v. Glucose/Insulin pumps

b. Smart Speakers – A smart speaker is a type of wireless speaker and voice command device with an integrated virtual assistant that offers interactive actions and hands-free activation with the help of an activation phrase, or "wake word.". The particular "wake word" may be changeable by the user. Some smart speakers can also act as a smart device that utilizes Wi-Fi, Bluetooth and other wireless protocol standards to extend usage beyond audio playback, such as to control home automation devices. This can include, but is not limited to, features such as compatibility across a number of services and platforms, peer-to-peer connection through mesh networking, virtual assistants, and others. Each can have its own designated interface and features in-house, usually launched or controlled via application or home automation software. Some smart speakers also include a screen to show the user a visual response.

Device	**Virtual Assistant / AI Interface**	**Default Wake Word**
Echo	Alexa	Alexa
Google Home	Google	Hey Google
Facebook Portal	Alexa	Alexa
Home Pod	Siri	Hey Siri

c. Sensors – A sensor is a device which detects or measures a physical property and records, indicates, or otherwise responds to it.
   i. Motion
   ii. Lumen
   iii. Sound
   iv. Break/Separation Contact
   v. Vibration
   vi. Position
   vii. Temperature
   viii. Humidity
   ix. Gas

d. Control Systems – A control system bridges and manages, commands, directs, or regulates the behavior of other devices or systems.
   i. Actuators (e.g., door lock)
   ii. Thermostats

e. Capture – Devices that capture information/data, may store for later exfiltration, and may broadcast data externally.
   i. Cameras
   ii. Audio
   iii. Magnetic Card Readers (Skimmers, Square, etc.)

   iv. Point of Sale (PoS) peripherals
   v. Automated Teller Machines (ATM)

f. Implants – Devices not readily accessible, since they are designed to operate internal to another body, typically a living being such as a human or animal.
   i. Cochlear
   ii. Pacemaker/Defibrillator
   iii. Radio-Frequency Identification (RFID) Module
   iv. Near-Field Communication (NFC) Module

g. Vehicles – A machine, device, or craft designed to travel and often contains a payload of some kind, whether it be a capture device (e.g., camera) or cargo. For information on vehicle systems, see *SWGDE Best Practices for Vehicle Infotainment and Telematics Systems*.
   i. Infotainment
   ii. Telematics
   iii. Small Unmanned Aerial Systems (SUAS), AKA Drones

h. Appliances – Machines/devices used to perform household functions.
   i. Refrigerators
   ii. Coffee maker
   iii. Washer/Dryer
   iv. TVs
   v. Robotic vacuum

4.2. Functionality and Control

An IoT device may control different aspects of a home environment, including light switches, power outlets, cameras, door locks, refrigerators, and thermostats. Some IoT devices are accessible through manufacturer-developed software across multiple operating systems, while others may be additionally accessed through third-party applications (e.g., video monitoring apps) or sub-applications. Some also may be accessible through a web-interface or Application Programming Interface (API) and may require an authentication process to gain access. The technical capabilities and interactive monitoring or control of comparable product offerings from different manufacturers may vary widely. Becoming familiar with a specific device will assist in identifying capabilities and limitations of that device. Functions to consider when investigating IoT devices include but are not limited to:

a. Home Automation
b. Security
c. Health
d. Fitness
e. Medical

5. Collection, Preservation, Acquisition and Analysis

5.1. Collection

When collecting any digital evidence it is best to first reference the *SWGDE Best Practices for Digital Evidence Collection.* In addition to those best practices, the following should be considered.

While documenting the scene, be sure to include the contents of a display or other device status indicators prior to taking any further action. Special attention should be paid to the preservation process and its impact on collection as well as the potential for additional evidence (e.g., latent prints, DNA, spatter evidence on the surface of devices, etc.).

5.2. Preservation

Just as the integrity of the data of more traditional devices needs to be preserved through write-blocking or other means, IoT devices similarly need information of interest protected and preserved.

IoT devices frequently communicate through a local area network, such as a home router or proprietary hub with wired or wireless access, and send or receive commands or information to/from cloud service providers. IoT devices can also communicate with other devices and services through Bluetooth, mobile data (cellular), and proprietary communication protocols (e.g., zigbee).

While attempting to isolate the device from the network, the collector also needs to be aware of trigger events. Trigger events may include, but are not limited to, manipulation of the device itself, motion/movement caused by collectors (which may be detected by connected sensors), manipulation of connected switches (e.g., light switch), verbalizing wake-words (e.g., stating that you found an Alexa device where “Alexa” is also the wake-word), making sounds above a detectable threshold, disconnecting the power and/or data connection, etc., and may cause an update/alteration of the data to be investigated and/or possibly alert the owner that a trigger event has occurred, and may cause the alteration and/or loss of volatile data of interest. Consideration should also be taken in preserving (e.g., by sending in a preservation order to the service provider) and capturing data that is possibly stored in the cloud, on mobile and other linked devices, and with other parties.

Although IoT devices may not currently store a significant amount of data on the device, they could provide information leading to data stored elsewhere, such as with a cloud service provider, personally owned computer, mobile device, or other IoT devices. Relevant data may be accessible from those devices. If additional devices are discovered, the same collection and acquisition procedures should be followed to secure/isolate the newly discovered devices.

One method of isolating a device from the network is to unplug the power to the device or remove the battery power. If the device cannot be powered off using these methods, use a Faraday bag/box or other network isolation method. In cases where IoT devices are hardwired into power supplies, and first responders lack either the knowledge or agency authority to remove the device, remove power at the circuit breaker, while being mindful of other devices of evidentiary interest that may be on the same circuit. Where the power cannot be removed, and the devices cannot be directly isolated from the network, removing Internet connectivity can be achieved by disconnecting the network cable, wireless access point, switch, router or modem. This action should be weighed against the potential impact of removing network connectivity to any non-targeted devices.

5.3. Acquisition

When performing an acquisition on IoT devices it is best to first reference the *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices*.

IoT devices commonly store data in one or more locations: the onboard memory of the IoT device, the connected mobile or computing device used for monitoring and control, other connected devices, the manufacturer's cloud, and with other parties/clouds. Analysis of network traffic of the device in its original environment, transactional logs from a manufacturer's device hub (if present), router or Internet service provider may establish the fact that data was sent or received at a specific date and time; however, the content is typically encrypted or otherwise protected/obfuscated.

Technical investigators seeking information directly from an IoT device may be required to utilize invasive, and potentially destructive, forensic techniques similar to those used for mobile devices (e.g., smartphones and tablets). See *SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition*, *SWGDE Best Practices for Chip-Off*, and *SWGDE Tech Notes regarding Chip-off via Material Removal Using a Lap and Polish Process*. However, in many cases, minimally invasive techniques (e.g., JTAG, ISP, UART) may be used to acquire even a full physical acquisition of the on-board memory of IoT devices. See *SWGDE Best Practices for Examining Mobile Phones Using JTAG*.

The majority of readily-accessible and retrievable data relating to an IoT device can be expected to reside within the manufacturer's cloud or designated cloud service provider, and should be retrieved utilizing the appropriate legal process. See *SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage*, and *SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers*. An API may allow an investigator to acquire data from the manufacturer's cloud or cloud service provider on their own without needing the manufacturer or cloud service provider to retrieve and provide it to them. Data obtained through the use of an API often contains additional information, metadata, and/or granularity, and thus should be considered regardless of whether similar data is available in other locations.

It is important to recognize that IoT devices may contain relevant data within volatile memory that is not generally accessible with today's technology and processing tools. At the time of this publication, limited research exists regarding the viability of unencrypted data recovery from volatile memory contained on IoT devices. Unless accessing volatile memory is necessary and critical to an investigation, IoT devices should generally be powered off.

5.4. Analysis

File systems that are commonly implemented on IoT devices may include the following: Unsorted Block Image File System (UBIFS), Yet Another Flash File System (YAFFS), Temporary File System (TMPFS), or proprietary file systems. There is little support for these file systems implemented in many digital forensics software suites, and oftentimes files will need to be manually carved by the examiner. Many of the files in these file systems that may be of interest are in the form of log files written in a clear text format that some forensic tools may be able to carve using their embedded functions.

IoT devices themselves may also store a variety of data that could be relevant to an investigation. Examples include connectivity logs, user information, time/date stamps, SSIDs (identifying current and possibly even previous networks where the device has established a connection), Bluetooth device addresses (of one or more of the devices that have been connected previously), access times, etc., and sometimes the password in clear text may be displayed. This information can be important lead material for an investigation, and could also be used to gain access to other devices that need to be considered for potential evidence.

Through the course of an examination and analysis of a mobile device that has connected to an IoT device, evidentiary data from the mobile device may be linked to data generated from the IoT device. In addition, data obtained from the cloud service provider associated with the IoT device may also provide evidentiary data to be analyzed.

6. Considerations

One of the major challenges in data acquisition from IoT devices is the lack of available training, tools, research documents, and collection procedures. Manufacturers may be reluctant to provide assistance or access to information regarding their proprietary intellectual property and may not be forthright regarding the device or user data available.

Relevant investigative data may be found on one, or across multiple IoT devices in a network, as they communicate and share data with each other. This data may be stored within a particular device, within a companion app stored on a mobile device or tablet, or with a cloud service provider. The totality of the scene, the nature of the investigation and the potential for a device to store data of interest should dictate the necessity to interrogate or seize particular IoT devices.

There may also be data located in unexpected places due to the integration of devices and platforms via third-party and other connective services. An example of this is “If This Then That” (IFTTT.com), which allows for triggers and data from one cloud (e.g., Amazon) to cause events and/or replicate data in another cloud (e.g., Google) in ways that may not have been originally intended or particularly advocated/featured by each manufacturer.

Many devices have the capability to record audio/video or perform live-listening which collectors and others on-site should be cognizant of, as it may alert the owner to the presence of people on-site and/or create concerns of recorded or broadcasted movement and conversations. If an IoT device records audio while investigators are on scene and the resulting speech-to-text conversion is inaccurate, the statements made could be misinterpreted.

Some devices may require additional safety considerations (e.g., wearables have a higher propensity of skin contact and may allow for transfer of blood-borne pathogens or biological hazards, while some devices may have moving parts that could cause bodily injury).

7. References

[1] Christopher Greer, Martin Burns, David Wollman, Edward Griffor, NIST Special Publication 1900-202 Revision 1 Cyber-Physical Systems and Internet of Things https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

History

Revision	Issue Date	Section	History
1.0 DRAFT	2020-01-15	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0	2020-09-17		Voted for release as final publication