The Internet of Things Disruptive Evolution for Intelligence Collection

Peter Chuzie (Mercyhurst University) and Michael Klipstein, PhD (Arnold A. Saltzman Institute of War and Peace Studies at Columbia University)

Introduction

What is the Internet of Things (IoT)? This is a loaded question that often changes based on who answers, but the simple answer is the network formed of any devices that can be or is currently connected to the Internet.[1] These devices range from pacemakers to cameras to refrigerators, among other consumer home products, and include any objects that are readable, recognizable, locatable, and addressable over the Internet as well as information sensing devices. They can communicate data and metadata, which is information about the actual data, over the Internet through many different vectors, including among others wired or wireless. A major goal of IoT is to enable an ecosystem of devices and connections anytime, anyplace, and with anyone over different networks and paths.[2] The IoT, bolstered by the continued production of different connectable devices, has resulted in a dramatic increase in the convenience of communication, productivity, and daily task efficiency to its users and society in general. Currently 23.14 billion devices connect to the Internet, and by the year 2020 that number will grow to 30.73 billion.[3] The forecasted popularity of these devices and associated applications continues to grow, resulting in

[1] Keyur K. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application, and Future Challenges," *International Journal of Engineering Science Computing*, 6, no. 5 (2016): 1–10.
[2] Ibid.
[3] "IoT: Number of Connected Devices Worldwide 2012–2025," Statista, 2018, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed September 28, 2018.

increased interconnectivity and advancements in every aspect of society.[4]

While the purpose of the IoT is to provide a platform for innovation and progress into the future, it is also vital to realize that many previously unknown opportunities for exploitation have accompanied the dramatic growth of these devices. These exploits can be seen most obviously on individual devices, where vulnerabilities are rampant and allow for control to be given up or used in undesired ways. A Hewlett and Packard (HP) study concluded that 70 percent of the most commonly used IoT devices are exploitable in one or more ways.[5]

Furthermore, our ability to collect and analyze large amounts of data and metadata is expanding at an unprecedented rate, leading to further risks as well as opportunities for intelligence gathering. This is now possible because 23.14 billion devices are currently acting as nodes producing data and associated metadata available for exploitation. These conditions allow for targeted reconnaissance missions to discover vital information on a target.

The proliferation of Internet-connected devices, combined with a widespread lack of security and operating system vulnerabilities, has set conditions for the Intelligence Community (IC) to reap copious quantities of data to facilitate operations. IoT weaknesses can facilitate the IC's ability and practice of collecting intelligence in a covert and effective way that can furthermore aid in intelligence targeting, operations, and decision making. In this paper we bring attention to a new form of intelligence for the IC, Temporal Intelligence (TEMPINT).

Dr. Shay Hershkovitz defines TEMPINT as a comprehensive approach to data analysis

[4] James Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype," *The Dialogue*, June 2015, https://tinyurl.com/y7dmutgz.

[5] "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," Material Safety Data Sheets (MSDSs) | HP® Official Site, July 29, 2014, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.W1gtF_ZFxPb. Accessed September 27, 2018.

from the many nodes (devices) that are now able to collect data or metadata.[6] An argument exists that this evolving form of intelligence may be better classified under electronic intelligence and more specifically technology electronic intelligence.[7] However, we argue it is important to recognize that TEMPINT can stand alone as a new paradigm of intelligence because it explores the new routes of intelligence collection that have only recently become possible due to the growing number of devices producing data. Whereas currently TEMPINT has limited adoption in small circles, Hershkovitz suggests that a seventh intelligence paradigm is emerging, based around the connectivity that is now offered by IoT.[8] While TEMPINT is an evolving paradigm and not widely accepted, it is certainly a viable option for integration into the IC.

A Princeton research effort describes a specific and targeted example of what is possible due to the increasing intrusion of IoT devices into a person's life.[9] The study illuminates how these machines may assist in human intelligence (HUMINT) recruitment. HUMINT operators are trained to develop a relationship with the targeted individual to eventually convince them to do the bidding of the case officer, such as divulging secrets from their own government. TEMPINT may hasten the process of helping understand when and wherein a target's daily routine would be most effective to make the first encounter. Beyond targeting, TEMPINT could also aid in identifying the target's interests and allowing for that to be a topic of discussion, to limit the amount of trial and error. For example, if through a person's metadata it is determined that a target is home and in

[6] Ian Little, "Internet of Things Surveillance," TEMPINT, https://tempint.net/internet-of-things-surveillance/. Accessed September 30, 2018.
[7] "ELECTRONIC INTELLIGENCE (ELINT) AT NSA," NSA.gov., 2009, https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/misc/assets/files/elint.pdf. Accessed September 30, 2018.
[8] Shay Hershkovitz and Roey Tzezana, "Connected Devices Give Spies a Powerful New Way to Surveil," *Wired*, June 03, 2017, https://www.wired.com/2017/01/connected-devices-give-spies-powerful-new-way-surveil/. Accessed October 31, 2018.
[9] Noah Apthorpe et al., "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," August 16, 2017, https://arxiv.org/abs/1708.05044. Accessed September 30, 2018.

their living room with the TV on, it is possible to infer what shows they may be interested in, based on the time of day and what is available. Furthermore, insecure IoT devices could allow the infiltration of a wireless network, allowing for greater access to data about the target that could be leveraged later. Such data may involve embarrassing information about the target, personal contacts, browsed websites, and other patterns of life. These, and other forms of data can assist the case officer with the recruitment of the target.

Moreover, it is also important to note how the use of vulnerabilities on IoT devices that allow for access to and control of a device can lead to discovering key factors of a target's personality that are otherwise difficult to find covertly. In HUMINT, it is essential for an officer to discover what potentially motivates an agent and use that to eventually convince or have the target convince themselves to provide secrets. Many different things motivate people, and case officers seek the main motivational triggers before recruiting an agent.[10] The acronym for one theory of target motivation is MICE (Money, Ideology, Compromise, Extortion or Ego); a more recent, and less widely taught, framework goes under the acronym RASCLS (Reciprocation, Authority, Scarcity, Commitment and Consistency, Liking, and Social Proof).[11] All the concepts within MICE and RASCLS draw on and take advantage of basic human behavior and psychology. These methods, in practice, are thought to increase the likelihood of successfully recruiting an agent by focusing on the aspects that most effectively motivate that target. Still, both MICE and RASCALS rely on information that is often collected through trial and error; the use of TEMPINT may lead to greater certainty of the information's reliability.

[10] Randy Burkett, "An Alternative Framework for . . ." CIA.gov, March 2013, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE to RASCLS.pdf. Accessed September 30, 2018.
[11] Ibid.

Indeed, private sector businesses have taken note of the market for the use of IoT to gather intelligence about what motivates people and are beginning to sell their abilities to use IoT devices as a form of surveillance and intelligence collection. For example, in Israel, a group of former military experts has started a business selling their skills and abilities to hack IoT devices for different governments.[12] They make it clear that they are not in the market of offensive cyber-attacks; rather, what they are doing is intelligence collection by playing the role of metaphorical binoculars for government agencies.

Taking Advantage of What Is Produced

The increased presence of IoT devices at all levels of society and the vulnerabilities that go with them has created an opportunity and illuminated the need for a new form of intelligence that would not otherwise be possible. It is highly likely that a new era of what the intelligence field is capable of is emerging, rooted in the expanding IoT. TEMPINT is considered, by some, to be a broad-based approach to the storage and analysis of mass quantities of data and metadata to aid in intelligence. However, we believe that TEMPINT makes possible a more targeted approach of capturing and analyzing data and metadata to assist with specific operations.

Furthermore, once obtained, the information could be applied to alter a target's decision making, by allowing analysts to study the patterns in which the target receives their information and then inject manipulated information to discreetly make them think a certain way. For example, TEMPINT could provide intelligence such as what applications a targeted decision maker uses to receive the information on which they base their decisions. This knowledge would allow an

[12] Thomas Fox-Brewster, "Alexa, Are You A Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," *Forbes*, July 17, 2018, https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/#327b45961d0c. Accessed September 27, 2018.

offensive cyber team to direct its efforts to inject altered information, with the intent to shift the decision maker's thought process on a given topic. This application of TEMPINT provides a cyber-team with the best avenue to manipulate a target without them knowing. More in-depth examples exist in the following section's case study, as well as some suggestions for how TEMPINT can assist in other areas of intelligence, such as human intelligence, or facilitate other operations.

A question that often arises is the legality of such actions by a US agency, whether domestically or abroad. According to the Communication Assistance for Law Enforcement Act, the US government can collect data, tap communication devices, and listen to network traffic in a domestic setting.[13] This is not to say that the government monitors every home and business communication, but that depending on the situation the US government agencies can legally collect information in targeted instances. An example of this would be when an individual living in the United States is identified as a possible threat to national security. Furthermore, conducting similar operations with targets outside the US border necessitates a detailed process outlined in Executive Order 12333.[14] This executive order lays out the exact steps an intelligence agency must take to obtain raw signal intelligence (SIGINT) from locations outside the US. In the end, while this process requires detailed logs on the operations and handling of the raw intelligence data, it is not illegal under US law to obtain the latter from foreign entities.[15]

[13] Edwards, Don. "H.R.4922 - 103rd Congress (1993-1994): Communications Assistance for Law Enforcement Act," Congress.gov. October 25, 1994, https://www.congress.gov/bill/103rd-congress/house-bill/4922. Accessed September 30, 2018.
[14] National Archives, "Executive Orders," National Archives and Records Administration, https://www.archives.gov/federal-register/codification/executive-order/12333.html. Accessed December 18, 2018.
[15] "E.O. 12333 Raw SIGINT Availability Procedures: A Quick and Dirty Summary," *Lawfare*, April 04, 2017, https://www.lawfareblog.com/eo-12333-raw-sigint-availability-procedures-quick-and-dirty-summary. Accessed October 31, 2018.

Privacy Attacks and Collection on Encrypted IoT Traffic

The previously mentioned Princeton University research effort illuminates how the increased presence of IoT devices creates an opportunity to covertly capture information on a specific target. The study shows how determining information about a target can be carried out by monitoring the network traffic at a target's home even if it is encrypted. In such an attack, metadata analysis leads to conclusions on a target's habits and surroundings despite encryption. Assuming the third party listening in is able to gain access to tier three network traffic either through the Internet Service Provider (ISP), using Wi-Fi eavesdropping, or has other nation-state surveillance capabilities, the attack only requires two main steps. The first is the use of Domain Name System (DNS) queries to identify what IoT devices are in the home. As seen in Figure 1, this is possible through requested server names from the DNS.[16] Merely finding the existence of an IoT device puts the target's privacy at risk, because knowing what devices are in the home can reveal private information about the target. An example of this would be the identification of a pacemaker or blood sugar monitor, as their presence effectively leads to the conclusion that the target has heart disease or diabetes.

Device	DNS Queries
Sense Sleep Monitor	hello-audio.s3.amazonaws.com
	hello-firmware.s3.amazonaws.com
	messeji.hello.is
	ntp.hello.is
	sense-in.hello.is
	time.hello.is
Nest Security Camera	nexus.dropcam.com
	oculus519-vir.dropcam.com
Amcrest Security Camera	amcrestcloud.com
	command-3.amcrestcloud.com
	ftp.amcrestcloud.com
	media-amc-1.hostedcloudvideo.com
	p2p.amcrestview.com
	dh.amcrestsecurity.com
Belkin WeMo Switch	prod1-fs-xbcs-net-1101221371.us-east-1.elb.amazonaws.com
	prod1-api-xbcs-net-889336557.us-east-1.elb.amazonaws.com
TP-Link Smart Plug	devs.tplinkcloud.com
	uk.pool.ntp.org
Orvibo Smart Socket	wiwo.orvibo.com
Amazon Echo	ash2-accesspoint-a92.ap.spotify.com
	device-metrics-us.amazon.com
	ntp.amazon.com
	pindorama.amazon.com
	softwareupdates.amazon.com

Figure 1: Device-based on DNS Query

The second step in this attack is reading the changes in the devices' traffic. It is essential

[16] Apthorpe et al., "Spying on the Smart Home."

to understand what an IoT device is specifically doing correlates to what servers they send requests to and the frequency at which they do so.[17] The information gleaned from understanding the location and frequency of requests is metadata. The actual data being transferred does not need to be disclosed. Through step two, analysts discern the target's patterns of life, which can further be used to facilitate intelligence operations. Looking at an even more specific example than the Princeton research effort is necessary to expand on this concept.

Specifically, traffic rates of a Nest Cam Indoor security camera can reveal multiple activities, such as when the security camera activates based on motion, if it was activated because the target left the home, or if the target is currently monitoring the camera feed. The assumption that the target is home is confirmed by watching the security camera traffic. This small amount of information allows for the planning of activities such as raids or simply entering the home to plant other devices. This alone does not seem like a remarkable feat, but when the traffic from the security camera is coupled with traffic from other devices, it allows for more precise inferences. For example, when the security camera traffic and the traffic from a Belkin WeMo Switch or smart plug—which allows control of lights and outlets remotely—are used together, patterns can be laid out on a person's habits around their home, specifically, when a target is in a specific room, and learning what the target is doing.[18] This can be determined by noting when the security camera activates based on motion and observing which Belkin WeMo Switches activate, resulting in an analyst knowing the room and the possible activity taking place.

Even more specifically, an inference of activity level and the action can occur based on the amount of motion detected by the camera and switches used. For example, if there is low motion

[17] Ibid.
[18] Ibid.

detection coupled with the Belkin WeMo smart plug behind the entertainment center being activated, then the analyst can assume that the target is watching TV or listening to music. The analysis would indicate when the target entered the room, based on increased motion followed by the activation of the smart plug behind the TV; similarly, a decrease in motion or the activation of other devices around the home would indicate the target had left the room. The security camera and the Belkin WeMo switch, then, allow for the covert collection of private contextual information on a target. This does not take into consideration the rest of the devices surrounding the target's home or inferring information from those devices. When analyzing, collating, and cross-referencing the other devices and the metadata in a home or around a person, a detailed picture of a target's life appears.

To better understand why TEMPINT can become a budding intelligence paradigm, it is necessary to examine why IoT devices have weak security and what information is vulnerable because of them. First and foremost, inadequate security is primarily due to pressure from the market. Functionality and production speed have greater importance than security in the race to get products into the market. As a result, many companies rush devices to market and do not incorporate security into the design process.[19] Proactive measures can be taken by companies to prevent some of the vulnerabilities, but these actions are difficult due to limited amounts of memory and hardware capabilities in IoT machines.[20] This leads to cutting corners on security measures since there is simply no extra room to add features on IoT devices. This is only one of the issues with security on IoT devices; others include firmware vulnerabilities, the proliferation

[19] Mohammed Tawfik et al., "A Review: The Risks and Weakness Security on the IoT," *Journal of Computer Engineering.* no. 12-17 February 2015, http://www.iosrjournals.org/.
[20] Wei Zhou and Yuqing Zhang, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," *Institute of Electrical and Electronics Engineers*, January 2018, arxiv.org.

of operating systems, and exploitable metadata. These are the most common issues, and they are leaving devices intensely vulnerable to exploitation. Furthermore, the ramifications of the attacks on these devices span the spectrum of everyday life, from residential baby heartrate monitors, cardiac devices at hospitals, webcams, DVR players, and even cars.

Vulnerabilities

All IoT devices have one thing in common, which is that they all must communicate to carry out their intended functions. This communication occurs between many devices such as device-controlled locks for your house, Smart TVs in your home connected to online media services, digital cameras uploading your pictures to social media platforms, or smart meters communicating your power consumption to the utility company.[21] Firmware is the software carrying out this communication. Firmware is a permanent software, programmed into read-only memory (ROM).[22] This software resides on the hardware device at the time of manufacturing and supplies instructions on how that hardware should execute low-level functions. Therefore, firmware that cannot update can hold a vulnerability.

This firmware vulnerability can take multiple forms, such as memory corruption flaws, command injection vulnerabilities, and application logic flaws. The most common exploitation of IoT devices occur when authentication vulnerabilities are bypassed a category of hack informally referred to as "backdoors." This occurs when there is an error in the authentication routine placed in the firmware either by accident or because a backdoor was maliciously programmed in. There are also cases where the manufacturer purposely places a backdoor, such as hardcoded credentials

[21] Yan Shoshitaishvili et al., "Firmalice: Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware," Proceedings of the 2015 Network and Distributed System Security Symposium, 2015. doi:10.14722/ndss.2015.23294.
[22] Ibid.

to gain access to preproduction or deployed devices to allow for development or maintenance. The issue of hardcoded credentials has been on SANS Top 25 security vulnerabilities list since 2011.[23] There is no question that this practice leaves devices vulnerable and has led to attacks such as the ones carried out by the Mirai Botnet,[24] which spread by taking advantage of unsecured IOT devices with hardcoded or easily guessable login credentials, such as admin/admin. Regardless of the reason for the backdoor's presence, it results in major security issues for the many deployed devices.

Operating System Proliferation and Recycling of Kernels

Over the past two decades, there has only been a handful of prevalent operating systems (OS): Windows, Android, IOS, and Linux. This limited number of standardized operating systems allows for OS vendors and security vendors, such as Bitdefender or Kaspersky, to direct their efforts into finding vulnerabilities on them specifically.[25] The standardization increases their ability to find vulnerabilities and produce patches promptly, as well as the ability of manufacturers to build stronger operating systems with greater security. At the same time, the recent explosion in popularity of IoT devices has brought many new and poorly secured operating systems into play. Some manufacturers produce devices with the poor practice of resurrecting discontinued OS kernels with known vulnerabilities.[26] These obsolete OS kernels—which are mostly Linux based, as they are open-source—are then modified for application-specific devices.[27] This practice allows

[23] "CWE/SANS TOP 25 Most Dangerous Software Errors." SANS Institute, https://www.sans.org/top25-software-errors#cat1. Accessed November 05, 2018.
[24] Manos Antonakakis, "Understanding the Mirai Botnet," 2017, http://ljournal.ru/wp-content/uploads/2017/03/a-2017-023.pdf. Accessed October 26, 2018.
[25] Marc Berejka, and Ari Schwartz, "Cybersecurity, Innovation, and the Internet Economy," *Journal of Research of NIST*, 2011. https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf. Accessed August 3, 2018.
[26] Nikolia Hampton, "The Working Dead: The Security Risks of Outdated Linux Kernels," *Computerworld*, https://www.computerworld.com.au/article/615338/working-dead-security-risk-dated-linux-kernels/. Accessed November 06, 2018.
[27] Ibid.

for lower research and development costs for new products and therefore increases profit.[28]

However, these short cuts can lead to the new devices being fundamentally weak in terms of security. Due to IoT device proliferation, it is an insurmountable task to monitor and fix vulnerabilities on all devices.[29] Also, many of these vulnerabilities are unfixable or much more difficult to fix due to the issues existing in the firmware.[30] Furthermore, it is not mandatory for companies to put resources into the security of devices and it is therefore a reasonable option to cut out in order to minimize the space needed. This minimization allows the producer to fit the IoT device's capabilities on a small amount of memory. .[31] These OS are also often proprietary and constructed as application specific. This niche development and use results in few, if any, personal security products or forensic capabilities available for a specific IoT device. In the end, the proliferation of small operating systems is creating issues in the monitoring of vulnerabilities, making it difficult to find them, much less create patches to fix them.

Metadata Exploitability

Metadata may be described as data about data.[32] Metadata supplies insight into a piece of data allowing for easy and deep understanding of what it means. It is even possible to determine what the actual data means by only looking at the metadata. This process is analogous to looking at the context around a situation to figure out what is occurring, similarly to how investigators collect information about a crime to determine the culprit.

---

[28] Ibid.
[29] Hemant Jain, "A Multitude of IoT Operating Systems Is Bad News for the Safety of the Internet," *Fortinet*, January 04, 2017, https://www.fortinet.com/blog/industry-trends/a-multitude-of-iot-operating-systems-bad-news-for-the-safety-of-the-internet.html. Accessed September 28, 2018.
[30] Lukas Kvarda et al., "Software Implementation of Secure Firmware Update in IoT Concept," *Advances in Electrical and Electronic Engineering*, vol. 15, 2017. doi:10.15598/aeee.v15i4.2467.
[31] Arslan Musaddiq et al., "A Survey on Resource Management in IoT Operating Systems," *IEEE Access 6* (February 21, 2018): 8459–82. doi:10.1109/access.2018.2808324.
[32] "Metadata," Merriam-Webster. https://www.merriam-webster.com/dictionary/metadata. Accessed September 30, 2018.

Metadata divides into three main categories: structural metadata, descriptive metadata, and administrative metadata.[33] Structural metadata describes how similar pieces of information are stored and indicates the sequence in which they are put together.[34] An abstraction of this concept would be how pages' number and order form a chapter in a book. Next, descriptive metadata is information about the content of a resource that aids in finding or understanding the greater meaning.[35] An example of this type of metadata can describe a film's title, director, and genre. Finally, administrative metadata is an umbrella term that further decomposes into technical metadata, preservation metadata, and rights metadata.[36] Technical metadata is used for decoding and rendering files, preservation metadata is used for long term management of files, and rights metadata is the intellectual property rights of the content to which it is attached. While this is an attempt to categorize metadata into main groups, it is important to understand that metadata also comes in many other forms.

Arguably having access to the metadata is just as valuable as having access to the actual data. Collecting metadata allows for analysis and conclusions even when the actual data is encrypted or inaccessible, as seen in the Princeton research effort. This became a public discussion point when the National Security Agency collected over 500 million call records in 2017, up from 151 million the year prior.[37] When discussing metadata, people are inclined to think of it as stored in massive quantities on the cloud and its applications. At the same time, this is not the only way to exploit metadata. Exploitation can occur in more targeted manner due to the streams of metadata

[33] Jenn Riley, "Understanding Metadata: What Is Metadata, and What Is It For?,." *Cataloging & Classification Quarterly* 55, no. 7–8 (2017): 669–70. doi:10.1080/01639374.2017.1358232.
[34] https://groups.niso.org/apps/group_public/download.php/17446/Understanding%20Metadata.pdf.
[35] Ibid.
[36] Ibid.
[37] United States, ODNI, Office of Civil Liberties, Privacy, and Transparency. "STATISTICAL TRANSPARENCY REPORT Regarding Use of National Security Authorities ~ Calendar Year 2017 ~," https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.

originating off every device that connects to the internet. This opportunity to observe metadata based on specific devices facilitates collecting and determining information regarding a targeted person and can be used to assist in HUMINT operations by providing covertly obtained details on a target.

Conclusion

The exploitable vulnerabilities of the IOT are currently able to aid in HUMINT and other operations by allowing a deeper understanding of a potential agent's patterns of life and motivations. While TEMPINT does not completely alter the fabric of intelligence, it does offer a new and more covert and comprehensive way of obtaining valuable information and intelligence. The Princeton research effort is only a simple and surface-level example of what is possible with the ever-growing IoT. Whether these future applications create the seventh paradigm of intelligence or integrate into existing disciplines, the possibilities are endless for the use of IoT to improve the effectiveness of the intelligence community.