Examining the Current State of the Field for IoT and Raspberry Pi Malware Forensics

Patrick Muradaz
CS8395-52: Digital Forensics
Vanderbilt University
Nashville, Tennessee
Patrick.Muradaz@Vanderbilt.edu

***Abstract* – This paper summarizes my comprehensive analysis of the current landscape of Internet of Things (IoT) and Raspberry Pi security and malware forensics. The objectives of this analysis include evaluating, compiling, and presenting some of the current security incident detection techniques and response strategies used in academia and industry. Key findings include manual methods for malware detection, as well as the growing use of Machine Learning (ML) algorithms in automating the detection of malware related anomalies. Through an analysis of incident response techniques discussed in the literature, this paper presents a standard procedure which overlaps heavily with the techniques we learned in this course. By synthesizing these findings, I hope to convey the current methodologies used in the malware forensics field, as they apply to IoT and specifically Raspberry Pi devices. I also plan to utilize much of the knowledge gained from writing this paper in my own work on maintaining security while using these devices.**

I. Introduction

The Raspberry Pi is a small, lightweight, resource efficient, single-board computer developed by the Raspberry Pi Foundation [1]-[3]. These small machines have emerged in recent years as a transformative force in the world of computing [1]. Originally conceived as a low-cost tool to promote computer science education, the Raspberry Pi has evolved into a versatile platform with applications spanning from at-home "maker" projects to enterprise-level solutions [1]-[3]. Its widespread adoption is attributed to its affordability, compact and efficient design, and accessibility, as well as the rise of IoT popularity among the general public [1]. In fact, I myself am currently using a Raspberry Pi to host my personal website (www.patrickmuradaz.com) from my home, and I have plans to expand my personal use of these devices.

Due to the increasing popularity of Raspberry Pi devices, there is a growing need to address security concerns associated with the platform [4]. Threat actors are constantly seeking vulnerabilities to exploit and as these devices spread into critical infrastructure, including industry automation, smart home IoT setups, and edge computing systems, the potential impact of security breaches is becoming more significant [5]. Thus, the use of malware forensics techniques on Raspberry Pi devices is imperative to ensuring the integrity and resilience of systems relying on them. Furthermore, I am personally motivated to research this topic by my need to ensure the security my own Raspberry Pi, and other IoT, devices.

This paper aims to delve into the current state of the field of IoT malware forensics with a focus specifically on Raspberry Pi forensics. We will explore and discuss detection techniques, incident response strategies, and emerging trends in securing the Raspberry Pi platform.

On a personal note, I plan to take the knowledge gained from writing this paper and apply it in my personal life by implementing or developing systems for monitoring and securing my own Raspberry Pi devices. Furthermore, as these devices continue to proliferate, I would not be surprised if I encounter them in my professional life, where I can apply the methods outlined in this paper as well.

II. Literature Review

The existing literature on Raspberry Pi security and malware forensics reflects the growing interest in understanding and addressing the unique challenges associated with the growing, yet already wide, adoption of the platform. The literature surveyed in this report spans from journal entries on general IoT security to industry reports on Raspberry Pi platform forensics.

Numerous studies have investigated security concerns specific to Raspberry Pi devices. For instance, Sainz-Raso et al., in their paper "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses" [5], emphasized the vulnerability of these devices to unauthorized access due to their plug-and-play nature, leading to most users never changing the vulnerable default settings. This study highlights the fact that any device connected to the internet, Raspberry Pi devices not excluded, is potentially vulnerable to penetration. Thus, further emphasizing the need to secure Raspberry Pi devices as they increasingly find applications in areas like industrial automation and smart homes.

Detection techniques in the context of IoT and Raspberry Pi malware forensics have also been explored in various studies. Victor et al., in their paper "An attribute-based taxonomy, detection mechanisms and challenges" [6], presented an IoT malware taxonomy while conducting an analysis of malware detection methods including methods applicable to Raspberry Pi devices. Their findings provide a concise synopsis of multiple detection methods while adding valuable insights into the challenges associated with the different detection approaches discussed.

Incident response strategies following security incidents have also been a subject of investigation. Kent et al., in their paper "Guide to Integrating Forensic Techniques into Incident Response" [7], provide a broad strokes explanation for how to utilize forensic techniques, from an IT rather than law enforcement point of view, while responding to security incidents. This research provides a concise source of information on relevant forensic technologies and practices that can be used to enhance incident response.

Fascinatingly, there is robust, and growing, utilization of Machine Learning techniques in malware forensics investigations on IoT and Raspberry Pi devices. HaddadPajouh et al., in their paper "A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting" [8], propose a novel method for using Recurrent Neural Network deep learning for the detection of malware in IoT devices.

In summary, the literature reviewed on IoT and Raspberry Pi security and malware forensics provides a solid foundation for the understanding and implementation of robust Raspberry Pi monitoring and incident response techniques. Such forensic investigation techniques can be utilized to improve the security and reliability of Raspberry Pi devices both in industry and at home.

III. Methodology

The methodology used in the selection of relevant literature for this work was relatively simple. If the work materially concentrated on IoT security or forensics and was published in a peer reviewed journal or produced and published by a reputable institution, including universities and industry organizations, then it was considered relevant. While the scope of this paper is more narrowly focused on Raspberry Pi devices, research into IoT security and forensics more generally was conducted and is included.

IV. Malware Detection Techniques

In my investigation of the literature on the field of IoT and Raspberry Pi malware forensics, some methods of investigation and incident detection were repeatedly discussed. An overview of the insights learned from my research is compiled in this section.

The two main methods I found for monitoring IoT and Raspberry Pi devices in the malware forensics field are as follows [6], [8-9], [13]:

1. Monitoring algorithms for known signatures

These algorithms include network intrusion monitoring, file binary scanning, malware signature matching in system calls, and limited heuristics to detect malware activity on IoT or Raspberry Pi devices. While this is a foundational technique in the field of malware forensics, it is being overshadowed and out competed by the newer methods for detecting malware in IoT ecosystems.

2. ML based algorithms for anomaly detection

These algorithms make use of Machine Learning advancements, specifically unsupervised data mining algorithms, to learn from mass amounts of malware forensics data. These ML models can then be employed live on systems to monitor for threats that have not been strictly cataloged. This provides an advantage over traditional signature or heuristic based algorithms by allowing for the detection of malware that may not have signatures that have been expressly documented. Furthermore, as more data on malware is collected, these systems can improve their own performance over time.

V. Incident Response Procedures

In my research, I repeatedly came across the same techniques for responding to the discovery of security incidents on IoT and Raspberry Pi devices. This section provides a more in depth look at the standard response techniques, many of which overlap with the techniques discussed in this Digital Forensics course.

Though not always presented in this order, there is consensus that the broad-strokes steps for responding to IoT security incidents are as follows [7], [10]-[11]:

1. Containing and preserving affected device(s)

While containment of the affected device(s) is imperative to prevent the spread of any malware, it is also important to attempt to preserve the state of the device(s). Device state preservation can be a deciding factor in determining the quality and quantity of evidence that can be gathered from the affected machines on the network. Furthermore, before evidence gathering is attempted, care should be taken to ensure that any malware present won't be able to jump to any machines used in the investigation.

2. Collecting and cataloging evidence data

Once the IoT or Raspberry Pi device is contained and in a safe state, the next step is to collect and catalog evidence from the device. As discussed in this course, care should be taken to both document the steps involved in the evidence gathering and ensure the secure containment of evidence once cataloged. Evidence should be stored in a secure location once taken off the IoT or Raspberry Pi device and the proper chain of custody should be documented and maintained.

3. Analyzing evidence and documenting steps

Furthermore, when accessing and analyzing the evidence gathered from the target devices, care should be taken not to alter the evidence in any way and all data accesses should be properly documented. Failure to maintain data integrity could lead to the loss of evidence or its inadmissibility in any litigation. Likewise, a lack of properly documented chain of custody and access could lead to evidence being dismissed in any prosecution of perpetrators.

4. Compiling and sharing conclusions

Once the relevant data has been gathered, secured, documented and analyzed, conclusions can begin to be drawn from the investigation. It is vitally important that these conclusions be shared with relevant institutions such as law enforcement agencies, software security organizations (i.e. the CVE Program and partner orgs like NIST) [12], and even affected customers or partners. The sharing of this kind of information not only ensures sound conclusions are being drawn, through the process of peer review, but it also makes all users affected ecosystems, like the Raspberry Pi safer. Through the sharing of this kind of information, law enforcement agencies can "go after" perpetrators and software communities can develop solutions and safeguards against the malware that was investigated.

5. Refining operations to prevent future incidents

Finally, once the investigation is concluded and findings have been disseminated, time should be spent on consolidating the new knowledge learned from the incident so as to plan a more secure path forward. Affected resources should be more thoroughly hardened against the malware which brought them down and should be subsequently brought back online.

Most of these techniques reflect the industry standards that were covered in this course. The need for device containment and preparation, the requirement of evidence data integrity and chain of custody documentation, and the specific analysis methods for gathering evidence from device memory dumps, hard drives, etc. were all heavily emphasized in class. It was heartening to find repeated examples of others in academia and industry relying on these methods for responding to security incidents. This gives me further confidence that following these processes and procedures in my personal interactions with IoT and Raspberry Pi devices will yield desired results.

VII. Challenges and Future Directions

Throughout my research, one challenge surfaced as the being the most impactful. That challenge being the absolute scale of the problem of IoT intrusion and malware. As stated in the introduction of this paper, there are threat actors constantly trying to gain unauthorized access to IoT and especially Raspberry Pi devices. As these systems become more complex, so to do the number of potential vulnerabilities rise. Furthermore, as tools like ChatGPT continue to permeate the general public, it is becoming easier and easier for individuals to write their own malware and set it loose on the internet. Therefore, as time goes on, the number of vulnerabilities, as well as the number of automated systems seeking out those vulnerabilities, will likely continue to rise.

The use of automation, and in particular Machine Learning algorithms, to combat these challenges is likely to also pick up speed. As ChatGPT-like tools have fueled growth in threat actor capabilities, these systems have also given legitimate actors more power to combat malicious software. I see the future of this field leaning more and more heavily into researching and implementing these autonomous and human-AI partner tools for forensic investigation and incident detection.

VIII. Conclusions

In summary, the field of IoT forensics, and specifically the growing field of Raspberry Pi malware forensics, is, like many industries today, moving increasingly towards the use of Machine Learning algorithms. This push towards high ML utilization may be especially impactful in this area of computer science due to its potential to be able to actually handle the increasing prevalence of malware on the internet, specifically the Internet of Things today. ML algorithms, put in place to monitor devices like the Raspberry Pi, and utilized to aid in incident response forensic investigations, will likely be instrumental in defending critical connected infrastructure in the years to come.

Closing on a personal note, this paper has given me the opportunity to dive deep into the exciting and varied field of IoT security and forensics generally and Raspberry Pi forensics specifically. I have learned quite a bit that surprised me, and I am looking forward to taking this newfound knowledge forward with me as I continue to tinker and build personal projects with my IoT and Raspberry Pi devices, and even potentially as I encounter these devices in the systems I help build and support in the future of my professional career.

References

[1] Johnston SJ, Cox SJ. The Raspberry Pi: A Technology Disrupter, and the Enabler of Dreams. *Electronics*. 2017; 6(3):51. https://doi.org/10.3390/electronics6030051

[2] https://opensource.com/resources/raspberry-pi

[3] https://www.raspberrypi.com/

[4] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.

[5] J. Sainz-Raso, S. Martin, G. Diaz and M. Castro, "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses," in IEEE Consumer Electronics Magazine, vol. 8, no. 6, pp. 47-52, 1 Nov. 2019, doi: 10.1109/MCE.2019.2941347.

[6] Victor, P., Lashkari, A.H., Lu, R. *et al.* IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. *Peer-to-Peer Netw. Appl.* **16**, 1380–1431 (2023). https://doi.org/10.1007/s12083-023-01478-w

[7] Kent K, Chevalier S, Grance T and Dang H 2006 *Guide to Integrating Forensic Techniques into Incident Response* (Gaithersburg: National Institute of Standards and Technology Special Publication) p 800

[8] Hamed HaddadPajouh, Ali Dehghantanha, Raouf Khayami, Kim-Kwang Raymond Choo, *A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting*, Future Generation Computer Systems, Volume 85, 2018, Pages 88-96, ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.03.007.

[9] Visu P., Lakshmanan L., Murugananthan V., Meenaloshini Vimal Cruz, Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance, Computer Communications, Volume 147, 2019, Pages 14-20, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2019.08.013.

[10] C. Itodo, S. Varlioglu and N. Elsayed, "Digital Forensics and Incident Response (DFIR) Challenges in IoT Platforms," 2021 4th International Conference on Information and Computer Technologies (ICICT), HI, USA, 2021, pp. 199-203, doi: 10.1109/ICICT52872.2021.00040.

[11] Rizal, R.; Riadi, I.; Prayudi, Y. Network forensics for detecting flooding attack on internet of things (IoT) device. Int. J. Cyber-Secur. Digit. Forensics 2018, 7, 382–390.

[12] https://www.cve.org/ProgramOrganization/ProgramRelationshipwithPartners

[13] Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, S.M. Ahsan Kazmi, Choong Seon Hong, Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges, Future Generation Computer Systems, Volume 92, 2019, Pages 265-275, ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.09.058.