HAL open science

Digital forensic acquisition kill chain – analysis and demonstration

Gunnar Alendal, Geir Olav Dyrkolbotn, Stefan Axelsson

To cite this version:

Gunnar Alendal, Geir Olav Dyrkolbotn, Stefan Axelsson. Digital forensic acquisition kill chain – analysis and demonstration. 17th IFIP International Conference on Digital Forensics (DigitalForensics), Feb 2021, Virtual, China. pp.3-19, 10.1007/978-3-030-88381-2_1 . hal-03764382

HAL Id: hal-03764382

https://inria.hal.science/hal-03764382v1

Submitted on 30 Aug 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Chapter 1

DIGITAL FORENSIC ACQUISITION KILL CHAIN – ANALYSIS AND DEMONSTRATION

Gunnar Alendal, Geir Olav Dyrkolbotn and Stefan Axelsson

Abstract The increasing complexity and security of consumer products pose major challenges to digital forensics. Gaining access to encrypted user data without user credentials is a very difficult task. Such situations may require law enforcement to leverage offensive techniques – such as vulnerability exploitation – to bypass security measures in order to retrieve data in digital forensic investigations.

This chapter proposes a digital forensic acquisition kill chain to assist law enforcement in acquiring forensic data using offensive techniques. The concept is discussed and examples are provided to illustrate the various kill chain phases. The anticipated results of applying the kill chain include improvements in performance and success rates in short-term, case-motivated, digital forensic acquisition scenarios as well as in long-term, case-independent planning and research scenarios focused on identifying vulnerabilities and leveraging them in digital forensic acquisition methods and tools.

Keywords: Digital forensic acquisition, security vulnerabilities, kill chain

1. Introduction

Several digital forensic process models have been proposed in the literature [2]. Regardless, a generic digital forensic process can be viewed as comprising four phases: seizure, acquisition, analysis and reporting. The digital forensic acquisition phase covers the retrieval of digital forensic data from seized devices and other data sources. Its main goal is to gain access to data for forensic analysis. Clearly, digital forensic acquisition tasks are changing as technology advances, but the overall goal is the same – accessing data in a forensically-sound manner [4, 7].

Embedded devices and online services are important sources of digital evidence in criminal cases, which makes digital forensic acquisition a priority for law enforcement. In recent years, smartphone vendors such as Apple and Samsung have instituted mechanisms for securing user data. Data in their devices is often encrypted and secured against a variety of attacks, local as well as remote. Gaining access to encrypted user data without user credentials is a very difficult task.

Garfinkel et al. [9] mention encryption as posing major challenges to law enforcement as they conduct digital forensic investigations. Arshad et al. [3] discuss the impacts of mandatory encryption and increased focus on privacy on the effectiveness of digital forensics. Balogun et al. [5] estimate that encryption alone prevents the recovery of digital forensic data in as much as sixty percent of cases that involve full disk encryption. In the FBI-Apple encryption dispute of 2015-16, Apple denied the FBI's request to create special firmware that would enable the recovery of user credentials from an iPhone 5C seized in a terrorist investigation [3]. Apple considered product security and user privacy to be more important than supporting the terrorism investigation.

Since law enforcement cannot rely on assistance from vendors to bypass security mechanisms in their products, the best option is to leverage offensive techniques to retrieve protected data in digital forensic investigations. Specifically, it is necessary to apply sophisticated techniques to discover published (n-day) and unpublished (0-day) vulnerabilities in the targets, and exploit them to acquire forensic data.

The idea of law enforcement leveraging published vulnerabilities is a concern because law enforcement assumes the role of an attacker in order to pursue justice. However, discovering and holding on to undocumented vulnerabilities in order to bypass security mechanisms are even more concerning. New vulnerabilities should be reported promptly to the affected vendors to enable them to mitigate risks, but this would prevent the continued use of the vulnerabilities. The conflicting interests between offensive and defensive uses of security vulnerabilities are not new. Indeed, they have been discussed publicly [8] and are addressed by the U.S. Government [21]. Whether to restrict discovered vulnerabilities for offensive use or disclose them for defensive purposes is determined by a vulnerability equities process, where U.S. agency representatives gather to evaluate and decide the fate of new vulnerabilities discovered by government agencies [21]. This policy is understandably controversial [19, 20].

This research does not take a stand on the vulnerability equities dilemma. Rather, it seeks to inform law enforcement about the possibility of discovering vulnerabilities in electronic devices and leveraging

them to acquire forensically-sound data in criminal investigations. It focuses on a methodical approach called the "digital forensic acquisition kill chain," which is based on the "intrusion kill chain" concept used in computer network defense [10]. The intrusion kill chain is a systematic process for targeting and engaging an adversary to achieve the desired security effects [10]. The digital forensic acquisition kill chain turns this around – it is a systematic process for law enforcement (acting as an adversary) to target electronic devices using offensive techniques to facilitate digital forensic acquisition.

Law enforcement has some advantages when developing and employing offensive techniques. These include access to resources as well as police authority (ability to seize devices). Unlike attackers, law enforcement may have the time to execute offensive actions and impose patch prevention. A seized device may be fully patched with no known vulnerabilities at the time of seizure. However, the same device becomes vulnerable in the future as n-day vulnerabilities are published and 0-day vulnerabilities are discovered. Since law enforcement can prevent seized devices from receiving updates, it can leverage both types of vulnerabilities in digital forensic acquisition.

2. Related Work

Several digital forensic process models that focus on practitioners and the use of digital evidence in court have been proposed. The Advanced Data Acquisition Model [1] addresses the needs of practitioners and the expectations of courts for formal descriptions of the processes undertaken to acquire digital evidence. Montasari [17] has proposed a standardized model that enables digital forensic practitioners to follow a generic approach that can be applied to incident response as well as criminal and corporate investigations. In an attempt to further address the need for a generic digital forensic investigation process for use in the three domains, Montasari et al. [18] have proposed the Standardized Digital Forensic Investigation Process Model that draws on existing models and renders them generic enough for wide applicability. However, although digital forensic investigative processes are discussed, neither the scope nor the details of key processes such as examination and analysis are provided.

The three models address the need for trustworthy and court-accepted methods and processes. The focus is on ensuring the reliability of digital evidence presented in court using formal, standardized processes. In contrast, the digital forensic model presented in this chapter differs substantially from the three models in that it concentrates on using of-

fensive techniques for digital forensic acquisition. However, the proposed model will have to be augmented in the future to guide the development of trustworthy, court-accepted methods.

3. Digital Forensic Acquisition Kill Chain

The primary goal of the proposed digital forensic acquisition kill chain is to articulate a structured process for developing new digital forensic acquisition methods based on offensive techniques. It is intended to improve performance and success rates during the time-constrained, case-motivated development of digital forensic acquisition methods as well as during the long-term case-independent development of digital forensic acquisition methods that take into account trends in consumer adoption of technology.

3.1 Background

Hutchins et al. [10] have specified a kill chain model that describes the network intrusion phases employed by advanced adversaries, often referred to as advanced persistent threats. Engaging a model that describes adversarial intrusion phases to inform defensive postures reduces the likelihood of success on the part of attackers. Specifically, detecting patterns that are signs of a campaign supports proactive computer network defense. This is referred to as intelligence-driven computer network defense, where identifying intrusion patterns facilitates responses before compromise occurs. The kill chain phases specify the goals and content as an adversary goes from intelligence gathering on a potential target to achieving full compromise and the ultimate goal of penetrating the target (e.g., exfiltrating sensitive data). Such a model is required because advanced adversaries invest considerable intellectual and technical resources to penetrate high value targets. The kill chain paradigm has proven to be very valuable, and several new ideas and models have been proposed [6, 11–13, 16].

The intrusion kill chain of Hutchins et al. [10] is motivated by the U.S. military targeting doctrine that encompasses six phases: find, fix, track, target, engage and assess. They adapted the targeting doctrine to computer network intrusions by introducing new phases. The resulting kill chain phases are: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. This methodical way of describing the expected adversarial phases views computer network defense from the adversaries' perspectives, facilitating detection by predicting the subsequent phases and the ability to execute proactive defensive operations. The research described in this

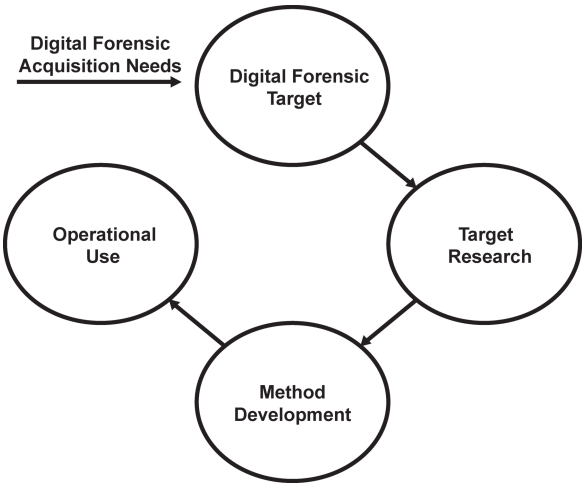

Figure 1. Generic digital forensic acquisition needs.

chapter adapts the intrusion kill chain to facilitate offensive actions in digital forensic acquisition scenarios.

3.2 Kill Chain Overview

Figure 1 shows a simplified view of digital forensic acquisition using offensive techniques. The proposed digital forensic acquisition kill chain adapts the original kill chain to specify a methodology for using offensive techniques in digital forensic acquisition, where law enforcement assumes the role of the adversary and seized devices (evidence containers) are the targets. It brings an intelligence-driven perspective to applying forensic data acquisition methods as well as researching and developing new methods.

Figure 2 shows the nine phases of the proposed digital forensic acquisition kill chain. The phases are: reconnaissance, identification, surveillance and vulnerability research, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

The nine phases are grouped and generalized according to the digital forensic acquisition needs in Figure 1. The initial reconnaissance phase considers the target of digital forensic acquisition. The next two phases, identification, and surveillance and vulnerability research, focus on the discovery of possible digital forensic acquisition solutions (vulnerabilities). The weaponization and delivery phases cover the development and realization of the discovered vulnerabilities. The last four phases,

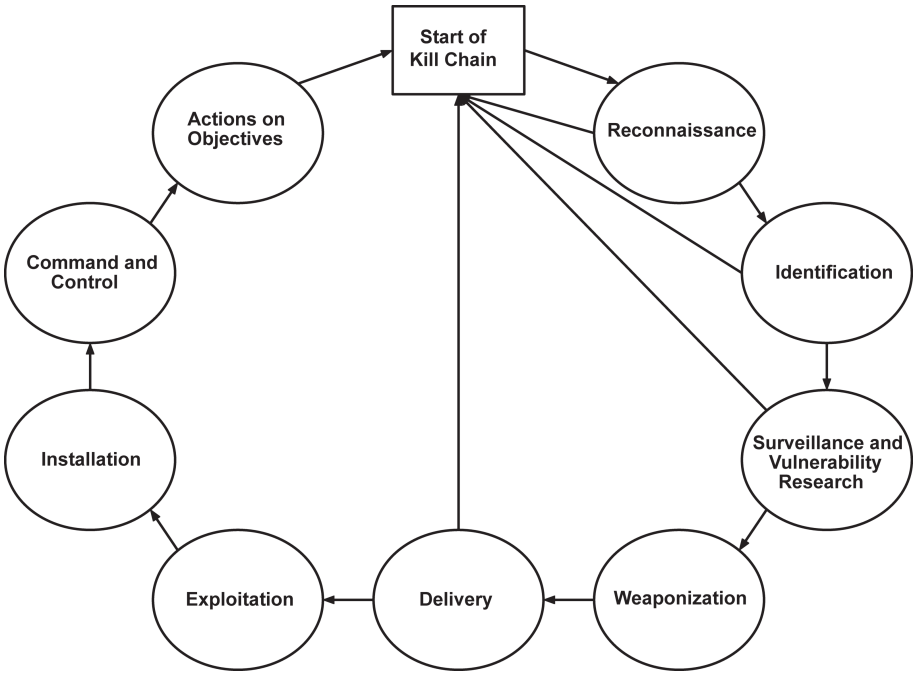

Figure 2. Digital forensic acquisition kill chain phases.

exploitation, installation, command and control, and actions on objectives, deal with operational issues.

A digital forensic acquisition kill chain is spawned in two general scenarios:

- **Case-Motivated Scenario:** This scenario is driven by a case-motivated need for a digital forensic acquisition method targeting a specific entity (e.g., device or service). Because digital forensic investigations are event-driven, law enforcement may not have applicable methods or be able to predict applicable methods for all possible scenarios. The kill chain focuses on solving the concrete challenge of acquiring forensically-sound data from the device or service, but it may spawn new kill chains to solve the sub-challenges that materialize. Several kill chains could be spawned in parallel and resources moved back and forth between them as the case foci and priorities change. The overall goal of a case-motivated kill chain is to apply digital forensic acquisition to a specific device or service.

- **Case-Independent Scenario:** This scenario is driven by a case-independent, intelligence-driven need for a digital forensic acquisition method that addresses a class of challenges. As the results of several case-motivated kill chains are obtained, a trend in the challenges encountered, such as the encryption of user data, could spawn its own kill chain. A challenge in another kill chain phase, say exploitation, could spawn a separate kill chain that focuses entirely on the challenges encountered during exploitation. A challenge related to a class of devices (e.g., from a specific vendor) could spawn a vendor-specific kill chain. The vendor could be Apple or Samsung, and the targets could be smartphones, services or components such as processors and flash memory chips that are common to vendor products or services. The overall goal of a case-independent kill chain is to improve the performance of subsequent case-motivated kill chains by leveraging intelligence, knowledge, methods and tools.

Upon considering the general digital forensic acquisition needs in Figure 1, the completion of the reconnaissance, identification, surveillance and vulnerability research, or delivery phases could result in the kill chain being terminated. For example, as shown in Figure 2, a kill chain covering a trending device would terminate at the end of the delivery phase because no operational needs exist. Of course, the completion of a phase could initiate the next phase, or the phase could spawn a new kill chain.

The initial phases of reconnaissance and identification could be performed at the start of an investigation to set the direction of the investigation and prioritize resources. An initial kill chain could spawn several new (sub) kill chains that address specific devices and services. This would, of course, depend on the amount of resources available. Prioritization and resource management of the sub kill chains would be a continuous process as the investigation proceeds.

Kill chains can also be applied to trending challenges that are detached from concrete investigations. This is motivated by the fact that many current digital forensic acquisition challenges are too complex to be solved given the limited time and resources available for investigations. The kill chains would focus on longer term challenges that need dedicated resources and prioritization. The available resources would be put to best use at all times, even in the case of parallel kill chains where resources would be shifted between kill chains as priorities change and commonalities are discovered. The expected results are increased knowledge of trending challenges, increased security expertise and new digital forensic acquisition methods.

3.3 Kill Chain Phases

This section discusses the nine phases of the digital forensic kill chain in detail.

Reconnaissance. The reconnaissance phase focuses on the collection of information that would support the selection and prioritization of devices and services. This phase should be kept short if it is used as part of a specific case, where it would concentrate on selection and prioritization, and the estimation of the likelihood of success of a digital forensic acquisition method. In a case-independent scenario, the reconnaissance phase is more openly defined and may choose to focus on any target device or service of interest.

Multiple kill chains are expected to be initiated and terminated during the reconnaissance phase. Also, a single kill chain may spawn several kill chains for the identified devices and services. The basic idea is that the reconnaissance phase is based on the available information and information that is obtained easily.

Identification. The challenge to developing a new forensic acquisition method is approached in a bottom-up manner. The focus is on identifying forensic data of value and the layers of security features that may prevent its access (e.g., encryption could be the first layer to bypass).

Volatility of forensic data is always an issue. Embedded devices often keep log files and unencrypted app data in random access memory (RAM) only. Thus, the digital forensic acquisition method must take into account the fact that a device cannot be power cycled. Addressing this challenge follows a different path in the remaining phases and would require a separate kill chain.

Note that two challenges – encryption and volatility – have been identified during this phase. Thus, two kill chains would be created and resource allocation decisions have to be made to best address the challenges.

Surveillance and Vulnerability Research. During the surveillance and vulnerability research phase, existing vulnerabilities, techniques, tools and services are investigated. Also, resources are allocated to discover new vulnerabilities. Conducting activities in parallel can be efficient with regard to time. However, in order to optimize resources and not reinvent existing vulnerabilities and methods, the following two sub-phases are recommended:

- **Sub-Phase 1:** This short intelligence sub-phase focuses on gathering information about the identified challenges from open and closed sources. The goal is to discover published vulnerabilities that are potential candidates for direct use or are avenues for new vulnerability research. The sub-phase should not focus on the resource-intensive task of rediscovering low-level details about potential vulnerabilities, but only collect and prioritize potential vulnerabilities based on the available information.

- **Sub-Phase 2:** This sub-phase focuses on the active search for tools, services and vulnerabilities to address the identified challenges. It would also include a separate vulnerability research effort to discover new vulnerabilities.

The surveillance and vulnerability research phase is divided into two sub-phases in order to have a lightweight first sub-phase with a short time frame and low human resource needs. The results provide a basis for allocating resources to the much more intensive second sub-phase.

The second sub-phase has the most uncertainty with regard to resource needs and likelihood of attaining the end goal of a digital forensic acquisition method. However, in the event of success, a method that leverages a new vulnerability would have a longer life span than a method based on a published vulnerability. As multiple kill chains would be executed simultaneously during this sub-phase, efficient management of resources is required.

An example of a new kill chain is the discovery of new vulnerabilities and the acquisition of knowledge about existing vulnerabilities. Information about fixed vulnerabilities may be found at vendor web sites and in change logs and published patches. Although the information about a patched vulnerability often lacks the detail needed to isolate and trigger the vulnerability, an experienced vulnerability researcher would be able to obtain the information in a reasonable period of time. This could be hours, days or months depending on the complexity of the technology and vulnerability. Additionally, since a vulnerability may not always be convertible to a successful exploit, it is necessary to research several vulnerabilities. Identifying and studying vulnerabilities, and developing exploits are time consuming; also, predicting the resource needs is difficult. Therefore, it is important to balance time, resources and success potential between discovering new vulnerabilities and rediscovering known vulnerabilities by studying patches.

Weaponization. Weaponization involves the development of a working exploit from a new or existing vulnerability, a task that can be com-

plex and potentially unrealizable. The weaponization of a vulnerability is hard to generalize, but it can be similar to the software development cycle. The steps proceed from developing a proof of concept to creating a production-quality exploit chain with quality assurance that minimizes the chance of failure when applied to digital forensic acquisition. A crucial step is to ensure that the method is forensically sound and complies with the law and established digital forensic standards [15].

Efforts in the weaponization phase also need to consider the users of the digital forensic acquisition method, especially their levels of expertise and access to special equipment and tools. Other considerations include ease of use, access to updates and support. Additionally, it is important to be aware that the type and sensitivity of the vulnerability may limit the number of users and cases where it can be applied.

Delivery. The delivery phase focuses on developing the channel or channels for executing the weaponized exploit. These could be physical interfaces such as USB, SPI, JTAG, UART and I2C or wireless channels such as Wi-Fi, Bluetooth and near-field communications (NFC). Even side channels that can be used to inject inputs into key components are potential delivery options.

Exploitation. During the exploitation phase, the focus is on applying the developed digital forensic acquisition method in a criminal case. Actions performed in this phase must adapt to the context of the device or service. Since the phase is operational in nature, it should consider all aspects of using the method, including device or service state, legality, special requirements, assumptions that do not hold (e.g., user credentials might be known), operational security and digital forensic principles. Special care should be taken if the exploitation is destructive (e.g., chip-off data acquisition), which would leave the device in a state where it cannot be returned to its owner after the investigation.

Installation. The installation phase is mostly concerned about the footprint required to achieve the goal of forensic data acquisition. A RAM-only installation is a good option when the goal is to acquire data from long-term storage and conform to forensically-sound principles [15]. Since a component installed in a device or service environment for forensic acquisition purposes may become a part of the acquired evidence, isolating and documenting the component and its behavior are vital in court proceedings. An alternative to installing a component is to enable device features to accomplish the same goal. For example, enabling `adb` and gaining root privileges on an Android smartphone would pro-

vide the required access. When executing custom code on a device, it is important that the footprint be as small as possible to reduce negative forensic impacts on volatile RAM storage. Alternatively, the available device debugging features could be leveraged.

Command and Control. In the command and control phase, control has already been gained over the execution and/or data on the target device or service. This could involve a generic interface such as a login shell with root access, arbitrary code execution or security feature (e.g., screen lock) bypass. Ideally, this phase should be detached from the earlier phases because it marks the start of the actual acquisition of digital forensic data. Activities could involve the use of special tools and commands that may not have been employed in the earlier device- or service-specific exploitation and installation phases. The advantage of separating command and control from other phases is the reuse of knowledge, code and tools. A login shell with root access may apply the same tools to acquire data from diverse Android devices, but activities in the exploitation and installation phases for Android devices from different vendors could be totally different and leverage completely different vulnerabilities to reach the command and control phase.

Actions on Objectives. The last phase in the kill chain is to simply execute the final goal of performing the digital acquisition to obtain data of forensic value from the device or service.

4. Case-Motivated Kill Chain Example

This section demonstrates the use of a digital forensic acquisition kill chain in a case-motivated scenario where law enforcement is interested in extracting data of forensic value from a broadband router seized at a crime scene. The data could constitute log files with network activity, including Wi-Fi logs pertaining to connected devices during a specific time period. The data could be used to gain information about the connected devices that would be identified by their MAC addresses. The device is a Zyxel router (model no. p8702n), which has a MIPS architecture and runs a uClinux-based operating system [14].

Reconnaissance. Open-source intelligence and reconnaissance activities for the Zyxel p8702n router focused on various discussion forums and on the availability of its firmware, which was eventually downloaded from a server located at `stup.telenor.net/firmwares/cpe-zyxel-p8702n`. Two firmware files, `100AAJX13D0.bin` and `100AAJX14D0.bin`, were obtained along with their `README` files.

Because change logs often contain valuable information about security patches, older files that were present on the server were also sought. The older files were downloaded from `web.archive.org`.

Thus, the reconnaissance phase yielded useful information from public forums along with publicly-available firmware files and their change logs.

Identification. Forensic data with the most value was expected to reside in the flash memory of the Zyxel p8702n router. However, like many low-end embedded devices, the Zyxel p8702n router stores much of its data, including logs, in RAM only. This means that valuable forensic data could be lost if the device were to be turned off. This discovery is important because it impacts how the device should be seized; specifically, the device should not be powered down before digital forensic acquisition. Addressing the RAM memory acquisition challenge requires a separate kill chain.

Thus, two directions have to be pursued and a decision must be made about where to focus the available resources. The RAM data was assumed to be more valuable, so the corresponding kill chain was pursued – gaining access to the Zyxel p8702n router RAM data without turning off or restarting the device.

Surveillance and Vulnerability Research. The shorter intelligence phase (sub-phase 1) sought to obtain information about acquiring RAM data, possibly by exploiting a vulnerability. In the case of the Zyxel p8702n router, a valuable source for vulnerability information was determined to be the vendor's patch reports. Because older firmware files and change logs were available, a reasonable approach was to examine the change logs for hints of security issues.

The examination revealed that firmware version `100AAJX7D0` had major security fixes. Therefore, the previous firmware version `100AAJX5D0` was inferred to have the security vulnerabilities.

The focus of the complex and resource-demanding sub-phase 2 was to rediscover the vulnerabilities patched in firmware version `100AAJX7D0`. This required firmware versions `100AAJX5D0` and `100AAJX7D0` to be unpacked and the differences between the two versions to be identified.

The analysis revealed a difference in the boot sequence, where a critical security vulnerability was exposed in the older version by a login shell on a serial console. The problem was that the login process `/bin/smd` had an SIGTSTP vulnerability – when `Ctrl-Z` was entered on the console, a `/bin/sh` shell was provided with the same credentials as the `/init` process. This enabled root access to the Zyxel p8702n router.

Thus, sub-phase 2 of the surveillance and vulnerability research phase resulted in the rediscovery of a vulnerability. However, the vulnerability still had to be triggered.

Weaponization. During the weaponization phase, it was determined that the vulnerability was not particularly difficult to exploit. The vulnerability was exploited by accessing the Zyxel p8702n router console and sending the SIGTSTP signal by entering `Ctrl-Z`. Thus, the goal of the weaponization phase was to discover an access method to the serial console of the Zyxel p8702n router; in this case, via the UART interface on the circuit board. The key result is that this could be done without powering off the Zyxel p8702n router.

Delivery. The delivery phase was also relatively simple. It involved sending `Ctrl-Z` over the attached serial console to the Zyxel p8702n router. The delivery was performed via the UART protocol using a standard RS232-to-USB serial converter and a `putty` terminal emulator.

Exploitation. Since the Zyxel p8702n router had to be powered on at all times, the digital forensic acquisition had to be performed without power-cycling the device. The considerations during the exploitation phase involved the ease of physical access to the device, speed of the operation (especially if it had to be covert), risk and likelihood of failure.

Important operational decisions had to made during the exploitation phase to prevent *ad hoc* decision making during the subsequent phases. Since the objective was to acquire data from RAM, any actions performed on the device (even as root) would affect the RAM (e.g., potentially overwriting valuable freed memory in RAM). Therefore, a bare minimum footprint had to be maintained.

Installation. The installation was restricted to digital forensic acquisition. Persistent access did not have to be maintained after the serial interface was detached. Therefore, no other tools were installed.

Command and Control. Root access to the Zyxel p8702n router rendered the digital forensic acquisition goal within reach. The command and control phase determined that only a few commands would be executed using on-device tools to preserve RAM content.

Actions on Objectives. At this point, all the digital forensic acquisition challenges were isolated and addressed. The final phase merely

involved the actual digital forensic acquisition of RAM data in the Zyxel p8702n router.

Note that the primary goal was to focus on the raw RAM in order to preserve freed memory data and structures. Since this goal was achieved, it was not necessary to pursue the lower priority goal focusing on temporary RAM-only filesystems that are common in many Linux distributions, or the even lower priority goal focusing on flash memory.

5. Conclusions

Criminal investigations are increasingly hindered by strong security mechanisms that prevent forensically-relevant data from being acquired from electronic devices and services. Absent technical assistance from vendors and service providers, the only option for law enforcement is to leverage offensive techniques such as vulnerability exploitation to bypass security measures and acquire evidentiary data. The notion of law enforcement becoming an attacker in order to pursue justice is controversial, but police authority and search and seizure laws and regulations may support such actions.

The digital forensic acquisition kill chain described in this chapter adapts the kill chain employed in computer network defense to articulate a systematic methodology for using offensive techniques in digital forensic acquisition, where law enforcement assumes the role of the adversary and the seized devices and services of interest (evidence containers) are the targets. Applying the digital forensic acquisition kill chain provides many benefits – improvements in performance and success rates in short-term, case-motivated, forensic data acquisition scenarios as well as in long-term case-independent, intelligence-driven planning and research scenarios focused on identifying vulnerabilities and leveraging them in the development of novel digital forensic acquisition methods and tools.

Future research will focus on validating the digital forensic acquisition kill chain. The case study described in this chapter focused on a single device. Realistic field evaluations with diverse and more complicated challenges will provide valuable guidance on adjusting the kill chain phases. At this time, a single kill chain model has been proposed for case-motivated and case-independent scenarios. These scenarios appear to pull the kill chain model in different directions. As a result, future research will focus on creating separate digital forensic acquisition kill chain models for the two types of scenarios.

Acknowledgement

This research was supported by the IKTPLUSS Program of the Norwegian Research Council under R&D Project Ars Forensica Grant Agreement 248094/O70.

References

[1] R. Adams, V. Hobbs and G. Mann, The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice, *Journal of Digital Forensics, Security and Law*, vol. 8(4), pp. 25–48, 2012.

[2] A. Al-Dhaqm, S. Razak, R. Ikuesan, V. Kebande and K. Siddique, A review of mobile forensic investigation process models, *IEEE Access*, vol. 8, pp. 173359–173375, 2020.

[3] H. Arshad, A. bin Jantan and O. Abiodun, Digital forensics: Review of issues in scientific validation of digital evidence, *Journal of Information Processing Systems*, vol. 14(2), pp. 346–376, 2018.

[4] R. Ayers, S. Brothers and W. Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2014.

[5] A. Balogun and S. Zhu, Privacy impacts of data encryption on the efficiency of digital forensics technology, *International Journal of Advanced Computer Science and Applications*, vol. 4(5), pp. 36–40, 2013.

[6] S. Caltagirone, A. Pendergast and C. Betz, The Diamond Model of Intrusion Analysis, Technical Report ADA586960, Center for Cyber Threat Intelligence and Threat Research, Hanover, Maryland, 2013.

[7] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Elsevier, Waltham, Massachusetts, 2011.

[8] M. Daniel, Heartbleed: Understanding when we disclose cyber vulnerabilities, *White House Blog*, The White House, Washington, D.C. (`obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities`), April 28, 2014.

[9] S. Garfinkel, Digital forensics research: The next 10 years, *Digital Investigation*, vol. 7(S), pp. S64–S73, 2010.

[10] E. Hutchins, M. Cloppert and R. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, in *Leading Issues in Information Warfare and Security Research*, J. Ryan (Ed.), Academic Publishing, Reading, United Kingdom, pp. 80–106, 2011.

[11] G. Ioannou, P. Louvieris, N. Clewley and G. Powell, A Markov multi-phase transferable belief model: An application for predicting data exfiltration APTs, *Proceedings of the Sixteenth International Conference on Information Fusion*, pp. 842–849, 2013.

[12] M. Khan, S. Siddiqui and K. Ferens, A cognitive and concurrent cyber kill chain model, in *Computer and Network Security Essentials*, K. Daimi (Ed.), Springer, Cham, Switzerland, pp. 585–602, 2018.

[13] R. Luh, M. Temper, S. Tjoa and S. Schrittwieser, APT RPG: Design of a gamified attacker/defender meta model, *Proceedings of the Fourth International Conference on Information Systems Security and Privacy*, pp. 526–537, 2018.

[14] D. McCullough, uCLinux for Linux programmers, *Linux Journal*, vol. 2004(123), article no. 7, 2004.

[15] R. McKemmish, When is digital evidence forensically sound? in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 3–15, 2008.

[16] B. Messaoud, K. Guennoun, M. Wahbi and M. Sadik, Advanced persistent threat: New analysis driven by life cycle phases and their challenges, *Proceedings of the International Conference on Advanced Communications Systems and Information Security*, 2016.

[17] R. Montasari, A standardized data acquisition process model for digital forensic investigations, *International Journal of Information and Computer Security*, vol. 9(3), pp. 229–249, 2017.

[18] R. Montasari, R. Hill, V. Carpenter and A. Hosseinian-Far, The Standardized Digital Forensic Investigation Process Model (SDFIPM), in *Blockchain and Clinical Trial*, H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou and H. Al-Khateeb (Eds.), Springer, Cham, Switzerland, pp. 169–209, 2019.

[19] T. Moore, A. Friedman and A. Procaccia, Would a "cyber warrior" protect us? Exploring trade-offs between attack and defense of information systems, *Proceedings of the New Security Paradigms Workshop*, pp. 85–94, 2010.

[20] B. Schneier, Disclosing vs. hoarding vulnerabilities, *Schneier on Security Blog* (`www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html`), May 22, 2014.

[21] The White House, Vulnerabilities Equities Policy and Process for the United States Government, Washington, D.C. (`trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External-UnclassifiedVEPCharterFINAL.PDF`), November 15, 2017.