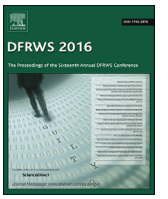
Digital Investigation 18 (2016) S87–S96

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin



DFRWS USA 2016 — Proceedings of the 16th Annual USA Digital Forensics Research Conference

Deleting collected digital evidence by exploiting a widely adopted hardware write blocker

Christopher S. Meffert*, Ibrahim Baggili, Frank Breitinger

Cyber Forensics Research & Education Group, Tagliatela College of Engineering, ECECS, University of New Haven, 300 Boston Post Rd., West Haven, CT, 06516, United States

Keywords:
Digital forensics
Digital forensic tool testing
Hardware write blocker
Root access
Anti-Forensics
Vulnerability
Frameworks
Gismo
NIST
TD3

A B S T R A C T

In this primary work we call for the importance of integrating security testing into the process of testing digital forensic tools. We postulate that digital forensic tools are increasing in features (such as network imaging), becoming networkable, and are being proposed as forensic cloud services. This raises the need for testing the security of these tools, especially since digital evidence integrity is of paramount importance. At the time of conducting this work, little to no published anti-forensic research had focused on attacks against the forensic tools/process. We used the TD3, a popular, validated, touch screen disk duplicator and hardware write blocker with networking capabilities and designed an attack that corrupted the integrity of the destination drive (drive with the duplicated evidence) without the user's knowledge. By also modifying and repackaging the firmware update, we illustrated that a potential adversary is capable of leveraging a phishing attack scenario in order to fake digital forensic practitioners into updating the device with a malicious operating system. The same attack scenario may also be practiced by a disgruntled insider. The results also raise the question of whether security standards should be drafted and adopted by digital forensic tool makers.

Introduction

There is an ever growing need for collecting digital evidence from media, especially from hard drives. As of 2004, claims have been made that eighty to ninety percent of cases in the United States involve some sort of digital evidence (Rogers, 2006b). Since 2004, no doubt, computing devices have increased in ubiquity and decreased in size. A logical assumption can be made that this percentage may continue to increase, thus, upholding the notion for the necessity of digital evidence collection in an accurate and efficient manner.

Digital forensic investigation is defined by Ieong (2006) as “a process to determine and relate extracted information and digital evidence to establish factual information for judicial review”. If data on a disk drive can be considered evidence then one may argue that the whole disk should be considered evidence; both physically and digitally. If this is to be the case then it becomes critical that the integrity of the data is not compromised especially for the admissibility of evidence into the court of law (Argy and Mason, 2007; Accorsi, 2009; Givens, 2003). Landwehr (2001) defines integrity conceptually as “assuring that digital information is not modified (either intentionally or accidentally) without proper authorization”.

Methods, procedures and tools exist to ensure that evidence maintains its integrity throughout the digital forensics process. The two prominent tools in use today are software and hardware write blockers, with hardware write blockers being the preferred tool of choice.

* Corresponding author.
E-mail addresses: cmeff1@unh.newhaven.edu (C.S. Meffert), IBaggili@newhaven.edu (I. Baggili), FBreitinger@newhaven.edu (F. Breitinger).
URL: http://www.unhcfreg.com/, http://www.FBreitinger.de/

http://dx.doi.org/10.1016/j.diin.2016.04.004

A software write blocker is a tool that handles write blocking at the software level via the mounting process. It ensures that the Operating System (OS) mounts the hardware with write blocking flags set to on. Software write blockers are easier to design and implement, but unless the write blocking settings are handled at the lowest levels possible (BIOS as an example), and the OS is secure, they tend to be easier to subvert (Lyle and Black, 2005).

A hardware write blocker is a device that attaches a host device (like a hard disk) typically to a forensic workstation with the purpose of preventing any possible modifications to the evidence drive before, during, and after the acquisition process. The name hardware write blocker comes from how the device prevents the write function from executing as it uses techniques for blocking writes to the media.

A hardware write blocker typically operates by breaking the bus that connects the hard drive to the host machine into two segments; a bus segment between the host and blocking device and another bus segment from the blocking device to the evidence drive. The two bus segments may consist of different protocols. One can be Small Computer System Interface (SCSI) and the other Advanced Technology Attachment (ATA). Once the devices are connected and the blocking device is powered on, all commands are intercepted by the blocking device. Once intercepted, the blocking device will filter any write commands from passing (Lyle, 2006). The Tableau TD3 used in this research is an example of a hardware unit that includes a hardware write blocker.

Initially, hardware write blockers were devices that simply blocked writes to disks after being connected to forensic workstations when digital media was either acquired or mounted for triage (Rogers et al., 2006). As products in this space continued to advance, devices became smarter, more efficient and packed with features. Devices such as disk duplicators with built-in hardware write blockers were developed to allow for use in forensic labs as well as on the field. As systems increased in size and storage, the need to accomplish network forensic imaging emerged. To tackle this challenge, these devices adopted networking features.

With this advancement came many benefits such as remote access via a user interface and the ability to remotely image a drive on a disk of interest. Tableau's TD3 model is one of these devices, and allows for browsing drives that are attached directly to the write blocker via the Internet Small Computer System Interface (iSCSI) protocol.[1] iSCSI works on top of the Transport Control Protocol (TCP) enabling the SCSI command to be delivered end-to-end over Local Area Networks (LANs), Wide Area Networks (WANs) or the Internet. The Ditto Forensic FieldStation from WIEBETECH[2] is another hardware write blocker and disk duplicator that allows for remote cloning and duplication of drives via iSCSI. Both devices allow for creating and modifying users and the settings associated with them.

Since most devices are proprietary and costly, an open source hardware write blocker and forensic imager alternative was developed by the Digital Forensics Investigation Research laboratory (DigitalFIRE) at University College Dublin (UCD). Their project aimed at providing law enforcement in underdeveloped countries with a cheap yet effective substitute to expensive hardware write blockers. The open source hardware write blocker and imager encourages practitioners to purchase the necessary parts, download an open source application, and assemble a device titled FIREBrick. The cost for its parts is approximately $200[3] (Tobin and Gladyshev, 2015).

Nevertheless, provided that evidence integrity is of paramount importance in digital forensics, we argue that it is important to test the security of these devices given their wide adoption by government and industry – especially due to their increased features and network connectivity. In this work the following contributions were accomplished:

- We present a primary study focused on the security of these hardware imaging and write blocking devices (In specific we tested the most widely adopted one – the Tableau TD3).
- We illustrate how one may gain root access to such equipment.
- We construct and share the results of a preliminary proof of concept attack against the integrity of the imaging process when using the Tableau TD3.
- We raise the much needed awareness within the digital forensics community for integrating security testing as part of the digital forensic tool testing process since digital forensic tool testing focuses on the accuracy and correctness of the tools without accounting for plausible security weakness.

The rest of the paper is organized as follows. In Sec. Related work, a review of the related literature is shared, setting the motivation for this work. In Sec. Tableau TD3, the widely adopted device used in our study – the Tableau TD3 – is presented. Sec. Methodology delineates the approach of gaining root access to the TD3, the constructed integrity attack scripts, and the testing approach used to validate the integrity attack. In Sec. Results the results are presented, followed by the limitation of our work in Sec. Limitations. The work presented is then discussed in Sec. Discussion, and concluded in Sec. Conclusion. Lastly, we open the door for future research in Sec. Future work.

Related work

The following sections review works related to digital evidence integrity. These works underpin the motivation for exploring the security of the TD3 device.

[1] https://www2.guidancesoftware.com/products/Pages/tableau/products/forensic-duplicators/td3.aspx (last accessed April 11, 2016).

[2] https://www.cru-inc.com/products/wiebetech/ditto_forensic_fieldstation/ (last accessed April 11, 2016).

[3] http://digitalfire.ucd.ie/?page_id=1011 (last accessed April 11, 2016).