Hardware Write Blocker Security Exploration

Christopher Meffert, Ibrahim Baggili, Frank Breitinger

Graduate Research Assistant, UNHcFREG Member
Presenting @ DFRWS, Seattle, WA, 2016

University of New Haven
Cyber Forensics Research & Education Group

UNHcFREG

Agenda

- Introduction
- Related work
- Contributions
- Methodology
- Experimental results
- Discussion
- Limitations
- Future work

Introduction

UNHcFREG

- 80 to 90% legal cases involve digital evidence (Rogers, 2006)
- Imaging is critical
- It was the goal of this research to explore and test the security of these devices
  - The Tableau TD3 was chosen as a proof of concept, as it is widely used by industry

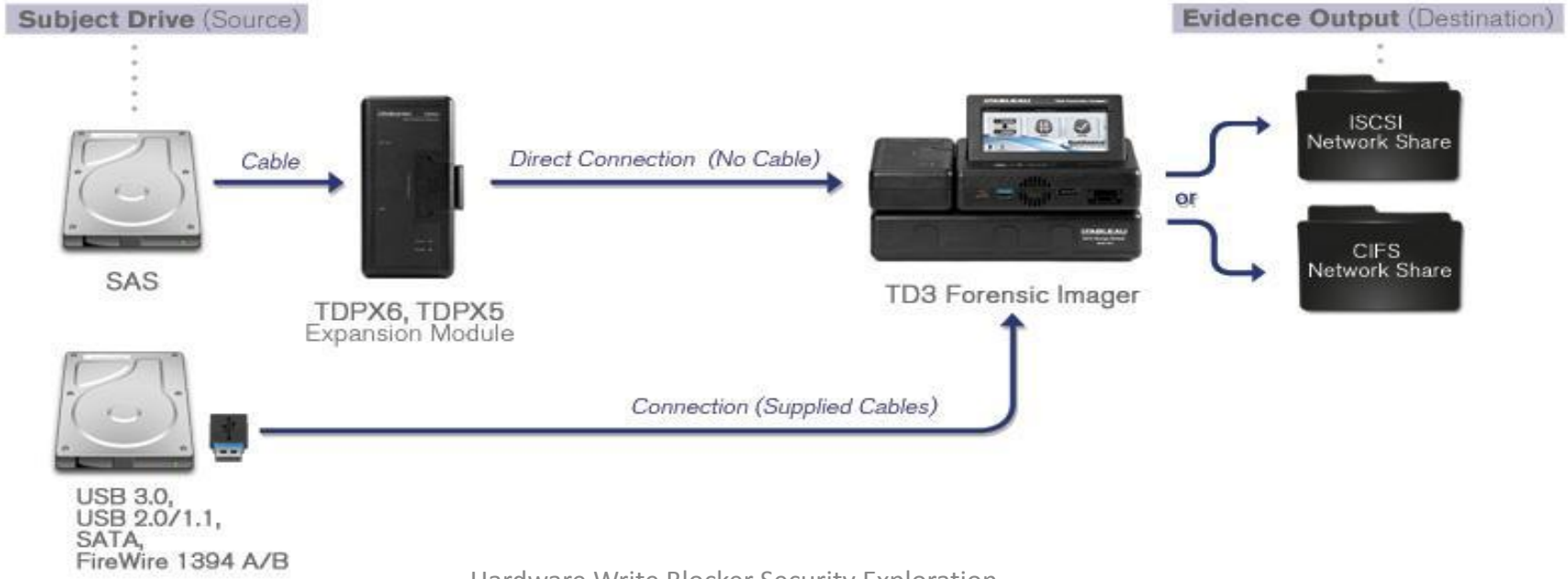
Contributions

- This research will highlight the oversight and the need to test forensic tools
- Little work has been done in this domain we hope that by showing this proof of concept others will also begin to think about this problem as a true threat

Note: This is not an attack against the tool and manufacturers

Related work

- Digital Forensic Tool Testing
  - Forensic tool growth
  - National Institute of Standards and Technology (NIST) is responsible for the bulk of tool testing
  - Department of Homeland Security did their own testing of the forensic soundness of TD3 (DHS, 2014)

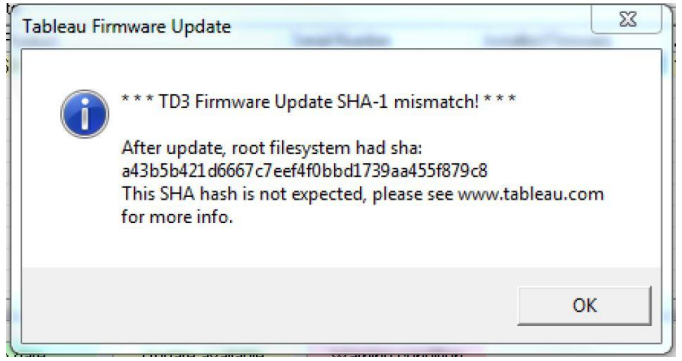


Related work cont.

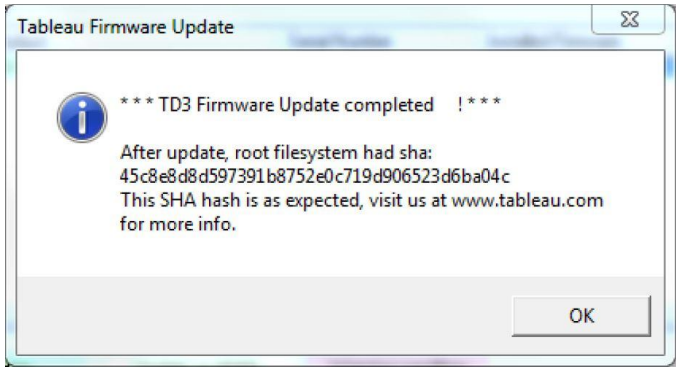
- Anti Forensics
  - Only about 2% of published research is related to anti forensics (Baggili et al.2012)
    - data hiding
    - artifact wiping
    - trail obfuscation
  - Examples of tool security
    - Ditto forensic field station [3]
    - Encases's software suite

Methodology

- Gaining root access
  - Reconnaissance on device
  - Explore SD card
- Attack Vector (Firmware Update)
  - Firmware Update can be modified
  - Modified Firmware Flags
- Integrity attack scripts construction
  - Developed scripts to corrupt data



Before Firmware Modification



After Firmware Modification

Methodology cont.

Algorithm 1 Process detection and execution of integrity attack using DD.

```
previous ⇐ 0
while TRUE do                                                    ▷ Loop runs until 'break'
    current = getCurrentCPUUsageOfGismo();                       ▷ Value between 0 and 100
    if ((current − previous) < −10) && (current < 1) then        ▷ Checks CPU drop (curr − prev) & done (curr < 1)
        execProgram();                                           ▷ In our test, we run DD
        Break Loop;
    else
        sleep(1);                                                ▷ Sleep for 1 s to not use all CPU
        previous ⇐ current;
    end if
end while
```

Methodology cont.

UNHcFREG

Testing

Phase I (Pre firmware update)

- Source drive hashed
- Disk to disk duplication
- Destination drive hashed

Phase II (Post firmware update script not running)

- Duplicate process Phase I

Phase III (Post firmware update script running)

- Duplicate process Phase I & II
- Destination drive hashed again

CALIBRATION (script not running) PHASE HASH VALUES

Destination drive hash pre-firmware update (Phase I)

MD5:1ac…137b4e

SHA1:76393…bfb502

Destination drive hash post-firmware update (Phase II)

MD5:1ac…137b4e

SHA1:76393…bfb502

SCRIPT RUNNING PHASE HASH VALUES

Destination drive hash shown to the user (Phase III)

MD5:1ac…137b4e

SHA1:76393…bfb502

Actual hash value of the destination drive

MD5:d352609773231d546b29766611ee0035

SHA1:f8976d0b3b2f8dfbe3936e417bb03182902723e7

Discussion

How plausible is physical access?

- Social engineering
- Insider threat

Ramifications of compromising device like TD3

- Potential for compromising the authenticity of the collected evidence
- Hash values accepted method to validate the authenticity of a duplication (Kerr 2001)
- Possible network security breach (reverse shell, viruses, malware)

Discussion Cont.

- Possible Phishing Vectors
  - Email
  - Twitter feed

XRY & XAMN v6.13.1

M

MSAB <info@msab.com> sent by MSAB <info=msab.com@mail1.atl161.mcsv.net>
Monday, March 30, 2015 at 12:07 PM

Enterprise Vault Manage Add-ins...

Dear Customer,

We are contacting you to let you know that both XRY & XAMN v6.13 have been updated.

There is a newer v6.13.1 release available which can be downloaded from the MSAB Customer Portal:
http://msab.us2.list-manage1.com/track/click?u=779f73ecba

For full details of the changes please visit the News section of the MSAB Customer Forum:
http://msab.us2.list-manage1.com/track/click?u=779f73ecbac2c

For a video about what's new in XRY v6.13 please visit:
http://msab.us2.list-manage1.com/track/click?u=

Kind Regards

Sales Support
MSAB
www.msab.com

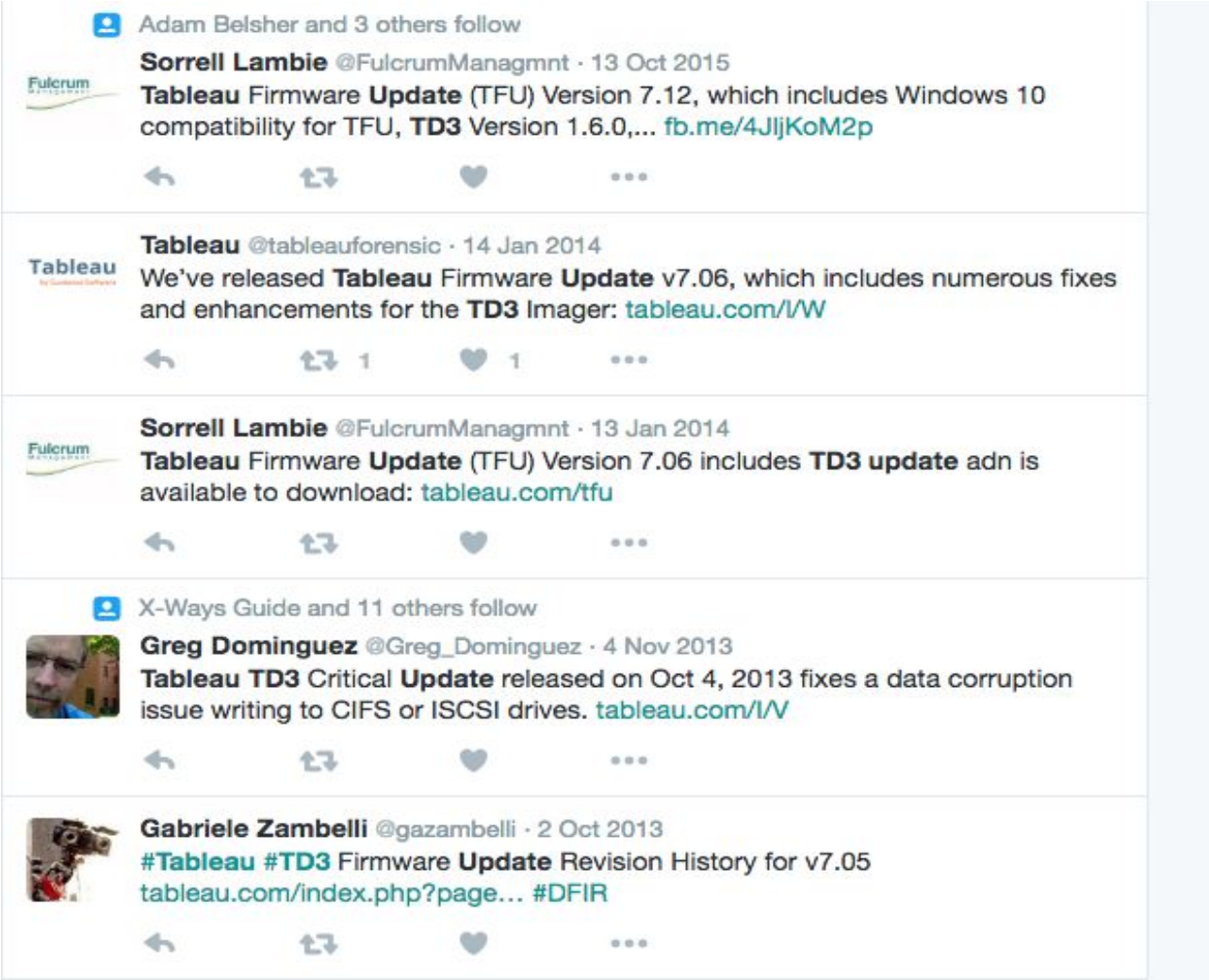
==========

You received this email because you are recorded as having opted into our marketing email updates. If you are no longer interested in receiving these emails then please use the links below to unsubscribe.

Unsubscribe from this list:
http://msab.us2.list-manage.com/unsubscribe?u=779

Our mailing address is:
MSAB
Hornsbruksgatan 28
Stockholm SE-117 34

Discussion Cont.



Limitations

- Physical access required
- Firmware Upgrade Hash Error (circumvented as seen above)
- Digital signature warning (Windows)
- DD command wipes drive (would be better to flip a bit or remove particular types of files)
- OS on device is limited in its tools, and some are proprietary. This limits the potential exploits as well as requires a more detailed approach (reverse engineering)

Future Work

- Continue to test security of TD3
  - Web Interface
  - Further develop script
  - Network (reverse shell)
- Explore the domain of where penetration testing meets forensic tools
  - Develop a methodology for testing security in forensic tools
  - Develop standards for both hardware and software forensic tools

Questions?

- Thank you to Google for the scholarship
- Thank you DFWRS community for your time and input
- Thank you to University of New Haven for feedback
- Thank you to MITRE for your feedback

Resources

[1] Rogers, M. (2006). Dcsa: A practical approach to digital crime scene analysis. West Lafayette, Purdue University, .

[2] DHS (2014). Test results for digital data acquisition tool:tableau td3 forensic imager version 1.3.0. URL: https://www.dhs.gov/sites/default/files/publications/ 508_Test%20Report_NIST_Tableau%20TD3%20Forensic%20Imager%201.3.0_August%202015_Final_0.pdf.

[3] Baggili, I., BaAbdallah, A., Al-Sa, D., & Marrington, A. (2012). Research trends in digital forensic science: An empirical analysis of published research. In Digital Forensics and Cyber Crime (pp. 144{157). Springer.

[4] Ditto Exploit http://www.cru-inc.com/products/wiebetech/ditto_forensic_fieldstation/