Scientific Working Group on
Digital Evidence

SWGDE UEFI and its Effect on Digital Forensics Imaging

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE UEFI and its Effect on Digital Forensics Imaging

Table of Contents

1. Scope

This document provides a general overview and guidance with regard to Unified Extensible Firmware Interface (UEFI) and its effects on media imaging. The implementation and standards for UEFI are currently evolving and changes to this document are anticipated as this technology and its standards develop and mature. The intended audience for this document is the trained forensics professional who may encounter UEFI for the first time.

2. Overview

The original model for computer forensics media imaging in a subject computer involved pulling the plug, removing the hard drive, and imaging the drive. Best practices have evolved over time to include live imaging of computers. This evolution has continued as computer operating environments, both hardware and software, have changed. Currently, one option for acquiring an image of a computer drive includes booting the subject machine into a controlled software environment using prepared media. Booting from forensic distribution media (e.g., Raptor, Windows FE) provides the examiner with the ability to image the drive(s) of the subject machine from a controlled boot environment. Recent changes in hardware and software architecture have affected the viability of this option.

Hardware and software vendors have become more attuned to the ways in which a computer system can be compromised by malware and hackers. The conventional Basic Input Output System (BIOS) and Master Boot Record (MBR) boot process created an environment ripe for exploitation by malicious code loaded at boot time. Malware infections impacting the boot process include key loggers installed at the boot-code level, boot-from-malicious-device attacks, and other mechanisms. Additionally, advances in storage device size, virtualization, and other technological changes have started to push the limits of the BIOS/MBR boot model.

The UEFI boot model was developed to fix some of the shortcomings of conventional BIOS/MBR based boot models, and is used in conjunction with technologies, such as Trusted Platform Module (TPM), to provide a trusted computing environment. The intent is to create an environment that resists hijacking or infection of the boot process by either hardware or software means.

A side effect of UEFI implementation is that it may not permit the subject machine to be booted from external media. This restriction removes a valuable acquisition method from forensic examiners.

UEFI implementation on a subject machine may be indicative of one or more challenges to the forensic imaging and analysis process, including:

- UEFI restriction against booting from media not native to the subject machine thereby preventing the use of forensic boot environments.
- Full disk encryption in conjunction with a TPM, which binds the hard drive to the computer in which it is installed.

3. Background

As modern computers surpassed the design limitation of the aging BIOS/MBR boot systems, many extensions and enhancements to the original BIOS were made. The Globally Unique Identification (GUID) partition scheme and Extensible Firmware Interface (EFI) boot framework were developed as a replacement allowing for continued growth in disk capacity and providing a more flexible interface between the OS and the underlying firmware/hardware.

The traditional MBR partitioning scheme supports a maximum of 2TB sized disk partitions. The GPT architecture supports much larger disks up to eight (8) Zettabytes (i.e., 8 Billion TB). The maximum number of possible partitions has been increased to 128 on a GPT disk.

Most of the mainstream forensic tools recognize GPT disks and provide access to file systems on GUID partitions. The forensic analysis possibilities for extracting useful information are much greater than previously possible with BIOS/MBR style partition tables. The GPT provides unique identifying information for both disks and individual partitions.

4. SecureBoot

SecureBoot is a feature of UEFI 2.2 requiring the operating system that is attempting to load to have a valid certificate. The UEFI firmware will then validate this certificate against a database of known signatures that are loaded into firmware by the OEM at the time of manufacture. The OEM can and may update a list of revoked certificates with firmware updates in the future. Prior to allowing the loading of any boot code, the signature must be validated against this database and if none is found the system will not boot from the device presented. As of the time of this writing there are two signed Linux kernels (Ubuntu 12.10, Redhat Fedora 18) in existence but none of the forensically sound distributions have adopted one yet.

At the time of the writing of this document, Microsoft supports SecureBoot for: Windows 8, 8.1 and Server 2012, 2012 R2

5. Workarounds

Currently, UEFI and its related technologies are inconsistently implemented by hardware and software vendors. Hardware vendors may build-in varying degrees of UEFI support on a model-by-model basis. They may also include setup menus that enable UEFI features to be turned off, with the intention of allowing access, or even boot access, to non-UEFI boot media. The terminology for these options may vary, but can include “Compatibility Support Mode (CSM) mode” or “legacy mode”. The result is that it may be possible, in some cases, to turn off UEFI-based external boot restrictions while maintaining access to the subject device’s original boot media.

Should it not be possible to disable UEFI boot restrictions, the following workarounds may be possible:

- Remove the hard drive and image it externally (physical acquisition).
- Image the media while the OS is running (logical acquisition).
- Boot to a UEFI compatible boot environment, which MAY include:
    - Windows PE
    - Windows To Go

Best practices and universal precautions should still be followed when imaging UEFI systems (see SWGDE Best Practices for Computer Forensics for more details).

6. Resources

Booting UEFI imaged media with/without GPT using VMWare - http://justaskweg.com/?p=1093

Forensic Analysis of GPT disks and GUID partition tables – http://www.digitalforensics.ch/nikkel09.pdf

UEFI and the TPM: Building a foundation for platform trust - http://resources.infosecinstitute.com/uefi-and-tpm/

UEFI and secure boot in depth - http://www.zdnet.com/uefi-and-secure-boot-in-depth-7000012138/

UEFI Firmware - http://technet.microsoft.com/en-US/library/hh824898.aspx

Boot Windows PE in UEFI or legacy BIOS mode - http://technet.microsoft.com/en-us/library/dn293283.aspx

Install Windows PE to Run from a Drive (Flat Boot or Non-RAM) - http://technet.microsoft.com/en-us/library/hh825045.aspx

History

Revision	Issue Date	Section	History
1.0	09/13/2013	All	Completed drafting document; voted to release as a Draft for Public Comment.
1.0	09/14/2013	All	Formatted and released as a Draft for Public Comment.
1.0	01/16/2014	All	Voted as Approved by SWGDE; no changes made.
1.0	02/06/2014	All	Formatting and tech edit performed for release as Approved.
1.0	--	--	Updated document per current SWGDE Policy with: new disclaimer, removed Definitions section, and corrected SWGDE hyperlinks. No changes to content and no version/publication date change. (9/27/2014)