Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Digital Investigation

The growing impact of full disk encryption on digital forensics

Eoghan Casey [a,*], Geoff Fellows [b], Matthew Geiger [c], Gerasimos Stellatos [d]

[a] cmdLabs, 1101 E. 33rd Street, Suite C301, Baltimore, MD 21218, United States
[b] LG Training Partnership, United Kingdom
[c] CERT, United States
[d] CACI International, United States

ARTICLE INFO

Article history:
Received 16 March 2011
Received in revised form
17 September 2011
Accepted 24 September 2011

Keywords:
Digital forensics
Full disk encryption
Hard drive encryption
Volatile data
Memory forensics

ABSTRACT

The increasing use of full disk encryption (FDE) can significantly hamper digital investigations, potentially preventing access to all digital evidence in a case. The practice of shutting down an evidential computer is not an acceptable technique when dealing with FDE or even volume encryption because it may result in all data on the device being rendered inaccessible for forensic examination. To address this challenge, there is a pressing need for more effective on-scene capabilities to detect and preserve encryption prior to pulling the plug. In addition, to give digital investigators the best chance of obtaining decrypted data in the field, prosecutors need to prepare search warrants with FDE in mind. This paper describes how FDE has hampered past investigations, and how circumventing FDE has benefited certain cases. This paper goes on to provide guidance for gathering items at the crime scene that may be useful for accessing encrypted data, and for performing on-scene forensic acquisitions of live computer systems. These measures increase the chances of acquiring digital evidence in an unencrypted state or capturing an encryption key or passphrase. Some implications for drafting and executing search warrants to dealing with FDE are discussed.

1. Introduction

When digital investigators encounter encryption, it is often at the file system level and, even when it is not possible to recover any of the encrypted data, it may be possible to recover incriminating digital evidence from unencrypted areas of storage media sufficient to support prosecution. However, as full disk encryption (FDE) becomes more widely used, it may not be possible to recover any digital evidence in some cases. An earlier FDE paper presented a rather one-sided view of what to do when the FDE key/passphrase is available, but did not emphasize the negative impact that successful FDE can have on a digital investigation (Casey and Stellatos, 2008). This follow on paper is intended as a wakeup call to those who believe that FDE does not pose a problem from a forensic perspective.

There are a number of ways that FDE has hampered digital investigations. The first potential problem arises when there is a failure to recognize that FDE is in use on an evidential hard drive. When contraband is observed on a computer system that is running but digital investigators turn off the computer to preserve the digital evidence, FDE may prevent further access to the incriminating data. Alternately, when a hard drive is received by a digital forensic laboratory, it may not be part of the standard operating process to perform a forensic preview of stored media prior to acquiring a forensic duplicate. This omission can lead to a failure to recognize that FDE is present, resulting in wasted resources spent processing

* Corresponding author.
E-mail address: eoghan@disclosedigital.com (E. Casey).
1742-2876/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2011.09.005

encrypted data and lost investigative opportunities. Another potential problem arises when digital investigators fail to collect potential FDE passphrases or recovery keys at a crime scene. Such information may exist in written form or digital form on a recovery disk or in memory, potentially requiring digital investigators to acquire volatile data from computers at the scene. A more serious problem arises when a Trusted Platform Module (TPM) is involved and hardware alterations render encrypted digital evidence unrecoverable. In this situation, the damage may be irreversible and digital evidence may be unrecoverable even after an otherwise viable decryption mechanism becomes available.

Challenges can also arise when a defendant appears to be cooperative. For instance, the defendant may provide incorrect decryption details but the defense may claim that the encrypted container was damaged in some manner, which was why it would not open. In addition, encryption products such as TrueCrypt enable users to create two separate storage areas within an encrypted container, each with their own passphrases. Using this approach, a defendant could provide just one of the passphrases and digital investigators may not realize that additional evidence is concealed on the storage media.

With current resources, law enforcement's hands are tied when it comes to FDE when used by anyone who is diligent with the passphrase. In a growing number of cases it may be difficult to prosecute for a meaningful conviction because of the inability to access evidence on either FDE systems or in encrypted containers. In one case, a convicted computer criminal was found to be using computers, which was a violation of his probation. All of his computers were protected using TrueCrypt and he was never compelled to give up his passphrases by the court. Digital investigators tried everything in their immediate power to crack the encryption but to no avail. Digital investigators still do not know what was on the computers but suspect that the offender was involved in various criminal activities.

One desired outcome of this paper is to provide guidance for gathering items at the crime scene that may be useful for accessing encrypted data, and for performing on-scene forensic acquisitions of live computer systems prior to transporting the evidence to digital forensic laboratories. These measures increase the chances of acquiring digital evidence in an unencrypted state or capturing an encryption key or passphrase. Some implications for drafting and executing search warrants to deal with FDE are discussed. Finally, it is also our hope that this paper will motivate the development of new techniques to overcome FDE.

2. Increasing use of FDE

Until recently, offenders who use encryption rarely protected every piece of media in their entirety, and generally left some incriminating digital evidence in unencrypted form. As a result, digital investigators may have been able to recover sufficient evidence to support a prosecution but this is not always the case, particularly when FDE is involved.

There are a growing number of FDE products, and hard drive manufacturers are building FDE into storage media. Full disk or volume encryption products include open source (TrueCrypt), third party (McAfee's Safeboot, WinMagic's SecureDoc, Symantec's PGP and GuardianEdge), or integration within the native operating system itself. Although many of these products can be configured with an additional decryption key (ADK) that an organization can use to recover data, these options may not be employed by an individual who is using encryption to conceal criminal activities.

As an example, Microsoft Windows BitLocker Drive Encryption is available in the Enterprise and Ultimate editions of Windows Vista and Windows 7, and Windows Server 2008 (Microsoft, 2009, 2010). The implementation of BitLocker drive encryption requires a user to either initialize the TPM chip or configure authentication without a TPM via a USB flash drive. The TPM provides validation for the boot process, detection of hardware tampering, and storage of the Bitlocker master key. Authentication without a TPM requires a user to save the master key to a USB flash drive that must be connected to the device upon startup. Self-encrypting hard drives are being manufactured to meet the Opal standard established by the Trusted Computing Group in 2009. Fig. 1 shows the authentication screen for such an Opal-compliant self-encrypting hard drive. Any attempt to acquire data from such encrypted hard drives without the associated decryption passphrase will fail.

The growth of FDE solutions is not just limited to hard drives. Offenders can encrypt volumes on removable media natively with BitLocker, with open source tools such as TrueCrypt, or with tools purchased from vendors such as IronKey and SanDisk. The availability of encryption solutions and ease of implementation on hard drives and removable media have provided offenders with protection that cannot be circumvented if implemented correctly.

3. Investigations foiled by encryption

When encryption cannot be circumvented, it may not be possible to convict an offender of a crime. The following recent case examples are summarized to demonstrate the impact of encryption on an investigation.

Case Example: In the case of Brazilian banker Daniel Dantas, we see how a strong TrueCrypt passphrase has prevented access to encrypted data on hard drives seized from Dantas's apartment by the Brazilian police (Leyden, 2010). To date, neither dictionary-based attacks by the Brazilian National Institute of Criminology (INC) nor attempts by the FBI have succeeded in accessing the encrypted data.

In the United States, the Fifth Amendment protects defendants against self-incrimination, including disclosure of encryption keys in some cases.

Case Example: Customs officials observed potential child pornography on Sebastien Boucher's computer as he was crossing the Canadian border. However, his computer was turned off before a forensic duplicate was acquired, and all of the alleged child pornography was inaccessible apparently because it was locked in an encrypted volume. When