



Detecting & Collecting Whole Disk Encryption Media

Christopher L.T. Brown, CISSP
Technology Pathways, Founder & CTO
clbrown@techpathways.com
619-435-0906 / 888-894-5500

Copyright © 2005, Technology Pathways, LLC

Presentation Objectives

- Discuss the benefits for using live computer forensic investigation techniques to detect, examine, and collect whole disk encryption.
- Attendees will be introduced to the components of a live computer forensic investigation, shown tools for identifying whole disk encryption.

Agenda

- Evolution of Personal Encryption
- Whole Disk Encryption Products
- WDE Functionality
- WDE Identification
- WDE Collection
- Evolution of Digital Evidence Dynamics
- Tool Options
- Demo

Identification & Collection of Encrypted Disks

Evolution of Personal Encryption

- Simple application protection systems (word, etc.)
- File level application encryption apps
- Folder level application encryption apps
- Virtual volume encryption (PGP, etc.)
- TwoCows contains over 300 disk encryption products for file level encryption alone

Today users and businesses require many types of encryption.

Encryption Approaches

- Many approaches to protecting data by encryption with differing benefits.
 - Transport encryption (protect data in transit)
 - File encryption (data at rest system on)
 - Container encryption (protect data at rest system off)
 - Whole disk encryption (protect data at rest system off)
- Each approach has differing levels of impact to performance and complexity.

Whole Disk Encryption

This presentation is about “Whole Disk Encryption” some times referred to as “Full Disk Encryption” due to alarming growth in use.

- Two approaches:
 - Hardware (Seagate *Momentous* series)
 - Software (PGP, SafeBoot, MS, etc.)

Full Disk Encryption Products

- PGP 9.0
- SafeBoot
- PointSec
- Windows Longhorn/Vista TPM v. 1.2(Trusted Platform Model) Secure Startup (2006)
 - Requires hardware chipset or USB Thumb Drive
- PC Guardian “Encryption Plus” Hard Disk
- SafeGuard Easy
- DriveCrypt Plus Pack

And many more...

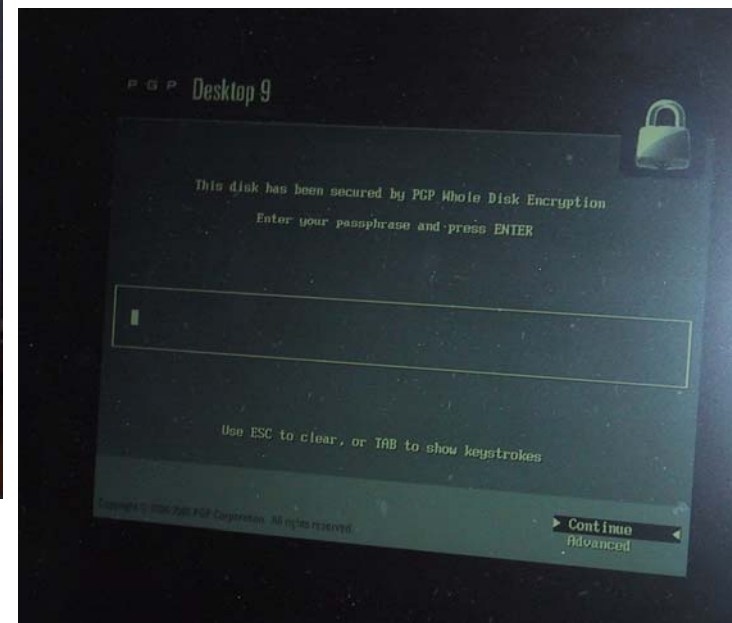
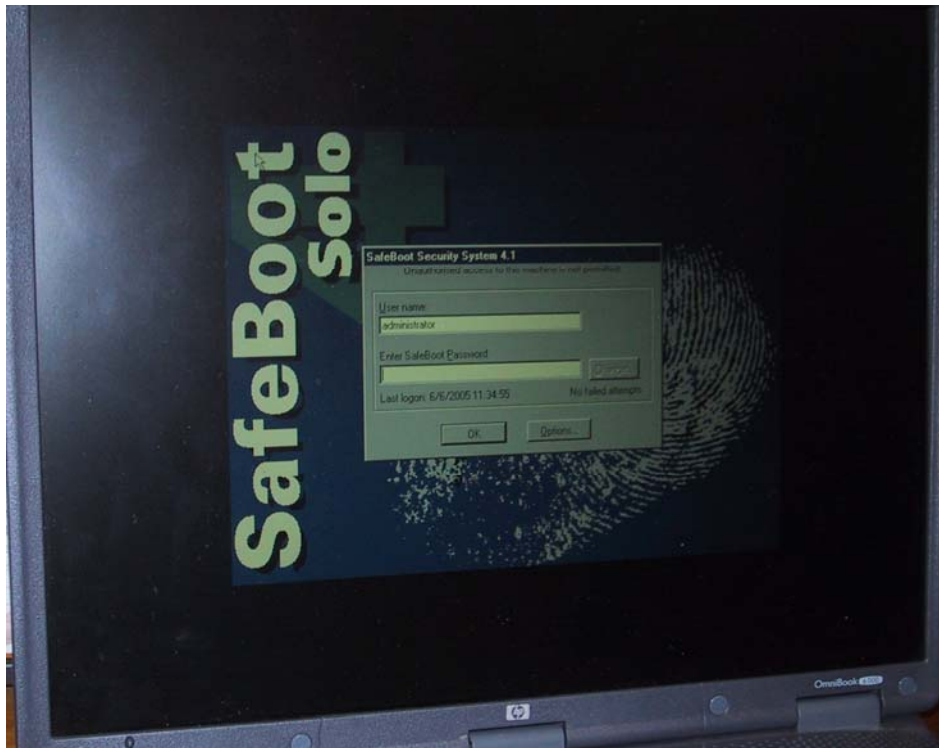
Authentication and Password Mgt.

- Pre-boot authentication
 - Simple Password
 - Smart Card
- Password Recovery
 - Floppy Boot Disk (DCPP, SafeBoot)
 - None required for PGP
 - Enterprise Recovery Agent
 - PointSec, Windows Longhorn/Vista

Architecture

- Where is encryption/decryption performed?
 - Kernel (lowest and best performing)
 - File System Filter (OK to poor performance)
 - Application library level (not really WDE, poor performance)

Pre-boot Logon



PGP 9 WDE Artifacts

- Memory
 - “PGPGUARD” in one or more (6) memory locations
 - “bootguard” in one or more (13) memory locations
 - “PGPWDE” in one or more (>100) memory locations
- Boot Sector
 - “PGPGUARD” at sector 0 offset 3
 - “bootguard” at sector 0 offset 16C
- Recovery Floppy
 - None

SafeBoot 4.13a Artifacts

- Memory
 - “SafeBoot” in one or more (>100) memory locations
- Boot Sector
 - “SafeBoot” at sector 0 offset 3
 - “SafeBoot” at sector 0 offset 168 and 183
- Recovery Floppy (may be burned to CDROM)
 - Uses FeeDOS on a FAT12 formatted floppy
 - Look for SBFIX.EXE, SAFETECH.EXE, SBREPAIR.COD, and SBCONFIG.SDB
 - SAFETECH.EXE appears to provide a backdoor for SafeBoot tech support.

Windows Vista (subject to change)

- Whole Disk Encryption is part of a concept called “Secure Startup” Branded as BitLocker Drive Encryption (*Available only in limited editions*)
- Requires TPM 1.2 System or external flash drive to hold the key.
E5B095CB-E647-4545-9300-BA27FF817FFB.FVE (now .bde)
- Currently complex to set up: Two partitions Boot and System. Boot is not encrypted
- **USB method now requires enabling through scripting “manage-bde” from command prompt.**

Windows Vista (2)

- The key in the TPM or USB flash drive is all that's needed to boot
- If Key is lost, a recovery key can be used by hitting the escape key.

105369-682363-444158-207053-485540-631268-327470-697345

User is encouraged to print, or save the recovery key to a file

Windows Vista (3)

Signatures:

Standard “NTFS” at boot partitions offset 3

“-FVE-FS-” at offset three of each encrypted partition

MS approach is “Full Volume Encryption” as seen above and is intended to be in the release product and not related to WinFS a file system to be added on after release

Conclusion

- Whole Disk Encryption & Full Volume Encryption provide pre-boot protection of data (encrypted at rest only)
- Authentication and Authorization mechanisms vary.
- If the system is live, the data is accessible in an unencrypted state
- Recovery keys often provide no-password access

First Responders

- If the system is using WDE and is live?
- Stop and Think
 - The disk can be collected in an unencrypted state
 - Artifacts allowing for password recovery can be collected

WDE Collection & Analysis

- Requires some level of live forensics to:
 - *Identify and/or Collect*
- Possible Exceptions:
 - *Get the password (you'll need to boot the system to analyze it)*
 - *Find the recovery boot disk (some allow full recovery without password or provide vendor tech support backdoor)*

What You are Looking For (1)

- Most WDE requires boot sector modification to allow for pre-boot authorization – looks like Linux Grub
- Backup or Recovery Disk (Floppy or CD)
- Extract Password recovery artifacts such as SAM, NTUSER.DAT and Registry files
- *Note: Application not always visible in system tray or process list*



Evolution of Digital Evidence Dynamics Or Why Live Forensics

Evidence Dynamics

- Anything that interacts (changes evidence) in any way:
 - Human Forces (investigator, other)
 - Natural Forces (time, environment)
 - Tool Forces (forensic collection, examination)
- Complex issues that cause great concern among first responders
- One of the biggest questions in evidence dynamics was...

Pull the Plug or Not? (1)

- Orderly Shutdown Process
 - Possible loss of virtual memory space on disk
 - Inability to control evidence destructive processes launched during shutdown
- Pull the Plug
 - Loss of physical memory contents
 - Possible damage to open files and the file system



Just to name a few...

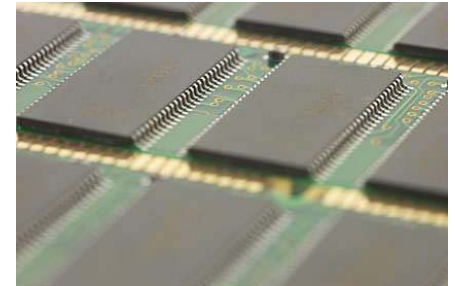
Pull the Plug or Not? (2)

- The answer can only be provided by examining each given situation and through investigator experience, but...
- No matter what the choice investigators **Will lose volatile memory** and system state if not collected first



What's lost?

- Types of information located in memory:
 - Cached passwords (encryption, email, etc.)
 - Memory resident only Malware code (SQLSlammer)
 - Fragments of open files, processes
 - Shimmed kernel processes from backdoors
 - Unencrypted data from encrypted disk source including **PGP Whole Disk Encryption, SafeBoot**, etc...



More...

Situations for Live Investigation

When to Collect Volatile/Live Data

- Running systems where investigators:
 - Can access in a least intrusive manner
 - The risks are weighed to benefits
 - Suspect running malware or memory only resident code
 - Benefit from password retrieval
 - Suspect strong encryption on files and applications
 - Hacker backdoors
 - **Desire to freeze system state**
 - **PGP Whole Disk encryption...**



When NOT to Collect Live Data

- Running systems where investigators feel there is a high likelihood of destructive or hostile actions in progress
- Investigator does not possess the tools or knowledge to collect live data in a least intrusive manner



What you Need (Live Collection)

- Option 1
 - ZeroView (freeware first responder utility from Technology Pathways)
 - Read the boot sector live to identify
 - DD and NetCat/CryptCat Combo
 - Use to collect live image of disk in unencrypted state
- Option 2
 - Live Forensics Tool
 - Conduct Live preview of boot sector with forensics grade tool
 - Conduct Live Imaging with forensics grade tool

Tools for Option 1 (1)

- Freeware Sector Viewer (to ID WDE)
 - ZeroView is a free application created for first responders that can be run from a CD or Thumb-drive. A read-only ASCII/HEX view of a disks sector zero is displayed when run.
 - <http://toorcon.techpathways.com/uploads/zeroview.zip>

Tools for Option 1 (2)

- Freeware Live Imaging
 - Linux (HELIX Boot CDRROM) – (netcat, dd, etc.)
 - <http://www.e-fense.com/helix>
 - Forensic Acquisition Utilities – (netcat, dd, etc.)
 - <http://users.erols.com/gmgarner/forensics/>

Tool for Option 2

- Commercial Tool Options
 - ProDiscover IR/IN
 - Preview, imaging, and physical memory image
 - <http://www.techpathways.com>
 - EnCase EEE/FIM
 - Preview and imaging
 - <http://www.encase.com>
 - SMART Mac/Linux – (disk only, no preview)
 - <http://www.asrdata.com/>

Demo Scenario Walkthrough

- Using ProDiscover Incident Response Edition
- PGP Encrypted Disk Collection
- Goals:
 - Identify whole disk encryption in use
 - Collect disk live in unencrypted state
 - Collect user artifacts useful in password recovery

COMPUTER EVIDENCE

Collection & Preservation

- Teaches investigators how to ensure case integrity when dealing with computer evidence
- Provides a practical resource for collection and preservation that will help ensure legal acceptability
- Covers key areas such as rules of evidence, evidence dynamics, network topologies, collecting volatile data, imaging methodologies, and forensics labs and workstations
- Includes a CD-ROM with shareware and commercial demo software tools as well as document templates, worksheets, and references



Networking & Security Series

CHRISTOPHER L.T. BROWN

Thank You Questions?

Technology
Pathways

**703 First Street
Coronado, Ca. 92118**

**Phone: 888-894-5500
FAX: 619-435-0465**

www.TechPathways.com

Technology Pathways provides comprehensive, affordable computer forensic tools for Law Enforcement, Corporate and Government.

ProDiscover solutions include: investigations, incident response, computer forensics, and electronic discovery.

ProDiscover can forensically examine live systems over networks and has been accepted in criminal and civil proceedings.