Forensics Issues in Full Disk Encryption

Dr Séamus Ó Ciardhuáin
Department of IT
Limerick Institute of Technology
Biography

• Systems management etc. Ireland and UK
• Research project management, UCD
• PhD computer forensics, UCD 2003
  – Garda and European training
• Lecturer LIT since 2004
  – MSc Security & Digital Forensics
Full Disk Encryption

• FDE is becoming common because:
  – Software/hardware support makes it easy.
  – Theft or loss of laptops and storage devices makes it necessary.

• Pressure to use it:
  – Security of valuable data
  – Data Protection legislation
  – Negligence claims?

• Users are more conscious of the risks (?)
FDE and Forensics

• Until recently FDE (or any encryption) was rather exotic and unlikely to be used.
• Investigators did not encounter it much.
• No real need for techniques to deal with it.
• This is no longer the case.
Examples (1)

- UK terrorism case
- TrueCrypt volume found on PC.
- Police had part of passphrase but could not decrypt.
- Court ordered suspect to give passphrase, but it didn’t work.
- Decision: no case because it took so long that suspect could have forgotten.
Examples (2)

- Brazil, 2008
- Banker named Daniel Dantas
- Police seized disks encrypted with TrueCrypt.
- Unable to decrypt, so sent them to FBI, who could not do it either.
- Reportedly dictionary attacks used.
- No legal means to compel disclosure.
Examples (3)

• US National Institute of Justice report on TrueCrypt software.
• Their objective was securing evidence.
• Findings:
  • You can easily tell TrueCrypt is installed.
  • The drive contents are inaccessible.
  • In certain circumstances the password might be recoverable from memory.
FDE and Forensics

• Traditional forensics ≈ disk analysis
  – Applications and system software leave many traces behind.
  – User files contain data and metadata.
• Physical access to disk means we can bypass security and copy disk content (imaging).
• Encryption changes this, and FDE makes it even harder.
Previous Encryption

• EFS in Windows
  – Files and folders
• Applications Packages
  – e.g. MS Office, WinZip: individual files
• The entire system is not encrypted, only parts of it.
• Unencrypted data may exist.
FDE Technologies (1)

- BitLocker in Windows
- FileVault on MacOS
- PGP, TrueCrypt, etc.
- Many others: Wikipedia lists 50+
  - Not all are \textit{FULL} disk encryption though.
FDE Technologies (2)

• BIOS and native disk encryption
  – OPAL standard
  – Trusted Computing Group
  – Thinkpads and similar
  – “Self-encrypting” drives
• This is even worse than BitLocker and similar systems.
• The OS or driver will not have the password or key so recovering it will be very hard.
Drives


• US standard for this: FIPS 140-2
Encryption Technology

• In practice, we must assume the encryption itself is unbreakable in most cases (AES or other good algorithms).

• Of course, there are
  – bad encryption systems
  – misconfigured systems
Perception…

• Irish Times letters, Thu, Nov 11, 2010

• Madam, – Regarding the article on Anglo’s encrypted documents (Business Today, November 10th), there are government agencies around the world that can easily decrypt complex passwords and documents. Perhaps the Government can ask our Israeli passport friends or, better still, some of the spooky individuals at the huge MI5 complex in Belfast. – Yours, etc.,

• KEITH NOLAN, Caldra House, Carrick-on-Shannon, Co Leitrim.
Sat, Nov 13, 2010

Madam, – Peter Faulkner comments that it “simply beggars belief that in a country that would see its place as at the forefront of the smart economy, we do not have the technical IT skills to open these vital Anglo documents” (November 12th, 2010).

The encryption technologies embedded in some popular word processors are certainly not perfect, and if these are what have been used to secure the documents, we may reasonably hope that they will be recovered. However, other software is readily available, for free, that can, if used properly, generate files that are essentially entirely resistant to decryption on the timescales required.

One would hope that a major financial institution would possess the “technical IT skills” to mandate the use of such tools in an appropriate manner. On the other hand, given the possible content of the documents, perhaps we should hope that this is not in fact the case. –

Yours, etc.,
Prof SIMON DOBSON,
Department of Computer Science,
University of St Andrews,
Scotland.
... and Reality (2)

• Sat, Nov 13, 2010

• Madam, – The only government security agencies that can easily decrypt complex passwords and documents are the ones headquartered in Hollywood. The rest of the world is constrained by the mundane reality that most encryption mechanisms are designed so that they cannot feasibly be broken. – Yours, etc.,

• NICK HILLIARD,
• De Courcey Square,
• Glasnevin, Dublin 9.
Dealing with FDE

- Technical approaches
- Legal approaches
- Investigative approaches
- Corporate policy issues
Technical Approaches
Avoid the Problem

• Additional Decryption Keys
  – These make sense in corporate environment.
  – “I forgot!”
  – If sysadmin cooperates with investigation…

• Misconfiguration
  – Many users don’t understand the technology.
Disk Imaging

• How to update traditional methods?
• Live imaging is essential – once the system is shut down we won’t be able to get a useful image of the disk contents.
• Encrypted volumes must be mounted.
• Chain of custody issues: how do we verify against the original disk?
Disk Imaging

- Standard tools mainly assume static imaging:
  - remove disk and image; or
  - reboot into imaging tool from CD/USB
- OS security may get in the way.
- Can we take the machine away to work on without powering down?
Moving a Running System

• This could allow more time to work on the volatile data: WiebeTech HotPlug
• www.wiebetechnology.com/products/HotPlug.php
Volatile Data

• How about recovering passwords/keys from memory?
• The key will be stored in RAM while the volume is in use. Passwords may not be stored though.
• Access to the system memory live, or as a dump, may allow the key to be recovered.
  – Hiberfile and pagefile inaccessible on encrypted disks after shutdown.
  – Have to force memory dumps to be written to unencrypted storage.

– Chain of custody issues
Volatile Data Problems

- We probably need administrator-level access to the system to collect the data.
- Interpreting memory dumps isn’t easy.
- Live acquisition of disk images isn’t easy, but is definitely possible.
- For native encryption on the disk itself, nothing will be in memory, so no choice.
Volatile Data

- FireWire attack – DMA access to memory of running systems. Requires physical access to the running system, which must have FireWire.
  - Recent hardware uses different DMA controllers – no access.
  - Recent software erases key from memory on dismount, or does not cache passwords.
- Freezing memory chips slows loss of data.
- How practical are these methods?
Password Cracking

- Is cracking becoming a viable tool?
  - Fast desktops, cloud, GPUs
- Bad password security is common!
- Password reuse in multiple accounts.
- User profiling to give input to password cracking means we don’t use brute force approaches.
- NB not the same as cracking the encryption!
- Even brute force: 8 character Windows pw cracked in 17 days on 2-core 4GB 2.8GHz PC with john the ripper s/w
Keyloggers

• Maybe the password can be captured in use: software or hardware logger.
• “Little Nicky” Scarfo in USA (2001):
  – FBI used a keylogger installed in his PC to obtain a PGP password.
  – Ruled admissible with warrants.
• Would it be legal in Ireland?
  – Gardaí
  – Corporate use

http://www.keydemon.com/
Bad Technology

• Raidon Staray S USB enclosures with encryption.

• Weak cryptosystem, easily broken.
Investigative Approaches
Planning

• Investigators must expect to encounter FDE.
• Plan for live acquisition.
• Plan to preserve volatile data.
• Try to ensure interactive access is possible to the running system, as admin if possible.
Forensics Tools

• Detecting encryption is in use
  – Too many packages for investigators to know all of them.
  – We need to develop tools to scan systems.

• Live acquisition of disk images

• Live data from the running system: keys, memory dumps.
Planning

- Accessing encrypted data requires much more work on the live system than traditional forensics.
- This opens up the possibility of legal challenges to the evidence.
- Careful planning and documentation of procedures reduces the risk of a successful challenge.
User Behaviour

• The user is a weak link.
• Bad passwords
• Shared/reused passwords
• Passwords written down somewhere
• Backups not encrypted
Weak Link

• Another UK terrorism case
• Suspect didn’t believe AES etc. were any good because they were known to the enemy.
• Devised his own algorithm which was the same as used in Ancient Greece and by Julius Caesar 2,000 years ago.
• 30 year sentence.
Corporate Environments

• ADKs, recovery disks, etc.. may be in use.
• Unencrypted backups may exist.
• Company policies may give avenues for recovery.
  – Recording passwords
  – Users can’t change passwords
  – Disciplinary procedures
  – Legal compulsion
User Profiling

• This can enable an attack on the security by “guessing” the password.
• Password lists are available.
• Common password types: names, car registration, phone number, birthdays, …
• Software can use these as the basis for guessing to give a feasible search space.
Legal Approaches
Irish Criminal Law

• Several pieces of legislation give power to Gardaí with warrants.
• New legislation addresses it directly.
Theft and Fraud 2001

- **Section 48** of the Criminal Justice (Theft and Fraud Offences) Act 2001, amended by section 192 of the Criminal Justice (Theft and Fraud Offences) Act 2006 which replaces section (2).
• (5) A member of the Garda Síochána acting under the authority of a warrant under this section may—
  • (a) operate any computer at the place which is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and
  • (b) require any person at that place who appears to the member to have lawful access to the information in any such computer—
    • (i) to give to the member any password necessary to operate it,
    • (ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or
  • to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.
Theft and Fraud 2001

• (8) “computer at the place which is being searched” includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer;

• Section 52 of the same Act allows a judge to

• order that the person shall—
  • (i) produce the material to a member of the Garda Síochána for the member to take away, or
  • (ii) give such a member access to it,
    • either immediately or within such period as the order may specify.
Criminal Justice Act 2011

• The new Act contains similar provisions to the 2001 Act.
• However, they appear to be applicable to a much wider range of offences, e.g. the Criminal Damage Act 1991 is included.
• We’ll have to wait and see how this is handled in court.
Other Irish Acts

• Electronic Commerce Act 2000
  – s.27
  – s.28 protects passwords etc..
Irish Civil Law

• Statutory Instrument No. 93 of 2009
• Rules of the Superior Courts (Discovery)
• Court can order document to be made available in “searchable form”.

29 Feb 2012
Forensics and FDE, ISACA, Limerick
Legal Situation Elsewhere

• UK
  – Regulation of Investigatory Powers Act (RIPA) gives police considerable power to compel disclosure.
  – Used a number of times.

• USA
  – Recent cases indicate there is still confusion.
  – Protection against self-incrimination.
Corporate Policy Issues

• How can an organization prepare in case it becomes involved in a situation where forensic analysis of encrypted systems is required?
  • ADKs if available
  • Password policies
  • Perhaps users sign an “acceptable use” policy – legal recourse available?
Conclusions

• FDE is a big challenge for forensic analysis of computers.
• Planning is essential:
  – Corporate
  – Investigative
• Technical means are interesting but offer no guarantees of success.
• Self-encrypting drives seem likely to make life even more difficult for investigators.
Another Approach...

http://xkcd.com/538/
Some References


Some References

• US National Institute of Justice (NIJ) publish test results and reports, e.g. on TrueCrypt.

• US National Institute of Standards and Technology (NIST) also publish useful reports.
Thank you!

Questions and discussion?
Advertisement

- LIT MSc in Security & Digital Forensics
- Taught modules + project
- Running since 2006
- Starts October
- Typically 2-3 years part time
- Lesser awards also possible from taught modules

29 Feb 2012 Forensics and FDE, ISACA, Limerick