

Home Page

Title Page



Page 1 of 13

Go Back

Full Screen

Close

Quit

Practical Approaches to Recovering Encrypted Digital Evidence

by Eoghan Casey in: International Journal of Digital Evidence (www.ijde.org)
Fall 2002

Jonathan C. Busey

busey@cs.fsu.edu

March 26, 2003

Purpose

- presents lessons learned from investigations involving cryptography in various contexts
- discusses legal challenges which arise when dealing with encryption
- proposes directions for future tool developments

Home Page

Title Page



Page 2 of 13

Go Back

Full Screen

Close

Quit

recovering encrypted data

It is infeasible to attack strong encryption directly using brute-force methods

- locating unencrypted copies of data
- obtaining encryption passphrases
- guessing passphrases

Home Page

Title Page



Page 3 of 13

Go Back

Full Screen

Close

Quit

Two types of cryptography

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter.

Bruce Schneier **Applied Cryptography** (Preface)

Weak Encryption

XOR

- evident when characters have decimal value > 127
- **Back Orifice** uses XOR to encrypt packets
- earlier version of Microsoft Word and Excel use XOR for ‘password protecting’ files
- Access Data’s **Password Recover Toolkit** and NTI’s **Advanced Password Recovery Software Tool Kit** can both recover such passwords
- prior to version 4, PalmOS used XOR for the user-selected password, which can be extracted from “Unsaved Preferences” or in **users.dat**

substitution also mentioned in passing

Home Page

Title Page

◀ ▶

◀ ▶

Page 4 of 13

Go Back

Full Screen

Close

Quit

Home Page

Title Page



Page 5 of 13

Go Back

Full Screen

Close

Quit

Strong Encryption

- can be compromised in practice
 - selection of weak passphrases
 - writing down strong passphrases
 - keystroke capturing (looking over shoulder)
 - an interrogator, lawyer, judge may convince or compel suspect to disclose key or passphrase

Some weaknesses

- 40-bit encryption (Adobe Acrobat and Microsoft Word/Excel files) can be feasibly broken with Access Data's **Distributed Network Attack** or a Beowulf Cluster
- $2^{40} < 1.1$ trillion or 100 computers working for under 5 days for every key (average time 2-3 days)
- shortcomings of Unix **crypt** utility
 - `% crypt -key 'birthday' <plaintext> ciphertext`
 - plaintext file
 - memory storage
 - swap file
 - external media backups
 - secret key itself (dictionary or other attack)

Home Page

Title Page

◀▶

◀▶

Page 6 of 13

Go Back

Full Screen

Close

Quit

Home Page

Title Page



Page 7 of 13

Go Back

Full Screen

Close

Quit

More weaknesses

- EFS makes temporary plaintext copy of file in case of problems during encryption, and often the file is stored in a paging file (`pagefile.sys`) if the file decrypted and re-encrypted at any time, a temporary file was probably stored on disk printing an EFS file copies it unencrypted to `System32\Spool\Printers`
- unencrypted data in RAM, such as when encrypting mail with PGP from an **Outlook** mail window or in **PGPTray** during any encryption. `pmdump` can then reveal message.

On obtaining passphrase

- passphrases often re-used or located near computer
- interviewing the suspect (?)
- surreptitiously monitoring computer use (last resort)
- prior to Windows XP, EFS private keys weakly protected—tools such as **chntpw** can change NT logon password
- when PGP crashes on Windows 2000, **Dr. Watson** creates a memory dump which includes the passphrase
(Documents and Settings\All Users\Documents\DrWatson\user.dmp)
- EFS—an encryption recovery agent is assigned and can decrypt messages when the original encryption key is unavailable.
 - Built-in Administrator account by default in Windows 2000
 - **efsinfo** displays contents of files

Home Page

Title Page

◀▶

◀▶

Page 8 of 13

Go Back

Full Screen

Close

Quit

Tools for obtaining password

- **Forensic Toolkit** by Access Data or **Password Recovery Toolkit**—search disk for remnants of keys, passwords
- Software: **Spector Pro**, **Back Orifice**, and **Subseven** enable key logging, screen captures, and remote file access
- Hardware: **KeyGhost** and **KeyKatcher** connect to PCs (not Macs, not Sun, not PDAs) and have internal memory

Advantages

1. every stroke (even BIOS protection)
2. persistent through wipes of drive or re-installation of OS

Real life examples I

- The Wall Street Journal decrypted files on an Al Qaeda computer using 40-bit (exportable) version of Windows NT Encrypting Filesystem (EFS generally 128 bit)
- Ramsey Yousef (World Trade Center bombing 1993) encrypted files on laptop, but plaintext files were also stored and obtained, as was his secret key
- an (unspecified) “offender” used PGP to encrypt Word documents. File was wiped, but fragments in temp files were scattered throughout the disk
- United States v. Hersh: data stored with **F-Secure** part of source code released to agents, enabling the procurement of filenames, size. The names of 120 of 1,090 files were consistent with known child abuse images, and 22 of those matched in size.

Home Page

Title Page



Page 10 of 13

Go Back

Full Screen

Close

Quit

Home Page

Title Page



Page 11 of 13

Go Back

Full Screen

Close

Quit

Real life examples I

- People v. Price in Yolo County (California) superior court prosecutors successfully compelled production of PGP passphrase
- United States v. Scarfo the FBI used a key logging system to obtain the suspects PGP passphrase (not deemed a privacy violation since logging occurred only when defendant was not online)

Home Page

Title Page



Page 12 of 13

Go Back

Full Screen

Close

Quit

regarding network traffic

generally impractical to attempt to decrypt communications with today's protocols, attacks may be mounted at end-points

client side SubSeven or Back Orifice

server side databases compromised or SSH modified so that passwords are stored in a file. Intruders have even compromised the official distributions of SSH servers; see [CERT 2002](#)

Home Page

Title Page



Page 13 of 13

Go Back

Full Screen

Close

Quit

Future directions

- as analysis tools evolve, extracting data from RAM ‘postmortem’ (after reboot) will become more feasible. This involves scanning probes or magnetic force microscopes
- more information sharing among examiners