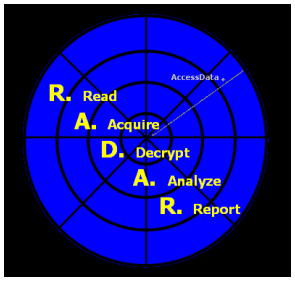
AccessData®

WhitePaper

Password Recovery with PRTK™/DNA®

March 2006



ACCESSDATA, ON YOUR RADAR

Password Recovery with PRTK™/DNA®

One way to keep information confidential is to encrypt it, rendering it unreadable until it is decrypted. To encrypt a file, the application you are using, for example Microsoft® Word®, will have you select a key or a password, which is used to both encrypt the file and to decrypt it.

Since the password owner must be able to remember the password, password recovery is based on these simple facts:

- The password will usually be in a language familiar to the owner
- The password will usually be an aspect of the owners life
- New passwords might be a modification of old passwords

Passwords should be difficult for others to guess. However, the owner of the password needs to be able to remember it, which means it must conform to some rules known and employed by the owner. That is, it should be something familiar enough for the owner to recall and repeat. That's why passwords are usually composed in a language familiar to the password owner.

In order to more easily remember a password, the owner often chooses one from the names of family, pets, product names, dates, or less wisely, telephone and social security numbers. If the password isn't obvious enough, or if it's chosen for the owner, the password owner may write down the password close to where it's needed, or into a file used to record all current passwords.

Understanding Password Recovery

Whether it has been forgotten or abandoned, you will eventually need to recover a password. Software products can help you discover a password by trying to decrypt the encrypted file with successively longer sequences of characters presented as the password. Even with the fastest computers, this trial and error approach (called an attack) can take a very long time. If many files need to be decrypted, the problem is multiplied.

Recovering passwords takes more than just dropping a file into a software product and hoping that it will find something. This approach would take more time than is practical. Because of the way people usually select passwords, finding the passwords can be done much more quickly by combining as much information about the owner as is available with an application that can apply that information fast and logically.

AccessData Corporation offers two software solutions for password recovery: Password Recovery Toolkit™, or PRTK, and Distributed Network Attack®, or DNA. These applications work on the same technologies, but provide a choice on distribution, or how the work load of guessing passwords is shared among multiple machines. For simple password recovery jobs, PRTK is the perfect application. If large numbers of encrypted

files need processing, consider DNA the solution. AccessData also provides classes training clients on password recovery strategies and on how to best exploit these tools.

Password Recovery Strategy

Given that encrypted files have been discovered and need to be opened, the following are a set of processes that are critical to the recovery of passwords using PRTK/DNA:

1. Determine the languages familiar to the creator of the password. Determine the language, codepage, or keyboard setting used on the owner's computer.
2. Search the location of the owner for any hand-written notes that may contain possible passwords. These possible passwords can be used to create a biographical dictionary, or entered into a wordlist file that can then be turned into a custom dictionary.
3. If the owner's hard drive has been imaged, process the image and export a wordlist file that can be turned into a custom dictionary.
4. Adjust the order in which the levels are processed, and add any new levels that may be necessary.

The more information that can be gathered about the person that created the passwords being recovered, the more likely that the passwords will be found quickly.

Password recovery is waiting for the set of target passwords to be tried against the encrypted file. Once all the background information about the creator of the password has been gathered and submitted to the recovery process, time becomes the limiting factor to recovering a password. A machine's speed, or the amount of machines available, will have a noticeable effect on the password recovery.

Password Recovery Operation

PRTK operates on a single computer to recover passwords from a wide variety of file types such as Excel®, Zip, or Quicken®. File types are supported through the use of modules[1]. Each module is designed to employ those attacks that are most effective for the particular file type for which it was developed.

Multiple files can be added as jobs, and each job is prioritized based on the complexity of the encryption algorithm used by the program that created the encrypted file. Simpler encryption algorithms are faster to process, so jobs with those kinds of files are attacked first. Recovered passwords are displayed with their corresponding job and are also stored in a filed called a Golden Dictionary.

Because files from the same source are likely to share the same password, those successfully retrieved from files with less complex encryption are applied to files with more difficult encryption.

[1] See Appendix B for the complete list of modules supported by PRTK and DNA.

Because passwords can be expected to be based on a language familiar to the person who encrypted the file, selecting the language to be used by PRTK is the first step toward successfully recovering the password.

Language and Character Groups

By selecting the appropriate language and character groups[2], target passwords will be constructed that are familiar and used by the person who created the password in order to constrain the amount of passwords to be guessed. If the password creator is known to favor using upper or lower case characters, for example, or if you suspect that symbols are used, you can enable or disable these options for each group.

Dictionaries

Words to try as passwords are taken from files called dictionaries[3], which contain a list of words in the languages to which they correspond. PRTK includes some predefined dictionaries for some languages. PRTK can create custom dictionaries from information about the person who created the encrypted files, if you suspect the password was created from that information.

Any recovered passwords are stored in a special dictionary called the Golden Dictionary, and are automatically tried every time a new job is added.

Levels

PRTK conducts password attacks using rules called levels. Levels provide the means by which the complexity of the passwords to be tested is gradually increased, starting with the simplest attacks (simple dictionary attacks) and proceeding to the more complex (enhanced dictionary and brute force attacks, where every possible character combination is tried). Of course, simpler attacks require much less time and resource than do more complex attacks.

Password recovery is a numbers game; the more passwords tried against an encrypted file, the more likely you'll find a password that can open it. The settings you apply to PRTK/DNA will provide the number of passwords generated, and determine the odds of recovering the one. They also determine the amount of time each attack will take. Carelessly selecting your settings will reduce the time it takes to test, and yet increase the chances of success. Thoughtlessly applying your settings will slow things down, and even prevent you from finding the password.

Improving Testing Performance

Password Recovery Tool Kit is an application for password recovery using a single machine to attack encrypted files. It has been designed to share the machine with other applications running at the time, which will slow down the recovery process.

---

[2] See Languages and Character Groups
[3] See Biographical and Custom Dictionaries

Distributed Network Attack (DNA) is a solution that addresses this issue by allowing many machines to be designated as resources for password recovery. DNA is able to use each processor in a multi-processor or multi-core processor machine, enhancing the overall performance. These machines may be used in one of two different worker modes: dedicated or nondedicated.

A dedicated worker is a machine designated for exclusive use by the DNA network. No other tasks are performed by this mode other than DNA password recovery. A nondedicated worker is a machine that serves other purposed as well, such as an employee station for regular business use. The advantage to using a collection of nondedicated machines is that your organization already has a base of machines, usually available after hours. By assigning them to DNA, these machines provide valuable computing power to your password recovery operation when not in use by their primary users.

To illustrate how multiple machines may impact a password recovery job, imagine a single machine capable of testing 1,000,000 passwords per hour. A single machine can therefore test approximately 24,000,000 in a 24-hour period. If a DNA network with ten nondedicated workers is put on the job and the machines are available for about 14 hours each day, they are able to test approximately 140,000,000 passwords in the same 24-hour period—an increase of about six times.

By making more machines available as DNA workers, the number of passwords that can be tested increases.

DNA distributes the current workload by providing each worker machine the IP address of the supervising machine. As long as each worker has a network connection and is able to resolve the provided IP address, it can establish a connection to the supervisor, which will allocate work for it as jobs are submitted. All machines assigned to the same supervisor form a cluster. As the size of the cluster increases, so does the number of passwords that can be tested.

The cost of the expertise and equipment needed to maintain a large DNA cluster should be carefully considered in deciding between PRTK and DNA, but with the correct personnel and hardware, a DNA cluster can dramatically increase the probability of password recovery.

Appendix A: System Requirements

All RAM requirements are based on memory available after the OS is loaded. USB is required.

PRTK™ Recommended Requirements

- Operating System: Windows® XP/2000
- Processor: Intel Pentium® III/P4/AMD Athlon™
- RAM: 2 Gb
- Hard Disk Space: 100 Mb

DNA® Supervisor Recommended Requirements

- Operating System: Windows® XP/2000
- Processor: Intel Pentium® III/P4/AMD Athlon™
- RAM: 2 Gb (more if running local worker)
- Hard Disk Space: 100 Gb
- Network: 100 Mb minimum/1Gb optimal

DNA® Worker Recommended Requirements

- Operating System: Windows® XP/2000
Macintosh OSX 10.3.9/10.4.x
Linux Red Hat/Fedora Core 4
Solaris
- Processor: Intel Pentium® III/P4/AMD Athlon™
Power PC G4/G5
Sparc
- RAM: 1 Gb
- Hard Disk Space: 40 Gb

Appendix B: Module List

Module	Supported Versions	Job Type
ABI Coder	3.5.7 through 3.6.1	Dictionary
ACT	1, 4, 5, 6, 2000	Decryption
AIM	Through AIM 5.9 and AIM Triton 1.0.2	Dictionary for AIM account passwords on nonTriton versions. Decryption for account passwords on Triton versions and for POP3 passwords.
Ami Pro	Last version supported	Dictionary
AOL	8.0 through 9.0 Security Edition	Decryption and Keyspace
ARJ	Through 2.82	Dictionary and Keyspace
Ascend	Last version supported	Decryption
Ashampoo	Security Manager 99, Ashampoo Power Incrypt, Ashampoo Privacy Protector, and Ashampoo Privacy Protector 2005	Reset and Dictionary
BestCrypt	4.x through 7.20	Dictionary
BulletProofFTP	2.3 through 2.45	Decryption
CD-Lock	5.08	Dictionary
CheckWriter	Up to 5.0	Dictionary
CodedDrag	2.4	Dictionary
CruzerLock	1.0 through 2.1	Dictionary
Crypt	MD5-based crypt, SHA1-based crypt, and fcrcrypt	Dictionary
Cryptainer LE	5	Dictionary
CryptalPix and CryptalFlix	CryptalPix 2.0 through 2.24 and CryptalFlix 1.0 through 1.1	Dictionary and Keyspace
Cryptext	2.3 through 3.40	Dictionary
CuteFTP	2, 4, and 7	Decryption or Dictionary
DataPerfect	2.6 (last version)	Dictionary
DriveCrypt	4.2	Dictionary and Reset
DriveCrypt Plus Pack	3.0	Dictionary
EasyCrypto	5.5	Dictionary for encrypted files, and decryption for the password store file
EFS	Protect Files from any Windows 2000 or Windows XP service pack	Dictionary

Module	Supported Versions	Job Type
Encrypted Magic Folders	3.x	Dictionary
Filemaker	3.x and 5.x	Decryption
Gifshuffle	1 and 2	Reset and Dictionary
Hello	1.0	Decryption
ICQ	2003b through 5.04	Decryption or Keyspace
Internet Explorer Content Advisor	IE 3.02 through 6.x	Dictionary
Invisible Secrets	4.3	Dictionary
Justsystem (Ichitaro and Hanako)	2004	Dictionary
Kai-Kei	05	Decryption
KeePass	0.8 through 1.03	Dictionary
Kremlin	2.21 through 3.0	Dictionary
LOCK-iT	XP	Dictionary
Lotus 1-2-3	Lotus 1-2-3 1A, 4, 97, 9, FRM, Japanese; Lotus Symphony 1, 2; Lotus SEAL	Decryption
Lotus Approach	3, 96, 97	Decryption
Lotus Organizer	1 through 4	Decryption
MaxCrypt	1.0 through 1.09	Dictionary
Messenger Plus!	3.50 through 3.61	Dictionary for chat logs; Decryption for lock and application lock passwords
Mozilla Master Password	Firefox and AOL Communicator, Netscape since 7.0, and Mozilla since 1.7	Dictionary
MS Access	All JetDB through 2003	Decryption
MS Backup		Decryption
MS Mail		Decryption
MS Money	Through 2006	Decryption for versions prior to 2002; Dictionary for versions since 2002
MS Office	All versions of Word and Excel; all password-enabled versions of PowerPoint (XP and later)	Decryption for versions prior to Office 97; Keyspace and Dictionary or Office 97/2000 compatible encryption; Dictionary for Office XP and later compatible encryption; Decryption in all cases where only nonencrypting passwords are present.
MS Project	98 through 2003	Decryption

Module	Supported Versions	Job Type
MS Schedule Plus	7.x	Decryption
MSN Messenger	Through 7.0	Decryption for the account password in the registry; Reset for the encrypted contact lists
MYOB (Mind Your Own Business)	Through 3.x and 2005 Premier	Decryption for 3.x and earlier; Dictionary and Reset for 2005 Premier
Netscape Mail	4.x to 6.x	Decryption
Omziff	1.0	Dictionary
OpenOffice	1.1 through 2.0	Dictionary
Paradox	5.x	Decryption
Password Pal	2.0	Decryption and Dictionary
Password Safe	1.0 through 2.x	Dictionary
PC-Encrypt	9.11	Decryption for password book files not encrypted with a password; Dictionary for all other cases
PDF (Adobe Acrobat)	Through 6.0	Dictionary and Keyspace
PFX	PFC files created by Windows 2000/XP	Dictionary
PGP	Through 9.0; GnuPG through 1.4.0	Dictionary
PGP Disk	Internal versions 4 and 6; 9.0 disk encryption	Dictionary
Protected Registry	Internet Explorer auto-complete data and Outlook Express SMTP passwords 5.0 and on	Decryption
ProWrite	Unknown	Decryption
PST (Outlook)	2003	Decryption
PWL	Win9X from Windows 95 release 2	Dictionary, Keyspace, and Decryption
Quattro Pro	1 through 12	Decryption
Quickbooks	2 through 2005	Decryption, Dictionary, and Reset
Quicken	Through 2006	Decryption, Dictionary, and Reset
RAR	1.x through 3.x	Dictionary
SafeHouse	2.0 through 2.1	Dictionary
SAM	All	Dictionary for NT and Keyspace LAN; Dictionary for startup passphrase job
Screensaver	Window 95	Decryption

Module	Supported Versions	Job Type
Secret Stuff (Norton)	1.0	Dictionary and Keyspace
SecureIT	3.1	Dictionary
SiFEU	0.9	Dictionary
SourceSafe	Through 6.x	Decryption
Steganos	7.1.x through 8.0.2; LockNote version 1.0.1	Dictionary and Decryption
S-Tools	4 (1996)	Dictionary
Symantec Q&A	4.x through 5.x	Decryption
Trillian	3.1	Decryption
VBA (Visual Basic for Applications)	Through Office 2003	Decryption, Dictionary, and Reset
VersaCheck	2001 (Home and Pro); Platinum 2004–2005; Enterprise 2004–2005	Decryption
Whisper32	1.16	Decryption
WinZip9	9.0 through 10.0	Dictionary
WordPerfect	5 through 12	Decryption
WordPro	96, 97, Millennium	Decryption
WS_FTP	2006	Decryption
XP Credentials	Windows XP, SP1, SP2	Decryption
Yahoo Messenger	5.x through 7.0	Decryption
ZIP	Pkzip, WinZip,	Dictionary and Keyspace