Password Protection And Encryption

J.P. McDonald
FBI Supervisory Special Agent
Laboratory Director
Philadelphia RCFL
jpmcdonald@rcfl.gov
www.phrcfl.org

Course Content

- Basic concepts in Cryptography
- Keyspace Dilemma
- Password Cracking/Recovery
- Rainbow Tables
- Other Code breaking tools
- Other ways to beat encryption

What is Cryptography

- Cryptography: The art and science of keeping messages/information secure
- Encryption: Transformation of data into unreadable form
- Decryption: Reverse of encryption

Applied Cryptography 2nd Addition – Bruce Schneier / RSA Laboratories FAQs about Cryptography Version 3 - 1996

Types of Encryption

- Access Protection
  - Not encrypted, just locked
- Data obfuscation
  - Encryption by way of scrambling (ROT13)
- Data encryption
  - Crypto systems

Password States

- Not stored
  - Application uses authentication sequence to verify (i.e. Word/Excel)
- Stored by User
  - Application offers to store, then obfuscate or encrypt (IE, Yahoo, Netscape)
- Stored by Application
  - EFS

Password Types

- Open/Modify Passwords (Word/Excel)
- Unlock
  - No encrypt, needed to open file (early Quicken)
- Administrator
- Password archives
  - PasswordSafe, PasswordsPlus, etc

Keyspace Values

Key: **Any One of a Larger Number of Values**

Keyspace: **Range of Possible Values**

(this can get big!)

20	1,048,576
30	1,073,741,824
32	4,294,967,296
33	8,589,934,592
40	1,099,511,627,776
50	1,125,899,906,842,620
56	72,057,594,037,927,900
60	1,152,921,504,606,850,000
70	1,180,591,620,717,410,000,000
80	1,208,925,819,614,630,000,000,000
90	1,237,940,039,285,380,000,000,000,000
100	1,267,650,600,228,230,000,000,000,000,000
110	1,298,074,214,633,710,000,000,000,000,000,000
120	1,329,227,995,784,920,000,000,000,000,000,000,000
128	340,282,366,920,938,000,000,000,000,000,000,000,000
160	1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000

Keyspace

Key Space Calculation Spreadsheet	
Key Space (# of bits)	40
Size of Key Space	1,099,511,627,776
Keys Tested Per Second	250,000
# of Machines	1
Time (in seconds)	4,398,047
Time (in hours)	1,221.680
Time (in days)	50.90
Time (in years)	0.139

Keyspace (Cont)

Key Space Calculation Spreadsheet	
Key Space (# of bits)	128
Size of Key Space	340,282,366,920,938,000,000,000,000,000,000,000
Keys Tested Per Second	250,000
# of Machines	1
Time (in seconds)	1,361,129,467,683,750,000,000,000,000,000,000
Time (in hours)	378,091,518,801,043,000,000,000,000,000.000
Time (in days)	15,753,813,283,376,800,000,000,000,000.00
Time (in years)	43,161,132,283,224,100,000,000,000.000

Code Breaking Tools

Password Cracking

Ability to recover passwords from well-known applications

- Decrypt files, folders, and hard drives
- Gain access to files protected by the Microsoft Encrypted File System (EFS)

Distributed Code Breaking

Ability to recover passwords and/or keys using:

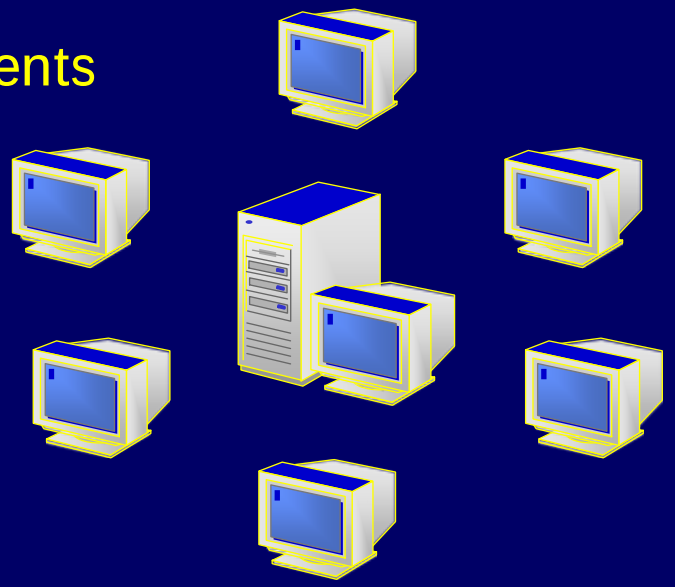
- Brute-Force attacks - Key-Space attacks - Pass-phrase attacks

– One system manages many Clients

– Distributed code breaking to many clients

- Apple Macintosh
- Linux
- UNIX
- Windows

– Uses 'Idle Process' time



Code Breaking Tools

- Access Data
  - Password Recovery Tool Kit (PRTK)
  - Distributed Network Attack (DNA)

Dictionary Attacks

- User Created – Inside/Outside PRTK
- Dictionaries
  - Common – Common English words
  - Passwords – Password lists (golden dictionary)
  - Crime – Sex and drugs
  - Misc – Keyboard combinations
  - Names – Common names
  - General – Webster like
  - Unicode
  - Registry information (Windows)

Code Breaking Lookup Tables
Rainbow Table Technology

- Use pre-generated cipher text – file encryption key lookup tables to derive the key that will open 40-bit encrypted MS-Excel and MS-Word files.
- Recovery time is on the order of 1-5 minutes per file regardless of the password
- Able to provide the users login LAN and Windows NT passwords (i.e. attacking the hashes in the SAM file)

Attacking 128-bit Cryptosystems

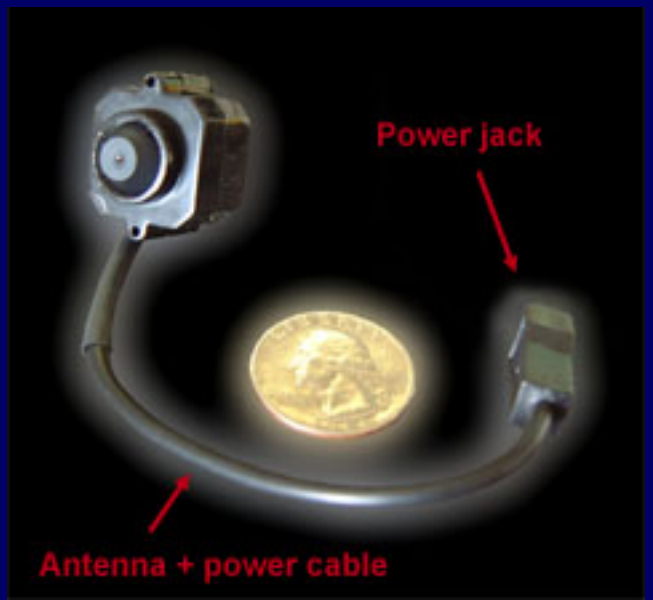
- BestCrypt, WinZip (AES), WinRAR, PGP, DriveCrypt, etc.
- Keyspace is to large for lookup tables to be an option
- Only option is to “guess” the user’s password
- Biographical Profiling Options
  - NTUSER.DAT File
  - Web Crawling
  - FTK Export Word List
- The sweet spot for password lengths are 7-10 characters.
- The more resources that can be dedicated to the problem the higher probably of success

Other Tools

- John the Ripper
  - Primarily a user authentication password cracker (logon)
    - Unix, Windows LAN hash
- LC5 L0phtcrack - @stake = Symantec
  - NLA

Other Ways to Beat Encryption

- Key Loggers
  - Hardware
  - Software
- Cameras




DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


PHILADELPHIA
RCFL
REGIONAL COMPUTER FORENSICS LABORATORY

Questions?