## Practical Issues

Of course my password is the same as my pet's name

My macaw's name was Q47pY!3 and I change it every 90 days

— Nick Simicich

## Practical Issues

Strong, effectively unbreakable crypto is universally available (despite US government efforts)

- Don't attack the crypto, attack the infrastructure in which it's used
- " " " " implementation
- " " " " users

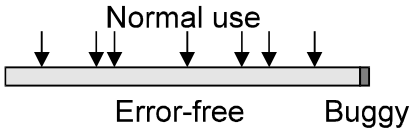
Many infrastructure/implementation details are treated as black boxes by developers

- Storage protection/sanitisation
- Long-term secret storage
- Key generation

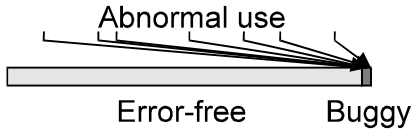
## Why Security is Harder than it Looks

All software has bugs

Under normal usage conditions, a 99.99% bug-free program will rarely cause problems




A 99.99% security-bug-free program can be exploited by ensuring the 0.01% instance is always encountered




This converts the 0.01% failure to 100% failure

## Why Security is Harder than it Looks (ctd)

Customers have come to expect buggy software

- Correctness is not a selling point
- Expensive and time-consuming software validation and verification is hard to justify

Solution: Confine security functionality into a small subset of functions, the trusted computing base (TCB)

- In theory the TCB is small and relatively easy to analyse
- In practice vendors end up stuffing everything into the TCB, making it a UTCB
- Consumers buy the product anyway (see above)

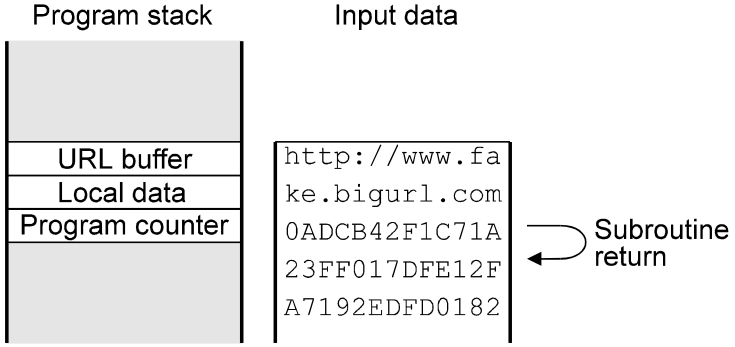
# Buffer Overflows

## In the last year or two these have appeared in

splitvt, syslog, mount/umount, sendmail, lpr, bind, gethostbyname(), modstat, cron, login, sendmail again, the query CGI script, newgrp, AutoSofts RTS inventory control system, host, talkd, getopt(), sendmail yet again, FreeBSD's crt0.c, WebSite 1.1, rlogin, term, ffbconfig, libX11, passwd/yppasswd/nispasswd, imapd, ipop3d, SuperProbe, lpd, xterm, eject, lpd again, host, mount, the NLS library, xlock, libXt and further X11R6 libraries, talkd, fdformat, eject, elm, cxterm, ps, fbconfig, metamail, dtterm, df, an entire range of SGI programs, ps again, chkey, libX11, suidperl, libXt again, lquerylv, getopt() again, dtaction, at, libDtSvc, eeprom, lpr yet again, smbmount, xlock yet again, MH-6.83, NIS+, ordist, xlock again, ps again, bash, rdist, login/scheme, libX11 again, sendmail for Windows NT, wm, wwwcount, tgetent(), xdat, termcap, portmir, writesrv, rcp, opengroup, telnetd, rlogin, MSIE, eject, df, statd, at again, rlogin again, rsh, ping, traceroute, Cisco 7xx routers, xscreensaver, passwd, deliver, cidentd, Xserver, the Yapp conferencing server, multiple problems in the Windows95/NT NTFTP client, the Windows War and Serv-U FTP daemon, the Linux dynamic linker, filter (part of elm-2.4), the IMail POP3 server for NT, pset, rpc.nisd, Samba server, ufsrestore, DCE secd, pine, dslip, Real Player, SLMail, socks5, CSM Proxy, imapd (again), Outlook Express, Netscape Mail, mutt, MSIE, Lotus Notes, MSIE again, libauth, login, iwsh, permissions, unfsd, Minicom, nslookup, zpop, dig, WebCam32, smbclient, compress, elvis, lha, bash, jidentd, Tooltalk, ttdbserver, dbadmin, zgv, mountd, pcnfs, Novell Groupwise, mscreen, xterm, Xaw library, Cisco IOS, mutt again, ospf_monitor, sdtcm_convert, Netscape (all versions), mpg123, Xprt, klogd, catdoc, junkbuster, SerialPOP, and rdist

# Buffer Overflows (ctd)

## Typical case: Long URL's




- Data at the end of the URL overwrites the program counter/return address
- When the subroutines returns, it jumps to the attackers code

## Fixing Overflow Problems

More careful programming

- Isolate security functionality into carefully-checked code

Make the stack non-executable

Compiler-based solutions

- Build bounds checking into the code (very slow)
- Build stack checking into the code (slight slowdown)
- Rearrange stack variables (no slowdown)

## Storage Protection

Sensitive data is routinely stored in RAM, but

- RAM can be swapped to disk at any moment
  - Users of one commercial product found multiple copies of their encryption password in the Windows swap file
  - "Suspend to disk" feature in laptops is particularly troublesome
- Other processes may be able to read it from memory
- Data can be recovered from RAM after power is removed

## Protecting Memory

Locking sensitive data into memory isn't easy

- Unix: `mlock()` usable by superuser only
- Win16: No security
- Win95/98: `VirtualLock()` does nothing
- WinNT: `VirtualLock()` doesn't work as advertised (data is still swapped)
- Macintosh: `HoldMemory()`

Scan memory for data:

```
VirtualQueryEx()
VirtualUnprotectEx()
ReadProcessMemory()
```

## Protecting Memory (ctd)

Create DIY swapfile using memory-mapped files

- Memory is swapped to a known file rather than system swapfile
- File is wiped after use

Problems:

- Truly erasing disk data is impossible
- Data isn't wiped on system crash/power loss

## Protecting Memory (ctd)

Force memory to remain in use at all times

- Background thread touches memory periodically

Allocate non-pageable memory

- Requires a kernel driver
- Mapping memory from kernel to user address space is difficult

## Storage Sanitisation

Problems in erasing disk data

- Defect management systems move/remap data, making it inaccesible through normal means
- Journaling filesystems retain older data over long periods of time
- Online compression schemes compress fixed overwrite patterns to nothing, leaving the target data intact
- Disk cacheing will discard overwrites if the file is unlinked immediately afterwards (Win95/98, WinNT)
  - Many Windows file-wipers are caught by this

## Recovering Data

One or two passes can be easily recovered by “error cancelling”

- Read actual (digital) data
- Read raw analog signal
- Subtract expected signal due to data from actual analog signal
- Result is previous (overwritten) data

US government standard (DoD 5200.28) with fixed patterns (all 0’s, all 1’s, alternating 0’s and 1’s) is particularly bad

Design overwrite patterns to match HD encoding methods

## Advanced Data Recovery

Ferrofluid + optical microscopes

- Defeated by modern high-density storage systems

Scanning probe microscopes overcame this problem

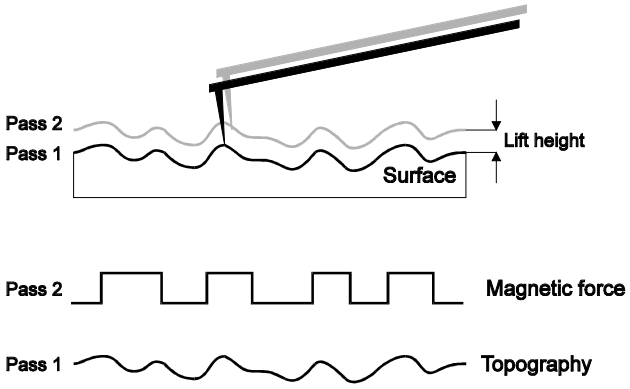
- Oscillating probe is scanned across the surface of the object
- Change in probe movement measured by laser interferometer

Can be built for a few thousand dollars

Commercial ones specifically set up for disk platter analysis are available

# Advanced Data Recovery (ctd)

Magnetic force microscope (MFM)




1. Read disk topography
2. Read magnetic force (adjusted for topography)

# Advanced Data Recovery (ctd)

MFM's can be used as expensive read channels, but can do far more

- Erase bands (partially-overwritten data at the edges) retain previous track images
- Overwriting one set of data with another causes track width modulation
- Erased/degaussed drives can often still be read with an MFM
  - Modern high-density media can't be effectively degaussed with commercial tools

## Advanced Data Recovery (ctd)

Recommendations

- Use the smallest, highest-density drives possible
- If data is sensitive, destroy the media
  - Where does your returned-under-warranty drive end up?
  - For file servers, business data, always destroy the media (there's always something sensitive on there)

## Recovering Memory Data

Electrical stress causes ion migration in DRAM cells

Data can be recovered using special (undocumented) test modes which measure changes in cell thresholds

- At room temperature, decay can take minutes or hours
- At cryogenic temperatures, decay can take weeks? months?

A quick overwrite doesn't help much

Solution is to only store data for short periods

- Relocate data periodically
- Toggle bits in memory

## Random Number Generation

Key generation requires large quantities of unpredictable random numbers

- Very difficult to produce on a PC
- Most behaviour is predictable
- User input can be unpredictable, but isn't available on a standalone server

Many implementations leave it to application developers (who invariably get it wrong)

## Bad RNG's

Netscape

```
a = mixbits( time.tv_usec );
b = mixbits( getpid() + time.tv_sec + ( getppid() <<
  12 );
seed = MD5( a, b );

nonce = MD5( seed++ );
key = MD5( seed++ );
```

Kerberos V4

```
srandom( time.tv_usec ^ time.tv_sec ^ getpid() ^
  gethostid() ^ counter++ );
key = random();
```

## Bad RNG's (ctd)

MIT_MAGIC_COOKIE

```
key = rand() % 256;
```

SESAME

```
key = rand();
```

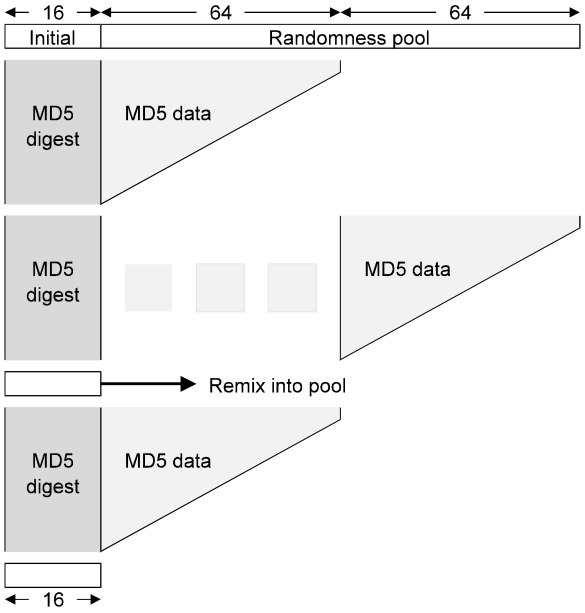
## Types of Generator

Generator consists of two parts

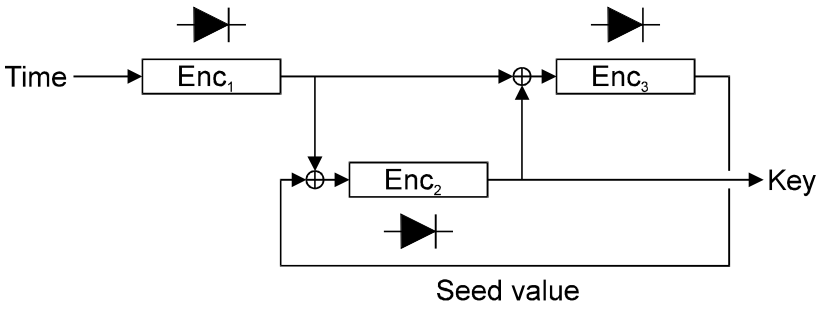
- Polling mechanism to gather random data
- Pseudo-random number generator (PRNG) to "stretch" the output

| | |
|---|---|
| Physical source | Various hardware generators, Hotbits (radioactive decay), Lavarand |
| Physical source + postprocessing | SG100 |
| Multi-source polling | SKIP, cryptlib |
| Single-source polling | PGP 2.x, PGP 5.x, `/dev/random` |
| Secret nonce + PRNG | Applied Cryptography, BSAFE |
| Secret fixed value + PRNG | ANSI X9.17 |
| Known value + PRNG | Netscape, Kerberos V4, Sesame, and many more |

# Example: Unix `/dev/random`




# Example: ANSI X9.17




Relies on strength of triple DES encryption and supplied encryption key

## Randomness Sources

- Process and thread information
- Mouse and keyboard activity
- Memory and disk usage statistics
- System timers
- Network statistics
- GUI-related information

Run periodic background polls of sources

Try and estimate the randomness available, if insufficient

- Perform further polling
- Inform the user

## Effectiveness of the Randomness Source

Effects of configuation

- Minimal PC hardware (one HD, one CD) produces half the randomness of maximum PC hardware (multiple HD's, CD, network card, SCSI HD and CD)

Effects of system load and usage

- Statistics change little over time on an unloaded machine
- A reboot drastically affects the system state
  - Reboot the machine after generating a high-value key

## TEMPEST

Sometimes claimed to stand for Transient Electromagnetic Pulse Emission Standard

Known since the 1950's, but first publicised by van Eck in 1985

- Provided details on remote viewing of computer monitors
- Required about $15 worth of parts (for sync recovery)
- The spooks were not happy

## TEMPEST Principles

Fast-rise pulses lead to harmonics radiated from semiconductor junctions

- Used to detect bugs
  - – Flood the room with microwaves
  - – Watch for radiated responses

Anything which carries a current acts as an antenna

TEMPEST monitoring gear receives and interprets this information

## TEMPEST Sources

Computer monitor/laptop screen

- Generally radiates huge amounts of signal (range of hundreds of metres)
- Most signal is radiated to the sides, little to the front and back
- Requires external horizontal/vertical sync insertion, since sync frequencies are too low to be radiated
- Individual monitors can be picked out even when other similar monitors are in use
- Jamming is often ineffective for protection
  - Eavesdroppers can still zero in on a particular monitor

## TEMPEST Sources (ctd)

Keyboard

- Some keyboards produce distinct RF signatures for each key pressed
- Active monitoring
  - Beam RF energy at the keyboard cable
  - Reflected signal is modulated by abscence/presence of electrical current

Ethernet

- UTP can be intercepted over some distance

## TEMPEST Sources (ctd)

Printer and serial cables

Leakage into power lines

Coupling into power lines, phone lines, metal pipes

- Further radiation from there

Surface waves on coax lines

## TEMPEST Protection

Extremely difficult to protect against

Stopping it entirely

- Extreme amounts of shielding on all equipment
- Run the equipment inside a Faraday cage

Stopping it partially

- FCC Class B computers and equipment
- RF filters on power lines, phone lines
- Shielded cables
- Ferrite toroids around cables to attenuate surface waves
- Radio hams have information on safely operating computers near sensitive comms gear

Use a portable radio as a simple radiation tester

## Snake Oil Cryptography

Named after magic cure-all elixirs sold by travelling medicine salesmen

Many crypto products are sold using similar techniques

- The crypto has similar effectiveness
- This is so common that there's a special term, "snake oil crypto", to describe it

## Snake Oil Warning Signs

Security through obscurity

- "Trust me, I know what I'm doing"
  - They usually don't
- Most security through obscurity schemes are eventually broken
  - Once someone finds out what your secret security system is, it's no longer a secret and no longer secure
  - It's very hard to keep a secret on the net

Proprietary algorithms and revolutionary breakthroughs

- "I know more about algorithm design than the entire world's cryptographers"
- Common snake oil warning signs are use of cellular automata, neural nets, genetic algorithms, and chaos theory
- See "security through obscurity"

## Snake Oil Warning Signs (ctd)

Unbreakability

- Usually claimed by equating the product to a one-time-pad
- Product isn't a one-time-pad, and therefore not unbreakable

"Military-grade crypto"

- Completely meaningless term (cf "military-grade spreadsheet")
  - Military tends to use hardware, civilians use software
  - Prefer shift-register based stream ciphers, everyone else uses block ciphers
  - Keys are generally symmetric and centrally managed, everyone else uses distributed PKC keys
- Products should therefore be advertised as "nothing like military-grade crypto"

## Snake Oil Warning Signs (ctd)

Technobabble

- Use of terms unknown to anyone else in the industry

Used by *xyz*

- Every product, no matter how bad, will gain at least one big-name reference customer

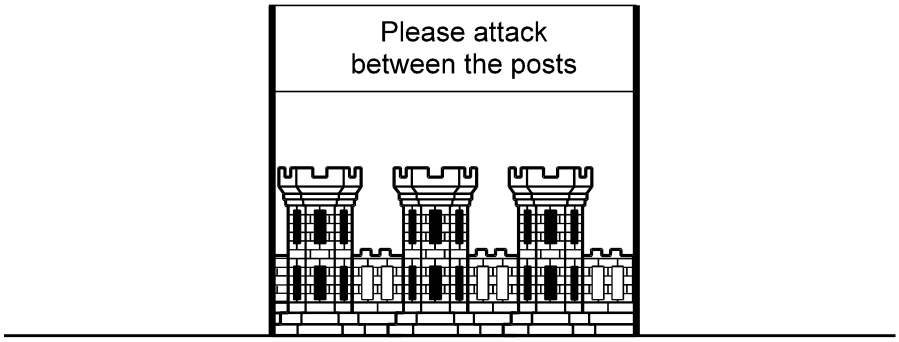
Exportable from the US

- Except for special-purpose cases (eg SGC), the US government will not allow the export of anything which provides real security
- If it's freely exportable, it's broken

## Snake Oil Warning Signs (ctd)

Security challenges

- Generally set up to make it impossible to succeed




- These things always get the media's attention, especially if the reward is huge (chance of press coverage = 20% per zero after the first digit)

## Snake Oil Warning Signs (ctd)

Would you buy this product?

- "Our unbreakable military-grade bi-gaussian cryptography, using a proprietary one-time-pad algorithm, has recently been adopted by a Fortune 500 customer and is available for use inside and outside the US"

Badly marketed good crypto is indistinguishable from snake oil

- If you're selling a crypto product, be careful how your marketing people handle it
  - If left to their own devices, they'll probably sell it as snake oil

## Snake Oil in the Media

Magazine reviews are a poor gauge of software security

WinXFiles (trivially broken file encryption)

- PC Answers: Listed in “10 proven security programs”
- Windows News: Listed in “75 best Windows utilities”
- FileMine: Rated as a Featured Jewel
- Shareware Junkies: 5 stars, “a must have for anyone sharing a computer with files they want to keep private”
- PC Format: “Unbeatable and excellent file encryption”
- TUCOWS: Rated 4 cows
- Ziff-Davis Interactive: 5 stars, “keeps files and data on your PC as safe as if they were under lock and key”

*more*

## Snake Oil in the Media (ctd)

*continued*

- The Windows95 Application List: “an excellent application for protecting your personal files”
- RocketDownload: Four smilies
- “Simply the Best” site award

One major publication once rated a collection of encryption programs by how good the user interface looked

## Snake Oil Case Study

Meganet Virtual Matrix Encryption

- "A new kind of encryption and a new algorithm, different from any existing method"
- "By copying the data to a random built-in Virtual Matrix, a system of pointers is being created. ..."
- "The worlds first and only unbreakable crypto"
- "We challenged the top 250 companies in the US to break our products. None succeeded"
  - They don't even know Meganet exists
- "55,000 people tried to break our product"
  - 55,000 visited their web page
- "Working on standardising VME with the different standards committees"

## Snake Oil Case Study (ctd)

Challenged large companies to break their unbreakable crypto

- Enumerate each company in the PR to ensure that their name is associated with large, publicly held stocks

Used accounts at organisations like BusinessWire and PRNewswire to inject bogus press releases into newswires

- Run anything at $500 for 400 words
- Claimed IBM was so impressed with their product that they were recommending it for the AES
  - IBM had never heard of them

## Snake Oil (ctd)

Big-name companies sell snake oil too

Tools exist to recover passwords for

- Adobe Acrobat
- ACIUS 4th Dimension
- Arj archives
- Clarion
- Claris Filemaker Pro
- CompuServe WinCim
- dBASE
- Diet compressed files
- Eudora
- ICQ
- Lotus Ami-Pro
- Lotus 1-2-3

*Continues*

## Snake Oil (ctd)

*Continued*

- Lotus Organiser
- Lotus Symphony
- LZEXE compressed files
- MS Access
- MS Excel
- MS Mail
- MS Money
- MS Outlook
- MS Scheduler
- MS Word
- MYOB
- Norton Secret Stuff
- Paradox

*Continues*

## Snake Oil (ctd)

*Continued*

- Pegasus Mail
- Pklite compressed files
- Pkzip archives
- Q&A Database
- Quattro Pro
- QuickBooks
- Quicken
- Stacker
- Symantec Act
- Trumpet Winsock
- VBA projects
- WinCrypt
- Windows 3.1/95/98 passwords

*Continues*

## Snake Oil (ctd)

*Continued*

- Windows Dial-up Networking (DUN)
- Windows NT passwords
- WinXFiles
- WordPerfect
- WS FTP

... and many, many more

## Selling Security

Security doesn't sell well to management

Many security systems are designed to show due diligence or to shift blame

- Crypto/security evidence from these systems is very easy to challenge in court

You get no credit if it works, and all the blame if it doesn't

To ensure good security, insurance firms should tie premiums to security measures

- Unfortunately, there's no way to financially measure the effectiveness of a security system

## Selling Security to Management

Regulatory issues

- Liability for negligence (poor security/weak crypto)
- Shareholders could sue the company if share price drops due to security breach
- US companies spend more on security due to litigation threats

Privacy/data protection requirements

Media stories of hacker/criminal attacks on systems

The best security customers

- Have just been publicly embarrassed
- Are facing an audit