



Hour 3:

**Information Disclosure;
Watermarking;
Steganography**



Assuring Confidentiality

Prevent unauthorized disclosure of confidential information.

Where is the data?

- *Data in flight*
- Stored data

Most data spends most of its time in *storage*.





Hard Drives Pose Special Problem For Computer Security

Do not forget data when power is removed.

Can contain data that is not immediately visible.

Today's computers can read hard drives that are 15 years old!

- Electrically compatible (IDE/ATA)
- Logically compatible (FAT16/32 file systems)
- Very different from tape systems

Strong social bias against destroying a working drive



Other Stories of Data Passed...

April 1997

- A woman in Pahrump, NV, purchases a used IBM PC and discovers records from 2000 patients who had prescriptions filled at Smitty's Supermarkets pharmacy in Tempe, AZ.

August 2001

- More than 100 computers from Viant with confidential client data sold at auction by Dovebid.

Spring 2002

- Pennsylvania state Department of Labor and Industry sells computers with "thousands of files of information about state employees."

August 2002

- Purdue student purchased used Macintosh computer at equipment exchange; computer contains FileMaker database with names and demographic information of 100 applicants to Entomology Department.



With so many used systems, why so few stories of actual data disclosure

Hypothesis #1: Disclosure of “data passed” is exceedingly rare because most systems are properly sanitized.

Hypothesis #2: Disclosures are so common that they are not newsworthy.

Hypothesis #3: Systems aren’t properly sanitized, but few notice the data.



How could people not notice the data?

DEL removes the file’s name...
... but doesn’t delete the file’s data

```
cmd C:\WINDOWS\system32\cmd.exe
C:\tmp>dir
Volume in drive C has no label.
Volume Serial Number is 1410-FC4A

Directory of C:\tmp
10/15/2004 09:20 PM <DIR> .
10/15/2004 09:20 PM <DIR> ..
10/03/2004 11:34 AM 27,262,976 big_secret.txt
               1 File(s)      27,262,976 bytes
               2 Dir(s)      4,202,078,208 bytes free

C:\tmp>del big_secret.txt

C:\tmp>dir
Volume in drive C has no label.
Volume Serial Number is 1410-FC4A

Directory of C:\tmp
10/15/2004 09:22 PM <DIR> .
10/15/2004 09:22 PM <DIR> ..
               0 File(s)      0 bytes
               2 Dir(s)      4,229,296,128 bytes free

C:\tmp>_
```



How could people not notice the data?

FORMAT C: writes a new root directory...

```
C:\WINDOWS\system32\cmd.exe - format c:
C:\>format c:
The type of the file system is NTFS.
WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)?
```



FORMAT is misleading

```
A:\>format c:
```

```
WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
proceed with Format (Y/N)?y
```

```
Formatting 1,007.96M
```

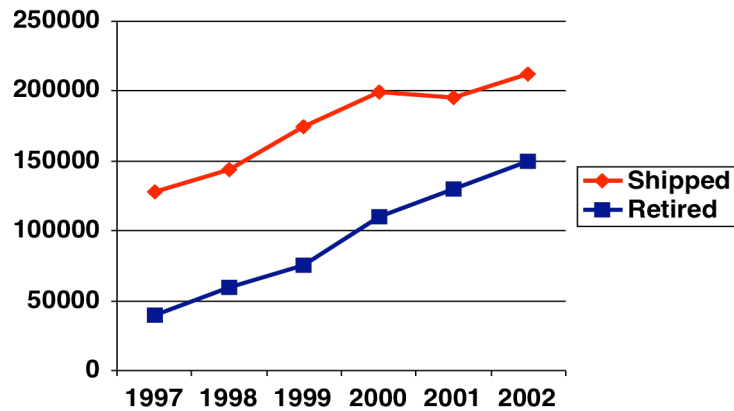
```
100 percent completed.
```

```
Writing out file allocation table
```

```
Complete.
```



149M Drives Retired in 2002!



Many hard drives are “repurposed,” not “retired”

Re-used within an organization

Given to charities

Sold on eBay



All Categories [Save this search](#)
350 items found for hard drives
Sort by items: [ending first](#) | [newly listed](#) | [lowest priced](#) | [highest priced](#)

Picture	Item Title	Price	Bids	Time Left
	Lot of hard and floppy drives	\$5.50	2	14h
	Lot of hard and floppy drives	\$5.50	2	22h
	Lot of hard and floppy drives	\$5.50	2	25h
	Lot of 2 hard drives IDE	\$8.00	12	29h
	3.2 gig Hard Drives	\$180.00	-	59h
	CD 1.2 hard drives & (10, 10/100 network	\$25.00	1	1h 00m
	Lot of 3 Quantum 9.1 gig SCSI Hard Drives	\$26.00	6	1h 25m
	IDE HARD DRIVES (3)	\$6.50	6	1h 46m
	LOT OF 5 Hard Drives! 3.2 Gig Western Digital	\$120.00	-	1h 50m
		\$124.95 <i>Buy Now</i>		
	QTY 3 IDE Hard Drives 2.5 Gig	\$20.50	5	2h 02m
	5 WESTERN DIGITAL 2.5 GIG HARD DRIVES	\$30.00	4	2h 03m
	QTY 3 IDE Hard Drives 1.0 Gig	\$9.99	1	2h 04m
	Western Digital 850 meg IDE Hard Drives (batch)	\$6.00	1	2h 57m
	WINDOWS	\$6.00	-	3h 18m



Long-Term Data Storage Threatens Confidentiality

Techniques for assuring confidentiality:

- #1 - Physical security
- #2 - Logical access controls (operating system)
- #3 - Cryptography (disk & link)



Repurposed disks...

Techniques for assuring confidentiality:

- ~~#1 - Physical security~~
- ~~#2 - Logical access controls (operating system)~~
- #3 - Cryptography (disk & link)

... and most data isn't encrypted



Weird Stuff, Sunnyvale California, January 1999

10 GB drive: \$19 “tested”

500 MB drive: \$3 “as is”



Q: “How do you sanitize them?”

A: “We FDISK them!”



FDISK does not sanitize disks

10 GB drive: 20,044,160 sectors

“FDISK”

- Writes 2,563 sectors (0.01%)

“FORMAT”

- Writes 21,541 sectors (0.11%)
- Erases the FAT
- (complicates recovery of fragmented files.)



The “Remembrance of Data Passed” Study

I purchased 235 used hard drives between November 2000 and January 2003

- eBay
- Computer stores
- Swap fests
- No more than 20 from the same vendor

Mounted the drives, copied off the data, looked at what I found.



A typical hard disk

Factory-Fresh Hard disk: All Blank

0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

Each block is
512 bytes

A 20G disk has
40M blocks.

Disk blocks (not to scale)



% format C:*

Writes:

- Boot blocks
- Root directory
- "File Allocation Table" (FAT)
- Backup "superblocks" (UFS/FFS)

B	F	F	F	/	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

May also:

- Validate surface

* Examples based on FAT32 running under Unix



% cp bfs1 /mnt/b1

% cp bfs2 /mnt/b2

Writes:

- File Contents
- File Directory Entry
- Bookkeeping

B	F	F	F	/b1	/b2	0
← Big Secret File #1						0
← Big Secret File #2						0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

root directory:

```
b1 _____ . ____  jan 1 2004  block  7
b2 _____ . ____  jan 1 2004  block 14
```

●
●
●
●
●
●

% rm /mnt/b1
% rm /mnt/b2

Writes:

- New root directory
- Bookkeeping

B	F	F	F	/?1	/?2	0
Big Secret File #1						0
Big Secret File #2						0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

new root directory:

```

?1 .      jan 1 2004  block  7
?2 .      jan 1 2004  block 14
  
```

●
●
●
●
●
●

% cp Madonna.mp3 /mnt/mp3

Writes:

- New root directory
- madonna.mp3
- Bookkeeping

B	F	F	F	/mp3	/?2	0	
Madonna						Big Secret File #1	0
← Big Secret File #2						0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	

new root directory:

```

Madonna .mp3  jan 2 2004  block  7
?2 .      jan 1 2004  block 14
  
```



What's on the disk?

Madonna.mp3
"Level 0 data"

Madonna.mp3's directory entry

All of B2
"Level 2 data"

Most of B2's directory entry

Part of B1
"Level 3 data"

B	F	F	F	/mp3	/?2	0
Madonna					et File #1	0
Big Secret File #2						0
0	0	0	0	0	0	0
0	0	0	0	0	0	0



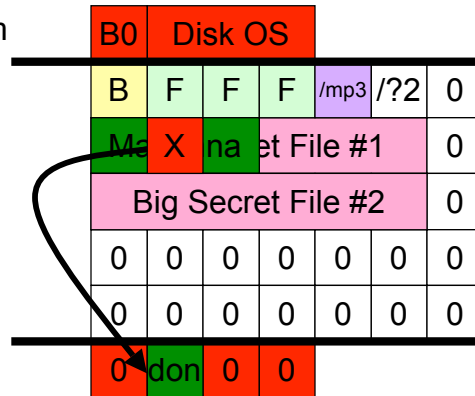
Taxonomy of hard disk data

Level 0	Files in file system
Level 1	Temp files (/tmp, /windows/tmp, etc)
Level 2	Recoverable deleted files
Level 3	Partially over-written files
Level 4	Data accessible by vendor commands
Level 5	Overwritten data



Level 4 Data: Vendor Area

Disk operating system

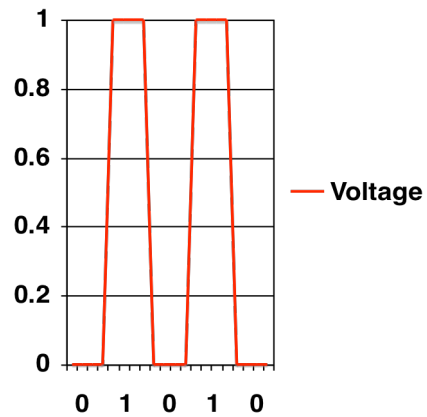


Bad block regions



Level 5: Overwritten Data

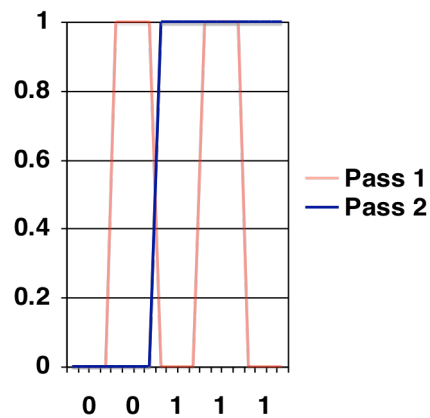
Disk Drives are analog devices





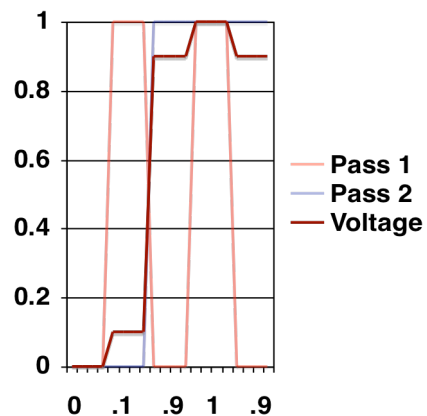
Level 5: Overwritten Data

Disk Drives are analog devices
Overwritten data doesn't just die...



Level 5: Overwritten Data

Disk Drives are analog devices
Overwritten data doesn't just die...
Read data *should* be a function of all previous data values...





Level 5: What to do?

DOD 5220.22-M

- “Degauss with a Type I degausser”
- “Degauss with a Type II degausser”
- “Overwrite all locations with a character, it’s complement, then a random character and verify”
- Destroy, Disintegrate, incinerate, pulverize, shred, or melt



Type 1 Degausser

Model HD-2000

73 seconds cycle time

260 lbs

\$13,995

Monthly rental \$1,400



Note:

- Your hard disk won’t work after it’s been degaussed (why not?)

<http://www.datadev.com/v90.htm>



Drive Slagging

Melting down the drives works just fine



<http://driveslag.eecue.com/>



Drive Slagging Cont...





Drive Slagging

“Good luck removing data from this.”



The Bad News:

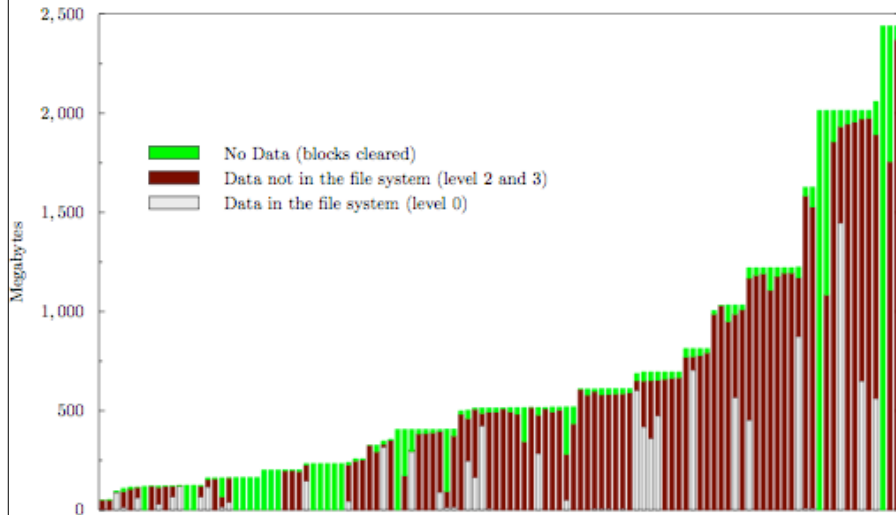
Most people aren't using these techniques

Data is discovered on old hard drives...

- Used computers with hard drives.
- Computers discovered in the trash.
- Drives purchased on the “used” market.



[Garfinkel '04] details 235 drives purchased on the used market.



Example: Disk #70 purchased for \$5 from a Mass. Retail store on eBay.

IBM-DALA-3540/81B70E32

541MB

- 1,057,392 disk blocks
- 67,878 blocks are all NULs

```
-rw-r----- 1 simsong project      675 Aug  9 2002 70.fdisk  
-r--r----- 1 root    project 541384704 Aug  9 2002 70.img  
-rw-r----- 1 simsong project  205892 Aug  9 2002 70.tar.gz
```



70.fdisk: the disk partition report

```
***** Working on device /dev/ad2 *****
parameters extracted from in-core disklabel are:
cylinders=524 heads=32 sectors/track=63 (2016 blks/cyl)

parameters to be used for BIOS calculations are:
cylinders=524 heads=32 sectors/track=63 (2016 blks/cyl)

Media sector size is 512
Warning: BIOS sector numbering starts with sector 1
Information from DOS bootblock is:
The data for partition 1 is:
sysid 11,(DOS or Windows 95 with 32 bit FAT)
  start 63, size 1054305 (514 Meg), flag 80 (active)
    beg: cyl 0/ head 1/ sector 1;
    end: cyl 522/ head 31/ sector 63
The data for partition 2 is:
<UNUSED>
The data for partition 3 is:
<UNUSED>
The data for partition 4 is:
<UNUSED>
```



70.tar.gz: Level 0 files

```
% tar tfz images/tar.gz/70.tar.gz
./
IO.SYS
MSDOS.SYS
COMMAND.COM
%
```




70.img ..

Appears to have some kind of medical information on it.

MAB-DEDUCTIBLE
MAB-MOOP
MAB-MOOP-DED
METHIMAZOLE
INSULIN (HUMAN)
COUMARIN ANTICOAGULANTS
CARBAMATE DERIVATIVES
AMANTADINE
MANNITOL
MAPROTILINE
CARBAMAZEPINE
CHLORPHENESIN CARBAMATE
ETHINAMATE
FORMALDEHYDE
MAFENIDE ACETATE
s@ MALATHION
MAZINDOL
NOMIFENSINE MALEATE
PIPOBROMAN



Drive #227

No obvious files, but lots of deleted files...

```
cluster 51152 looks like a directory...
07/17/1995 21:38      <DIR>          .                (cluster 51152 / sector 409677)
08/23/1993 11:41      1,818 ?GMLTR WPS:del (cluster 11381 / sector 91509)
08/23/1993 11:11      2,714 ?MDAGMT WPS:del (cluster 11382 / sector 91517)
07/22/1993 12:05      2,068 ?BBLTR WPS:del (cluster 11383 / sector 91525)
08/23/1993 11:56      1,434 ?BBLTR2 WPS:del (cluster 11384 / sector 91533)
06/21/1993 09:29      3,610 ?ONTRACTWPS:del (cluster 11385 / sector 91541)
07/26/1993 14:44      4,250 ?ONTRX90WPS:del (cluster 11386 / sector 91549)
07/26/1993 11:52      2,202 ?VRLTR WPS:del (cluster 11388 / sector 91565)
06/21/1993 10:12      2,202 ?VRLTR1 WPS:del (cluster 11389 / sector 91573)
07/09/1993 12:45      2,202 ?VRLTR2 WPS:del (cluster 11390 / sector 91581)
07/08/1993 12:41      5,018 ?CS1 WPS:del (cluster 11391 / sector 91589)
07/22/1993 11:11      5,414 ?CSLTR WPS:del (cluster 11393 / sector 91605)
09/06/1993 14:49      8,284 ?AILABL2WPS:del (cluster 11395 / sector 91621)
07/12/1993 10:59      788 ?AILLAB :del (cluster 11398 / sector 91645)
07/07/1993 11:18      8,808 ?AILLABLWPS:del (cluster 11399 / sector 91653)
07/26/1993 23:35      34,616 ?EWPRAC BFX:del (cluster 11402 / sector 91677)
07/27/1993 07:30      2,458 ?EWPRAC WPS:del (cluster 11411 / sector 91749)
06/02/1993 15:02      2,720 ?BSSRV :del (cluster 11412 / sector 91757)
06/02/1993 15:11      42,272 ?BSSRV BFX:del (cluster 11413 / sector 91765)
06/02/1993 15:02      2,720 ?BSSRV WPS:del (cluster 11424 / sector 91853)
08/01/1993 14:35      7,974 ?TRAGMT WPS:del (cluster 11425 / sector 91861)
06/21/1993 09:51      2,976 ?URVEY WPS:del (cluster 11427 / sector 91877)
```



Drive #227

Sometimes just the directory is deleted...

```
cluster 19401 looks like a directory...
06/18/1995 12:39      1,715 POEMS11 WPS      (cluster 14827 / sector 119077)
04/14/1995 17:34      7,620 LATADD WDB      (cluster 14828 / sector 119085)
06/19/1995 16:09      1,459 POEM7 WPS       (cluster 14829 / sector 119093)
06/12/1995 15:35      1,178 POEMS22 WPS     (cluster 14830 / sector 119101)
06/18/1995 12:39      1,452 POEMS13 WPS     (cluster 14831 / sector 119109)
06/18/1995 13:23      1,459 POEMS14 WPS     (cluster 14832 / sector 119117)
06/18/1995 12:39      1,459 POEM WPS        (cluster 14833 / sector 119125)
06/18/1995 12:46      1,196 POEMS17 WPS     (cluster 14834 / sector 119133)
06/18/1995 12:47      1,069 POEMS18 WPS     (cluster 14835 / sector 119141)
06/18/1995 12:47      1,197 POEMS19 WPS     (cluster 14836 / sector 119149)
08/24/1994 14:08        660 LABEL WPS        (cluster 14837 / sector 119157)
06/18/1995 12:48      1,331 POEMS20 WPS     (cluster 14838 / sector 119165)
11/18/1994 17:40      1,300 ENG WPS         (cluster 14839 / sector 119173)
06/18/1995 12:50      1,203 POEMS21 WPS     (cluster 14840 / sector 119181)
06/19/1995 16:33      4,847 POEMS3 WPS      (cluster 14841 / sector 119189)
06/18/1995 12:50      1,069 POEMS23 WPS     (cluster 14842 / sector 119197)
```



USB Drives & Digital Cameras

Everything about hard drives applies to other storage media that is treated as a “hard disk.”

Most are formatted with FAT32



Example: Digital Photography

Many police have forced photographers to “delete” images they didn’t want taken.

- Ground Zero, post-9/11. Unnamed photographer forced by police to delete photos. Was able to recover with help from slashdot.
- College student Mohammed Budeir, Philadelphia, Sept. 4, 2002, taking photographs of police cars.
<http://www.copcar.com/mo0902.htm>
- Airlines.net photographer Daniel Wojdylo, forced to delete photos photographed at BUF in April 2002.

Google for:

- officer made me delete pictures in my digital camera



Sanitizing requires special programs that are not included with the operating system.

`dd if=/dev/zero of=/dev/ad2`

AutoClave

- <http://staff.washington.edu/jdlarious/autoclave>

DBAN

- <http://dban.sourceforge.net/>

DataGone

- <http://www.symantec.com/> -- ?

SecureClean

- <http://www.bluesquirrel.com/so/secureclean/>



Watermarking and Steganography



Watermarks

First introduced in Bologna, Italy in 1282

Dandy Roll presses pattern into drying paper

- Changes thickness of paper fibers

Uses:

- By paper makers to identify their product
- Security for stamps, official documents.
- Stock certificates, money, etc.
- Chic

Other “watermarks”

- Printing on plastic with a window.
(Australian \$10 note)





Dandy Roll

Pressed into paper during paper-making process

- Dandy roll
- 7.25" diameter
- Watermarking possible



J. Plank Features

- In-house watermark design
- Computerized design process
- Quick-change sleeves and sections



Quality Dandy and Watermark Rolls
Since 1907



<http://www.uwsp.edu/papersci/PM/Machine/Dandy.htm>



Dandy Roll

Wet pulp sprayed onto moving belt

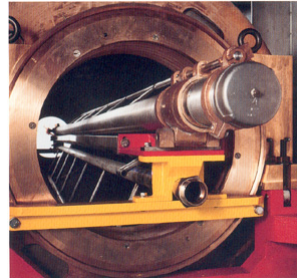
Dandy Roll pressed into pulp

Dandy Roll looks like oversized printer's roll covered with pattern

High grade stainless steel construction

Incorporates internal oscillating shower, internal pan, internal steam shower and external saveall pan

Extended Header Brush for easy cleaning of shower pipe



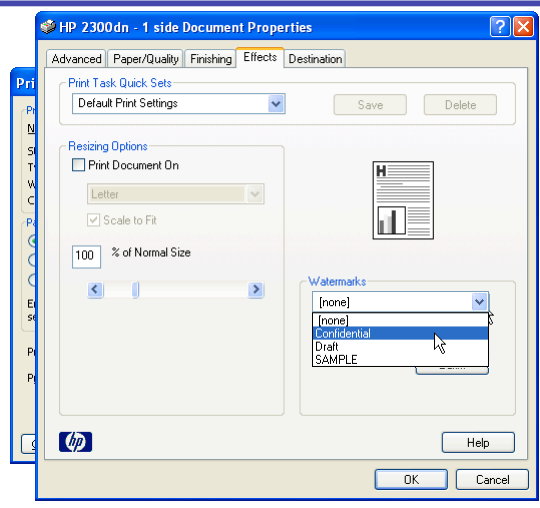


Laser Printed "Watermarks"

Used on bond paper, but who uses bond paper?

- Doesn't work well in inkjets or laserjets

"Watermarks" with most print drivers...

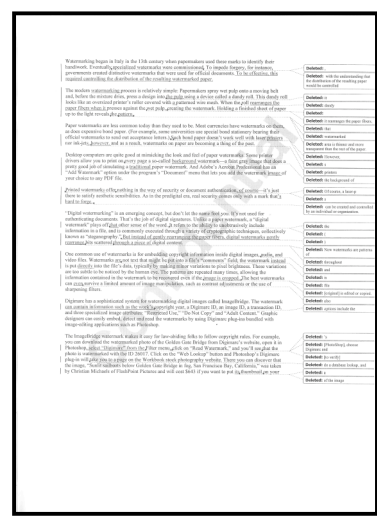


Printed Watermarks

Looks great

You can even put it in your PDF file...which is the problem!

No security





Printed Document Authentication Techniques

Microprinting – Print that is too small to produce or copy with conventional equipment

Intaglio –engraved pattern used to press ink with great force; raised letters

Letterpress – Ink rolled raised type, leaving depression. Used for printing numbers.

Simultan press – precise registration of front and back. (*see-through register*). Changing ink colors (*rainbowing*).

Optically variable inks (change color depending on angle)

Metal foils & threads embedded in paper

Security holograms



Lessons for paper authentication

Security features should convey a message relevant to the product.

- Use iridescent ink to print the banknote denomination

Should obviously belong where they are

- They become “embedded in the user’s cognitive model.”

Should be obvious

Should not have competitors

Should be standardized

Source: *Security Engineering*, Anderson



Information Hiding

Copyright Marks:

- Watermarks - Hidden copyright messages
- Fingerprints – Hidden serial numbers

Steganography

- Hidden messages.

Other applications:

- Closed captioning (hidden in first 21 scan lines)
 - <http://www.robson.org/gary/writing/nv-line21.html>
- Audio RDS (Radio Data Service)-like service
 - “What’s that song?”



Watermarks for Copyright Policy

“never copy”

“copy only once”

“copy only at low quality”

JPMG Linnartz, “The ‘Ticket’ Concept for Copy Control Based on Embedded Signaling” (Anderson [504]) Suggests a hash-based implementation of “copy only once.”

- X is the ticket
- Record $h(h(X))$ on DVD
- Provided with Y on the disk, DVD recorded stores $h(Y)$ on next-generation copy.
- Player refuses to play if it finds $h(h(X))$



Steganography means “hidden writing.”

- A message that can't be found by humans
- A message that can't be found by an algorithm.
- A message that can be found by an algorithm but not by a human.
- A message that can be found by some algorithms but not others.

[Wayner 2004]



What is Hidden?

Defining "Hidden" is not easy

- We run into the usual Gödel limits that prevent us from being logical about detection.
- Humans are very different. Some musicians have very good ears.
- Some algorithms leave statistical anomalies.
 - Messages are often **more random** than the carrier signal.
 - These statistics can give away the message.



Who wants steganography?

Evil doers.

- If evil messages can't be seen by good people, evil will triumph.
- *Osama bin Laden?*

Good doers.

- If the good guys can communicate in secret, then good will triumph.
- *U.S. forces?*

Content owners and copyright czars.

- Hidden messages can carry information about rights to view, copy, share, listen, understand, etc.

Software Developers.

- "Hidden" channels can be added to data structures without crashing previous versions. Steganography can fight bit rot.



Models for Steganography

Replace random number generators with the message.

- This works if the random numbers are used in a detectable way.
- TCP/IP, for instance, uses a random number for connections. Some grab this for their own purposes.

Replace noise with the message.

- Just replace the least-significant bit.
- Avoid the noise and tweak the salient features.

Anything not affected by compression.

- If you have the freedom to change data without hurting the data, then you have the freedom to include another message.



Structural Steganography builds the data into the original message.

Run some compression algorithm in reverse

- If the compression models the data accurately, then running it in reverse should spit out something that models the data well.
- Huffman algorithms give common letters short bit strings and rare ones long ones.

Change the structure or the order.

- GifEncoder changes the order of the colors in the palette.

Embed the data into the synthesis of the experience.

- Is the ghoul shooting with a revolver or a machine gun?
 - Revolver = 0
 - Machine Gun = 1
- Similar to product placement in movies!



Hidden data can be encoded into a scene with noise.

The least significant bit of pixels or sound files is very popular.

Tweaking the LSB is only a small change. Less than 1%.

- 140=10001100
- 141=10001101

Encrypt the data for added security

LSB modified to hide info





LSB Modification

Side Effects:

- The data may not have the same statistical pattern as the least significant bits being replaced.

Add a lot of noise, and it's obvious



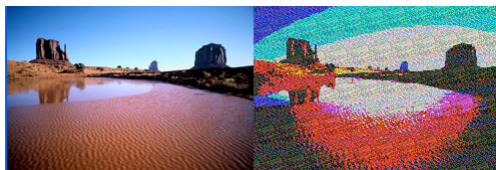
4 LSB modified produces banding



More LSB Modification



6 bits



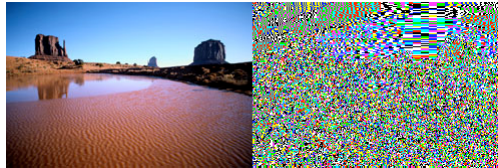
7 bits



Modifying 8 out of 8 bits!



All 8 bits shows the
“hidden” data better than
the image!



Bit 8 vs. Bit 1



Wayner Demos

Information hiding at the bit level:

- <http://www.wayner.org/books/discrypt2/bitlevel.php>

Encoding information through list order:

- <http://www.wayner.org/books/discrypt2/sorted.php#note2>



JPEG Watermarking



Provos, N., Honeyman, P.,
“Hide and Seek: An Introduction to
Steganography” IEEE Security &
Privacy, May 2003, pp. 32-44

Figure 2. Embedded information in a
JPEG. (a) The unmodified original picture;
(b) the picture with the first chapter of *The
Hunting of the Snark* embedded in it.

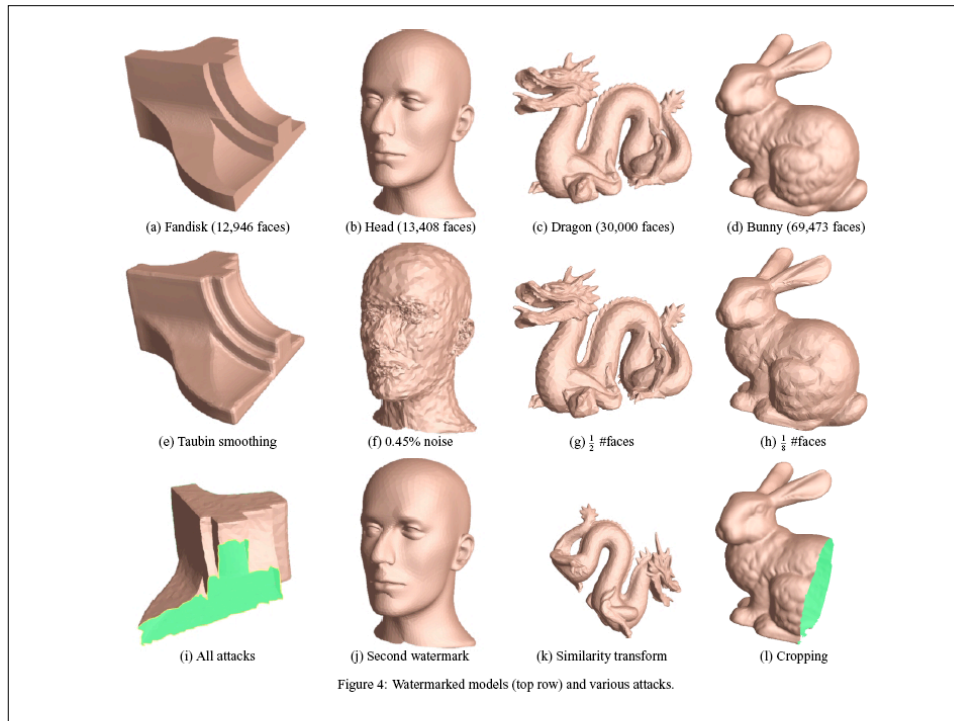



Mesh Watermarking

Robust mesh watermarking, Emil Praun,
Hugues Hoppe, Adam Finkelstein,

July 1999

*Proceedings of the 26th annual conference on
Computer graphics and interactive techniques*





DigiMarc

Leading provider of watermarking technologies
 Plug-ins for Windows, PhotoShop, etc.
 Communicates:

- Copyright ownership
- Image ID
- Image content – adult, etc.



Issues to evaluate

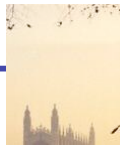
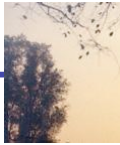
“Capability”

- Payload carrying ability
- Detectability
- Robustness

Securing information: Capacity is the wrong paradigm, Ira S. Moskowitz, LiWu Chang, Richard E. Newman ,
September 2002 Proceedings of the 2002 workshop on New security paradigms



“Mosaic attack”



Defeat an embedded watermark by chopping up image and serving it in pieces

```
<nobr>  
<img SRC="kings_chapel_wmk1.jpg" BORDER="0" ALT="1/6" width="116" height="140">  
<img SRC="kings_chapel_wmk2.jpg" BORDER="0" ALT="2/6" width="116" height="140">  
<img SRC="kings_chapel_wmk3.jpg" BORDER="0" ALT="3/6" width="118" height="140">  
</nobr>  
<br>  
<nobr>  
<img SRC="kings_chapel_wmk4.jpg" BORDER="0" ALT="4/6" width="116" height="140">  
<img SRC="kings_chapel_wmk5.jpg" BORDER="0" ALT="5/6" width="116" height="140">  
<img SRC="kings_chapel_wmk6.jpg" BORDER="0" ALT="6/6" width="118" height="140">  
</nobr>
```





Mosaic assembled



Some websites use mosaics to deter casual copying!



Copy Protection and Trusted Hardware



“Copy Protection” prevents people from making unauthorized copies.

Usually this is done with trusted hardware.

“Trusted” means that the security fails if the hardware does not behave as expected.

If something cannot willingly violate our trust, it cannot be trusted.

(It can be relied upon, however.)



Copy Protection Strategies

Distribution media that can't be copied

Program that only installs once

- Writable Media
- Activation Codes

Programs that only work on certain hardware

- Serial number (processor ID, Ethernet ID, hard drive ID, ...)

Programs that report misuse---call home



“Circumvention” is when the user circumvents some aspect of control.

- Unauthorized copying.
- Unauthorized use (viewing, reading, speaking.)
- Unauthorized destruction (watermark).

Technically-defined term under the Digital Millennium Copyright Act



License Management can be based on a hard ID or a soft ID:

Hard ID:

- Dongle
- Ethernet address
- Processor Serial Number
- Hard drive ID
- Hardware “fingerprint”

Soft ID:

- License strings (AD3F-2243-JJ92-9987-DDDS)





Preventing reuse of license strings

Tie the license string to a hardware fingerprint.

Real-time verification to a website.

Off-line verification and activation.

- Return something from email or web
- Program dies if not “registered” in 30 days



DVDs

Content Control:

- Encryption
- Decryption keys embedded in player

Implements:

- Region Coding
- License management

Cracked in 1999

- 1 key stolen from PC player
- DeCSS distributed over Internet
- Later algorithm cracked; other keys revealed
- Numerous court cases





Trusted Systems avoid this ad-hoc approach to anti-circumvention.

Trusted Software

- Secure operating systems & applications
- System protects itself from hostile code & users

Trusted Hardware:

- System will only work correctly
- System won't reveal "secrets"



"Orange Book" Trusted Systems

DOD 5200.28-STD (December 1985)

Division D: Minimal Protection

Division C: Discretionary Protection

- C1 – Discretionary Security Protection
- C2 – Controlled Access Protection

Division B: Mandatory Protection

- B1 – Labeled Security Protection
- B2 – Structured Protection
- B3 – Security Domains

Division A: Verified Protection

- A1 – Verified Design

<http://www.fas.org/irp/nsa/rainbow/std001.htm>



FIPS 140-1/140-2

FIPS 140-1: January 11, 1994

FIPS 140-2: May 25, 2001 (Supersedes 140-1)

Secure Requirements for Cryptographic Modules

<http://csrc.nist.gov/cryptval+>

Four Levels

- Level 1 – Least Secure
- Level 4 – Most Secure



IBM 4758

Tamper-responding hardware design

Hardware DES, RNG, modular math

Secure code loading

IBM Common Cryptographic

Architecture

FIPS 140-1 Level 4





Dallas Semiconductor Cryptographic iButton (DS1955B)

Java
"1-wire" interface
6 Kbytes NVRAM
64 kbyte ROM firmware
javacardx.crypto
Math accelerator performs RSA encryption in less than 1 second
\$34.22 (1)
\$31.78 (1000)
(release 2.2 w/ 134KB RAM and username/password software is \$53.21)



Smart Cards

Different kinds:

- Memory
- Crypto

Applications:

- Phone cards
- Satellite Broadcasts
- PKI





Attacks against smart cards

Destructive:

- Probes with wires
- Optical probes

Fault injection

Differential power analysis

A typical subroutine found in security processors is a loop that writes the contents of a limited memory

```
range to the serial port:
1 b = answer_address
2 a = answer_length
3 if (a == 0) goto 8
4 transmit(*b)
5 b = b + 1
6 a = a - 1
7 goto 3
8 ...
```

(From "Tamper Resistance --- A Cautionary Note" Ross Anderson)



Trusted PC Computing: Palladium/NGSCB; TCPA/TCG

Why?

- Increase consumer and business confidence
- Reduce business risks
- Protect end-user data

TCPA:

- Founded in 1999 by Compaq, HP, IBM, Intel, and Microsoft
- 180 members now



TCPA Concepts

“A platform can be trusted if it behaves in the expected manner for the intended purpose”

TCPA Provides:

- Platform Authentication and Attestation
- Platform Integrity Reporting
- Protected Storage



“Root of Trust”

Platform provides a “root of trust”

Platform’s root is certified by an outside party

Root is able to keep secrets from untrusted storage

Implemented with a “Trusted Platform Module” (TPM)

- Uniquely serialized
- Isolated from the CPU
- tamper-proof, like a smartcard inside the computer
- Runs at boot before the rest of the system



What would the TPM be like?

You might never know it's there...

- Hard disk encryption
(with keys in protected storage)
- License management that can't be circumvented.
- Anti-virus that can't be circumvented
(won't boot an infected OS)



NGSCB — Next Generation Secure Computing Base (aka Palladium)

Reverse approach --- adds security to an existing Windows-based system

Goal is to “protect software from software”

Provides:

- Sealed storage
- Attestation
- Curtained memory
- Secure input and output

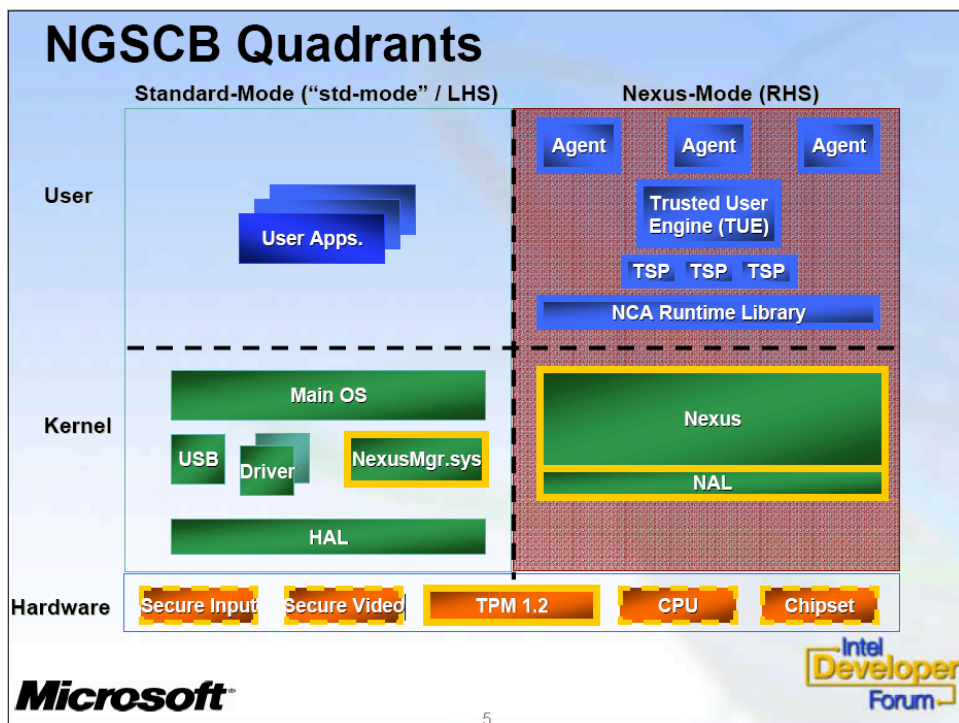


NGSCB Concepts

Standard environment: User vs. Kernel

Standard-Mode: Left Hand Side

Nexus-Mode: Right Hand Side





Palladium Changes

CPU changes

MMU changes

Motherboard changes – new chip

Trusted USB hub

Trusted Graphics Card

Security Service Component

- Another smart-card on the motherboard
- Key storage, PCR registers, RNG



NGSCB has a *lot* of engineering and usability issues to work out.

Access to sealed storage

- A program can only have the decrypt key if it can prove that it is the correct program!
- Prevents viruses from getting your credit card numbers

Software upgrade

- Older version must explicitly trust the next version

Secure input/output

- Encrypted keyboard, mouse & screen
- How do you really get this to work?