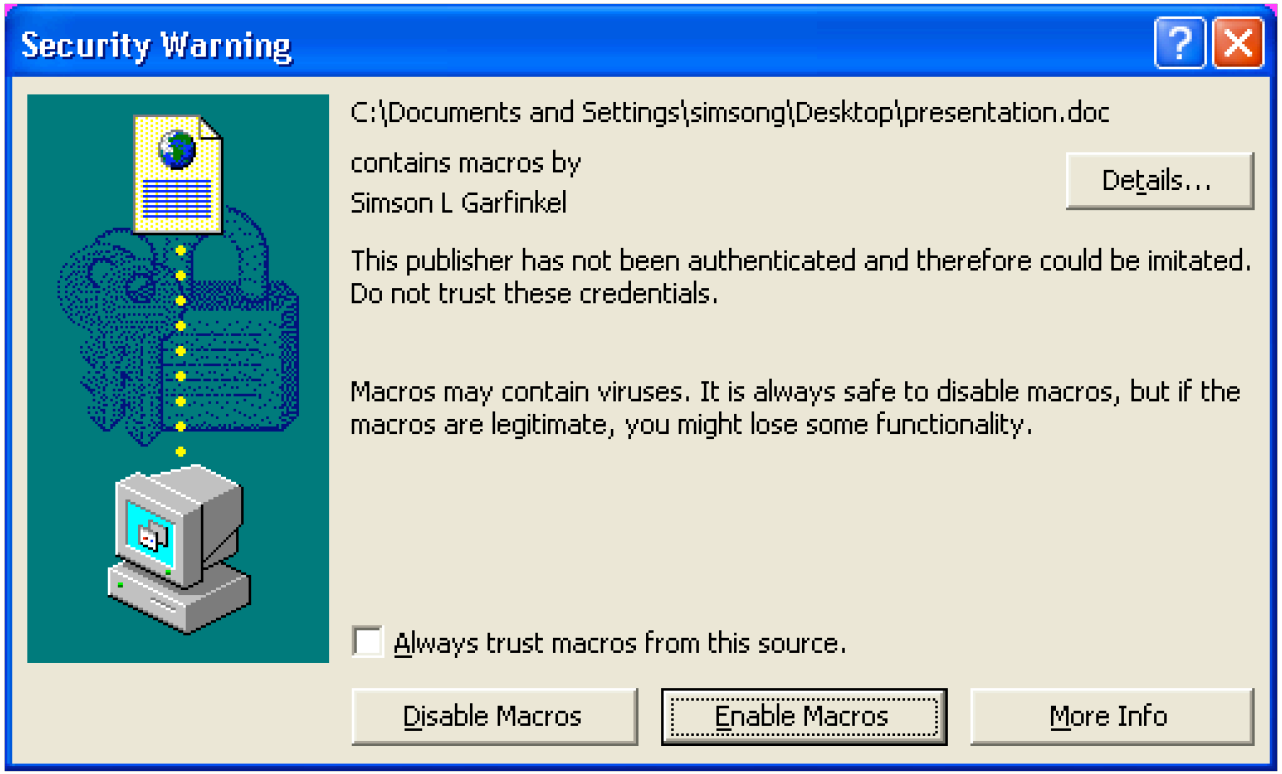
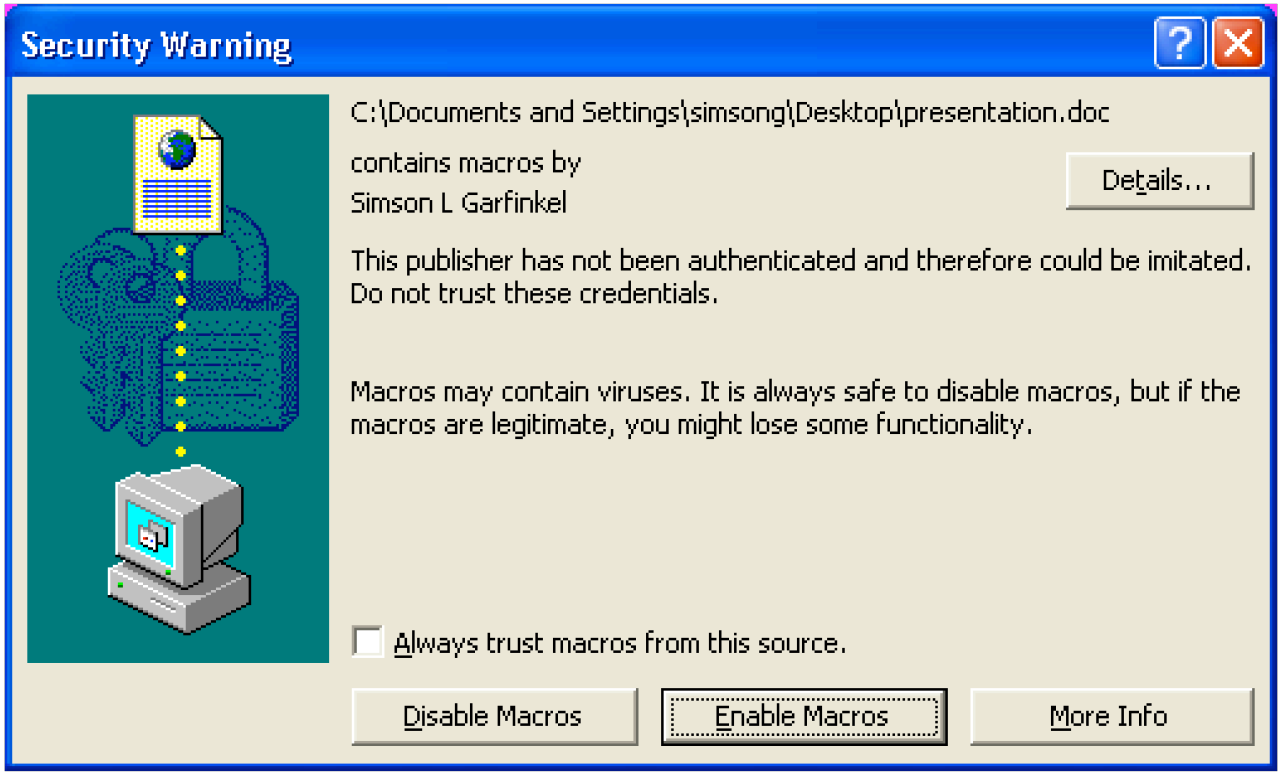
Will Networks Work?

User-Centered Security in a
Networked World

Simson L. Garfinkel
June 2005


Security Warning
C:\Documents and Settings\simsong\Desktop\presentation.doc
contains macros by
Simson L Garfinkel
Details...
This publisher has not been authenticated and therefore could be imitated.
Do not trust these credentials.
Macros may contain viruses. It is always safe to disable macros, but if the macros are legitimate, you might lose some functionality.
Always trust macros from this source.
Disable Macros
Enable Macros
More Info



This pop-up forces the user to make a decision—a decision that the user is not qualified to make.

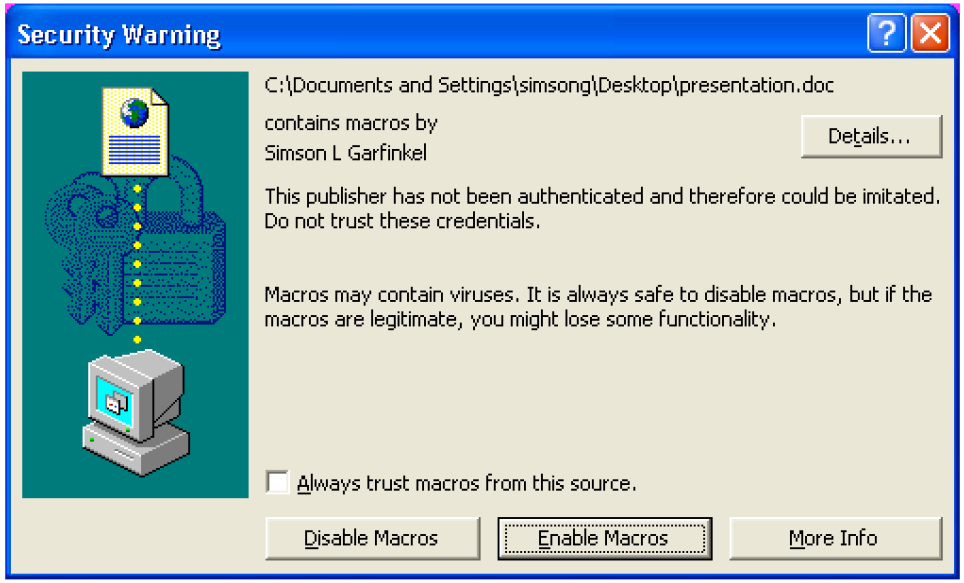
Should I enable macros?

Pros:

- Get my work done.
- Most macros are okay.
- I can always reformat my PC.

Cons:

- Something bad could happen...



What we would really like is a kind of “Zero-Click” security:

“Zero-click:”

- Do the right thing.
- Do what a security expert would do.

Not Zero-Visibility:

- Tell the user what the program is doing.
- Preserve a record so the user can audit what happened.

Not Zero-Recourse:

- Give the user an opportunity to correct mistakes.

Today's security systems are dominated by mechanism.

Typical mechanisms include:

- Anti-virus
- Anti-spam
- Anti-spyware
- Encryption (SSL, S/MIME, PGP)
- Backup

Many of these mechanisms are intentionally noisy.

Users have tasks and goals.

Communicate with others:

- Reliable message delivery.
- Private messaging.

Create and edit documents:

- Document integrity.
- Privacy of thoughts & writings.
- Control of computer resources.

Home banking:

- Control of funds.
- Privacy of financial data.

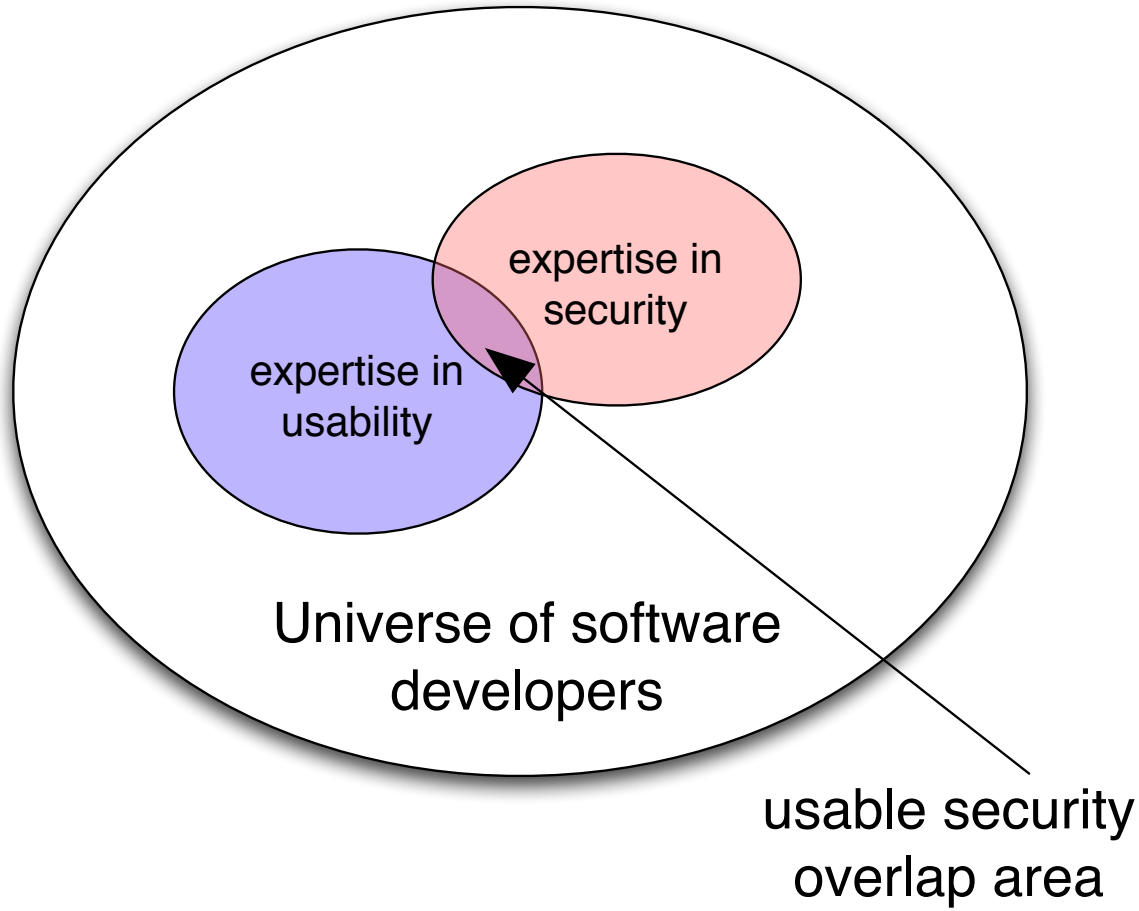
Security have traditionally been viewed as being “at odds” with the usability of these tasks and goals.

This talk explores opportunities for aligning security and usability in today's computing environment.

✔ Background

- Emerging work in HCI-SEC
- Principles for aligning security and usability
- Clean delete
- Opportunistic Encryption
- Q&A

The root of the conflict: security and usability are different skills that *must both be applied from the beginning*.



Thesis: By reworking underlying systems, we can bring security and usability into alignment.

Work to date in HCi-SEC has focused on authentication and secure messaging.

Passwords & pass faces

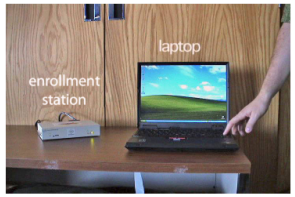
Biometrics

PGP usability studies

New work is aimed at improving the usability of real-world systems.

Analysis of smart cards vs. USB tokens [Coffetti]

“Instant PKI” work at Xerox PARC [Balfanz]



Protection mechanisms in Windows XP SP2 and Firefox [Microsoft]

The goal of this work is to make sure computing *natural* and *organic*.

Principles for aligning security and usability:

1. **Least Surprise** — match the user's expectations.
2. **Good Security Now** — don't wait for perfection.
3. **Standardized Security Policies** — auditable & teachable.
4. **Consistent Vocabulary** — between applications and vendors.
5. **Consistent Controls and Placement**.
6. **No External Burden** — on users or others.

Full details at http://www.simson.net/thesis

The Sanitization Problem: Confidential information is left behind after it is no longer needed.

Data discovered on second-hand hard drives is an obvious case.

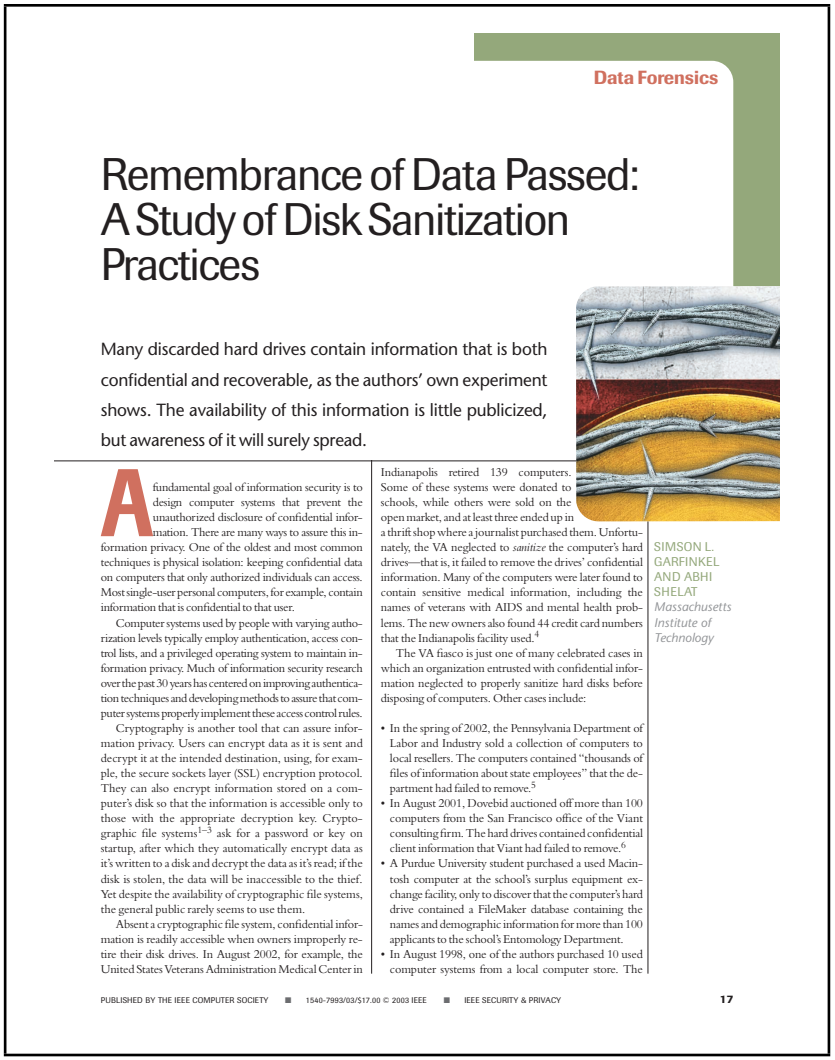
- Woman in Nevada bought a used PC with pharmacy records [Markoff 97]
- Paul McCartney's bank records sold by his bank [Leyden 04]
- Pennsylvania sold PCs with "thousands of files" on state employees [Villano 02]

Between January 1999 and April 2002, 236 hard drives were acquired on the secondary market.

Initial results published in *Remembrance of Data Passed* paper.

Data found included:

- Thousands of credit card numbers (many disks)
- Financial records
- Medical information
- Trade secrets
- Highly personal information



Data Forensics

Remembrance of Data Passed: A Study of Disk Sanitization Practices

Many discarded hard drives contain information that is both confidential and recoverable, as the authors' own experiment shows. The availability of this information is little publicized, but awareness of it will surely spread.

SIMSON L. GARFINKEL AND ABHI SHELAT
Massachusetts Institute of Technology

A fundamental goal of information security is to design computer systems that prevent the unauthorized disclosure of confidential information. There are many ways to assure this information privacy. One of the oldest and most common techniques is physical isolation: keeping confidential data on computers that only authorized individuals can access. Most single-user personal computers, for example, contain information that is confidential to that user.

Computer systems used by people with varying authorization levels typically employ authentication, access control lists, and a privileged operating system to maintain information privacy. Much of information security research over the past 30 years has centered on improving authentication techniques and developing methods to assure that computer systems properly implement these access control rules.

Cryptography is another tool that can assure information privacy. Users can encrypt data as it is sent and decrypt it at the intended destination, using, for example, the secure sockets layer (SSL) encryption protocol. They can also encrypt information stored on a computer's disk so that the information is accessible only to those with the appropriate decryption key. Cryptographic file systems[1–3] ask for a password or key on startup, after which they automatically encrypt data as it's written to a disk and decrypt the data as it's read; if the disk is stolen, the data will be inaccessible to the thief. Yet despite the availability of cryptographic file systems, the general public rarely seems to use them.

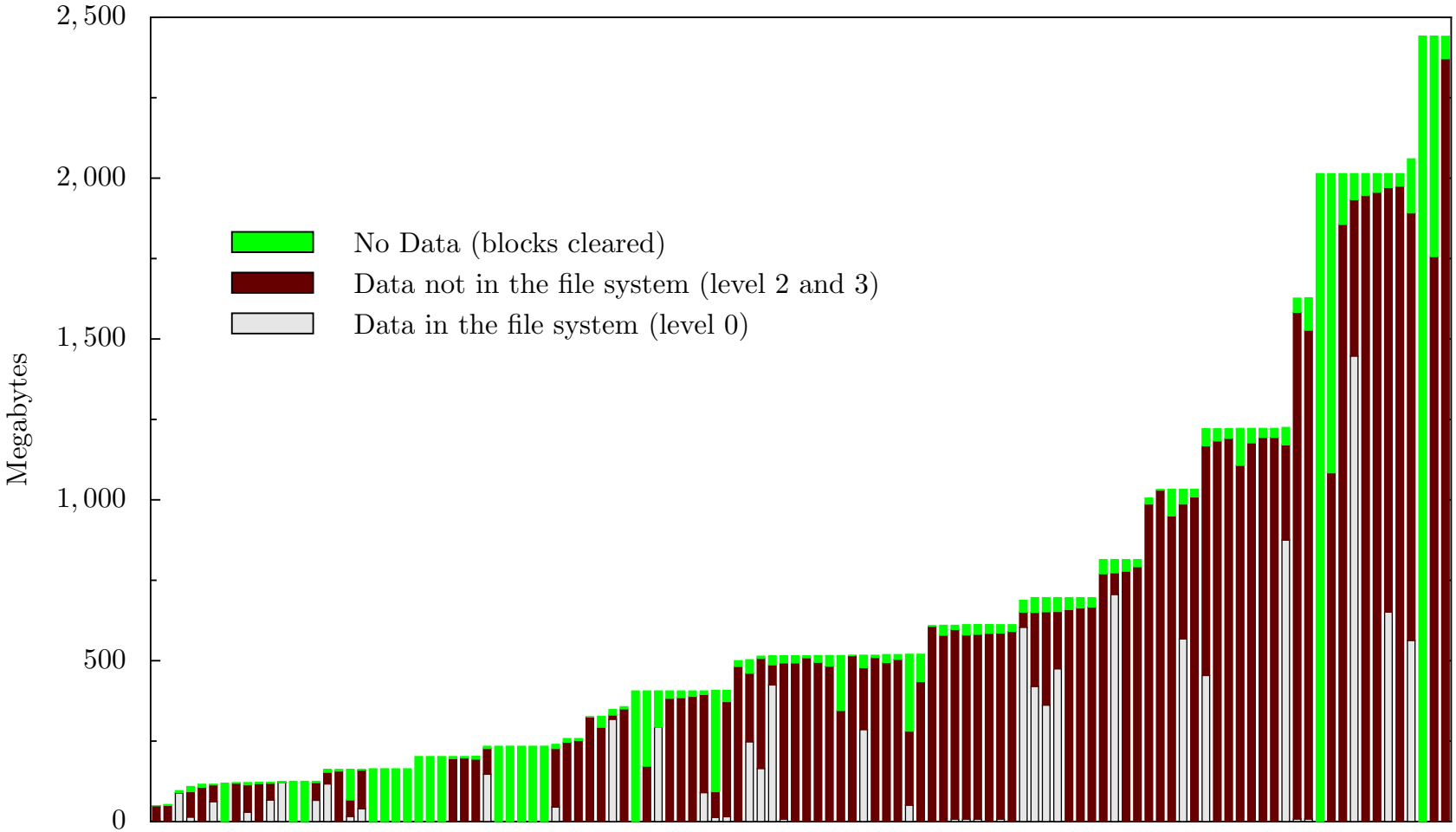
Absent a cryptographic file system, confidential information is readily accessible when owners improperly retire their disk drives. In August 2002, for example, the United States Veterans Administration Medical Center in Indianapolis retired 139 computers. Some of these systems were donated to schools, while others were sold on the open market, and at least three ended up in a thrift shop where a journalist purchased them. Unfortunately, the VA neglected to *sanitize* the computer's hard drives—that is, it failed to remove the drives' confidential information. Many of the computers were later found to contain sensitive medical information, including the names of veterans with AIDS and mental health problems. The new owners also found 44 credit card numbers that the Indianapolis facility used.[4]

The VA fiasco is just one of many celebrated cases in which an organization entrusted with confidential information neglected to properly sanitize hard disks before disposing of computers. Other cases include:

- In the spring of 2002, the Pennsylvania Department of Labor and Industry sold a collection of computers to local resellers. The computers contained "thousands of files of information about state employees" that the department had failed to remove.[5]
- In August 2001, Dovebid auctioned off more than 100 computers from the San Francisco office of the Viant consulting firm. The hard drives contained confidential client information that Viant had failed to remove.[6]
- A Purdue University student purchased a used Macintosh computer at the school's surplus equipment exchange facility, only to discover that the computer's hard drive contained a FileMaker database containing the names and demographic information for more than 100 applicants to the school's Entomology Department.
- In August 1998, one of the authors purchased 10 used computer systems from a local computer store. The

PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/03/$17.00 © 2003 IEEE ■ IEEE SECURITY & PRIVACY

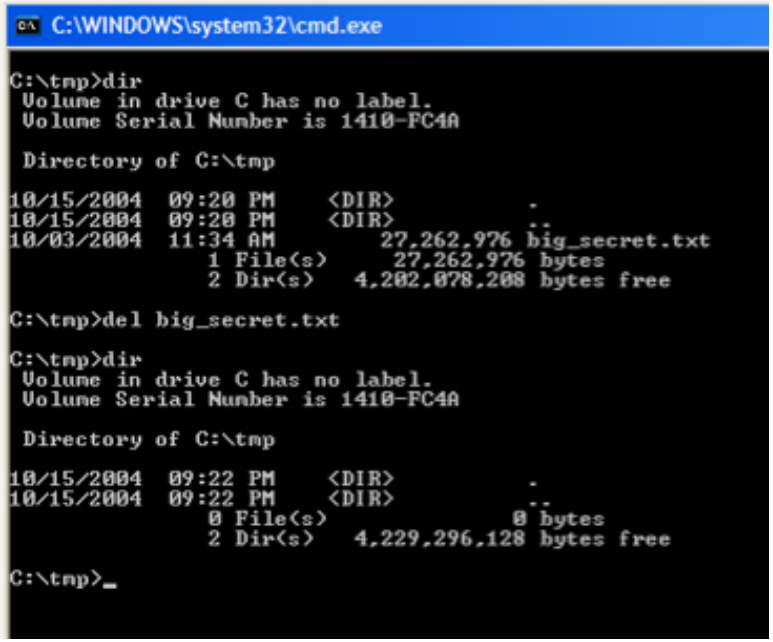
An analysis of the 236 drives shows many failed sanitization attempts.



Modern systems violate the “principle of least surprise” when deleting data.

DEL removes file names

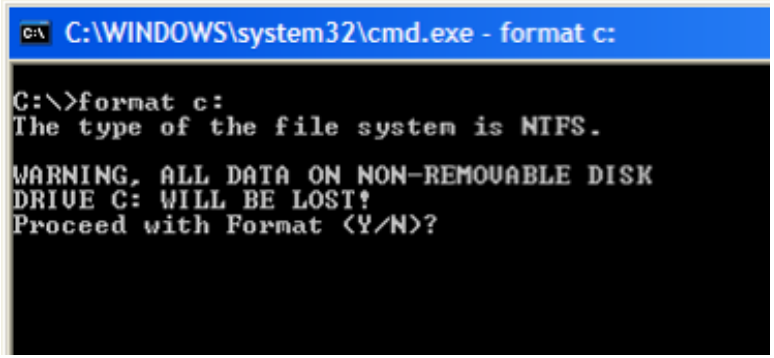
—but not file contents.



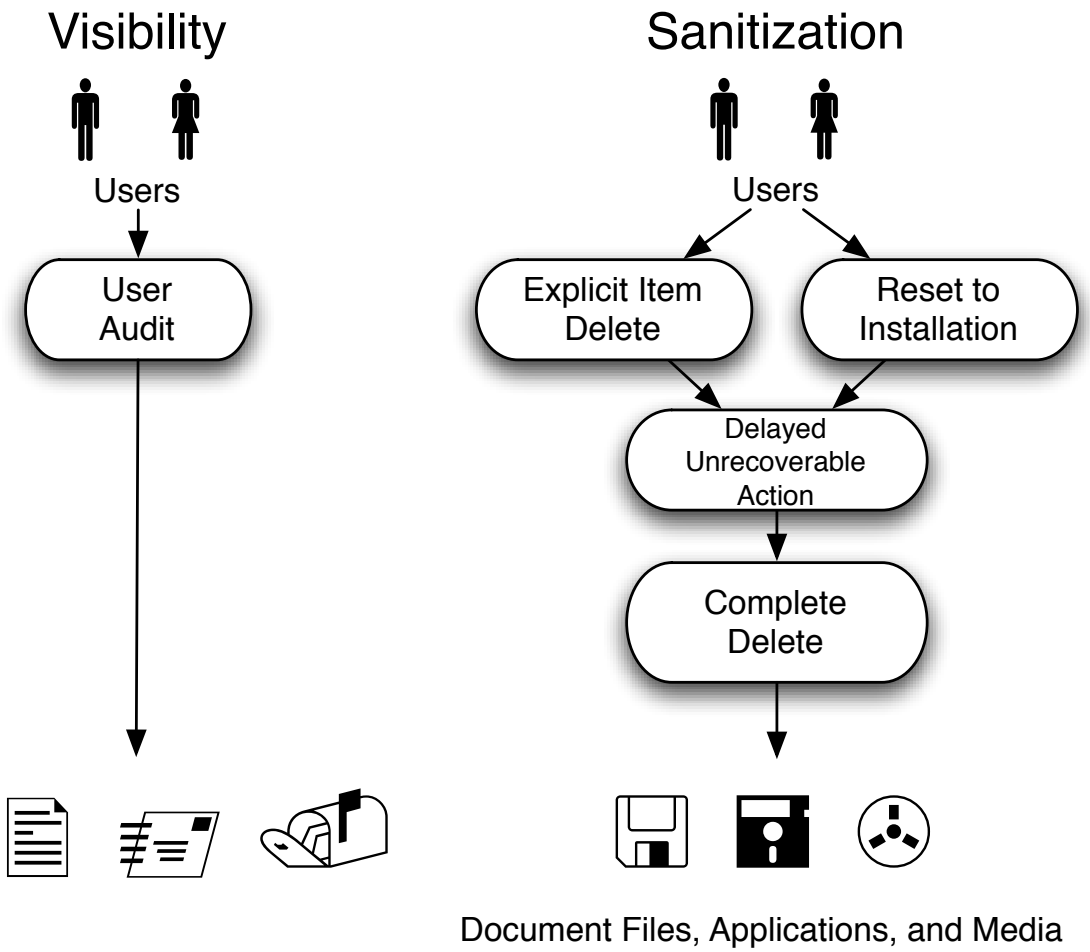
FORMAT claims

“ALL DATA ... WILL BE LOST”

—but it’s not.



The solution: five distinct techniques can be used to address the sanitization problem.



http://www.simson.net/thesis/sanitize1.pdf

Public key cryptography was invented nearly 30 years ago to secure electronic mail.

- 1976 – Public Key Cryptography (Diffie & Hellman)
- 1977 – RSA Encryption (Rivest, Shamir & Adelman)
- 1978 – Certificates (Kornfelder)
- 1987 – Privacy Enhanced Mail
- 1992 – PGP
- 1998 – S/MIME

With so much work and investment, why don't we use this exciting technology?

Most mail sent over the Internet isn't secure. Why not?

	Theories of Disuse	Solution
#1	People don't have the software	Distribute with the OS
#2	The software is too hard to use	Make it automatic
#3	People don't want to use it!	Automate & Educate

This is what the industry did with SSL/TLS, and it worked pretty well.

“Email Security” means different things to different people.

Email security traditionally meant:

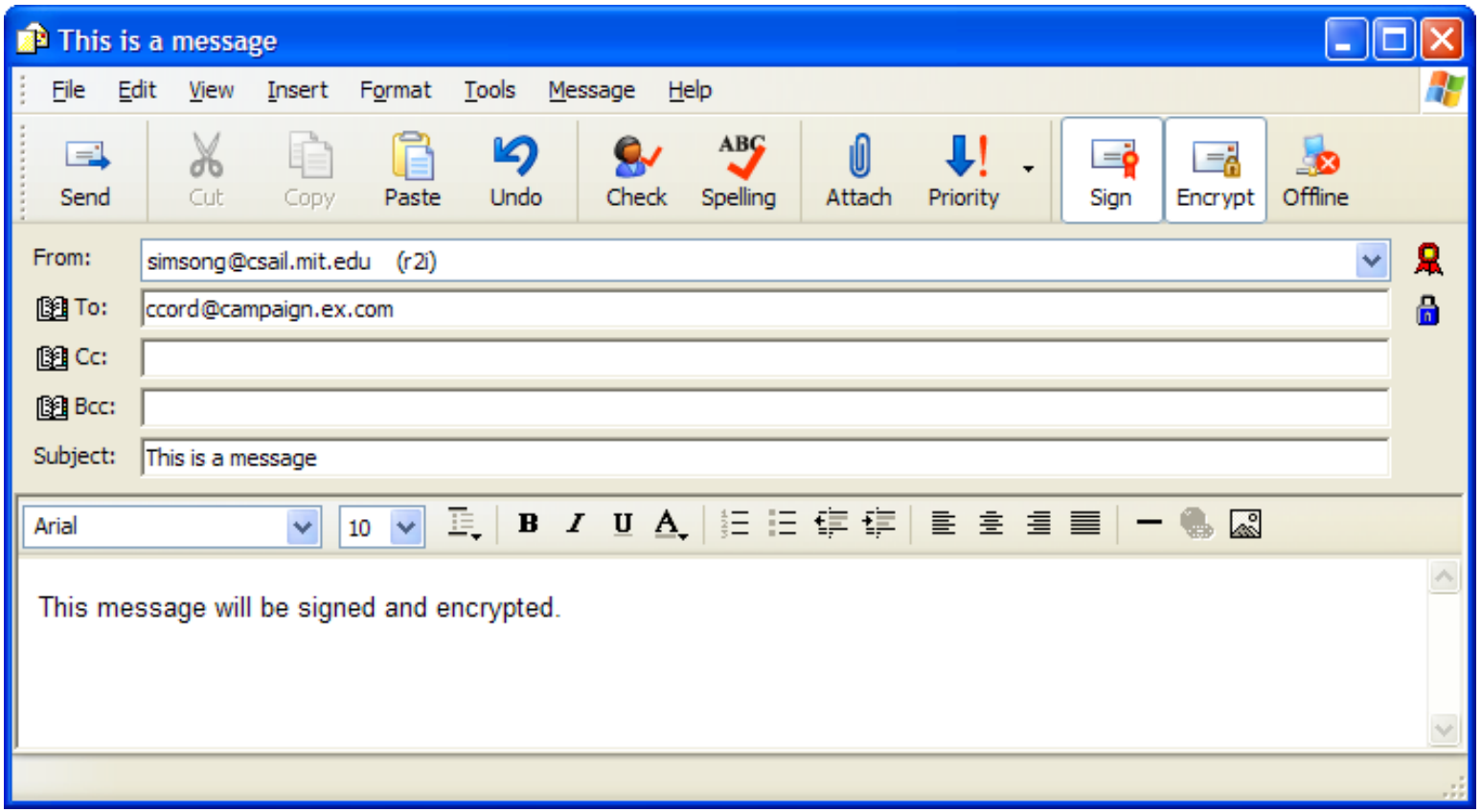
Preventing Eavesdropping.

Today email security means:

Stopping Spam and Phishing.

This creates an opportunity for advancement, because there are some senders that send *a lot* of mail.

S/MIME is built into many modern email programs.



Sending signed mail requires a certificate.
Receiving sealed mail requires a certificate.

We surveyed 470 Amazon.com and discovered most could receive S/MIME-signed messages.

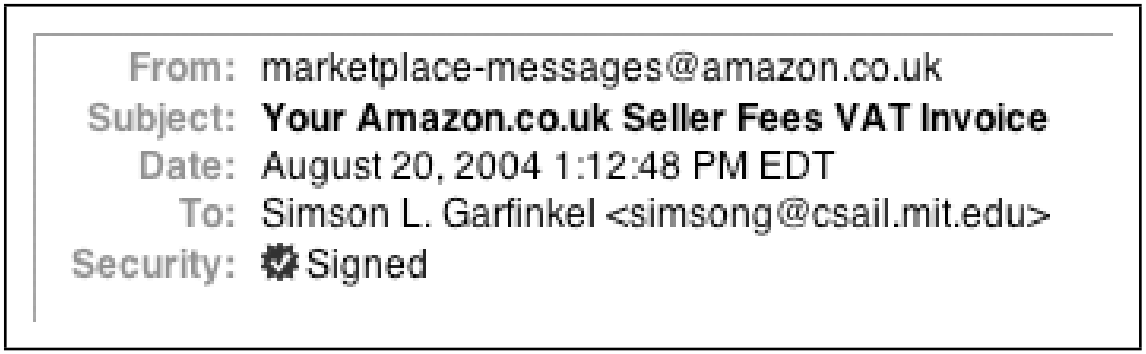
"Which computer programs do you use to read your email?
Check all that apply:"

Outlook Express	42%
Outlook	31%
AOL	18%
Netscape	10%
Eudora	7%
Apple Mail	3%
Mozilla Mail	3%
Lotus Notes	2%
Any S/MIME	54%
Total Responding	435
No Response	(19)

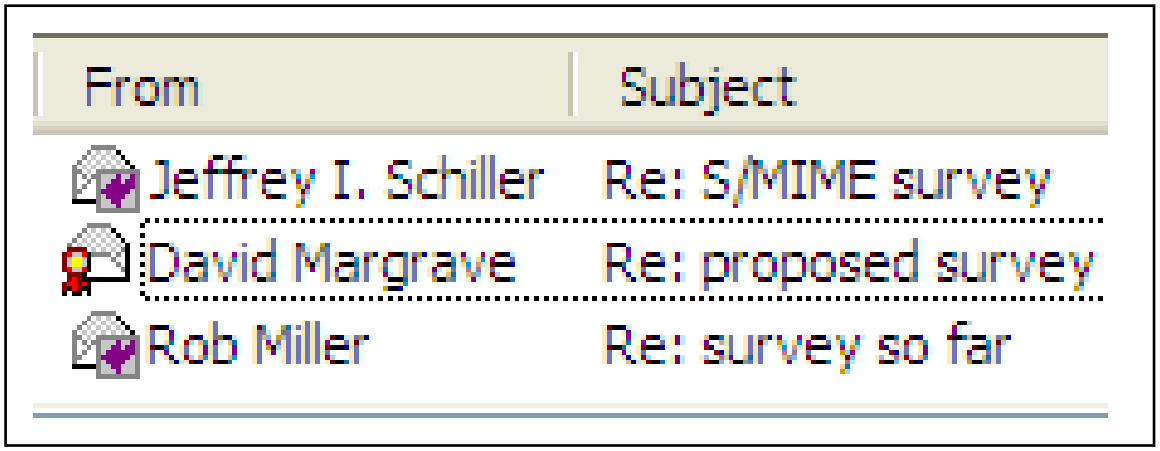
Eliminate AOL and Hotmail, and nearly all have support for S/MIME.

S/MIME signatures are well-integrated in some mail clients.

Apple Mail:



Outlook Express:



Recommendation: organizations sending bulk email should sign with S/MIME.

In conclusion, there is a lot of room for incremental advancement in HCI-SEC.

Some approaches discussed here are:

- Implement “Complete Delete.”
- Sign outgoing mail.

Other approaches:

- Improved log files
- Better visibility and “undo” (for configurations, installation, etc.)

Many of these ideas are ready for deployment.

Questions?