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

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.


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

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.

A fundamental goal of information security is to design computer systems that prevent the unauthorized disclosure of confidential information. Data or entire systems to ensure information privacy. One of the oldest and most common techniques in physical isolation: keeping confidential data on computers that only authorized individuals can access. Many discarded personal computers, for example, contain information that is confidential to that user.

Computer systems and the people with access to them typically carry no information on users, so access control lists, and a privileged operating system to maintain information privacy. Much of information security research recently is focused on the study of access control mechanisms and developing methods to ensure that computer systems properly implement these access control rules.

Cryptographic techniques for access control include encryption and decryption at the intended destination, using, for example, the secure shell encryption (SSH) encryption protocol. They can also encrypt information stored on a computer disk so that the information is accessible only to those with the appropriate decryption key. Cryptographic file systems ask for a password or key on startup, after which they automatically encrypt data as it's written to a disk and decrypt data as it's read; if the disk in niches, the data will be inaccessible to the thief. Yet despite the availability of cryptographic file systems, the general public rarely uses them.

An automated cryptographic system allows a user to store information on a computer's hard drive. 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 thrift shops where they were purchased by thieves. Unfortu- nately, the VA neglected to buster the computer's hard drive—that is, it failed to erase the drives' confidential information. Many of the computers even later found contain sensitive medical information, including the names of veterans with AIDS and mental health problems. The news seems to have found 46 miles and found that the Indianapolis facility had sold.

The VA is just one of many celebrated cases in which an organization entrusted with confidential information neglected to properly maintain 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 schools. The computers contained "Researched files of information about state employees" that the department had failed to remove.
- In August 2001, Dell, bought off more than 100 computers from the San Francisco office of the Weyerhaeuser consulting firm. The hard drives contained confidential client information that Weyerhaeuser had failed to remove.
- A Pacific University student purchased a used Macin- tosh computer from a school's surplus equipment exchange facility, only to discover that the computer's hard drive contained a file named "dataset" containing the names and demographic information from more than 100 applicants to the school's meteorology Department.
- In August 1998, one of the authors purchased 10 used computer systems from a local computer store.
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.
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?

<table>
<thead>
<tr>
<th>Theories of Disuse</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 People don’t have the software</td>
<td>Distribute with the OS</td>
</tr>
<tr>
<td>#2 The software is too hard to use</td>
<td>Make it automatic</td>
</tr>
<tr>
<td>#3 People don’t want to use it!</td>
<td>Automate &amp; Educate</td>
</tr>
</tbody>
</table>

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:”

<table>
<thead>
<tr>
<th>Program</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Express</td>
<td>42%</td>
</tr>
<tr>
<td>Outlook</td>
<td>31%</td>
</tr>
<tr>
<td>AOL</td>
<td>18%</td>
</tr>
<tr>
<td>Netscape</td>
<td>10%</td>
</tr>
<tr>
<td>Eudora</td>
<td>7%</td>
</tr>
<tr>
<td>Apple Mail</td>
<td>3%</td>
</tr>
<tr>
<td>Mozilla Mail</td>
<td>3%</td>
</tr>
<tr>
<td>Lotus Notes</td>
<td>2%</td>
</tr>
<tr>
<td>Any S/MIME</td>
<td>54%</td>
</tr>
</tbody>
</table>

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:

![Email with S/MIME signature]

Outlook Express:

![Email with S/MIME signature]

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?