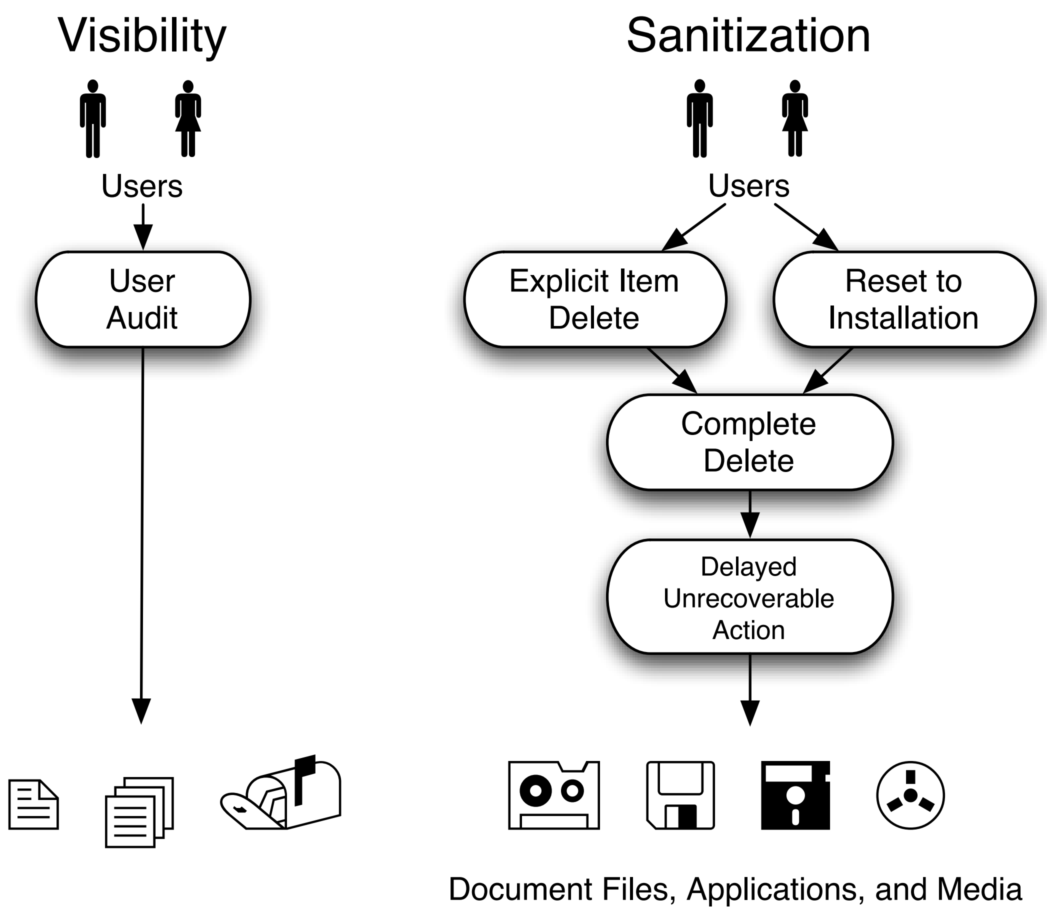
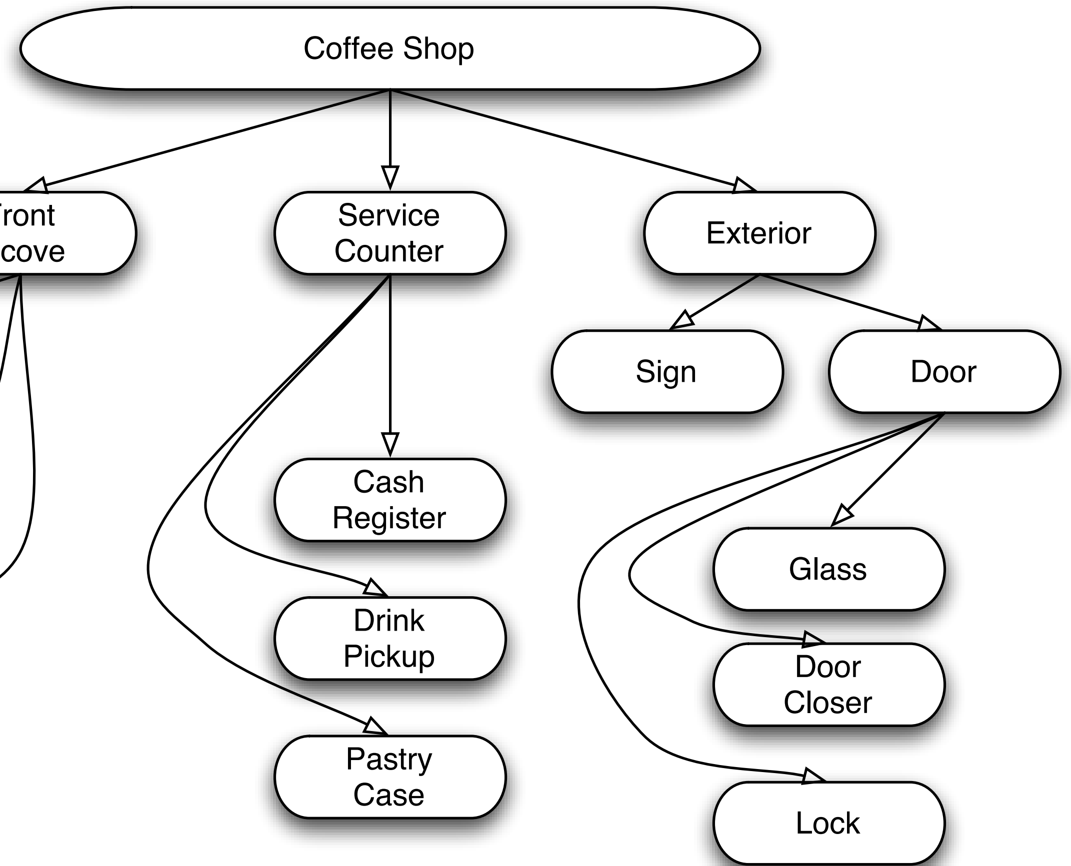
Design Principles and Patterns for Computer Systems that are Simultaneously Secure and Usable



Simson L. Garfinkel, April 26, 2005

A pattern is a recurring solution to a standard problem.



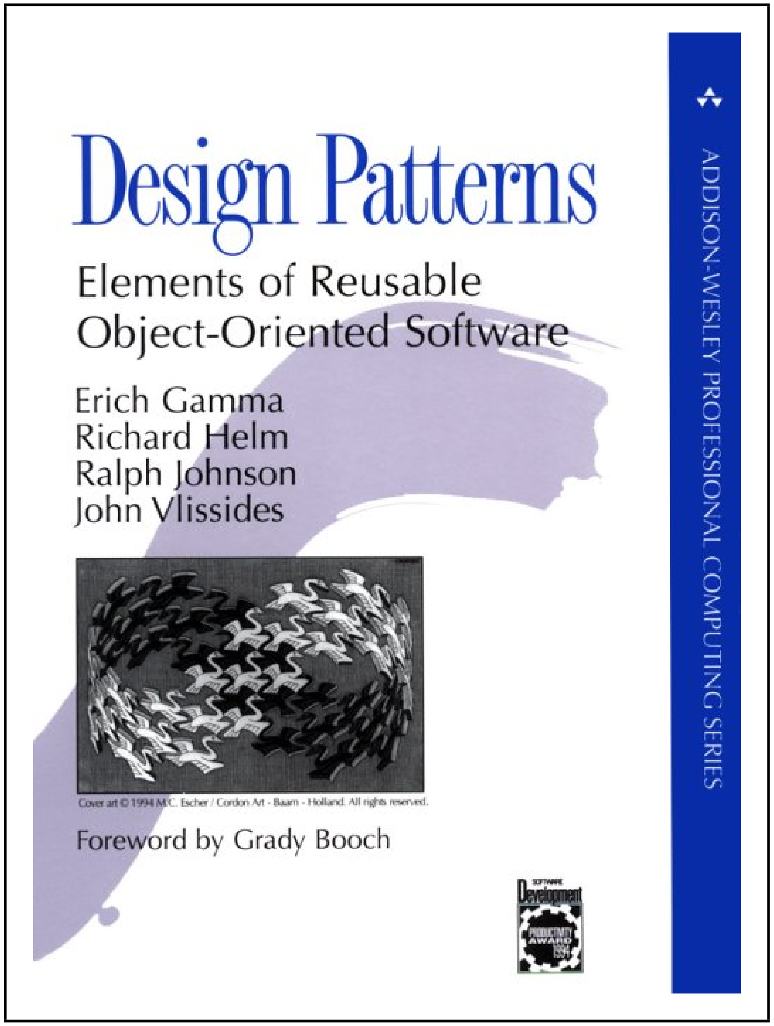
Patterns and “pattern languages” introduced by Architect Christopher Alexander in the 1970s.

Object Oriented Design adopted patterns in the 1990s.

Johnson *et al.*, [OOPSLA 91]; Coad [CACM, 92]; “Gang of four” [95]

Why? Because patterns help us:

- reuse successful practices
- reason about what’s done and why
- document abstractions other than algorithms and data structures. [Schmidt *et al.*, 1996]

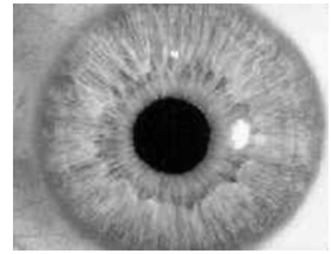


Patterns encapsulate knowledge and understanding, making it easier to teach and deploy solutions.

My thesis:

Usability and security can be made synergistic
by redesigning systems with
specific principles
and through the adoption of
well-defined patterns.

It has long been recognized that end-user security and usability are at odds in modern computer systems.

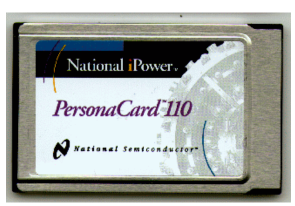


Username: simsong
Password: ••••••

ACCESS DENIED

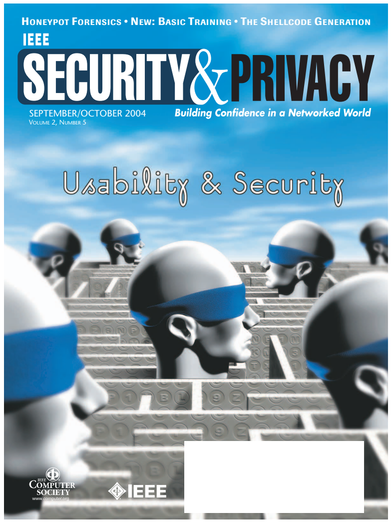
ACCESS DENIED

ACCESS DENIED



The need to align end-user security and usability is recognized as a priority for both computing and the nation.

- CRA 2003 “Grand Challenge”
- PITAC 2005 “priority”
- Special publications
  [IEEE S&P 2004] [O’Reilly 2005]
- CHI 2005; SOUPS 2005

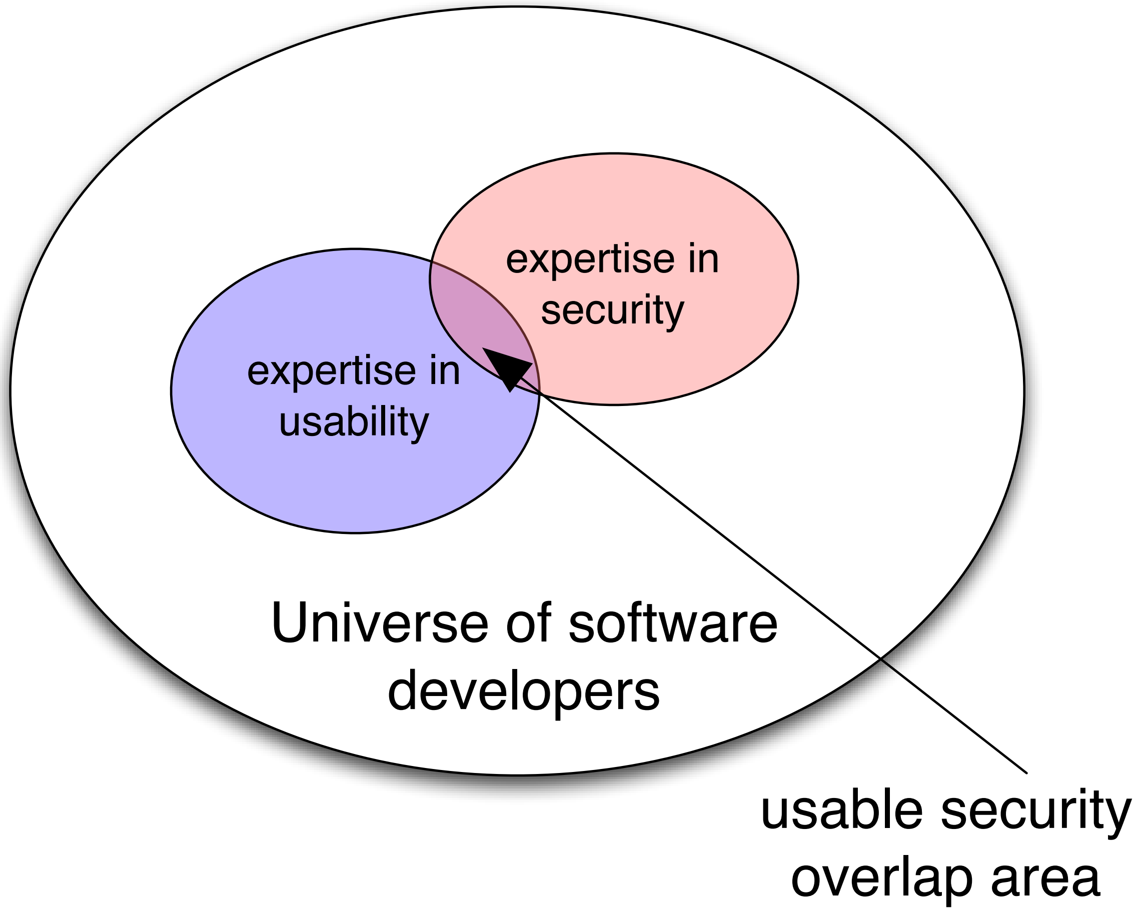


CRA

President’s Information Technology Advisory Committee

The traditional antagonism between usability and security can no longer be tolerated.

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

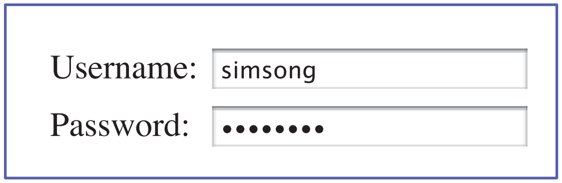


HCI-SEC: The emerging field that seeks to align Human Computer Interfaces with Security.

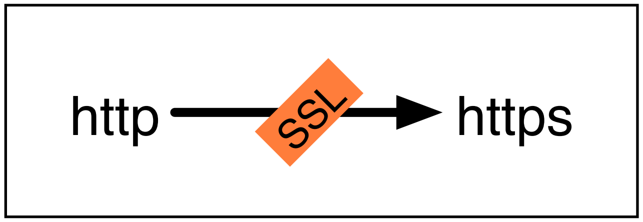
Today computer security has many "principles," "best practices" and "techniques."

- Biometric authentication

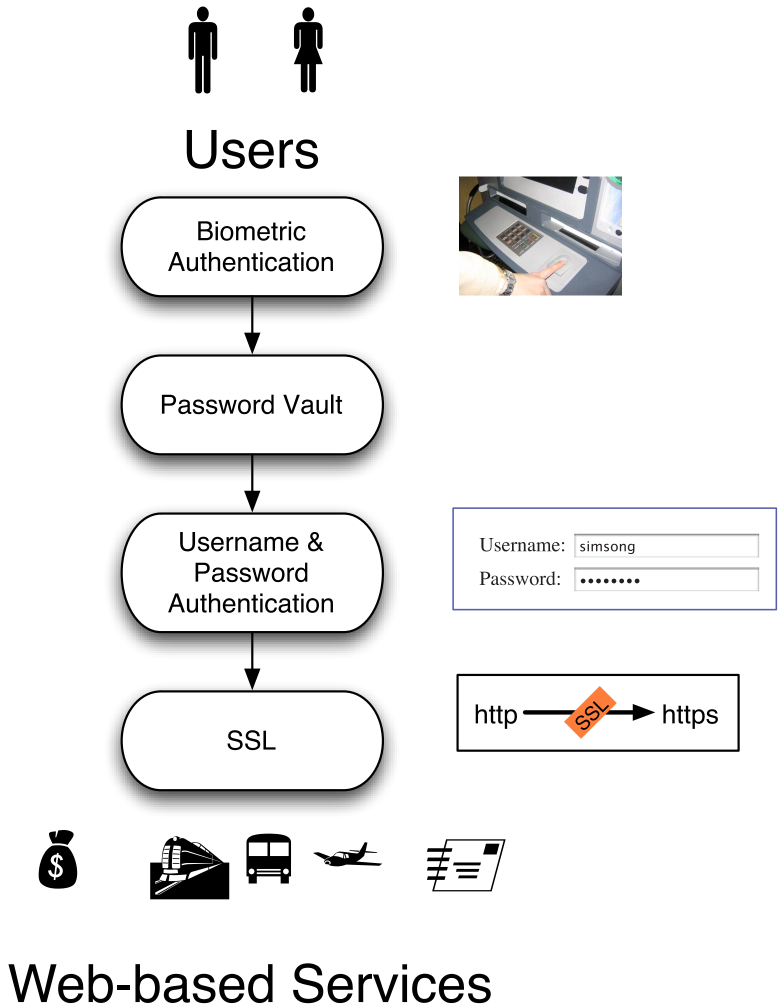
- The password field



- Wrapping plaintext protocols with SSL



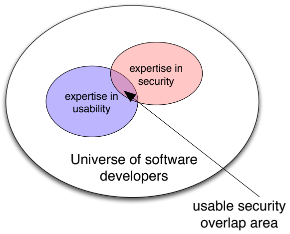
With patterns, we can decompose the problems and refactor the solutions.



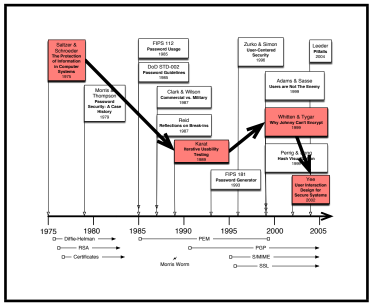
Patterns are an easy way to communicate solutions to students, implementors, and organizations.

This talk presents two sets of related patterns for aligning usability and security.

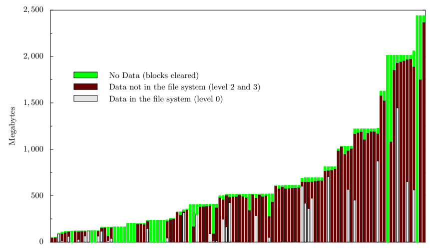
1. Introduction to patterns. ✔



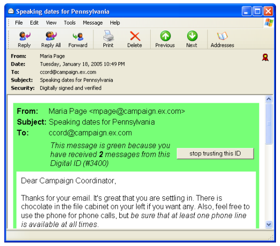
2. Prior work in HCI-SEC.



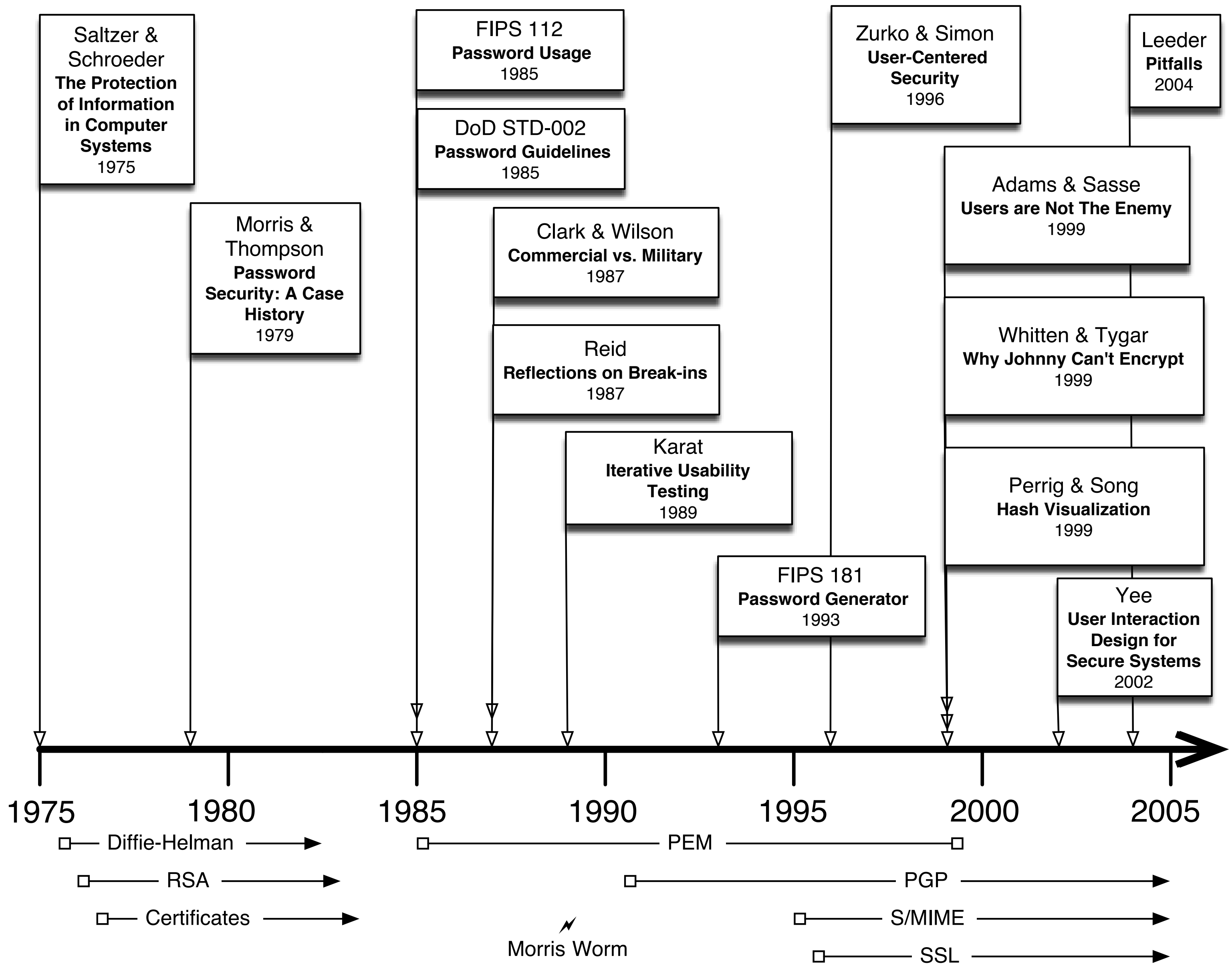
3. Patterns for sanitization.



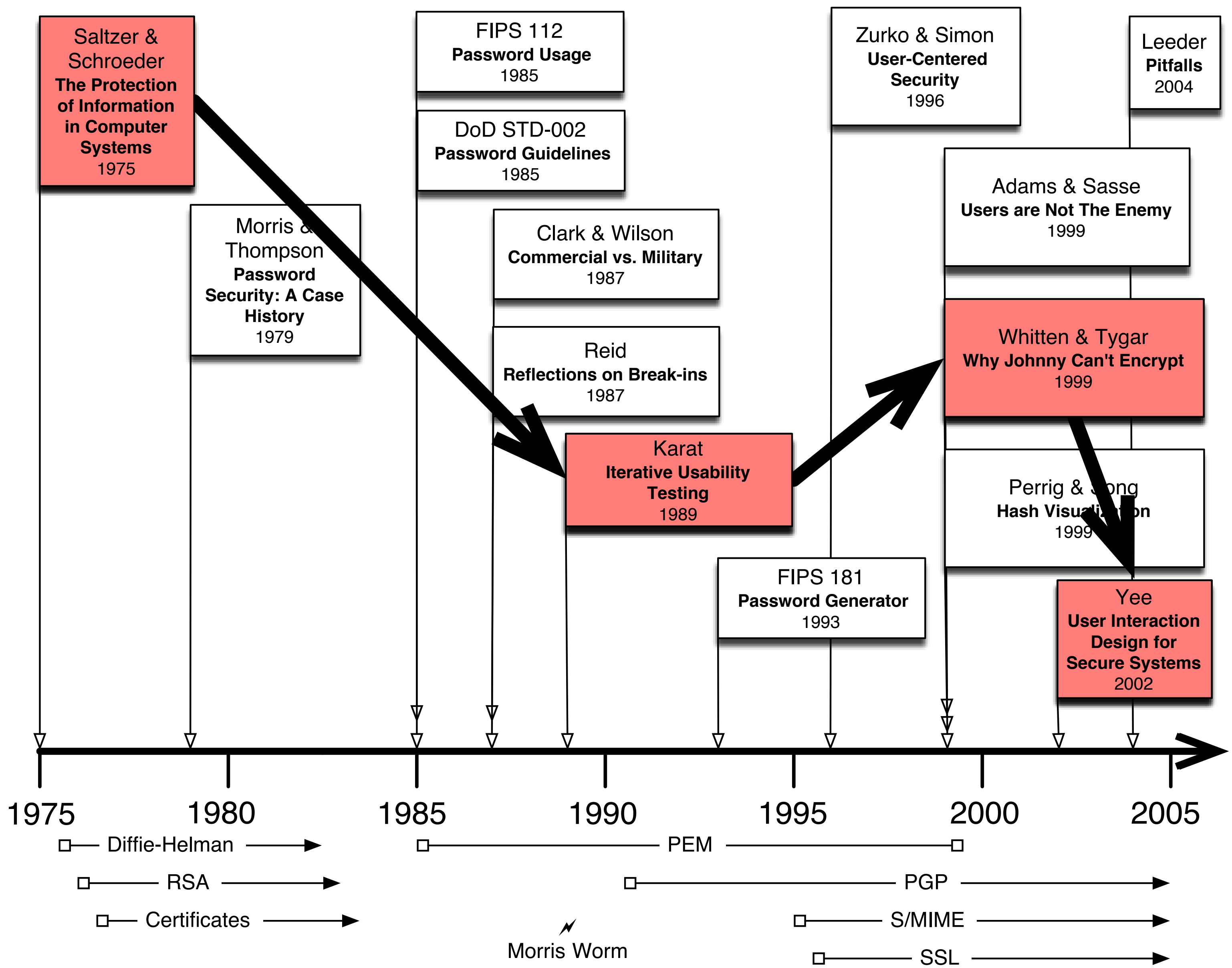
4. Patterns for secure messaging.



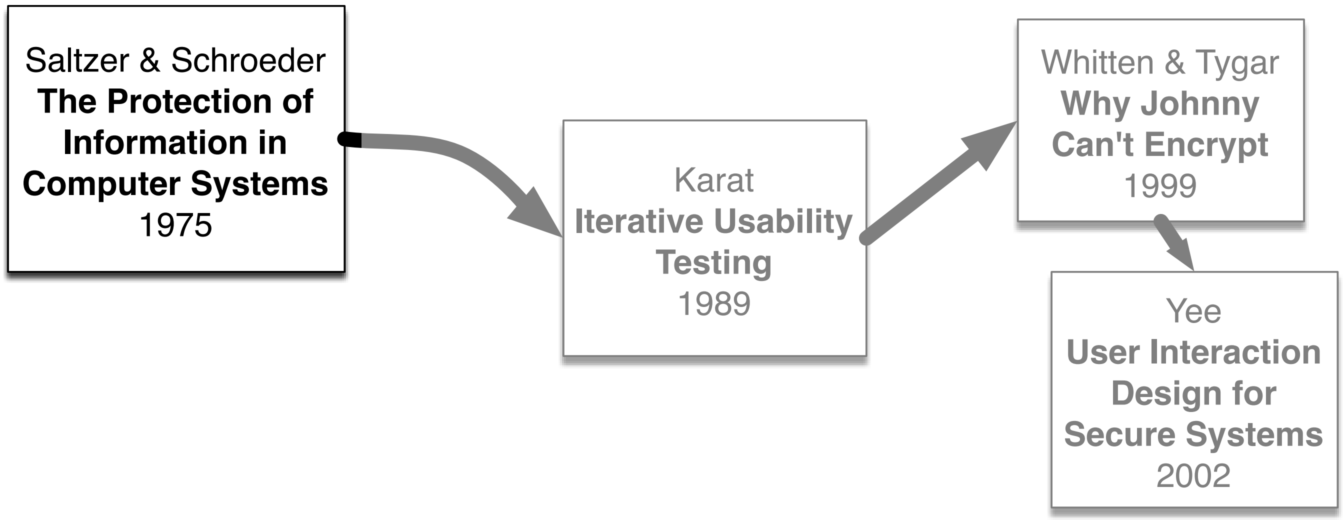
HCI-SEC seems hard because little work has been done!



I am going to focus on four HCI-SEC articles:



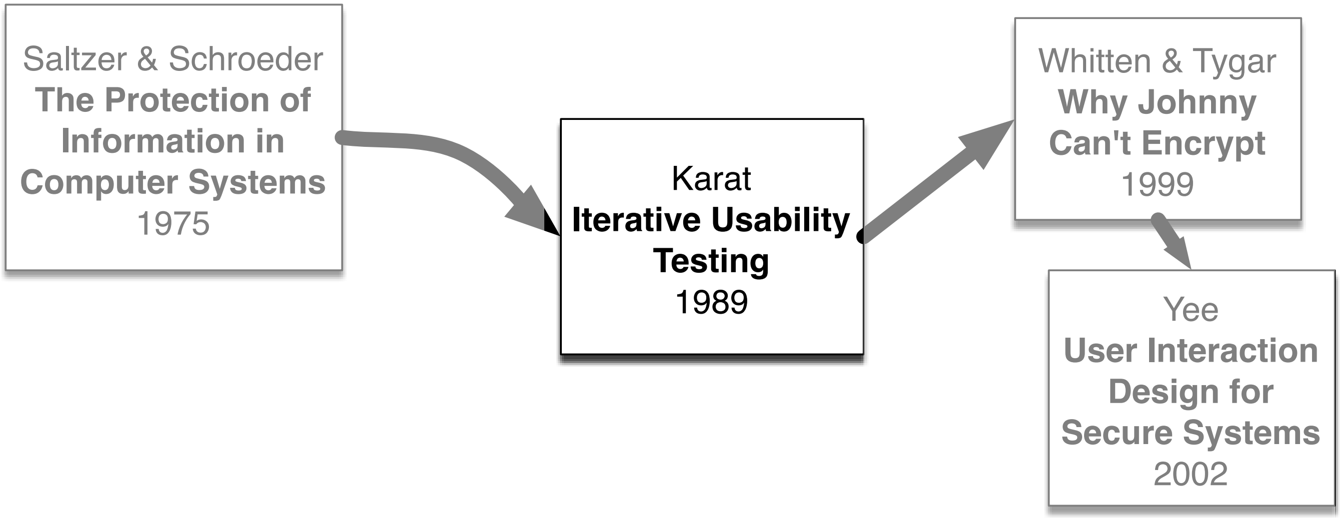
Saltzer & Schroeder: 1975



- Introduced the term “Psychological Acceptability”
- “... so that users routinely and automatically apply the protection mechanisms correctly.”
- Mental images should match protection mechanisms.

[SS 75] argues that security should naturally emerge from normal operations.

Karat: Iterative Usability Testing [1989]



- Applies user-centered design techniques to an IBM security application deployed to 23,000 users.
- Articulates a *usability goal* — "95% of users will complete the sign-in task error free within the first three attempts."
- Conducts field study; lab study; low-fidelity prototypes; live code tests;

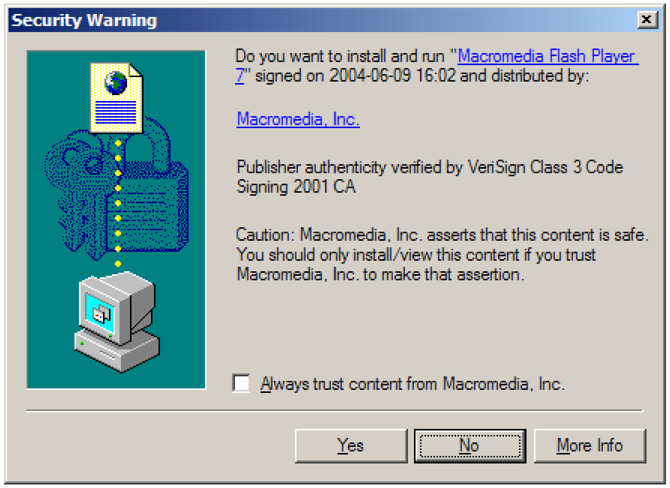
Karat and others (Sasse) argue that HCI-SEC is really just a usability problem.

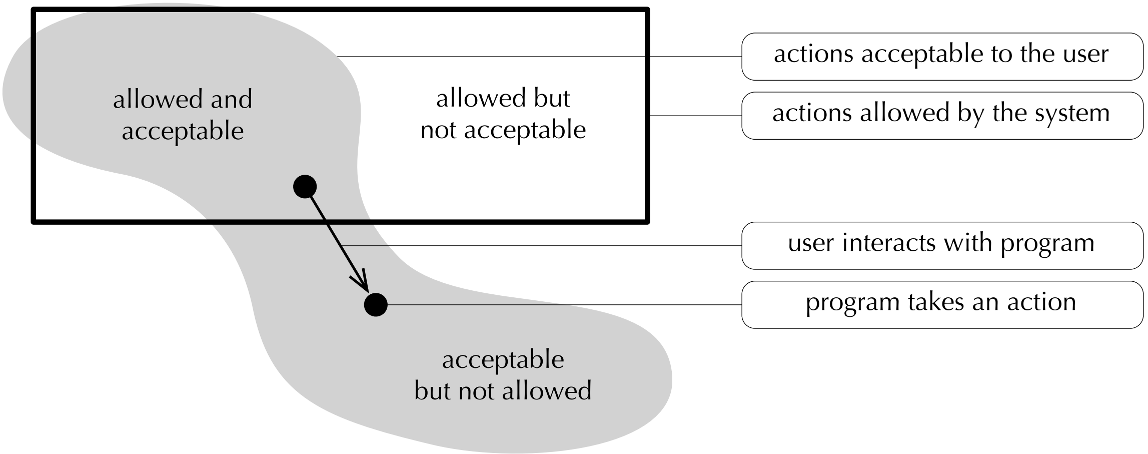
Whitten & Tygar identified five properties of “security software” [99]

- The secondary goal property
- The hidden failure property
- The barn door property
- The weakest link property
- The abstraction property

Primarily based on a study of PGP (secure messaging).

Yee [2002] argues that there is a fundamental mismatch between software capabilities and the user’s mental models.



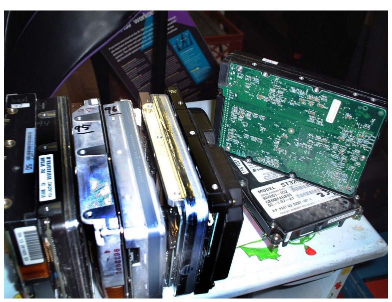


Yee’s 10 principles for aligning security and usability primarily address virus and spyware problems.

My work builds these ideas, with specific techniques in two key areas:

Sanitization:

Patterns that address the problem of confidential information left behind on computer media and in applications.



Secure Messaging:

Patterns that increase the security of email *today* and point the way to future improvements.

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.

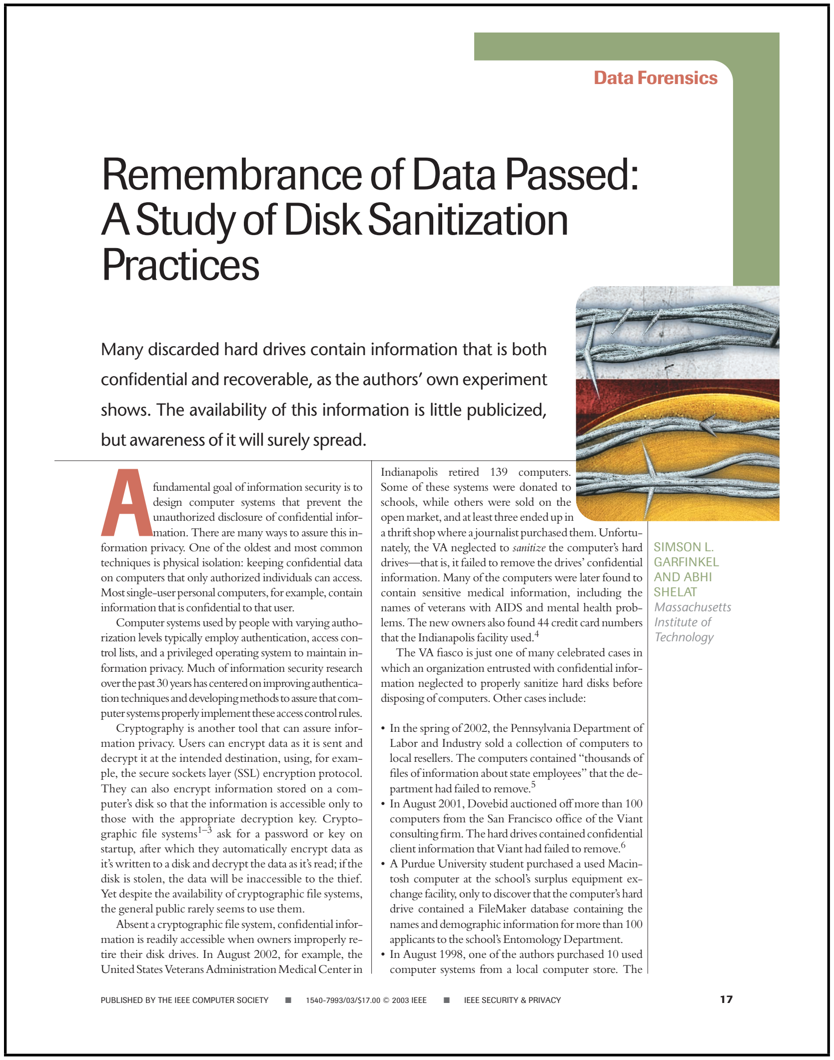
- Woman in Nevada bought a used PC with pharmacy records [Markoff 97]
- Paul McCartney's bank records sold by his bank [Leyden 04]
- Pennsylvania sold PCs with "thousands of files" on state employees [Villano 02]

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

[Garfinkel & Shelat 03] established the scale of the problem.

We found:

- 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

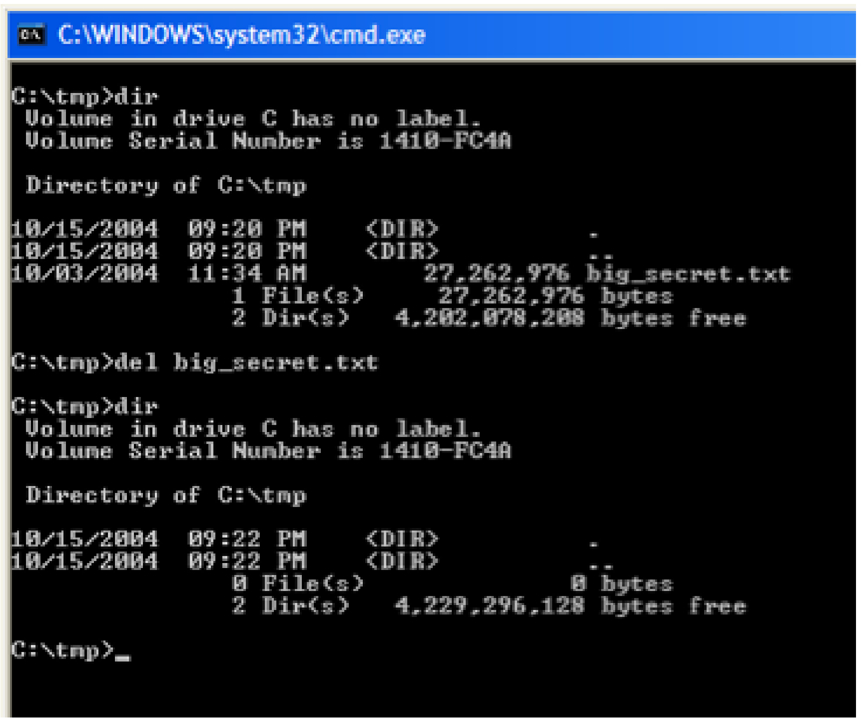
PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/03/$17.00 © 2003 IEEE ■ IEEE SECURITY & PRIVACY 17

We did not determine if this was a *usability* problem or an *education* problem.

Evidence for the usability problem: Computers *lie* when users delete data.

DEL removes file names

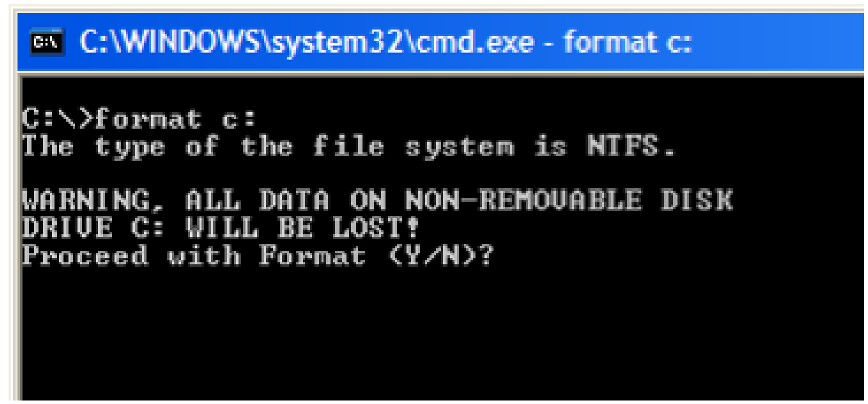
—but not file contents.



FORMAT claims

"ALL DATA ... WILL BE LOST"

—but it's not.



"...a fundamental mismatch between software capabilities and the user's mental models." [SS 75]

Oliver North had a mismatched mental model.

"We all sincerely believed that when we ... pressed the button 'delete' that it was gone forever.

Wow, were we wrong."
— Oliver North, 1987

Evidence for an educational problem: There is a huge secondary market for used disk drives.

- Re-used within organizations
- 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 hide	Item Title	Price	Bids	Time Left
	Lot of hard and floppy drives	$5.50	2	14m
	Lot of hard and floppy drives	$5.50	2	22m
	Lot of hard and floppy drives	$5.50	2	25m
	Lot of 2 hard drives IDE	$8.00	12	29m
	3.2 gig Hard Drives	$180.00	-	59m
	(5) 1.2 hard drives & (15) 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 $124.95 Buy It Now	-	1h 50m
	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 dutch	$6.00	1	2h 57m
	WINDOWS	$6.00	-	3h 18m

People could just be discarding disk drives without thinking about the consequences.

To be effective, patterns should address the root cause of the problem.

Usability Problem:

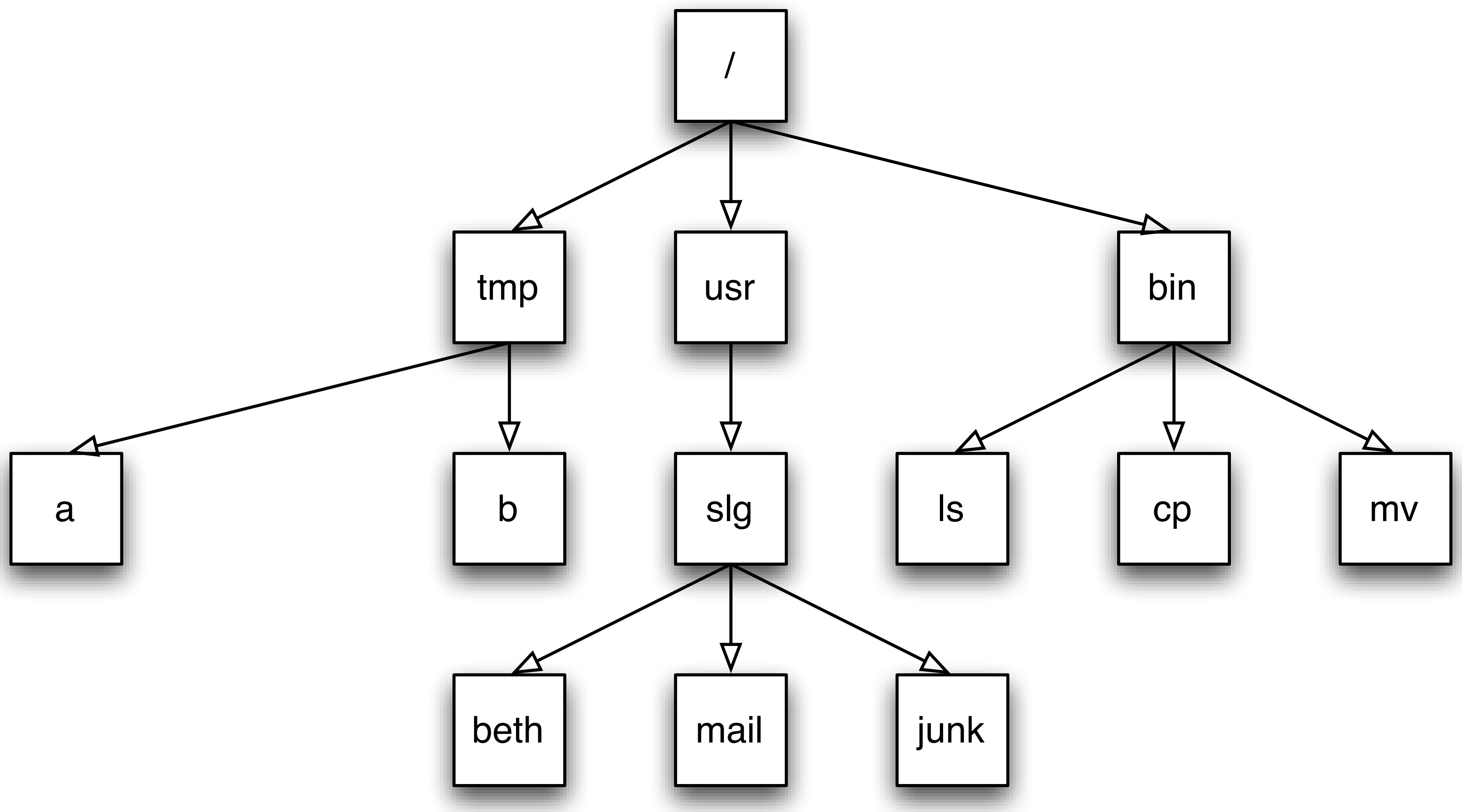
- Effective audit of information present on drives.
- Make DEL and FORMAT actually remove data. [Bauer & Priyantha 01]
- Provide alternative strategies for data recovery.

Education Problem:

- Add training to the interface. [Whitten 04]
- Regulatory requirements. [FTC 05, SEC 05]
- Legal liability.

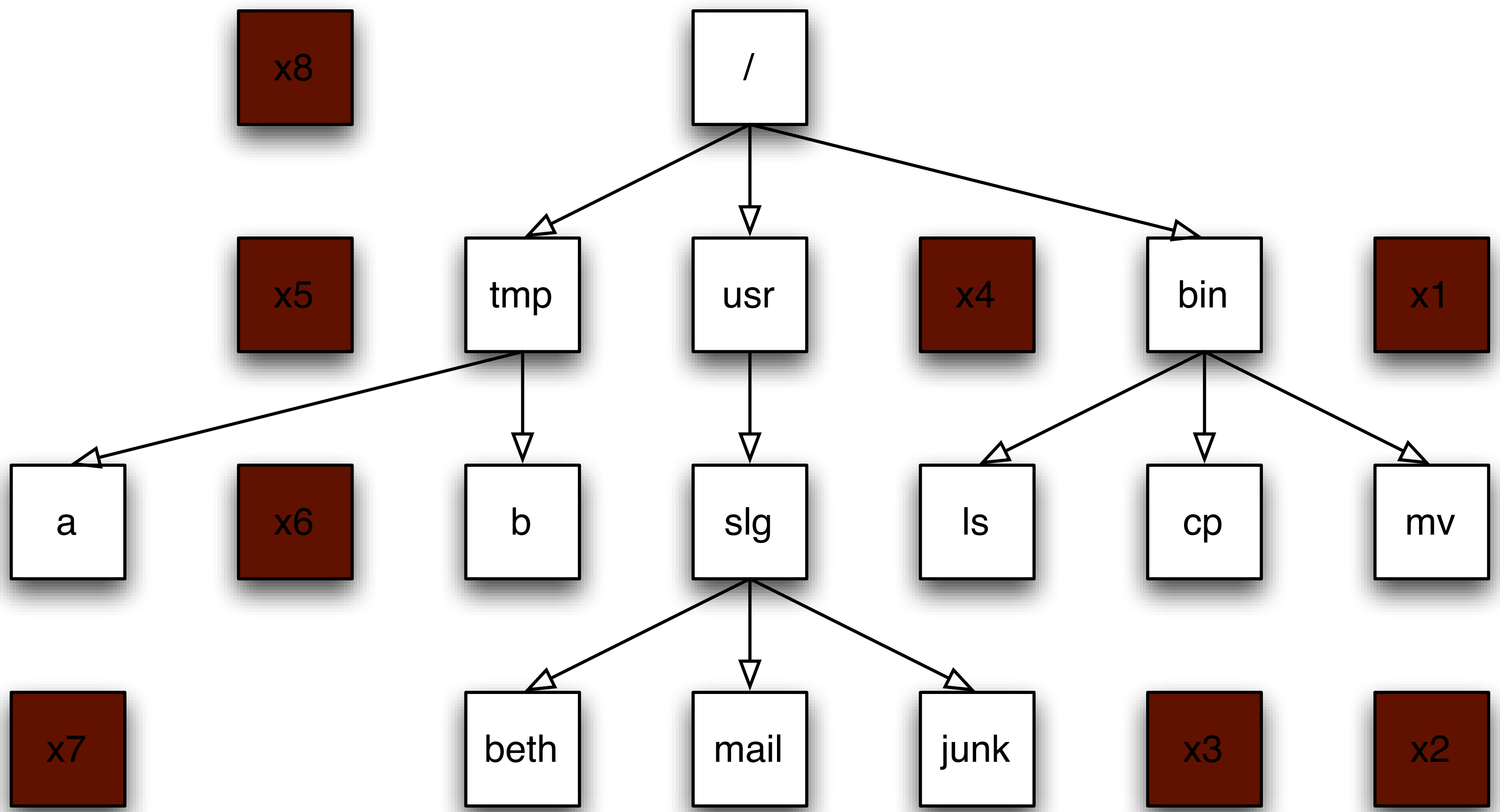
To determine the root cause, I looked *on the drives* and *contacted the data subjects*.

Data on a hard drive is arranged in blocks.



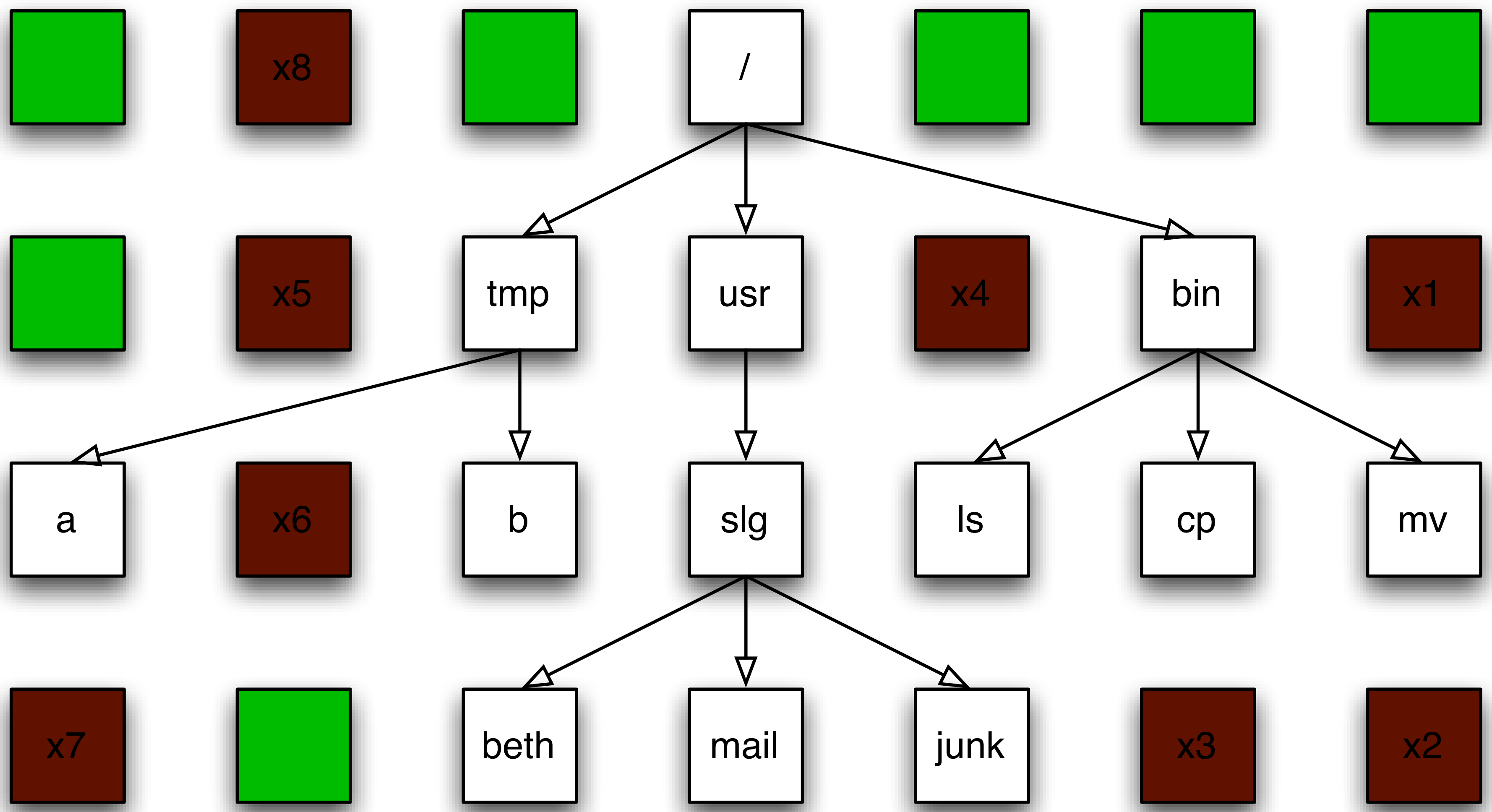
The white blocks indicate directories and files that are visible to the user.

Data on a hard drive is arranged in blocks.



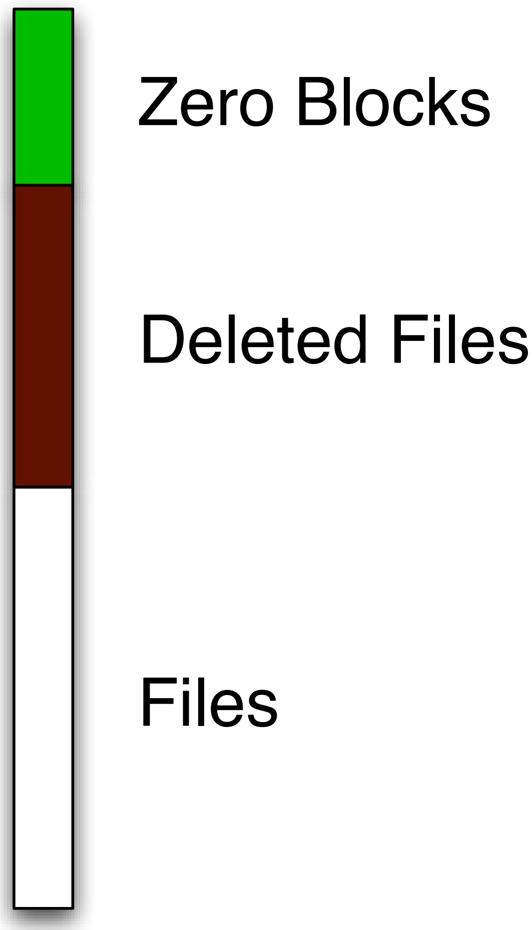
The brown blocks indicate files that were deleted.

Data on a hard drive is arranged in blocks.

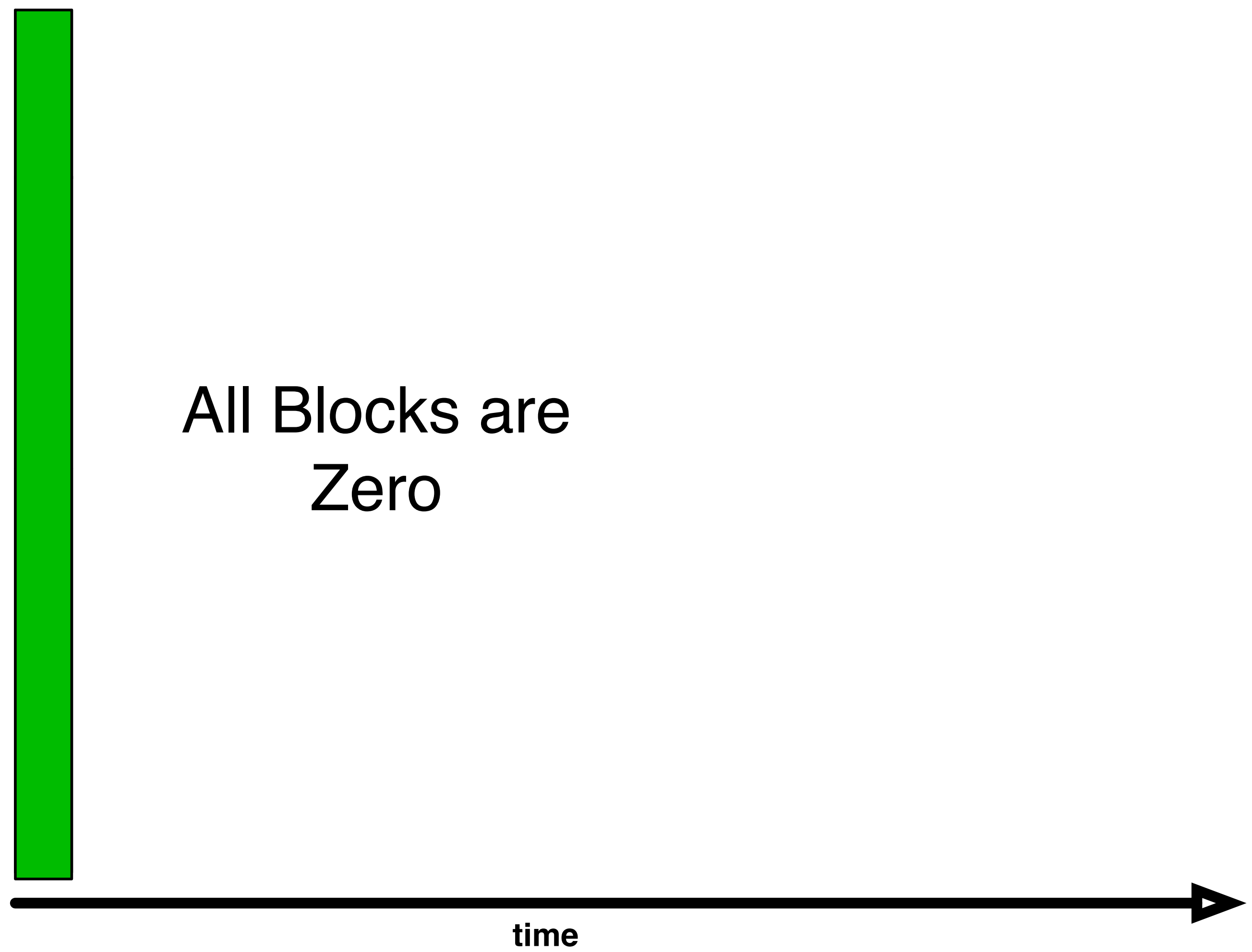


The green blocks indicate blocks that were never used (or that were wiped clean).

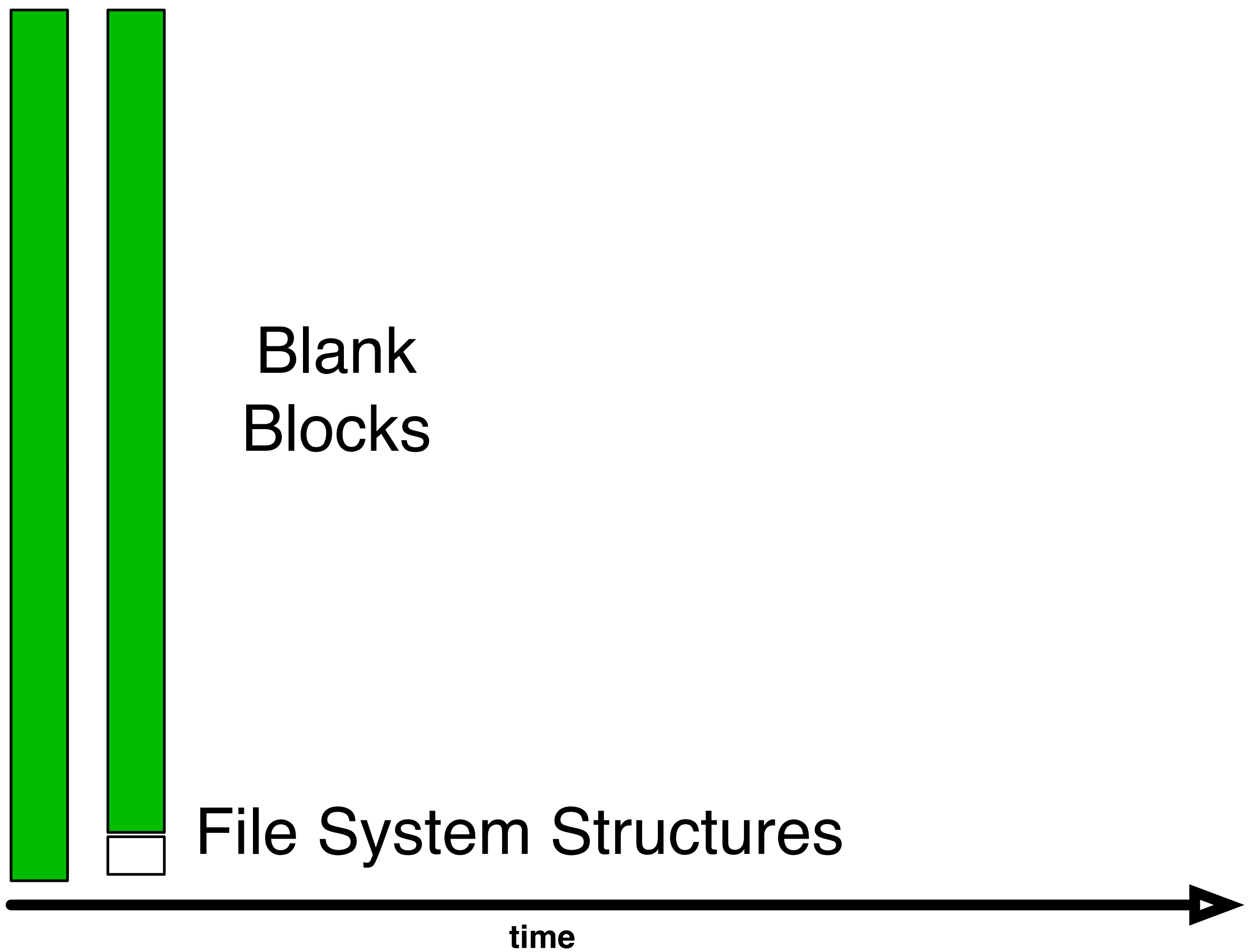
Stack the disk blocks:



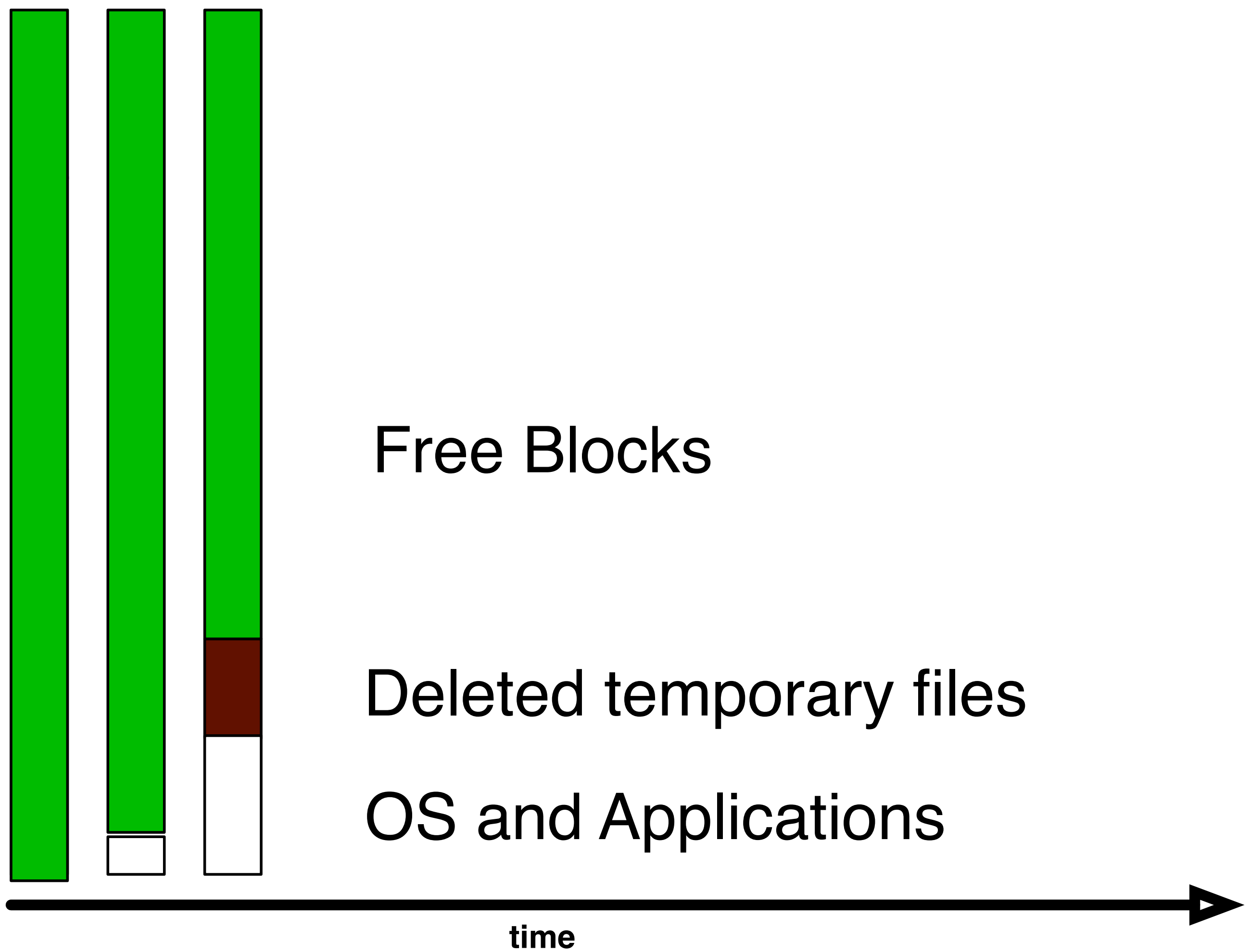
NO DATA: The disk is factory fresh.



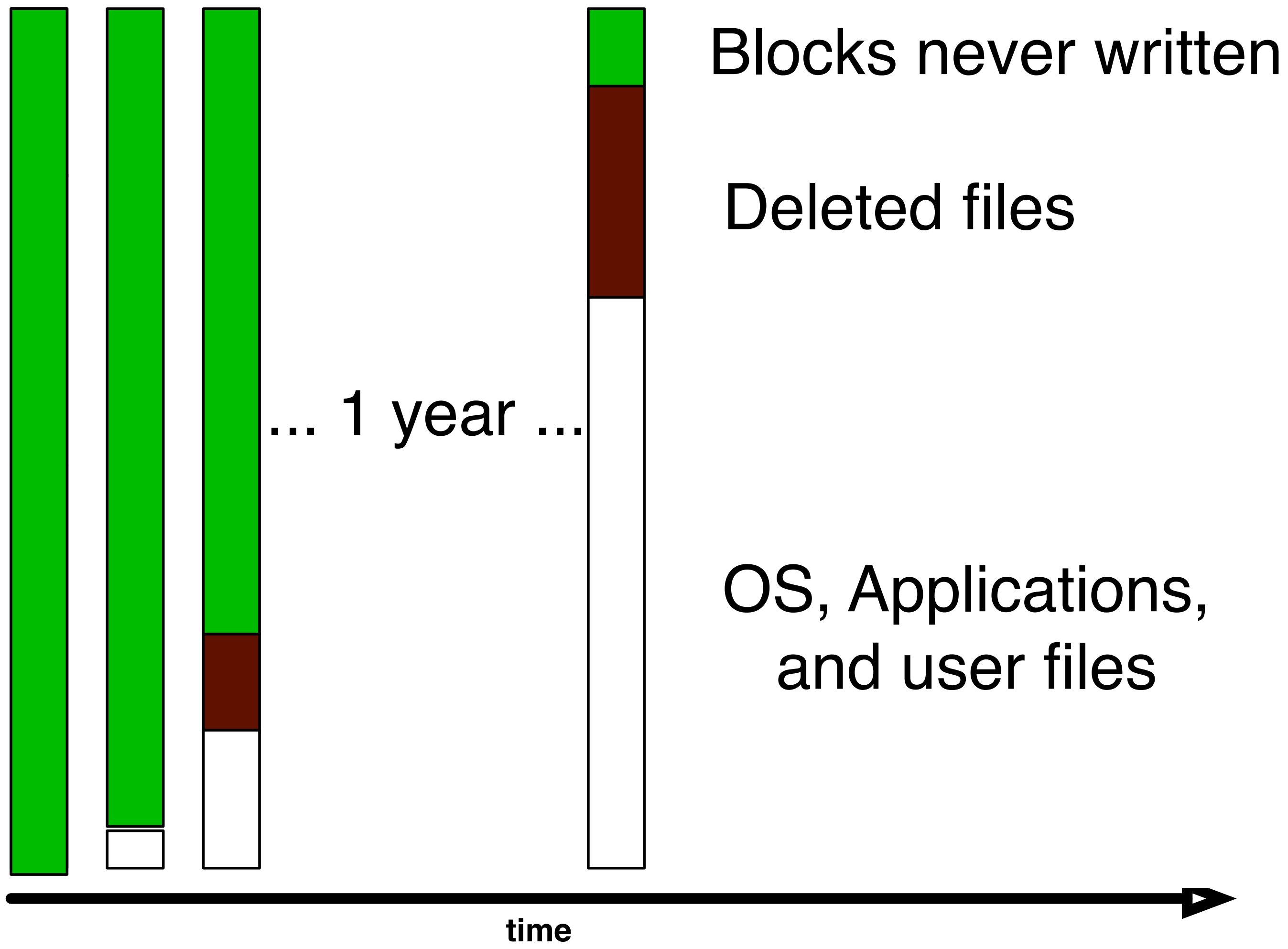
FORMATTED: The disk has an empty file system



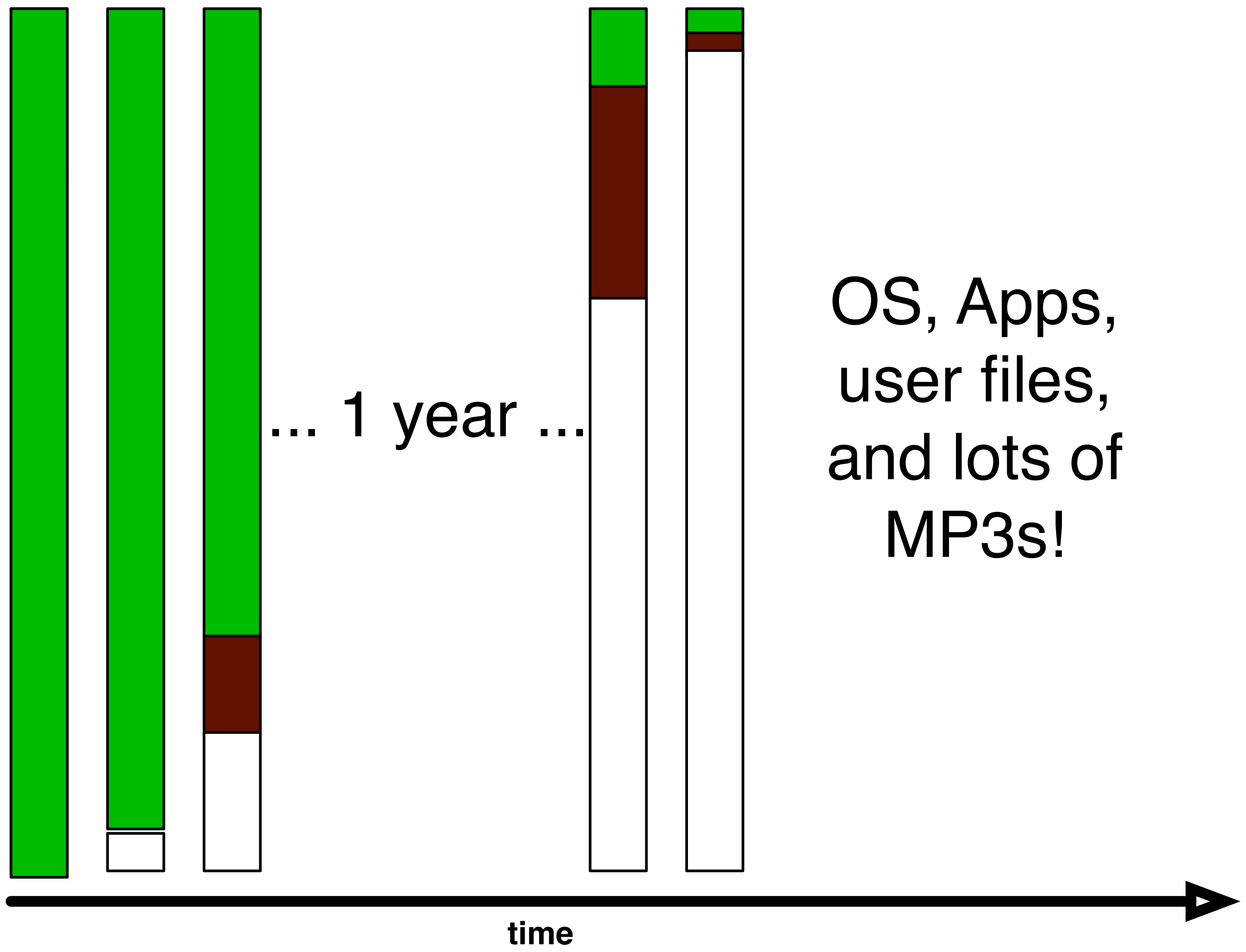
AFTER OS INSTALL: Temp. files have been deleted



AFTER A YEAR OF SERVICE

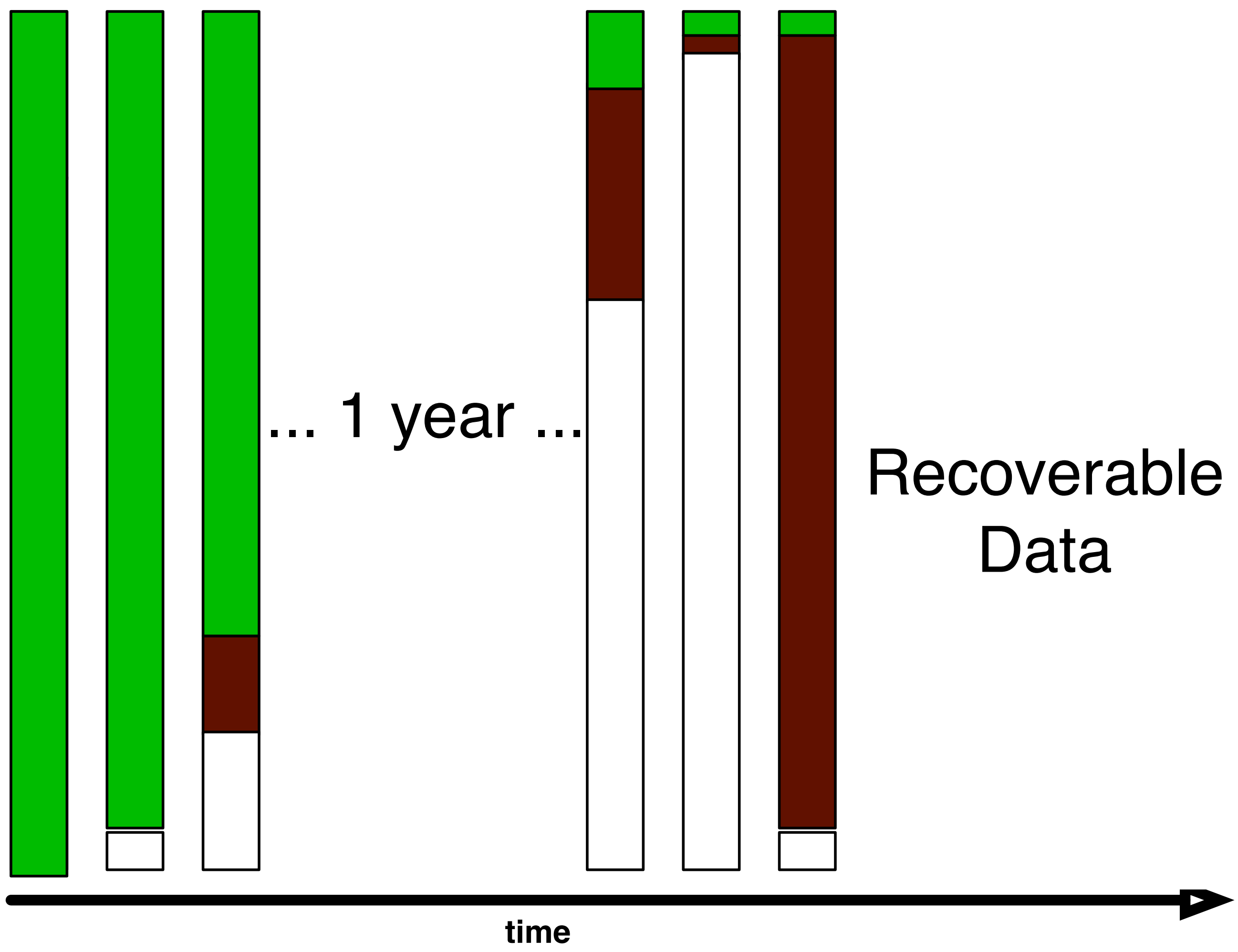


DISK NEARLY FULL!

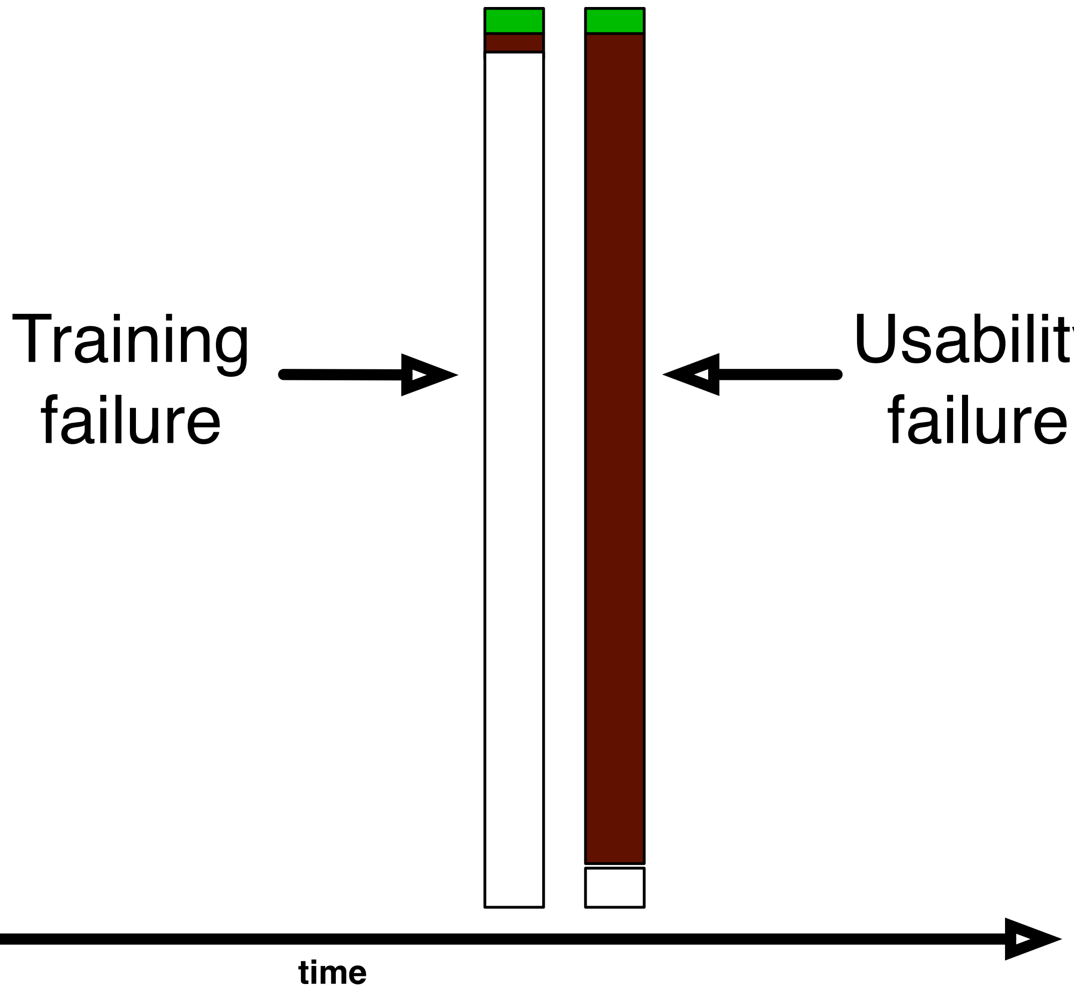


OS, Apps,
user files,
and lots of
MP3s!

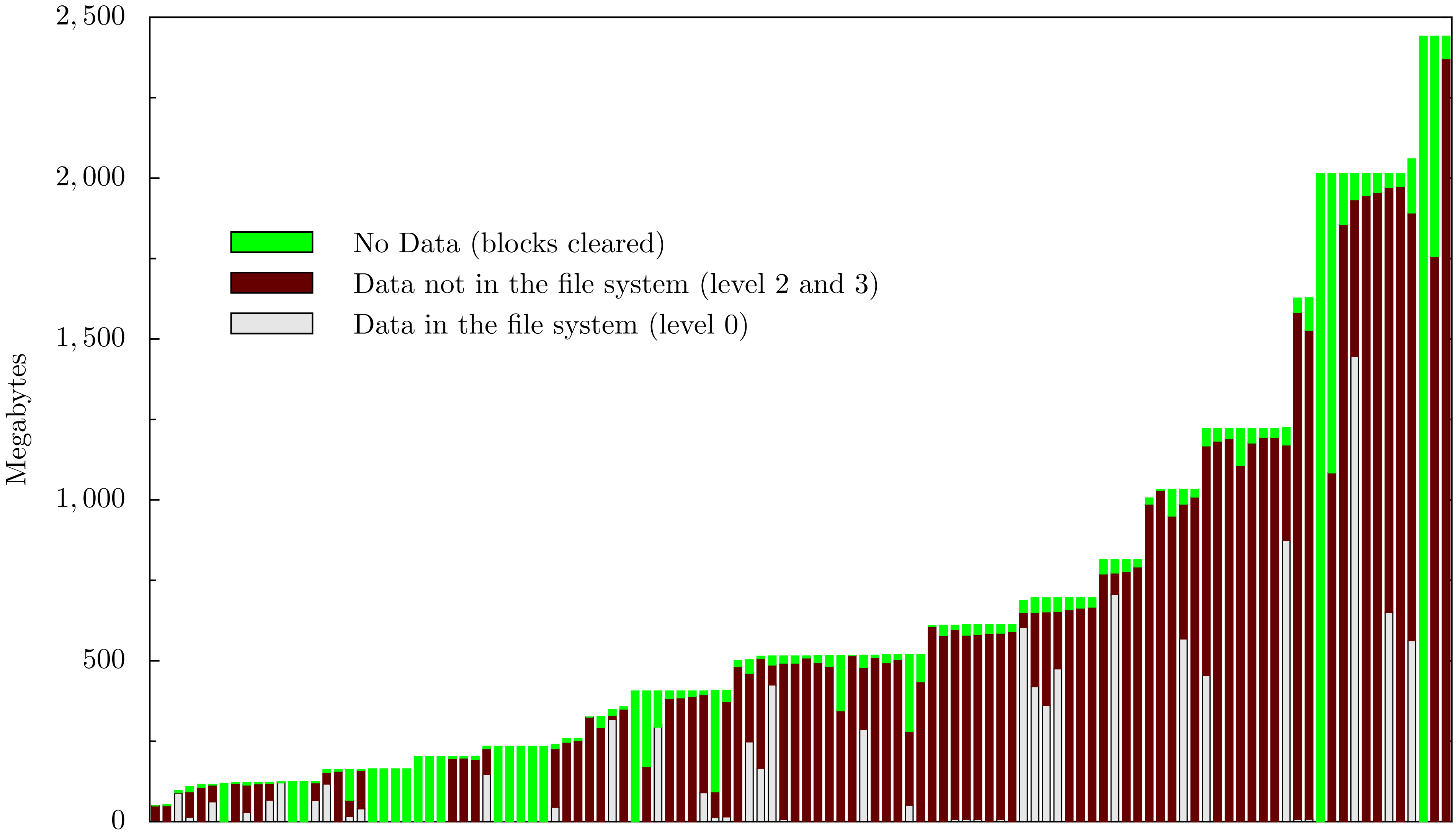
FORMAT C:\ (to sell the computer.)



We can use forensics to reconstruct motivations:



The 236 drives are dominated by failed sanitization attempts.



But training failures are also important.

But what *really* happened?

?

To answer this question, I needed to contact the original drive owners.

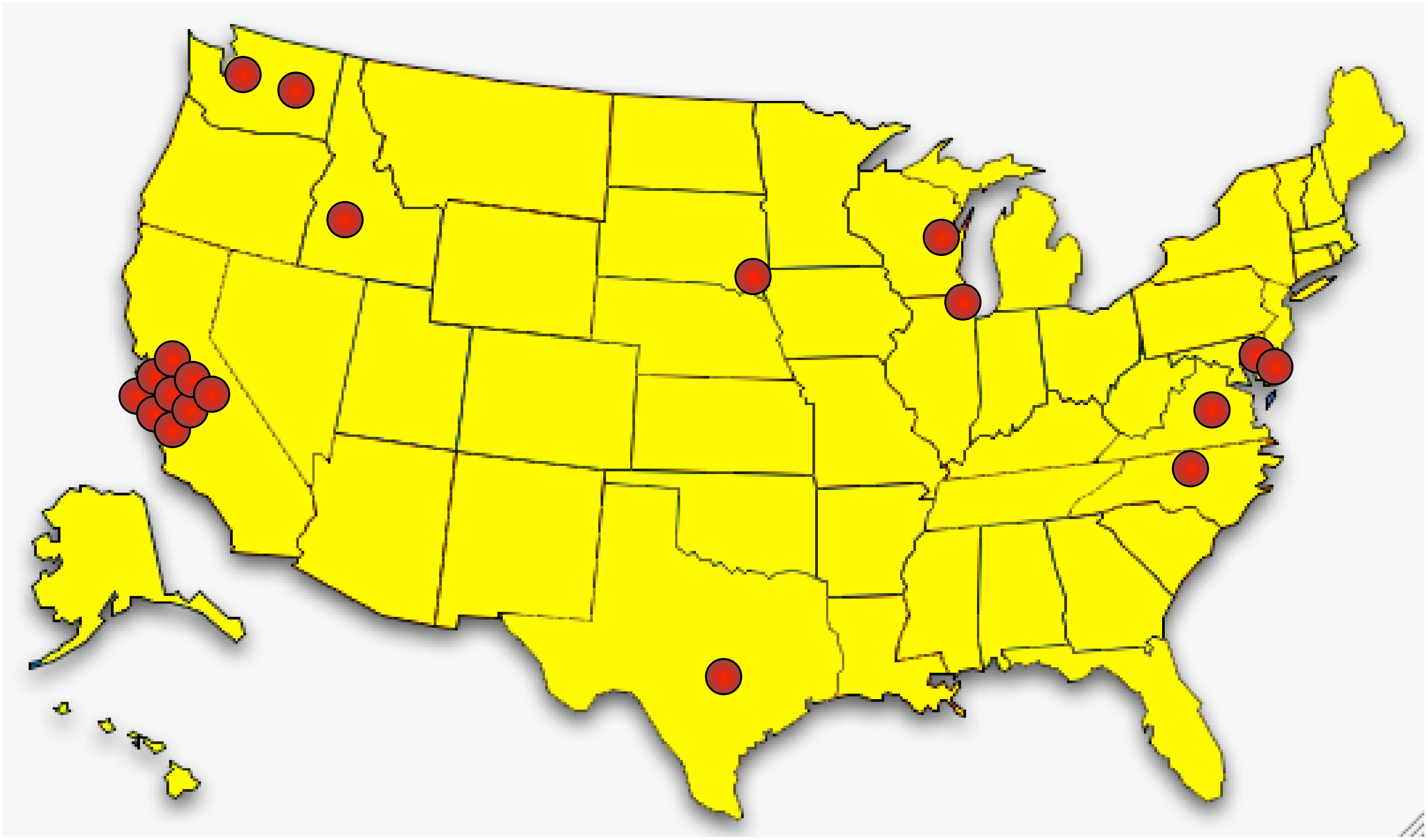
The *Remembrance of Data Passed Traceback Study*.

1. Find data on hard drive
2. Determine the owner
3. Get contact information for organization
4. Find the right person *inside* the organization
5. Set up interviews
6. Follow guidelines for human subjects work

```
06/19/1999 /:dir216/Four H Resume.doc
03/31/1999 /:dir216/U.M. Markets & Society.doc
08/27/1999 /:dir270/Resume-Deb.doc
03/31/1999 /:dir270/Deb-Marymount Letter.doc
03/31/1999 /:dir270/Links App. Ltr..doc
08/27/1999 /:dir270/Resume=Marymount U..doc
03/31/1999 /:dir270/NCR App. Ltr..doc
03/31/1999 /:dir270/Admissions counselor, NCR.doc
08/27/1999 /:dir270/Resume, Deb.doc
03/31/1999 /:dir270/UMUC App. Ltr..doc
03/31/1999 /:dir270/Ed. Coordinator Ltr..doc
03/31/1999 /:dir270/American College ...doc
04/01/1999 /:dir270/Am. U. Admin. Dir..doc
04/05/1999 /:dir270/IR Unknown Lab.doc
04/06/1999 /:dir270/Admit Slip for Modernism.doc
04/07/1999 /:dir270/Your Honor.doc
```

This was a lot harder than I thought it would be.

Ultimately, I contacted 20 organizations between April 2003 and April 2005.



The leading cause of compromised privacy was betrayed trust.

Trust Failure: 5 cases

- ✔ Home computer; woman’s son took to “PC Recycle”
- ✔ Community college; no procedures in place
- ✔ Church in South Dakota; administrator “kind of crazy”
- ✔ Auto dealership; consultant sold drives he “upgraded”
- ✔ Home computer, financial records; same consultant

This specific failure wasn’t considered in [GS 03]; it was the most common failure.

Poor training or supervision was the second leading cause.

Trust Failure: 5 cases

Lack of Training: 3 cases

- ✔ California electronic manufacturer
- ✔ Supermarket credit-card processing terminal
- ✔ ATM machine from a Chicago bank

Alignment between the interface and the underlying representation would overcome this problem.

In two cases, the data custodians simply didn't care.

Trust Failure: 5 cases

Lack of Training: 3 cases

Lack of Concern: 2 cases

- ✔ Bankrupt Internet software developer
- ✔ Layoffs at a computer magazine

Regulation on resellers might have prevented these cases.

In seven cases, no cause could be determined.

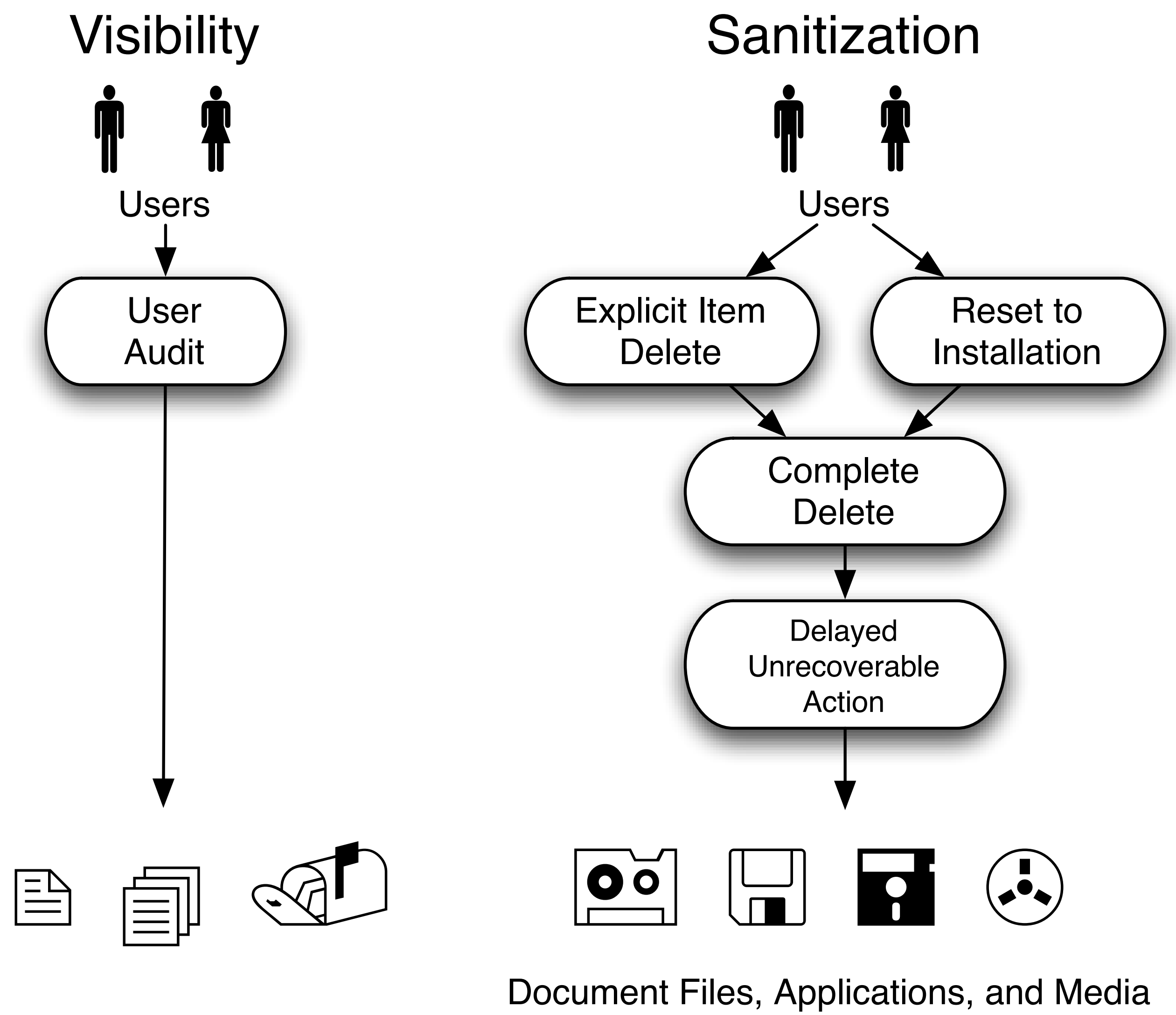
Trust Failure: 5 cases
Lack of Training: 3 cases
Lack of Concern: 2 cases

Unknown Reason: 7 cases

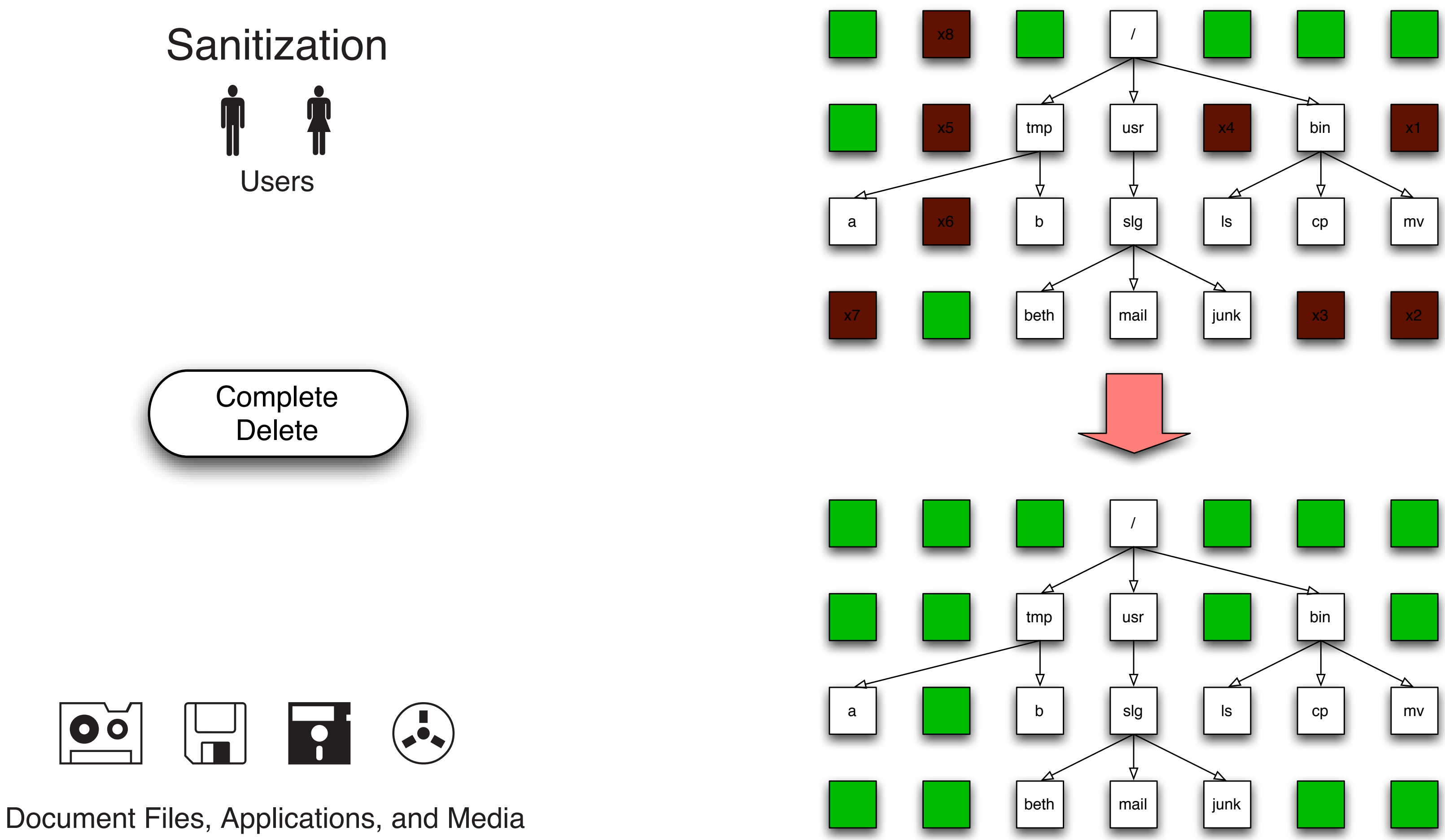
- ✘ Bankrupt biotech startup
- ✘ Another major electronics manufacturer
- ✘ Primary school principal's office
- ✘ Mail order pharmacy
- ✘ Major telecommunications provider
- ✘ Minnesota food company
- ✘ State Corporation Commission

Regulation might have helped here, too.

I have identified five distinct patterns for addressing the sanitization problem.

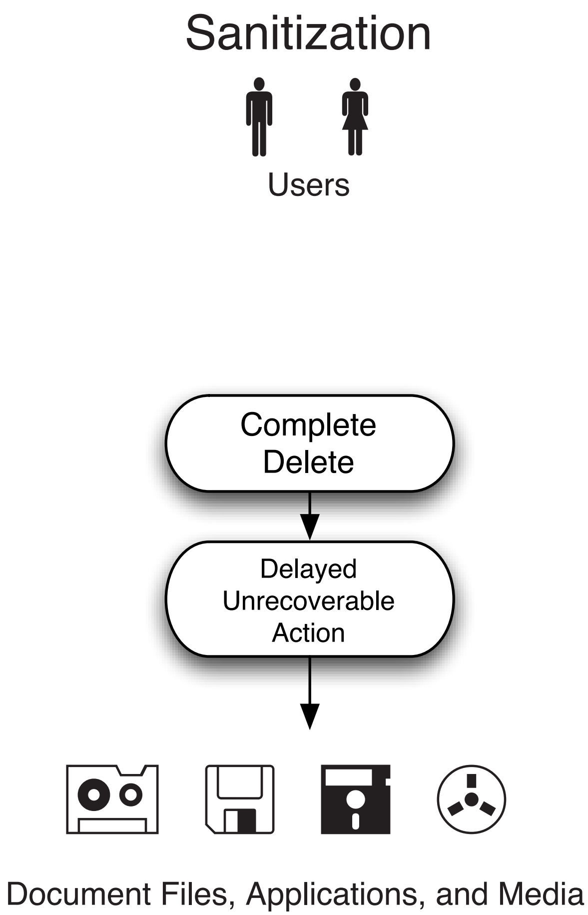


Complete Delete: assure that deleting the *visible* representation deletes the *hidden* data as well.



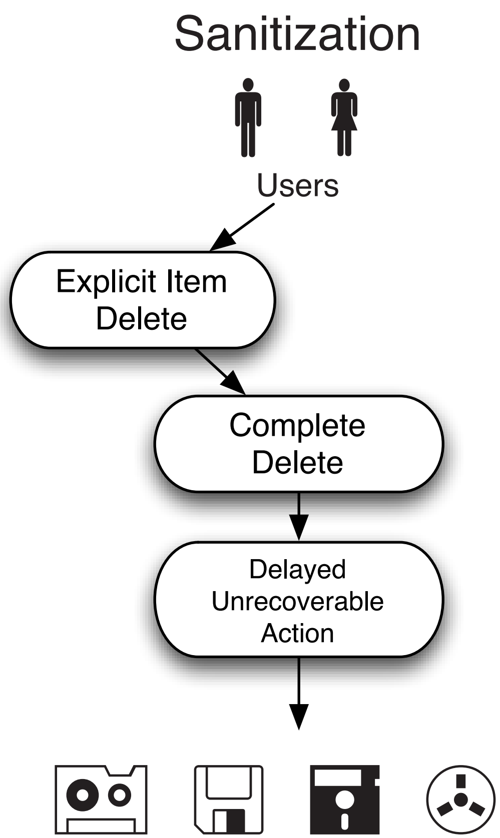
Naming this pattern lets us discuss its absence in modern operating systems.

Delayed Unrecoverable Action: give the users a chance to change their minds.

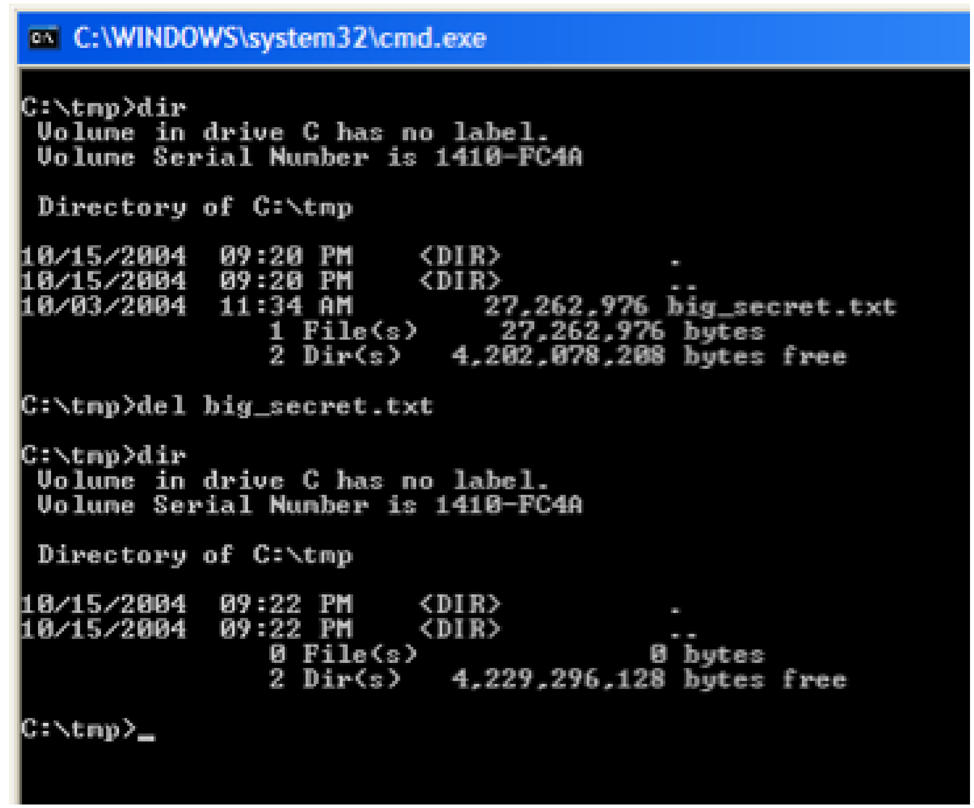


[Norman 83] and [Cooper 99] both suggest this functionality, but they do not name or integrate it.

Two ways to delete information. #1: *Explicit Item Delete*

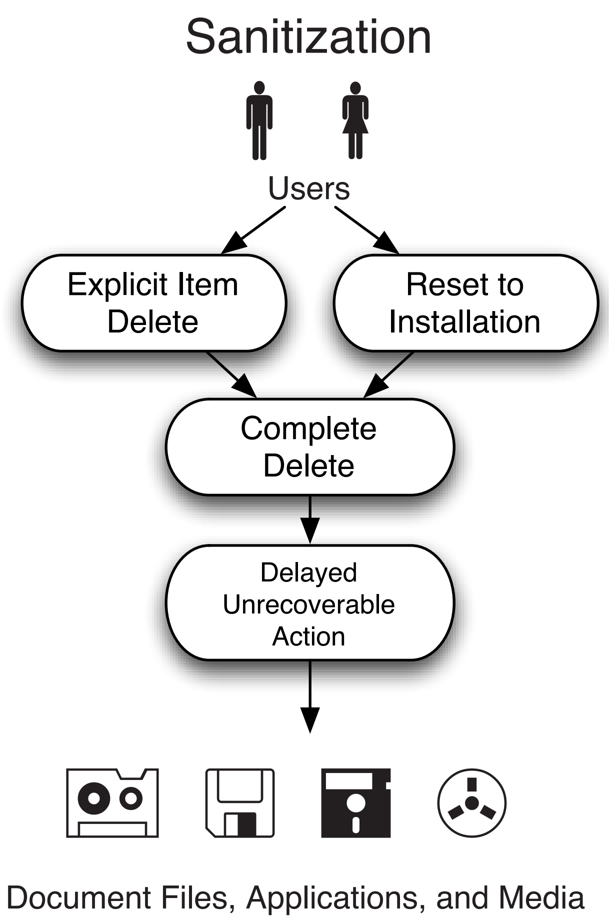


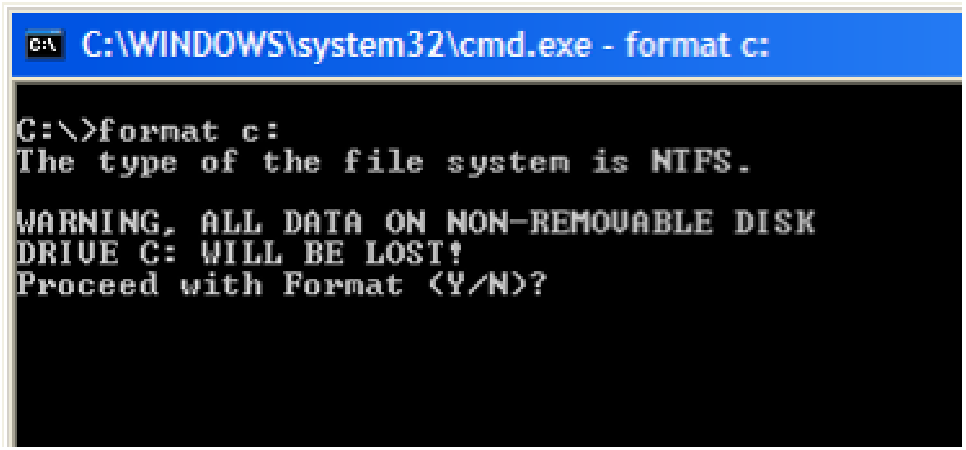
Document Files, Applications, and Media



"Provide a means for deleting information where the information is displayed."

Reset to Installation: Get rid of everything

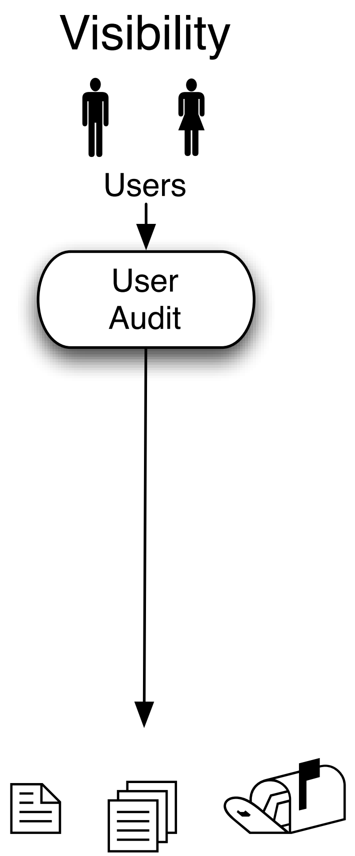


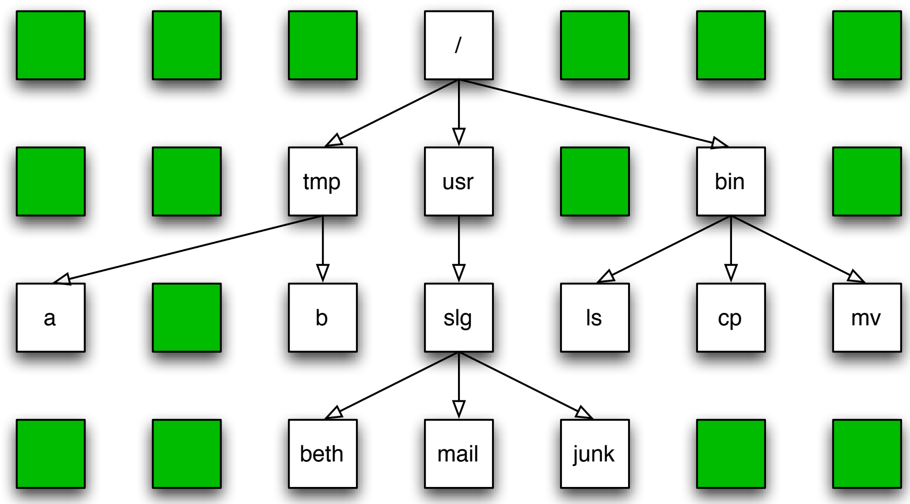


Reset/reinstall functionality is common (Windows; PalmOS; etc.).

This pattern framework clarifies *Reset's* security property.

User Audit: If the information is present, make it visible.

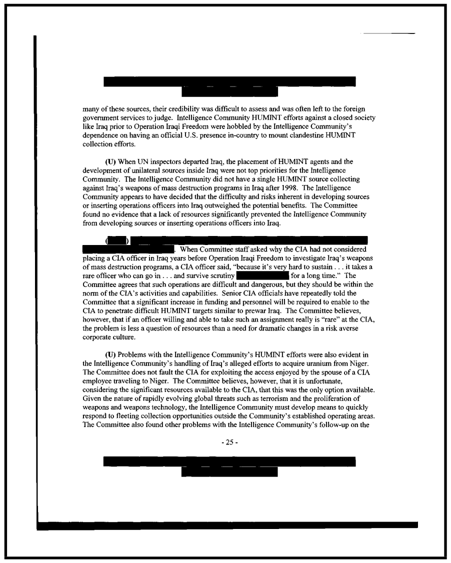




With files, this happens automatically when the *Complete Delete* pattern is implemented.

The power of these patterns is that they apply equally well to other sanitization problems.

- Document Files



[redacted]

many of these sources, their credibility was difficult to assess and was often left to the foreign government services to judge. Intelligence Community HUMINT efforts against a closed society like Iraq prior to Operation Iraqi Freedom were hobbled by the Intelligence Community's dependence on having an official U.S. presence in-country to mount clandestine HUMINT collection efforts.

(U) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unilateral sources inside Iraq were not top priorities for the Intelligence Community. The Intelligence Community did not have a single HUMINT source collecting against Iraq's weapons of mass destruction programs in Iraq after 1998. The Intelligence Community appears to have decided that the difficulty and risks inherent in developing sources or inserting operations officers into Iraq outweighed the potential benefits. The Committee found no evidence that a lack of resources significantly prevented the Intelligence Community from developing sources or inserting operations officers into Iraq.

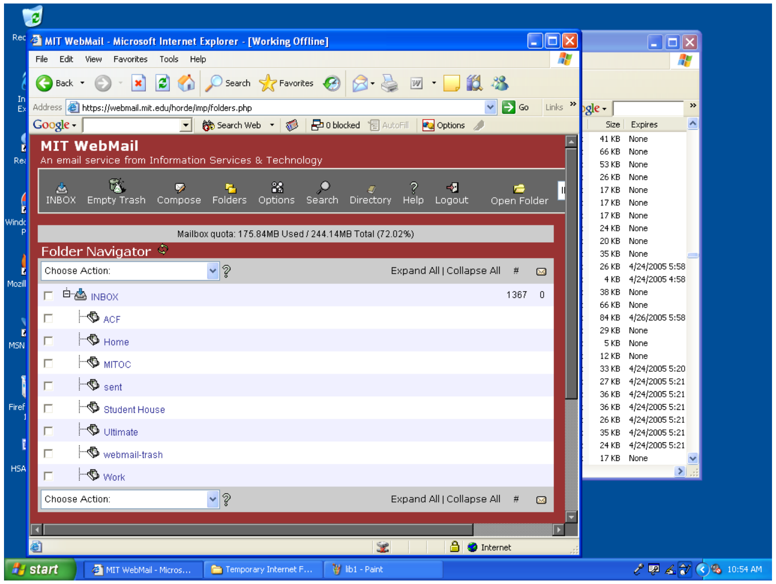
([redacted]) [redacted]. When Committee staff asked why the CIA had not considered placing a CIA officer in Iraq years before Operation Iraqi Freedom to investigate Iraq's weapons of mass destruction programs, a CIA officer said, "because it's very hard to sustain . . . it takes a rare officer who can go in . . . and survive scrutiny [redacted] for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the norm of the CIA's activities and capabilities. Senior CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable to the CIA to penetrate difficult HUMINT targets similar to prewar Iraq. The Committee believes, however, that if an officer willing and able to take such an assignment really is "rare" at the CIA, the problem is less a question of resources than a need for dramatic changes in a risk averse corporate culture.

(U) Problems with the Intelligence Community's HUMINT efforts were also evident in the Intelligence Community's handling of Iraq's alleged efforts to acquire uranium from Niger. The Committee does not fault the CIA for exploiting the access enjoyed by the spouse of a CIA employee traveling to Niger. The Committee believes, however, that it is unfortunate, considering the significant resources available to the CIA, that this was the only option available. Given the nature of rapidly evolving global threats such as terrorism and the proliferation of weapons and weapons technology, the Intelligence Community must develop means to quickly respond to fleeting collection opportunities outside the Community's established operating areas. The Committee also found other problems with the Intelligence Community's follow-up on the

- 25 -

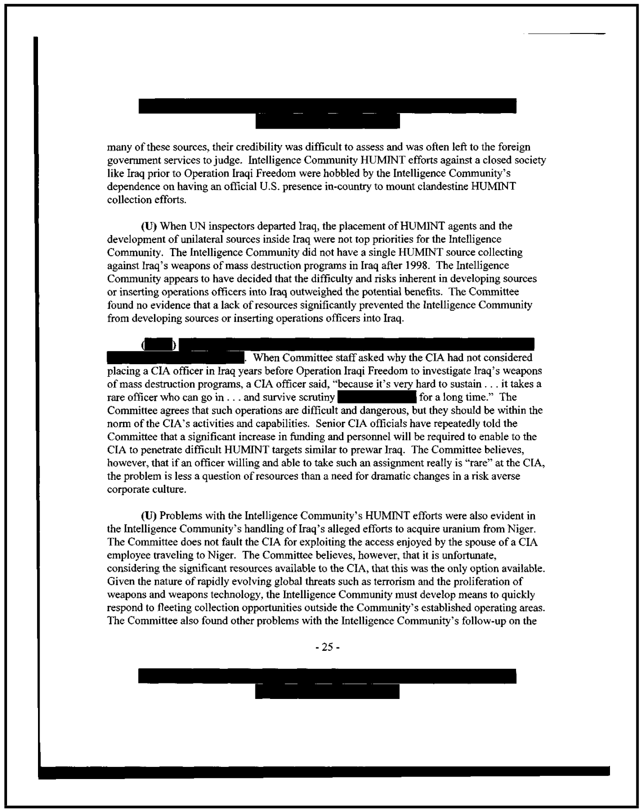
[redacted]

- Web Browsers



Information is left in document files.

- The *New York Times* published a **PDF file** containing the names of Iranians who helped with the 1953 coup. [Young 00]
- US DoJ published a **PDF file** "diversity report" containing embarrassing redacted information. [Poulsen 03]
- SCO gave a **Microsoft Word file** to journalists that revealed its Linux legal strategy. [Shankland 04]



[redacted]

many of these sources, their credibility was difficult to assess and was often left to the foreign government services to judge. Intelligence Community HUMINT efforts against a closed society like Iraq prior to Operation Iraqi Freedom were hobbled by the Intelligence Community's dependence on having an official U.S. presence in-country to mount clandestine HUMINT collection efforts.

(U) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unilateral sources inside Iraq were not top priorities for the Intelligence Community. The Intelligence Community did not have a single HUMINT source collecting against Iraq's weapons of mass destruction programs in Iraq after 1998. The Intelligence Community appears to have decided that the difficulty and risks inherent in developing sources or inserting operations officers into Iraq outweighed the potential benefits. The Committee found no evidence that a lack of resources significantly prevented the Intelligence Community from developing sources or inserting operations officers into Iraq.

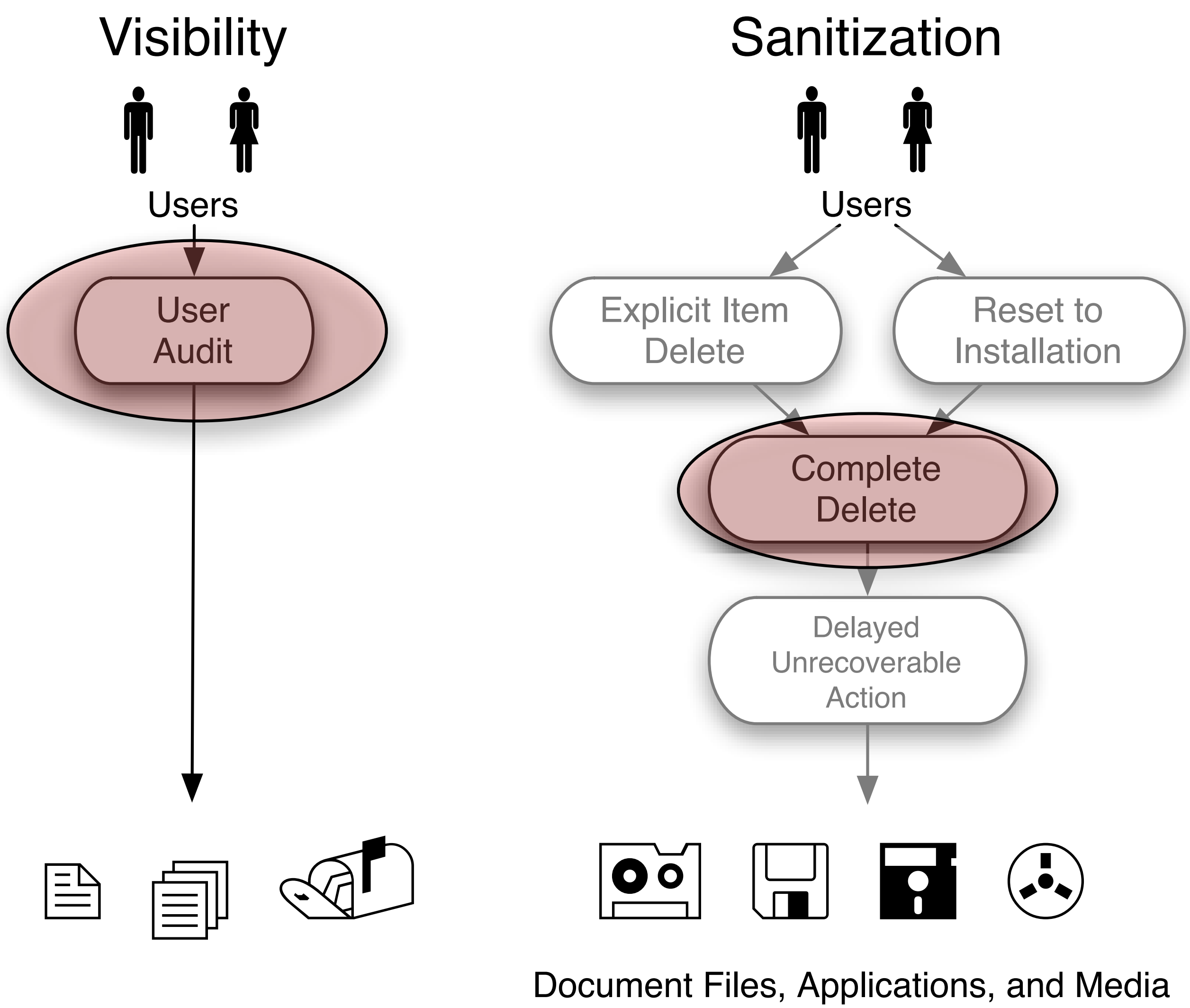
([redacted]) [redacted]. When Committee staff asked why the CIA had not considered placing a CIA officer in Iraq years before Operation Iraqi Freedom to investigate Iraq's weapons of mass destruction programs, a CIA officer said, "because it's very hard to sustain . . . it takes a rare officer who can go in . . . and survive scrutiny [redacted] for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the norm of the CIA's activities and capabilities. Senior CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable to the CIA to penetrate difficult HUMINT targets similar to prewar Iraq. The Committee believes, however, that if an officer willing and able to take such an assignment really is "rare" at the CIA, the problem is less a question of resources than a need for dramatic changes in a risk averse corporate culture.

(U) Problems with the Intelligence Community's HUMINT efforts were also evident in the Intelligence Community's handling of Iraq's alleged efforts to acquire uranium from Niger. The Committee does not fault the CIA for exploiting the access enjoyed by the spouse of a CIA employee traveling to Niger. The Committee believes, however, that it is unfortunate, considering the significant resources available to the CIA, that this was the only option available. Given the nature of rapidly evolving global threats such as terrorism and the proliferation of weapons and weapons technology, the Intelligence Community must develop means to quickly respond to fleeting collection opportunities outside the Community's established operating areas. The Committee also found other problems with the Intelligence Community's follow-up on the

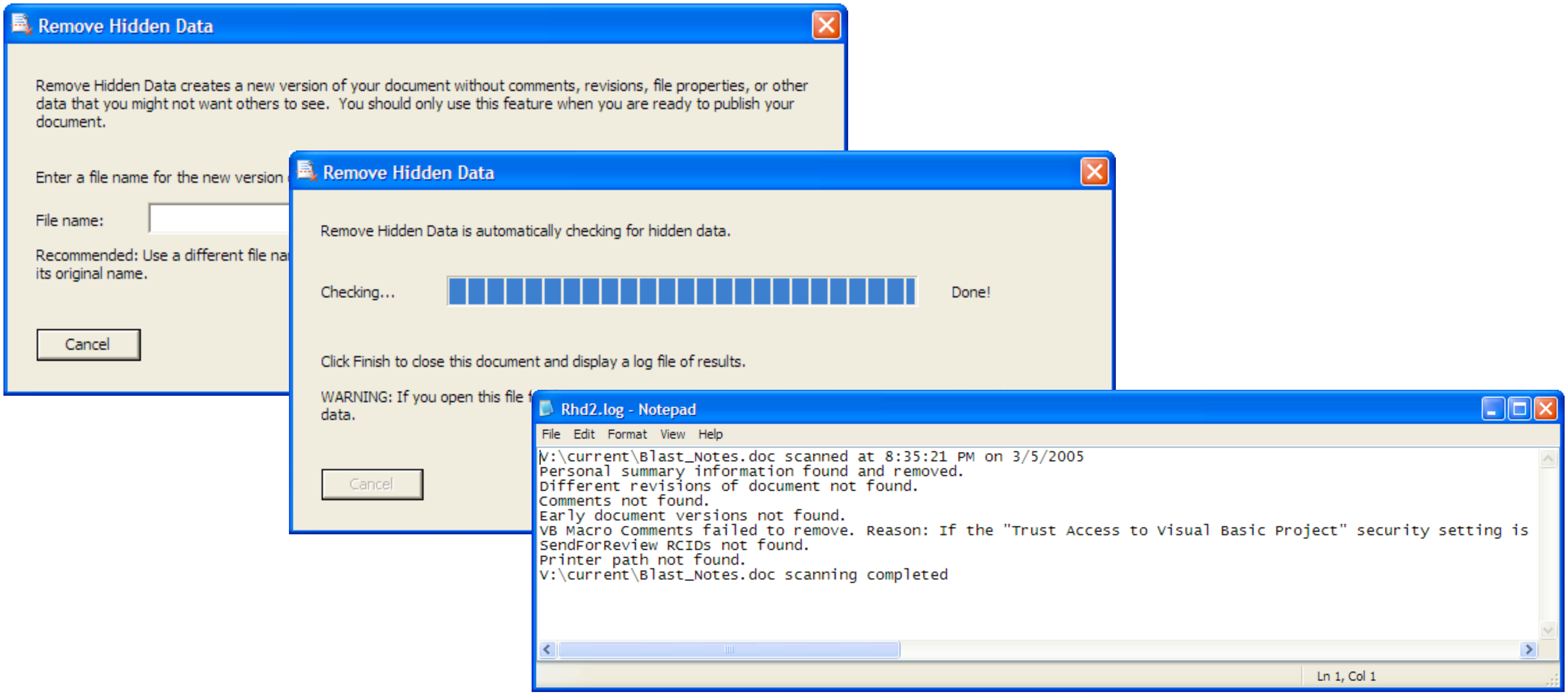
- 25 -

[redacted]

The information leaked because two patterns were not implemented.

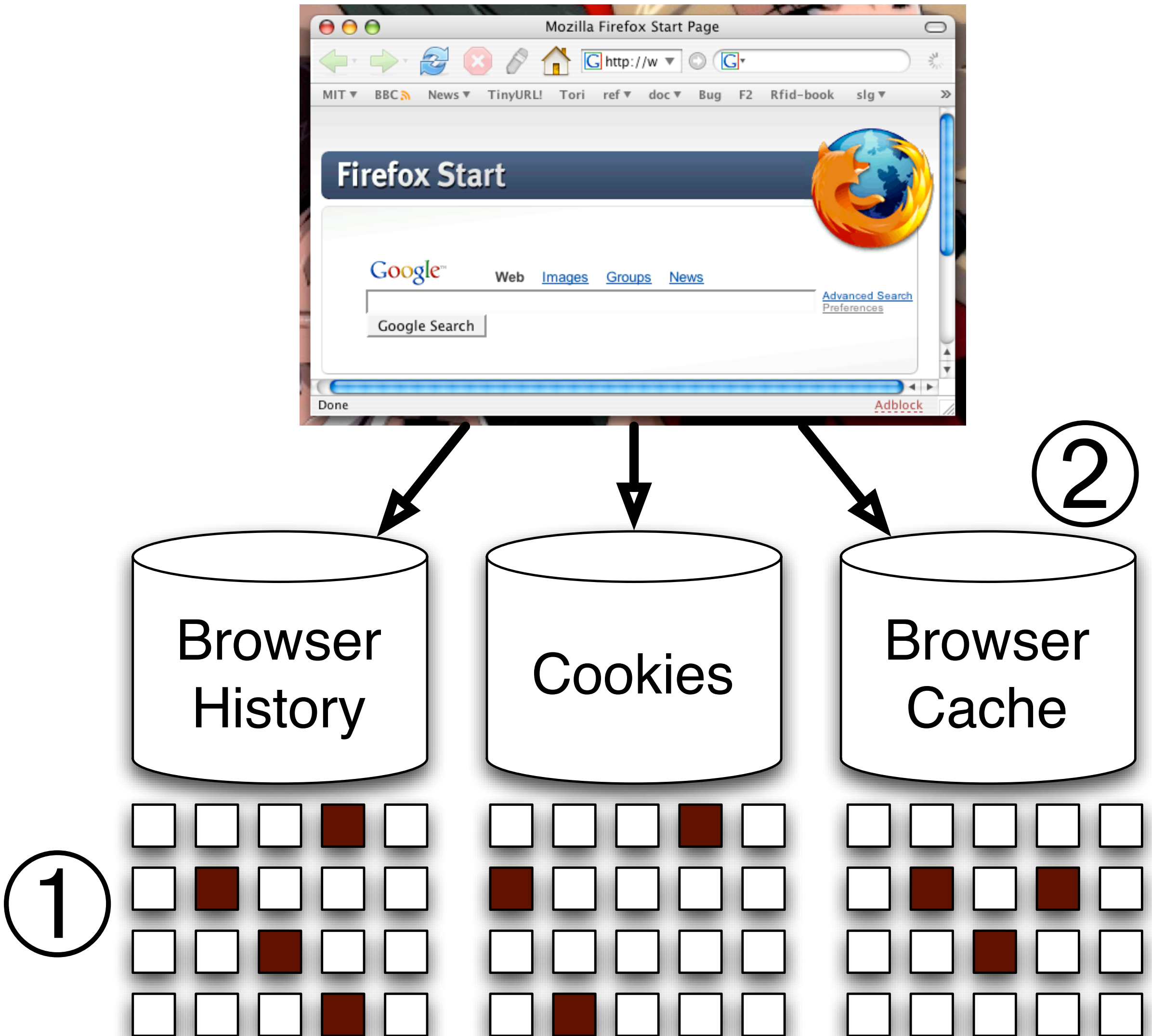


Microsoft has tried to solve this problem with "Remove Hidden Data" tool.



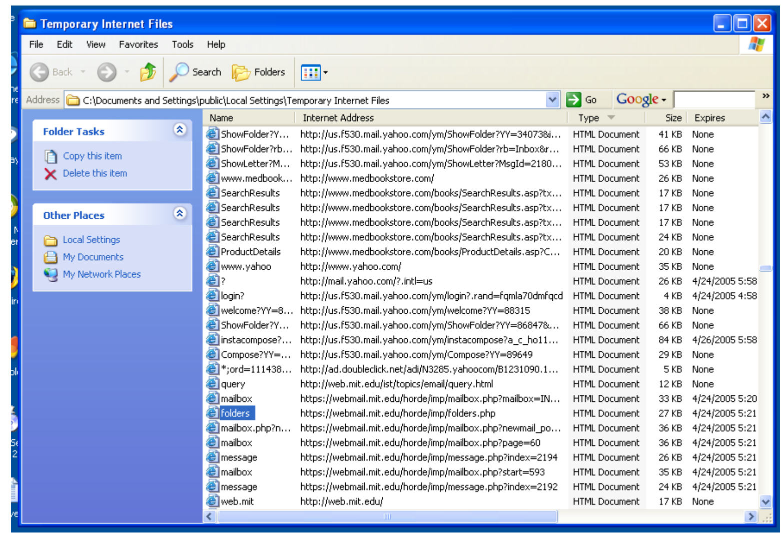
RHD doesn't integrate into the flow of document preparation. The patterns-based analysis predicts that RHD will fail in many cases.

Information is left behind in web browsers.



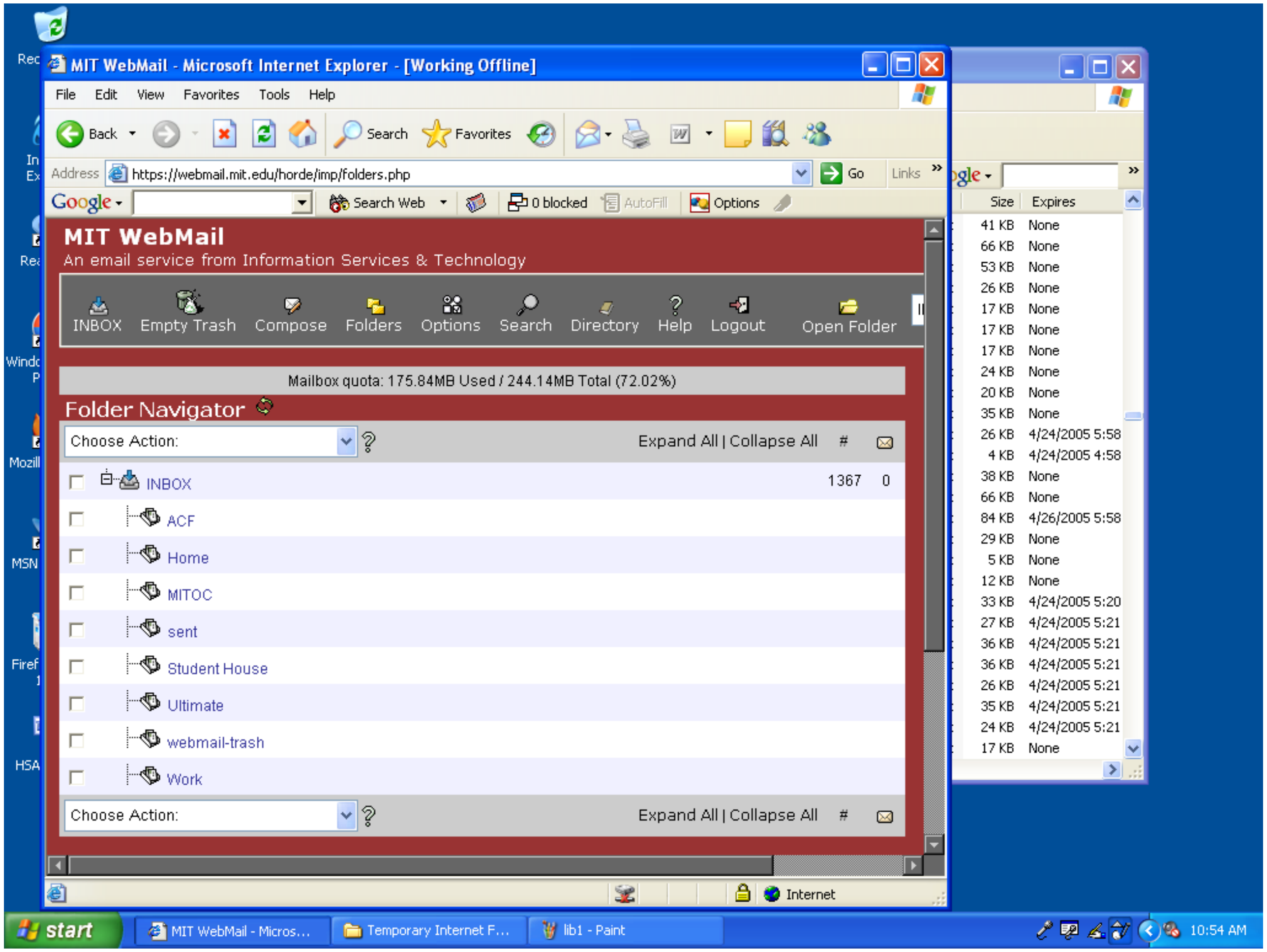
Two key problems: ① Deleted files; ② The cache

In fact, a lot of information is left behind in web browsers.



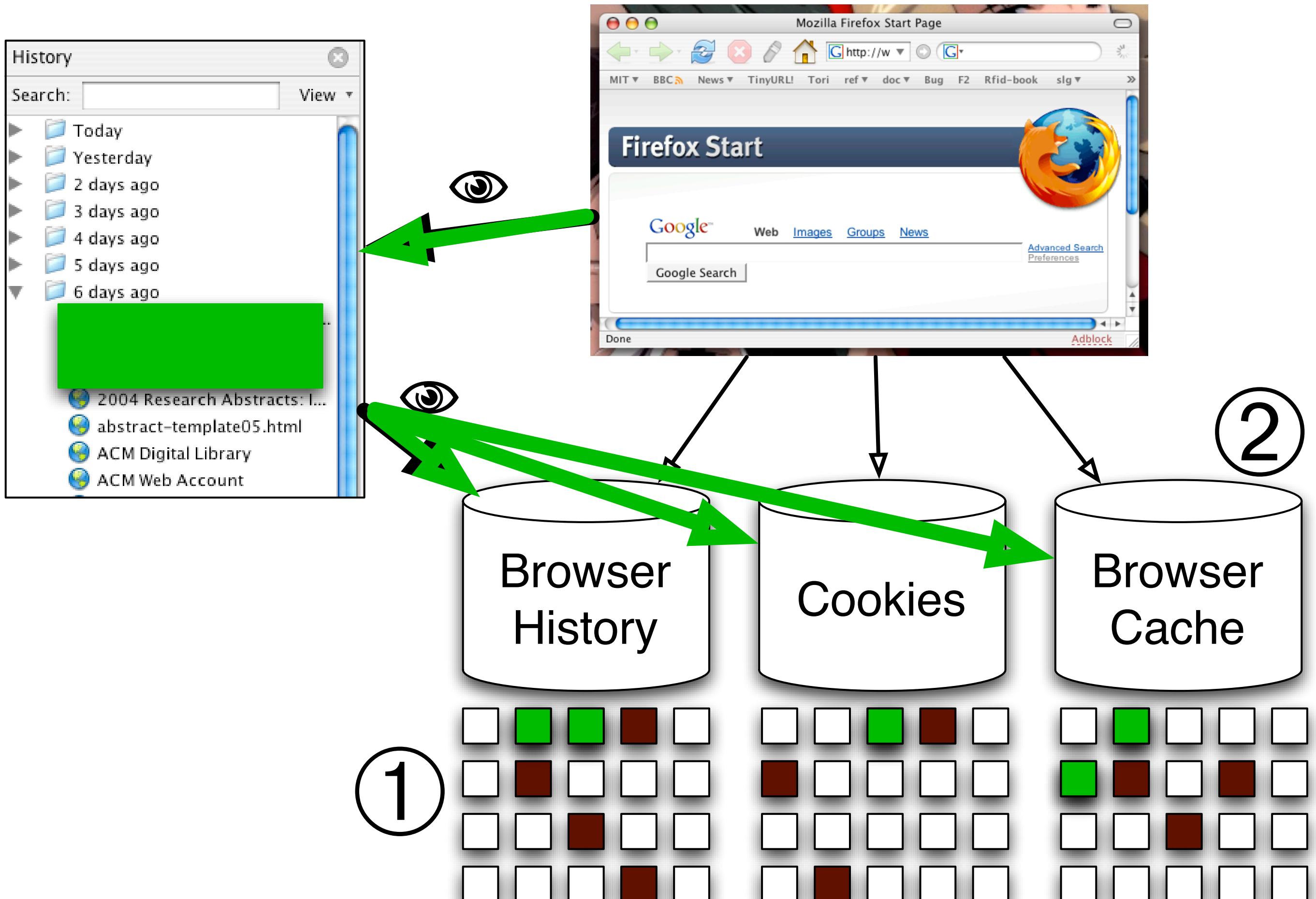
MIT Humanities Library, April 25, 2005

4 out of 4 computers inspected had significant quantities of personal email in their browser caches.



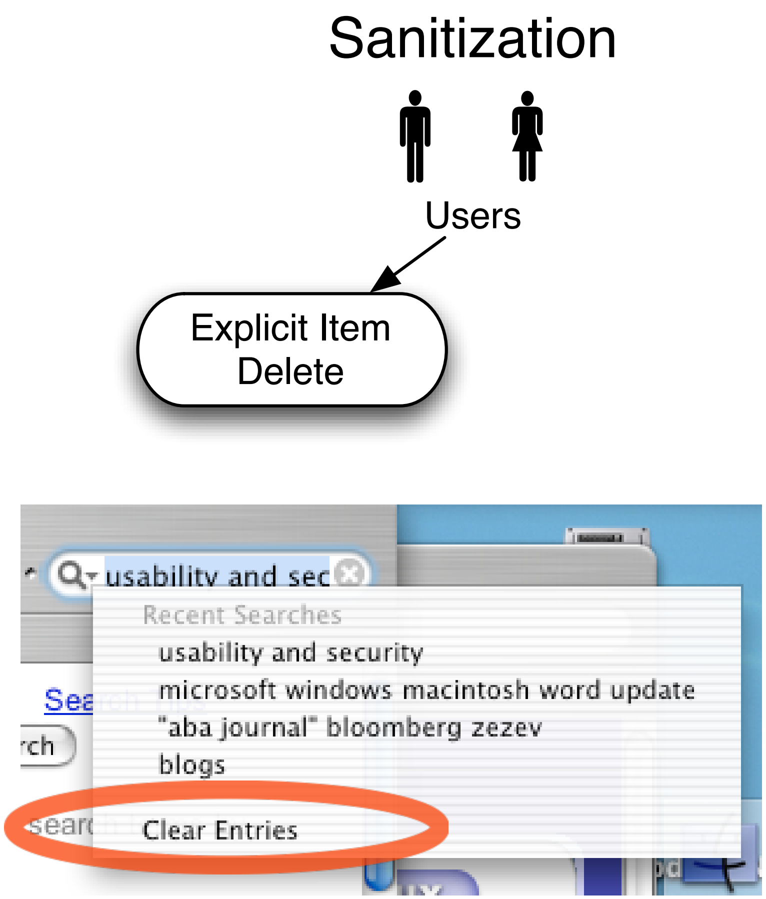
The American Library Association recommends software that automatically purges caches on a *daily* basis.[ALA 05] (It would be better to purge after each use.)

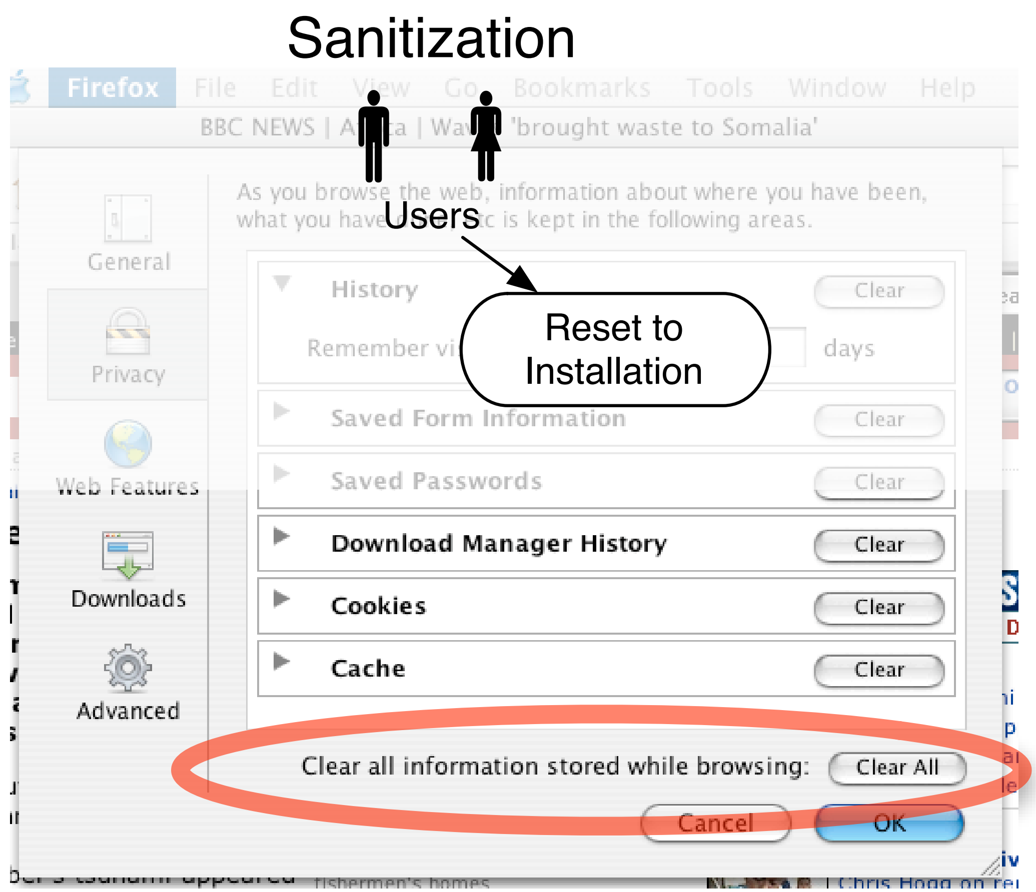
Applying the patterns, an obvious solution is to unify the history and cache:



The patterns make it easy to explain this concept to the browser developers—and users, too!

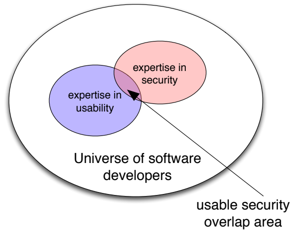
The patterns also suggest opportunities for further promoting HCI-SEC within the browser.



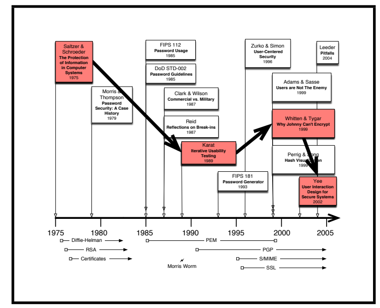


Without *Complete Delete* the data can still be recovered. This demonstrates the need for the complete pattern set.

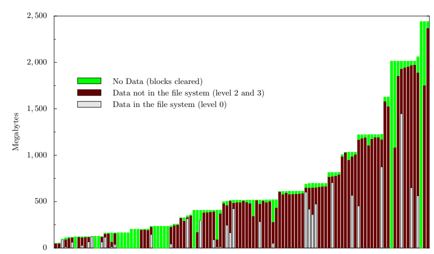
1. Introduction to patterns. ✔



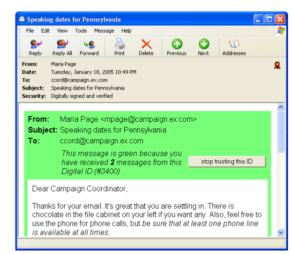
2. Prior work in HCI-SEC. ✔



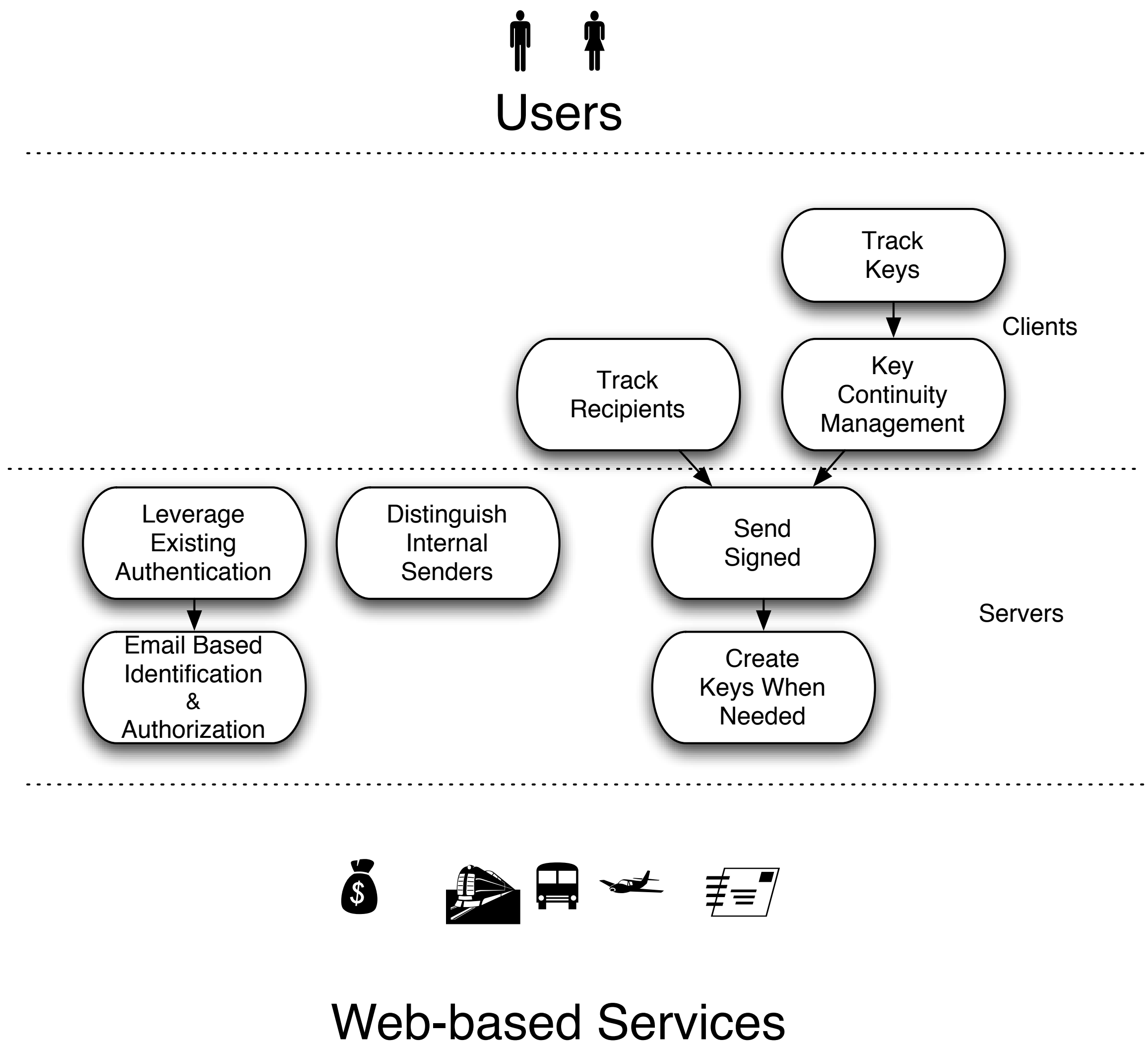
3. Patterns for sanitization. ✔



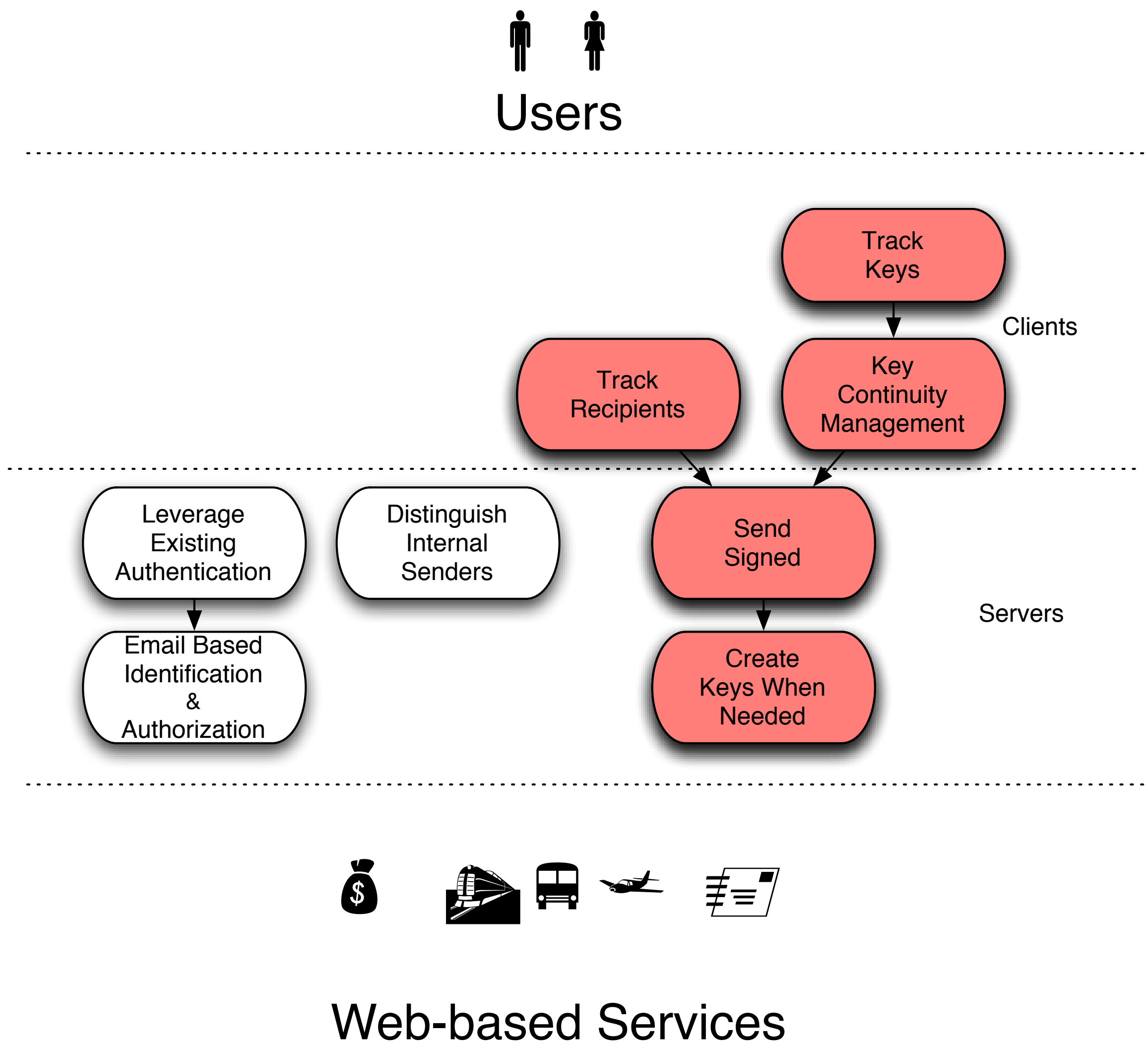
4. Patterns for secure messaging.



My thesis presents eight patterns for enhancing secure messaging.



My thesis presents eight patterns for enhancing secure messaging.



I am going to discuss five of the patterns.

Secure Messaging — email that is *signed* and *sealed* — seems to be the grand challenge of usability and security.

- Public key cryptography was developed for secure messaging.

- This project is nearly thirty years old:
  - → 1976 — Diffie-Hellman
  - → 1977 — RSA
  - → 1987 — RFC 989 (PEM)
  - → 1991 — PGP Released
  - → 1998 — S/MIME

- Today most people who engage in Internet mail have S/MIME-enabled clients, but there's virtually no secure email.

Either it's really hard to get this right, or nobody really cares.

People do care about email security. (Garfinkel *et al.*, FC05)

In our study of 470 Amazon.com merchants:

- 59% thought that receipts from *online merchants* should be digitally signed
- 47% thought receipts should be sealed

And they have the tools — sort of.

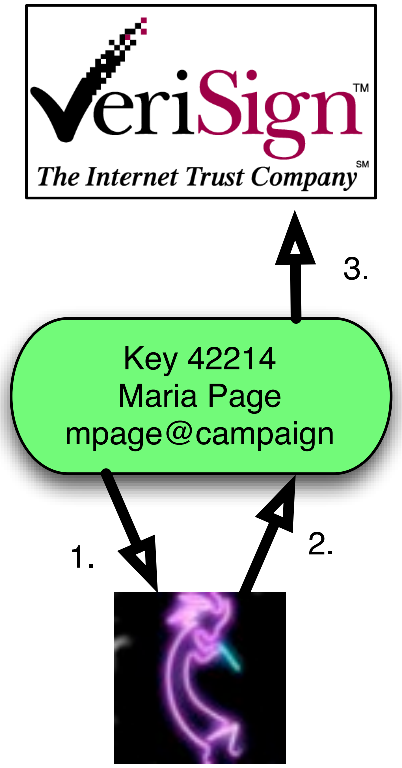
- 54% could handle S/MIME-signed messages.
- 60% didn't know if they could or not!
- 45% would upgrade their email client for more security.

Software for three public-key based communication security systems have been widely deployed.

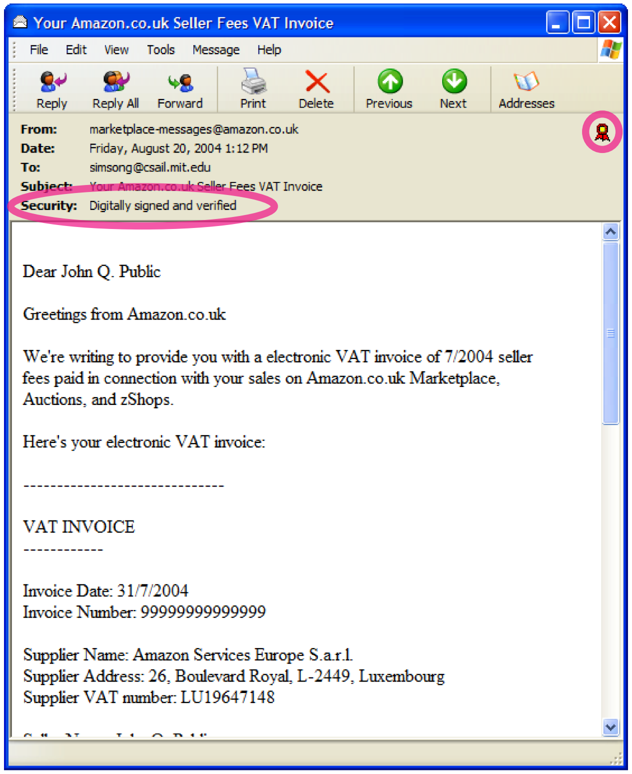
	SSH	SSL	S/MIME
Secures	remote login	web pages	email
Protects Against	eavesdropping spoof servers	eavesdropping spoof servers	eavesdropping spoof senders
3rd Party Certificates Needed	none	servers	sender & recipients
Protection Mechanism	Warns when key changes	CA trustworthiness	CA trustworthiness
Success	High	Somewhat	None

Success of these systems was inversely correlated with the need for third-party interactions.

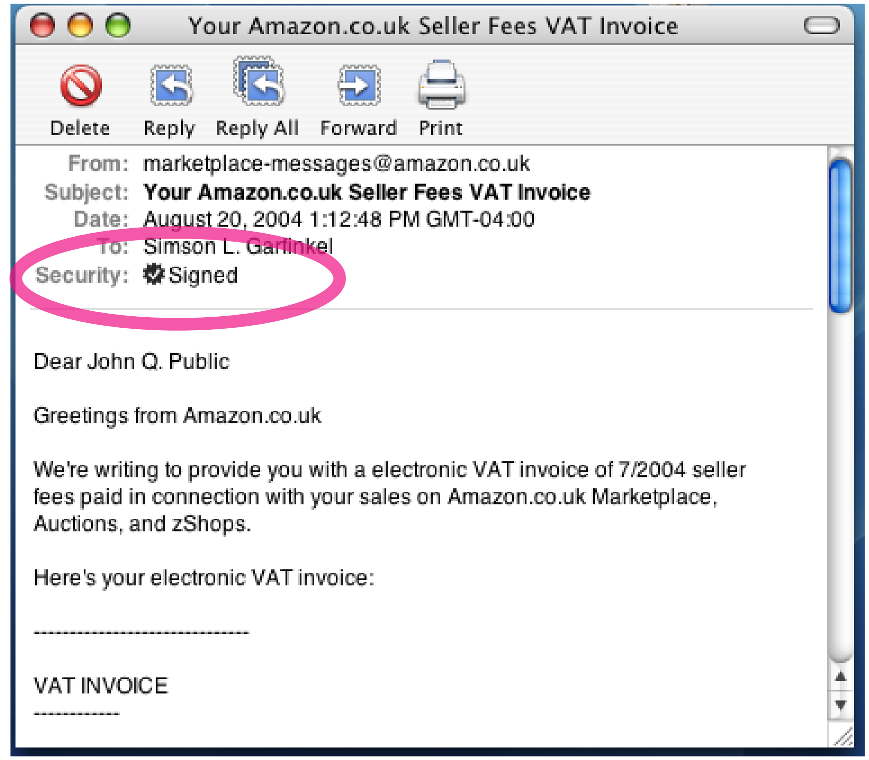
Today’s S/MIME systems use third-party certificates to assert identity.



Signature-only S/MIME mail is *automatically* verified by most email clients.



Outlook Express



Apple Mail

Amazon.com is sending signed VAT invoices to its European merchants. No usability problems reported.

Signature-only S/MIME eliminates the burden on the recipient, but loses protection against eavesdropping.

	full S/MIME	**signature-only S/MIME**
Protects Against	eavesdropping spoof servers	**spoof senders**
3rd Party Certificates Needed	senders recipients	**senders only**
Protection Mechanism	CA trustworthiness	**CA trustworthiness**
Success	None	**Good, when used**

Signature-only S/MIME eliminates the burden on the recipient, but loses protection against eavesdropping.

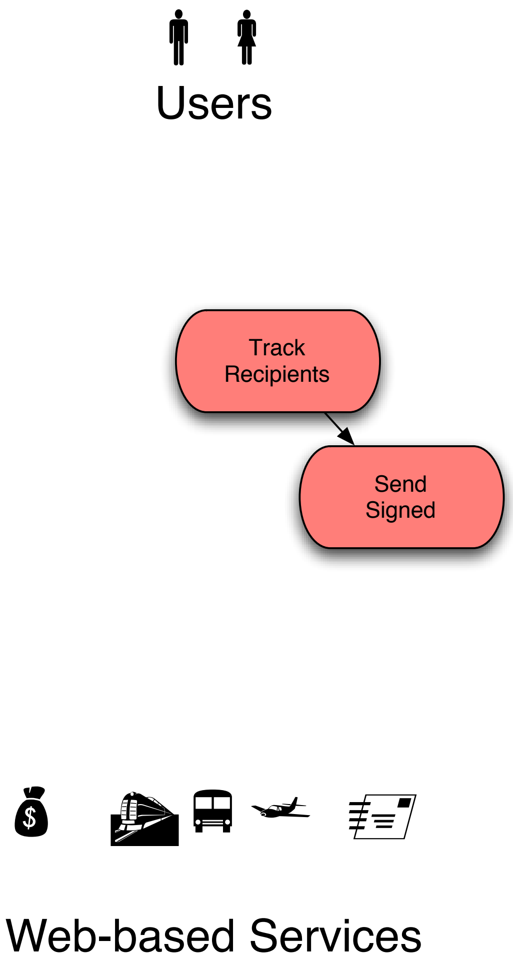
Attacks that rely on spoofed senders:

- Worms that forge "From:" address
- Some kinds of spam
- Many "phishing" attacks

	full S/MIME	**signature-only S/MIME**
Protects Against	eavesdropping spoof servers	**spoof senders**
3rd Party Certificates Needed	senders recipients	**senders only**
Protection Mechanism	CA trustworthiness	**CA trustworthiness**
Success	None	**Good, when used**

Signature-only S/MIME protects against the security problems facing E-mail today.

This is the motivation behind the *Send Signed* and *Track Recipients* patterns.



Typical candidates for *Send Signed* are high-volume “do not reply” senders:

- EBay and PayPal notifications.
- Domain expiration notices.
- Advertisements.

Removing AOL and Webmail users, between 80% and 90% of Internet email users in our sample could decode S/MIME-signed messages.

[Garfinkel *et al.* 2005]

The technology for *Send Signed* is already deployed. Articulating this pattern will create the reality.

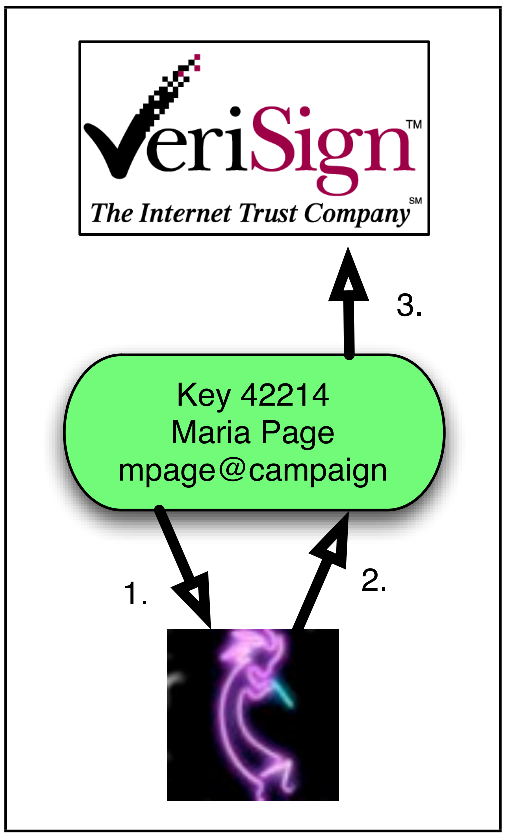
We can do even better by directly applying the SSH trust model to email:

	SSH	signature-only S/MIME	**KCM S/MIME**
Secures	remote login	email	**email**
Protects Against	eavesdropping spoof servers	spoof senders	**eavesdropping** **spoof senders**
3rd Party Certificates Needed	none	servers	**none**
Protection Mechanism	Warns when key changes	CA trustworthiness	**Warns when key changes**
Success	High	Somewhat	**High in lab**

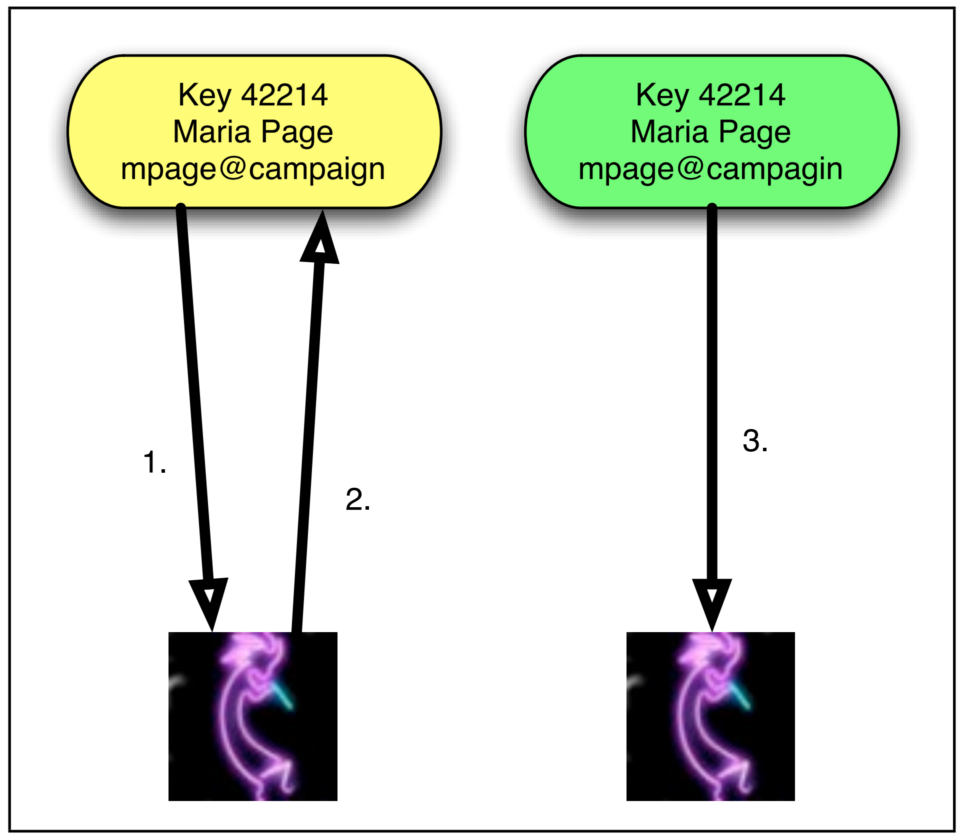
Key Continuity Management applies the SSH trust model to email. Unfortunately, KCM requires software changes.

Key Continuity Management is a strategy for managing untrusted certificates.

Traditional:



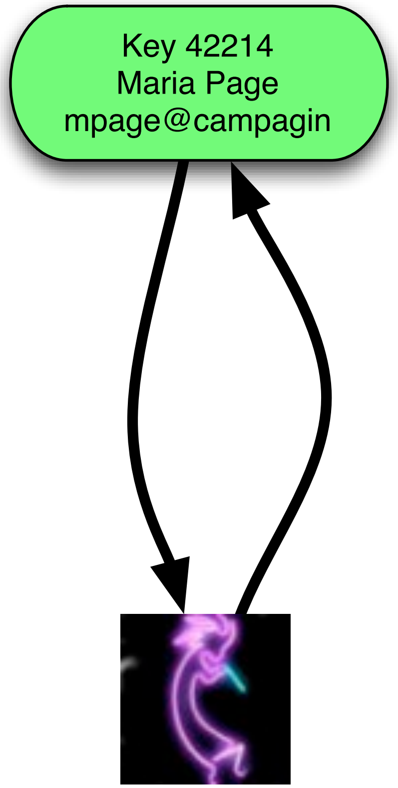
KCM:



KCM makes it possible to easily use S/MIME with self-signed certificates. (*Create Keys When Needed* pattern.)

Unfortunately, KCM creates a number of possible attacks:

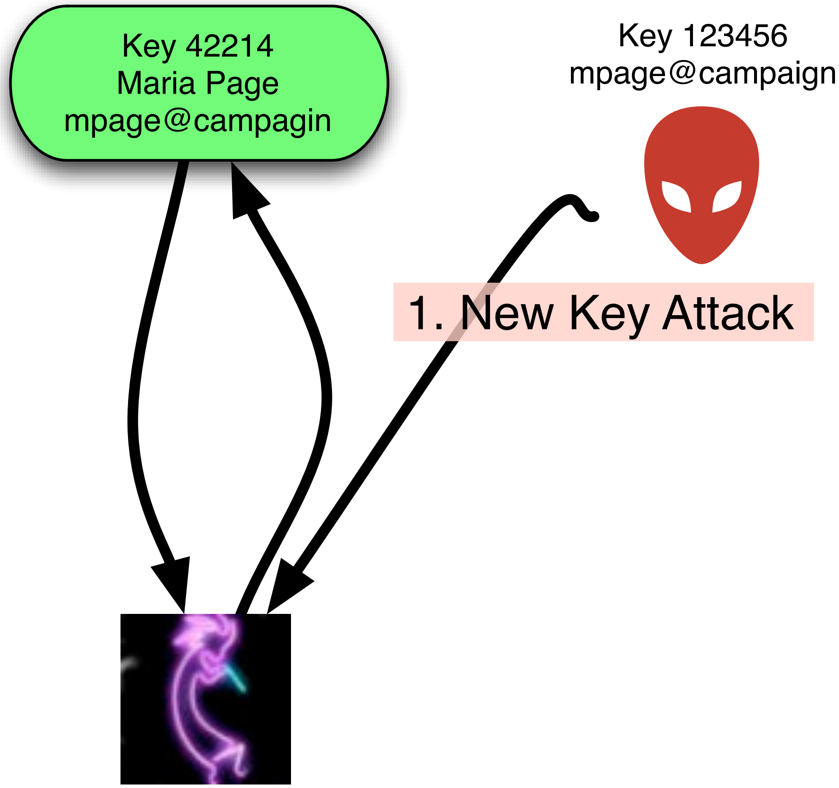
.



.

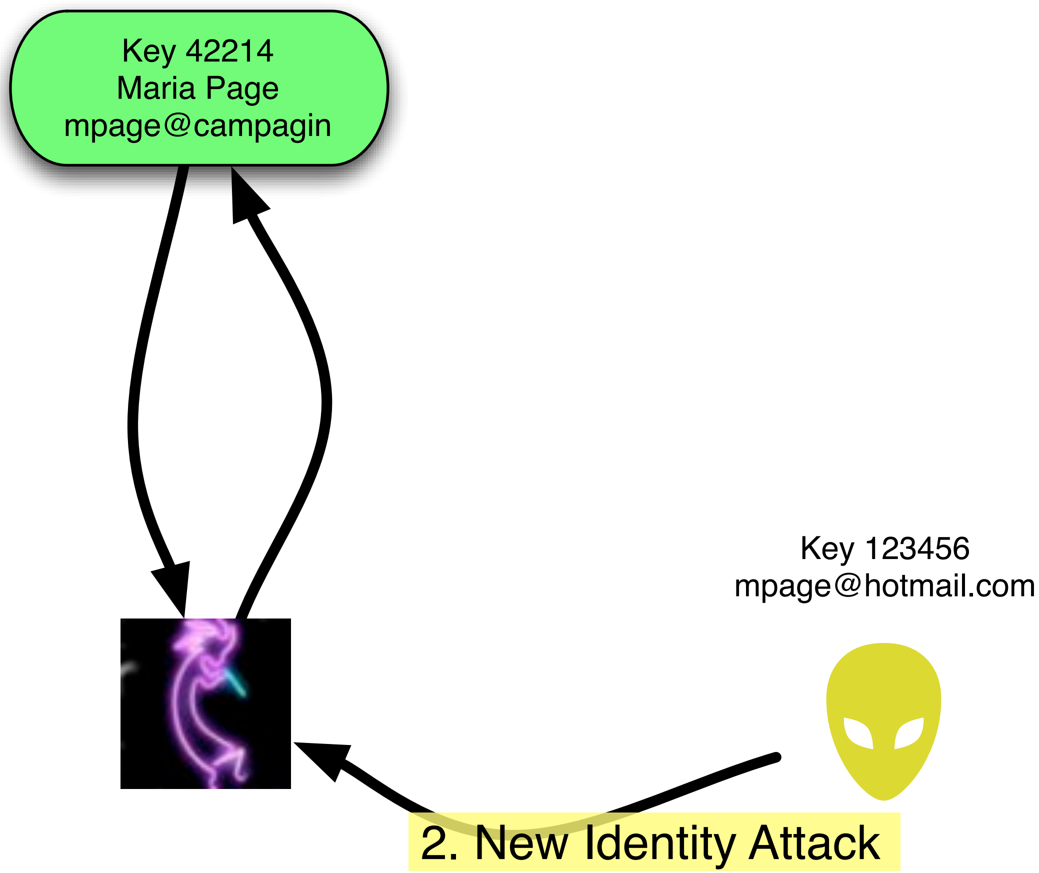
Normal Communications

Unfortunately, KCM creates a number of possible attacks:



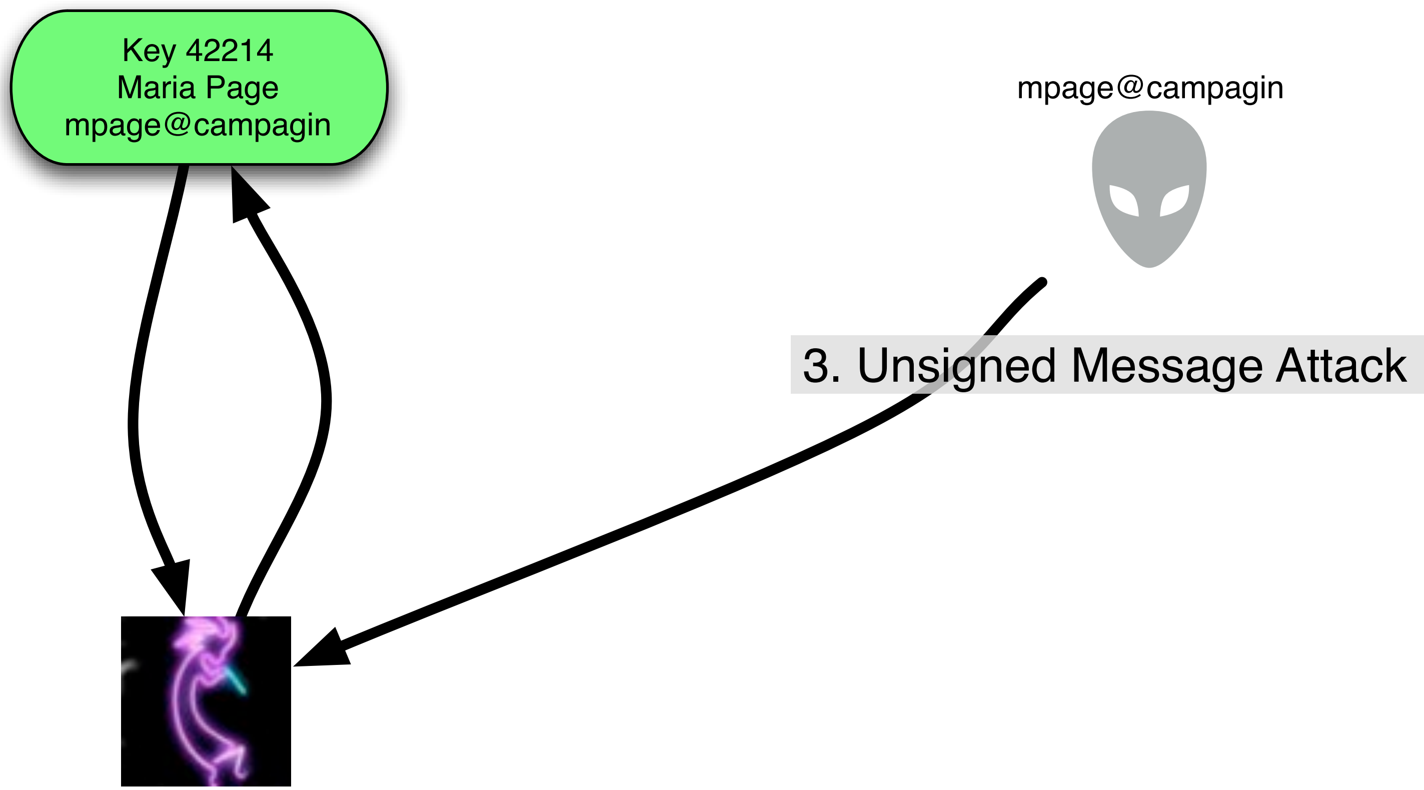
New Key Attack: (Forged From:, New Cert)

Unfortunately, KCM creates a number of possible attacks:



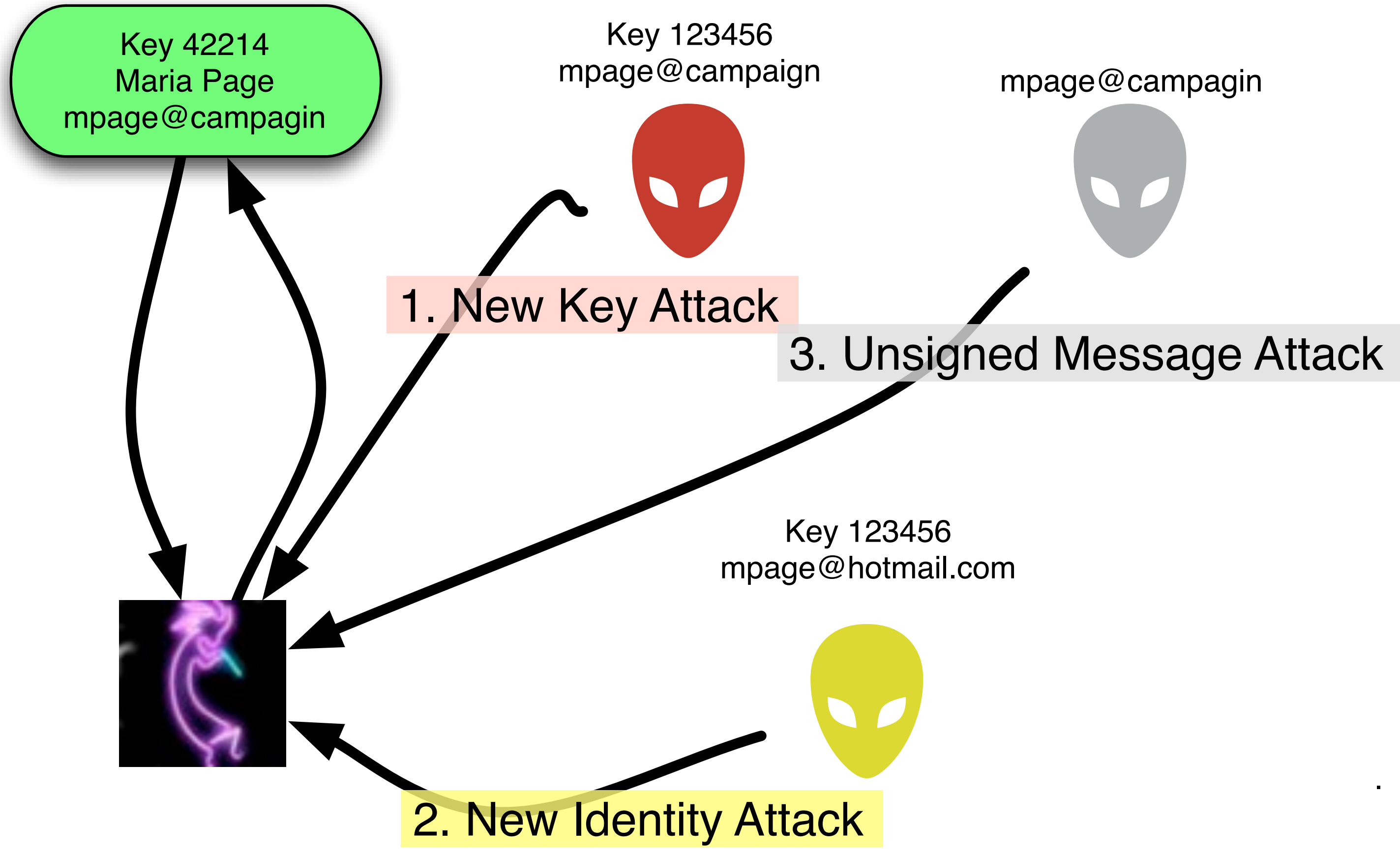
New Identity Attack (From Hotmail, New Cert)

Unfortunately, KCM creates a number of possible attacks:



Unsigned Message Attack (Forged From:, No Cert)

Unfortunately, KCM creates a number of possible attacks:



Can untrained end-users resist these attacks?

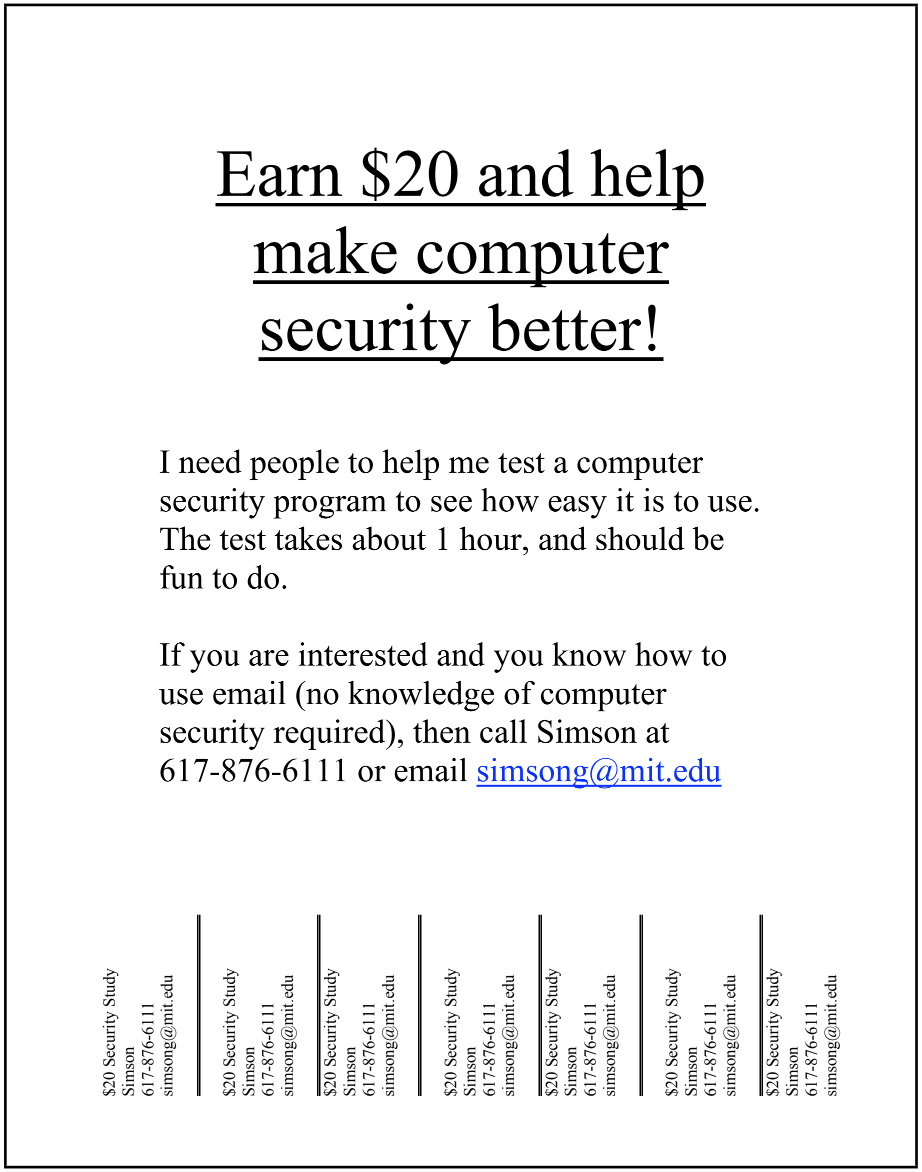
The Johnny 2 Experiment:

Designed to test KCM model:

- Subject plays the role of a political campaign worker.
- Enemy campaign tries to steal documents through a spoofing attack.
- Three attack messages.

Experimental Details:

- 43 subjects aged 18–63 ($\overline{x} = 33, \sigma = 14.2$)
- 19 Men, 24 Women
- 17 to 57 minutes ($\overline{t} = 41, \sigma = 10.32$)



Earn $20 and help make computer security better!

I need people to help me test a computer security program to see how easy it is to use. The test takes about 1 hour, and should be fun to do.

If you are interested and you know how to use email (no knowledge of computer security required), then call Simson at 617-876-6111 or email simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

$20 Security Study Simson 617-876-6111 simsong@mit.edu

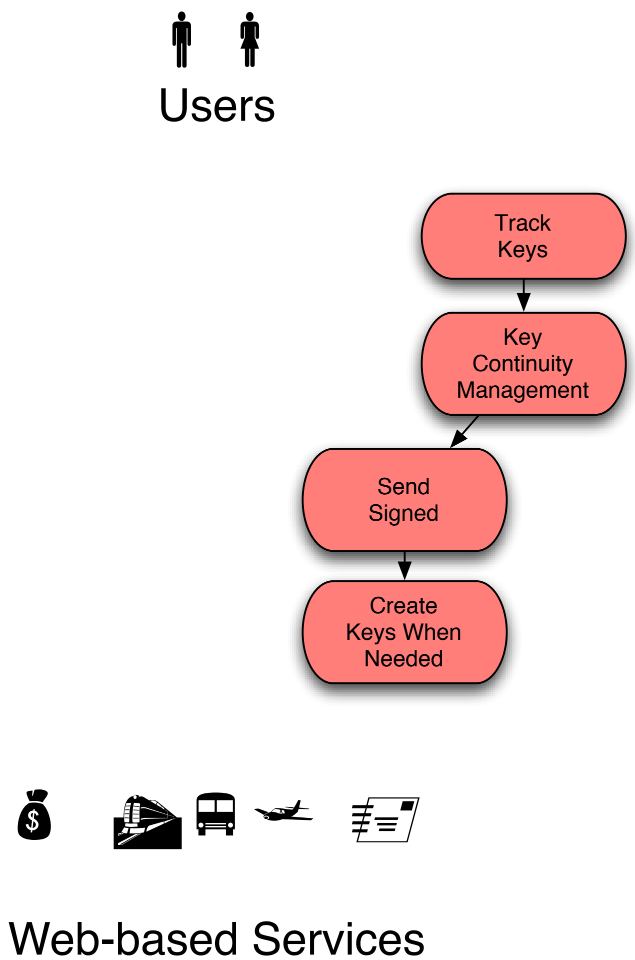
The Johnny 2 Results:

We compared KCM with no KCM and found:

attack	attack rate change
New Key Attack	81% drop***
New Identity Attack	43% drop**
Unsigned Message Attack	24% drop

$^{***}p < .001; {}^{**}p < .05$

The KCM patterns can increase mail security by promoting the use signing and sealing.



KCM clients must:

- Create keys when needed.
- Track capabilities of correspondents.
- Maintain database of correspondents and certificates.

This talk has presented a few of my original contributions. Here is the complete list:

On Sanitization:

- Novel hypothesis for the HCI-SEC conflict
- Comprehensive literature review and critique
- Analysis of 236 hard drives
- Traceback study of 20 organizations
- Cross-drive forensics
- Study of operating systems sanitization issues
- Study of web browser sanitization issues
- Study of Word and Acrobat sanitization issues

On PKI and secure messaging:

- Survey of 470 Amazon.com merchants
- Technique for embedding invisible digital signatures in MIME messages
- Application of Key Continuity Management model to email
- User study of KCM with Outlook Express
- A meta-analysis of the E-Soft SecuritySpace study.

On Regulatory techniques:

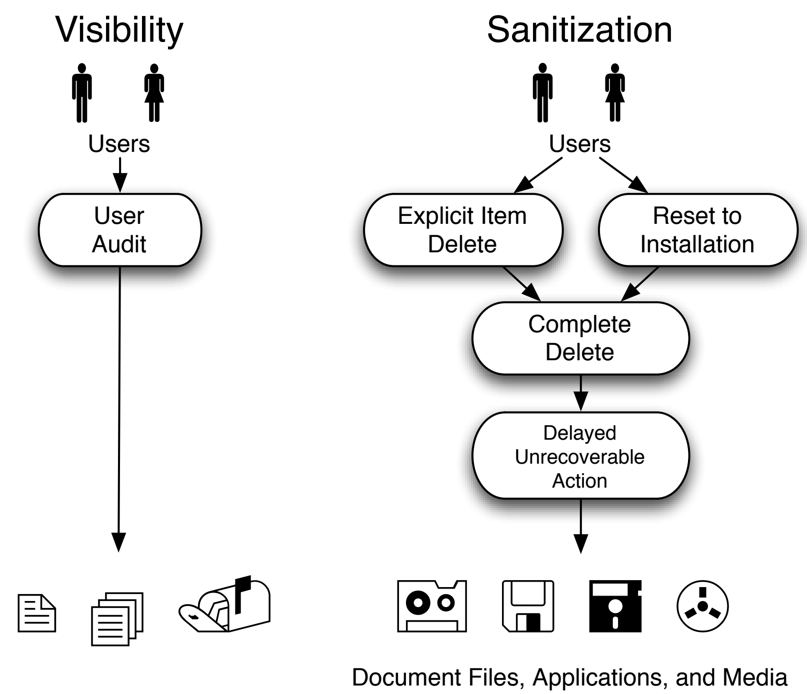
- A “Bill of Rights” for RFID labeling.
- A proposal for software labeling.
- A novel analysis of how ANSI Z535.4-2002 could be applied to software.

On HCI-SEC Patterns:

- Four original principles and more than 20 original patterns for aligning security and usability.
- An analysis showing why inconsistent vocabulary in the field of security damages usability.

In Summary

- ✔ Patterns are a promising technique for aligning security and usability.
- ✔ Sanitization can be made automatic and natural in many cases.
- ✔ Significant progress can be made on mail security with technology that is already deployed.



Acknowledgments

Thesis supervisors:

Robert Miller and David Clark

Thesis readers:

Ronald Rivest and Daniel Weitzner

Collaborators:

Abhi Shelat, Ben Gelb, Erik Nordlander

Presentation Critics:

Karen Sollins, Sian Gramates

Slide format:

Michael Alley, Virginia Tech

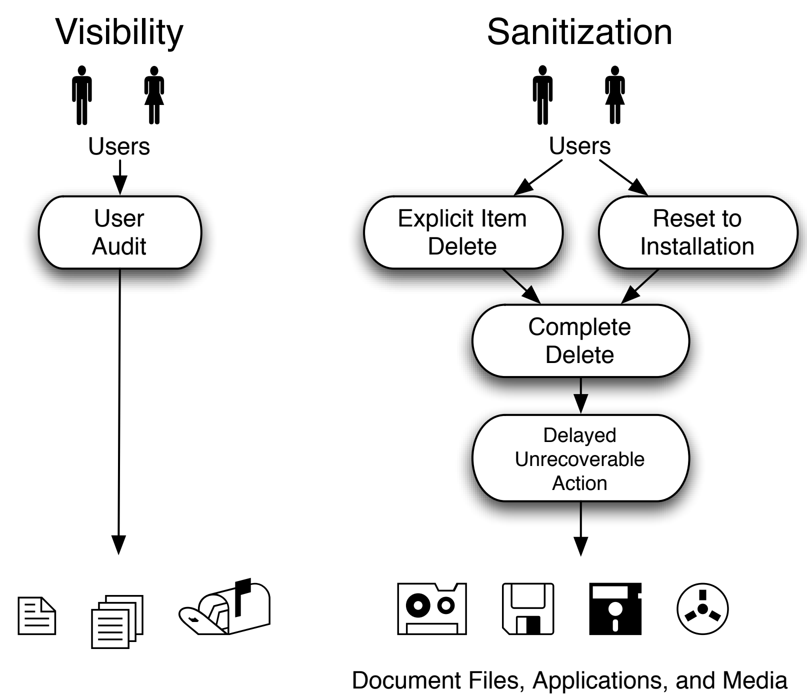
And special thanks to Beth Rosenberg, Sonia, Jared and Draken...


Sun
Free


DREYFOOS

In Summary

- ✔ Patterns are a promising technique for aligning security and usability.
- ✔ Sanitization can be made automatic and natural in many cases.
- ✔ Significant progress can be made on mail security with technology that is already deployed.



Questions?