CSCI E-170

Sept. 28, 2004

Lecture Plan

Odds & Ends from Lecture #1

Homework

LiveJournal - Discussion

Homework

- Assignment #1 - Security - Discussion
- Assignment #2 - Policies - Assigned

GUI Usability:

- Design Process, Principles & Bloopers

Sarbanes-Oxley

"Public Company Accounting Reform and Investor Protection Act" of 2002

Section 101: Established Public Company Accounting Oversight Board

Section 201: Prohibits Auditors from providing non-audit services "contemporaneously with the audit"

Section 203: Lead auditor must rotate every 5 years

Sarbanes-Oxley Cont.

Clarified and strengthened rules on:

- Insider Trading
- Conflict of Interest
- Public disclosures
- Assessment of internal controls
- Mandatory disclosures

Not really a privacy or security law, but improvement on internal controls can only help protection of personal information.

Saltzer & Schroeder points of confusion

Complete mediation — every access to every object must be checked for authority.

Separation of privilege — "Where feasible, a protection mechanism that requires two keys to unlock [is better] than one that allows access [with] a single key." (root is bad.)

Least privilege — Every program and user operates with the "lest set of privileges necessary.

Saltzer & Schroeder 2

Economy of mechanism — "Keep the [overall] design as simple and small as possible."

Least common mechanism — Do as little in the kernel as possible ("mechanism common to more than one user")

Saltzer & Schroder

What are the two missing principles?

- **Fail-safe defaults** — "Base access decisions on permission rather than exclusion." Make the system secure by default.
- **Psychological acceptability** — "It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly."

Quick Comments on Homework #1

Treat every assignment as if it is a finished work product.

- HTML: Make sure it is readable (break between paragraphs!)
- Paper/PDF: Name on every page; page numbers, etc.

Late Policy: Late Homework is not accepted

Confidentiality

Some students printed the name of their employer or clients, others didn't.

Q: When is there an obligation of confidentiality?

A: When you have exposure to *privileged* information

Some employers believe that *anything* involving the company needs to be approved prior to disclosure.

Remember, even "private" Internet groups *aren't*.

Why aren't private groups really private?

How can you subvert a private system?

- Copy & Paste (sometimes)
- Print
- Digital cameras
- Memorization & Repetition
- Rumor

Tips on Writing

Don’t raise questions that you don’t answer.

Explain the setting: kind of organization, operating systems, etc.

Don’t excessively quote

Don’t spend too much time on the “lessons learned” — the lessons should be obvious from the context!

Assignment #2

You will be asked to compare the privacy policies of 4 organizations and compare them:

- Amazon.com
- A federal agency
- A website belonging to a university
- One other organization (can be yours!)

Write an unbiased 3-page memo comparing them.

A chart is helpful, but not necessary.

Writing Tips

Avoid slang

It's safer to be formal than to be lax

Don't use acronyms without defining them.

Live Journal

By now, you should all have a Live Journal account

- Online participation is *mandatory*

Please put contributions in the <lj user='csci_e_170'> section, not on your home page.

"Friends"

- csci_e_170 - this class
- ms_secbulletin - MSFT security bulletins
- msft_brianj - MSFT commentator on security

Comments and other thoughts?

Reading

In general, you will get more out of class if you do the reading *before class*, rather than after it.

Starting next week, we will spend a portion of each class discussing the reading.

- Reading for today:
  - *Apple Human Interface Guidelines*
- Reading for next week: *5 papers* on information leakage (est. 3 hours)

Designing Usable Interfaces

What is the computer interface?

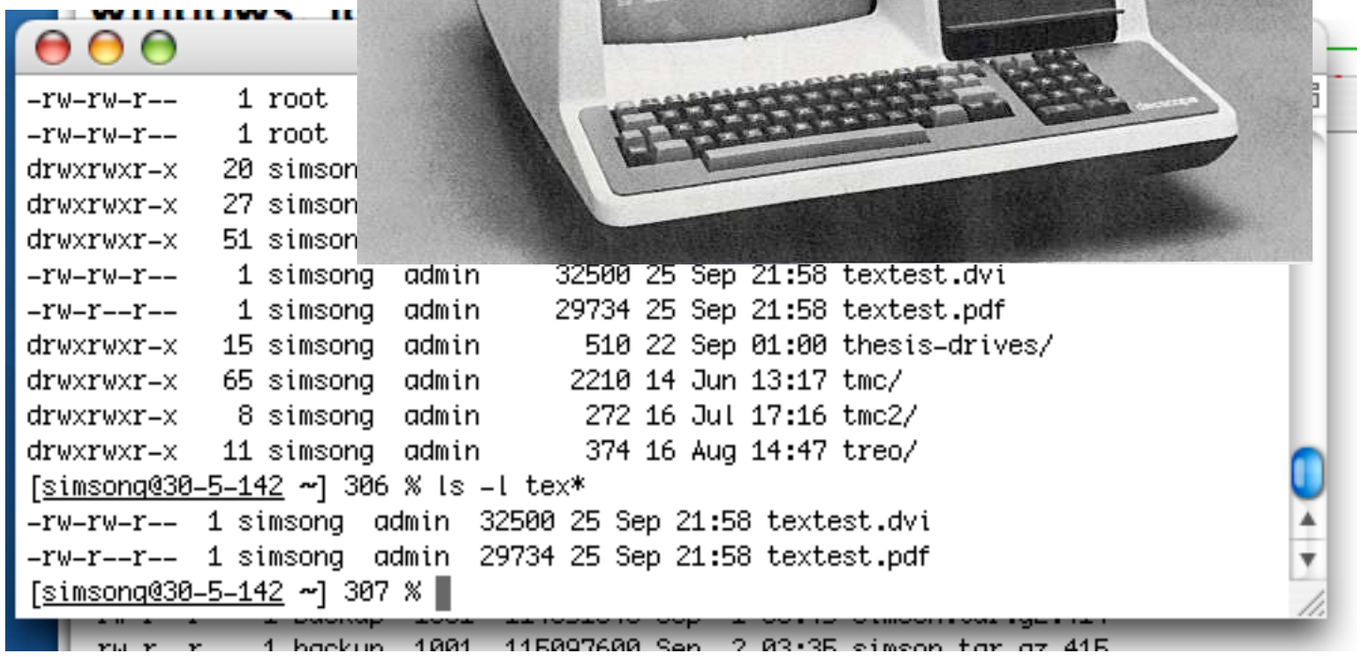
- (collect on board)

Command Line

- Originally developed with teletypes & printing terminals

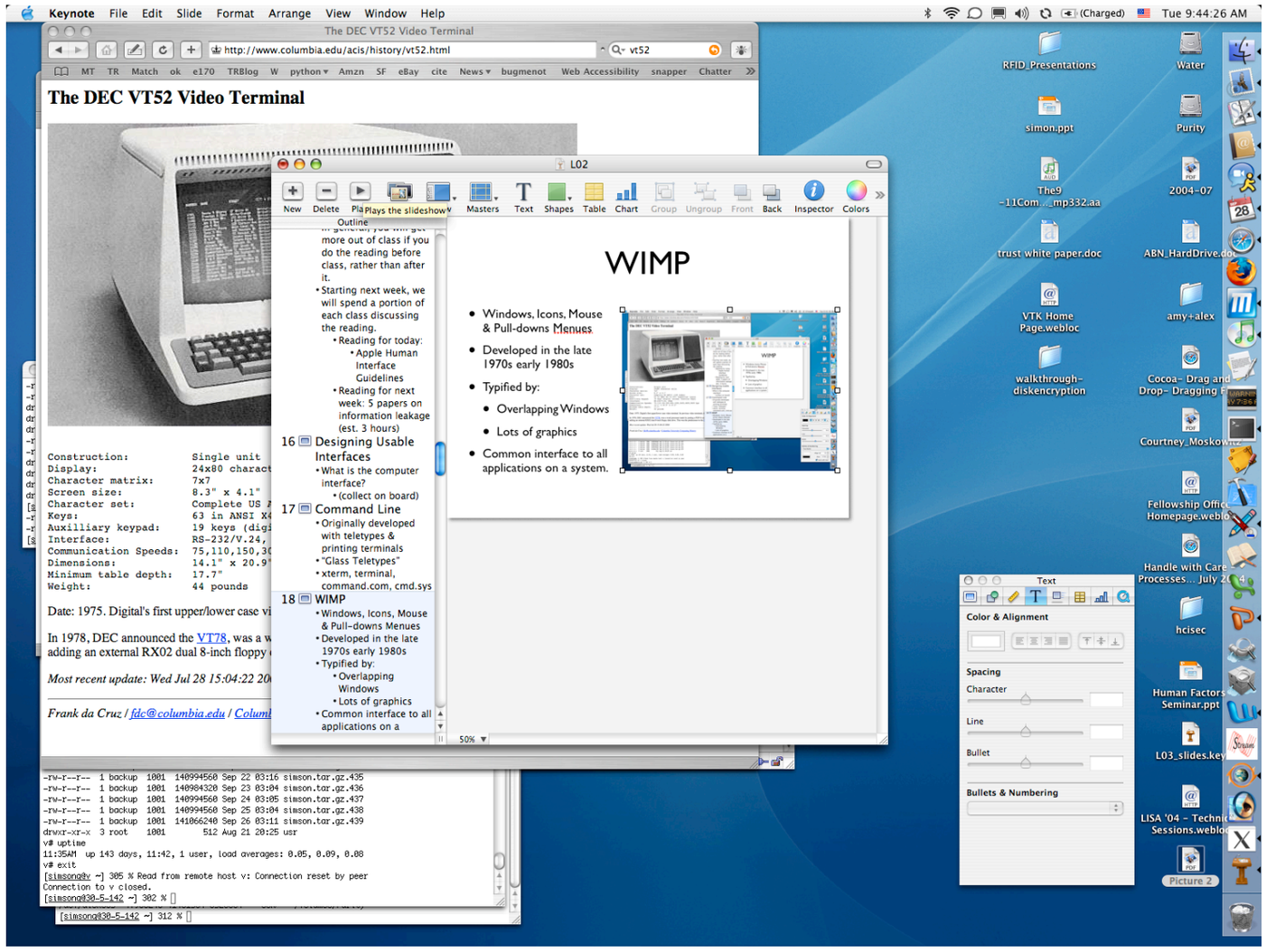
- “Glass Teletypes”

- xterm, terminal, command.com, cmd.sys



WIMP

- Windows, Icons, Mouse & Pull-downs Menues
- Developed in the late 1970s early 1980s
- Typified by:
  - Overlapping Windows
  - Lots of graphics
- Common interface to all applications on a system.



Alternative Interfaces

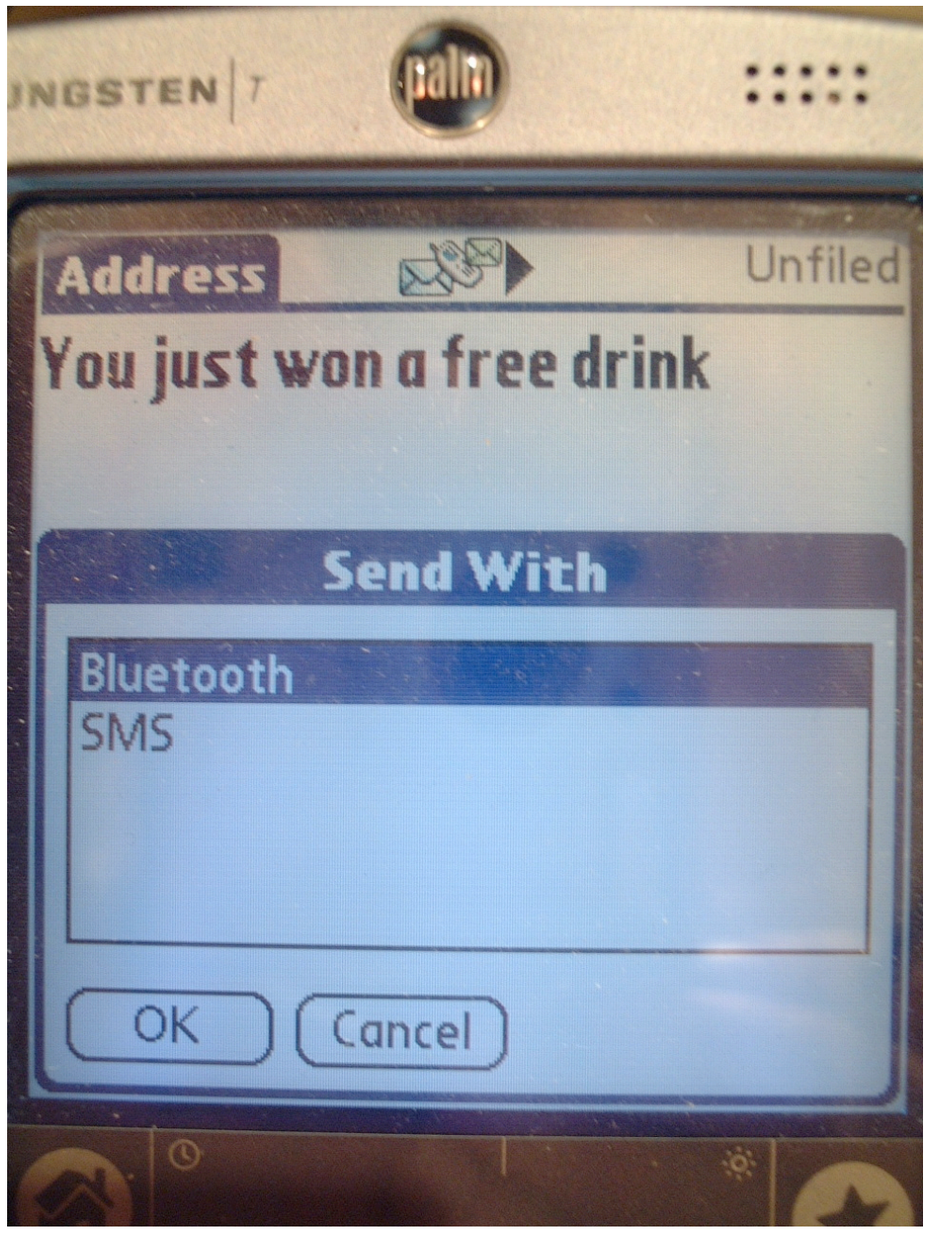
PalmOS

Pocket PC

Symbian

Speech

Dance & Gesture



Usability: What is it?

"I know it when I see it."

satisfaction: Interfaces we *enjoy* using ()

efficiency: Interfaces we are *fast* at using ()

learnability: Interfaces that we can *use without asking for help*

errors: Interfaces that we can use *accurately*

memorability: Interfaces we can use after time

The Design Cycle

Task Analysis — What problem is the user *really* trying to solve?

Iterative Design:

1. Design
2. Prototype
3. Evaluate
4. Repeat

Keep the customer in the picture!

Task Analysis

Observe existing work practices

Create scenarios

Create "customers"

- Sally in accounting
- Bob the new user

Discuss ideas with end-users

Show prototypes; try out ideas before committing to software

Does Task Analysis Always Make sense?

Q:
us
so

Rapid Prototyping

Build a mock-up

Low-cost techniques:

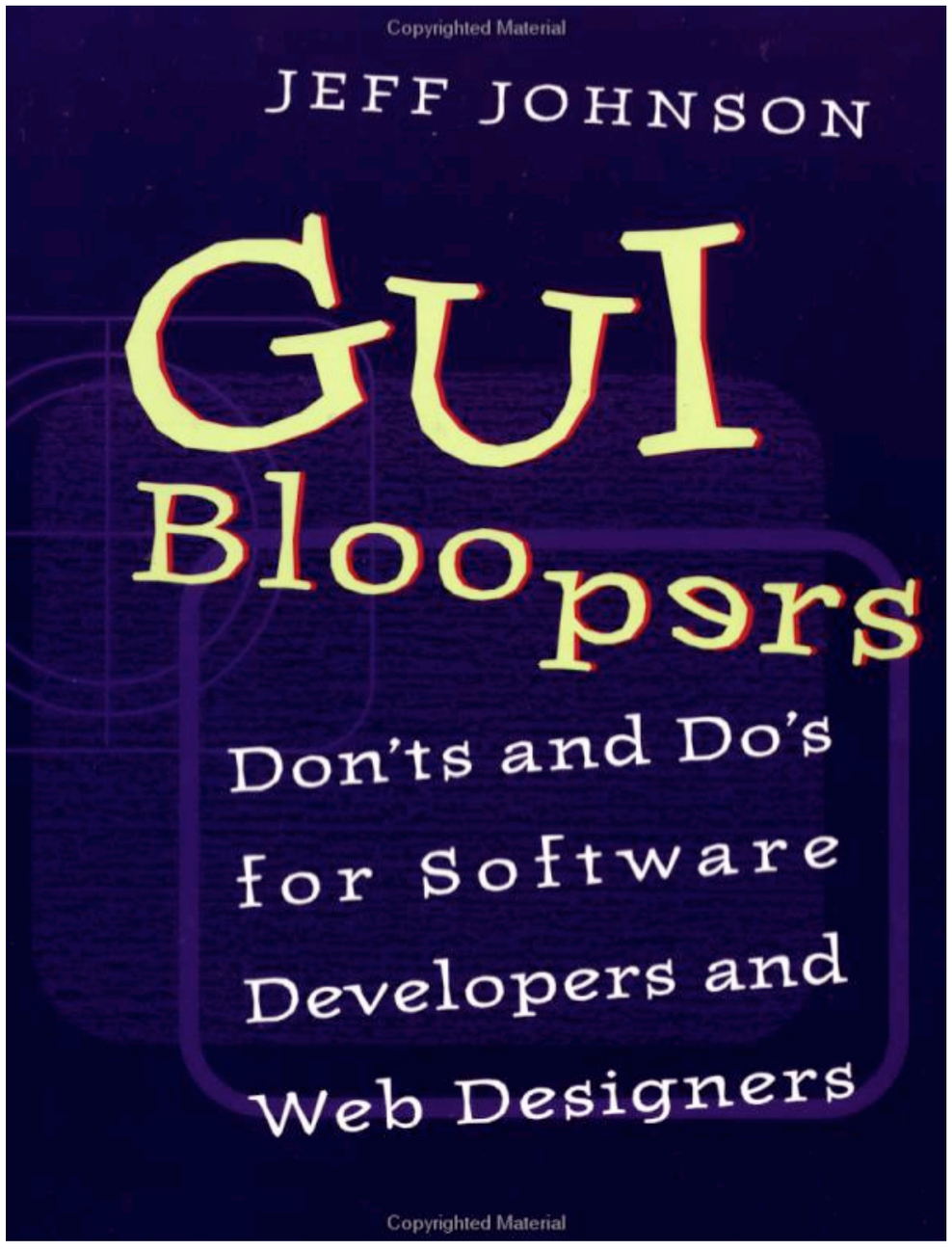
- paper!
- Adobe Illustrator / Photoshop

Cheap interfaces:

- GUI builder
- Flash

Designing usable interfaces

Jeff Johnson, *GUI Bloopers: Don't and Do's for Software Developers and Web Designers*, Morgan Kaufmann, 2000



Principle #1

Focus on the users and their tasks, not the technology

- For whom is this product being designed?
- What is the product for?
- What problems do the users have now?
- What are the skills and knowledge of the users?
- How do users conceptualize and work with their data?

Principle #2:

Consider function first, presentation later

- Does not mean "worry about the user interface later!"
- Develop a conceptual model
- Keep it as simple as possible, but no simpler
- Develop a lexicon (***)

Principle #3:

Conform to the users' view of the task

- Strive for naturalness
- Use the user's vocabulary, not your own
- Keep program internals inside the program (remember, the implementation can change!)

Principle #4

Don’t complicate the user’s task

- Common tasks should be easy
- Don’t give users extra problems to solve
  - Converting a file format from TIFF to JPG for web publishing
  - Installing program “A” in order to install program “B”
  - Looking up information one screen to type it on another

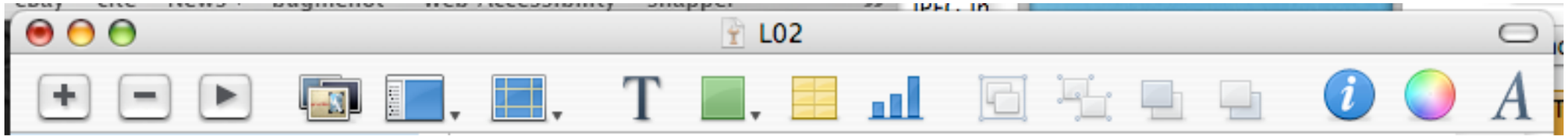
Principle #5

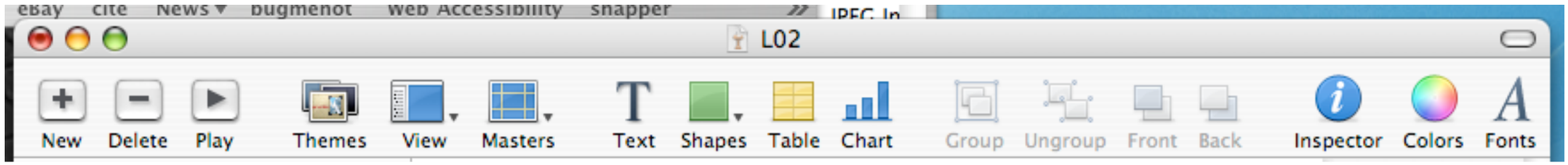
Promote Learning Inside the Interface

- Think "outside-in," not "inside-out" — The user wants to solve a problem, not learn how to use your program!
- Be careful of ambiguity
  - "He saw the woman with the telescope"
  - Icons that don't make sense
- Be consistent so there is something to learn!

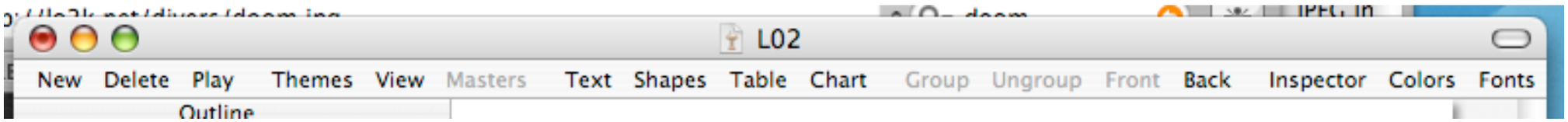
Icon Bars (Principle #5)

What do these icons mean?





How about if we just used text?



Principle #6

Deliver information, not just data

- Design displays carefully
- The screen belongs to the user
- Preserve display inertia

The Two Most Important Principles!

Principle 7: Design for responsiveness

- Many users will forgive a bad interface, as long as it is fast.

Principle 8: Try it out on users, then fix it!

- Testing and iteration are the keys to good interface design.
- In most cases, programmers design for themselves... Is that a good thing?

Rob Miller on UIs

User interface strongly affects perception of software

- Usable software sells better
- Unusable web sites are abandoned

Perception is sometimes superficial

- Users blame themselves for UI failings
- People who make buying decisions are not always end-users

User Interfaces are Hard to Design

You are not the user

- Most software engineering is about communicating with other programmers
- UI is about communicating with users

The user is always right

- Consistent problems are the system's fault

... but the user is not always right

- user's aren't designers

UI's are half the game:

Myers & Rosson, "Survey on user interface programming", CHI '92

User Interfaces account for 50% of:

- Design time
- Implementation time
- Maintenance time
- Code Size

(probably more now!)

UI Hall Of Shames

http://www.rha.com/ui_hall_of_shame.htm

http://pixelcentric.net/x-shame/

HCI-SEC: Usability & Security

Discussed by Saltzer & Schroeder, then largely ignored.

Recent Interest:

- Adams & Sasse, "Users Are Not the Enemy," ACM Communications Dec. 1999
- Whitten, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" (Usenix Security, 1999)
- http://groups.yahoo.com/group/hcisec/

Why is CHI-SEC Hard?

Whitten & Tygar suggest that it is *inherently difficult* to create interfaces for computer security applications.

Why would this be true?

The Secondary Goal Property*

"People do not generally sit down at their computers wanting to manage their security; rather, they want to send mail, browse web pages, or download software."

---

* previously called "the unmotivated user property"

The hidden failure property*

It is difficult to provide good feedback for security management and configuration because configurations are complex and not easy to summarize

---

* previously called “the lack of feedback property”

The abstraction property

Security policies are usually phrased as abstract rules that are easily understood by programmers but "alien and unintuitive to many members of the wider user population."

The barn door property

Once a secret gets out, it's out.

Information disclosure cannot be reversed.

Even worse, there is no way to know if an unprotected secret has been compromised is being privately circulated by others.

"Because of this, user interface design for security needs to place a very high priority on making sure users understand their security well enough to keep from making potentially high-cost mistakes."

The weakest link property

The security of a system is like a chain: it is only as strong as the weakest link.

“If a cracker can exploit a single error, the game is up.”

HCI-SEC and the WWW

Why is the web an HCI-SEC nightmare and what can we do about it?

(answers from class?)

WWW and HCI-SEC

Hidden Information at the Server:

- Log files
- Third-party Image Servers
- Web Bugs

Hidden Information at the Client:

- Cookies
- Browser History
- Browser Cache

Internet and HCI-SEC

DNS is opaque to most users:

- Many DNS names can map to one IP address
- Many IP addresses can map to one DNS name
- No relationship between a DNS name and a company

WWW Logfiles

sgpwebproxy2.net.asiapac.agilent.com - - [01/May/2003:21:52:58 -0400] "GET /ref/ugh.pdf HTTP/1.0" 302 286 "http://research.microsoft.com/~daniel/uhh-download.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; SIK1.02)"

67.knoxville-03rh15rt-ca.dial-access.att.net - - [01/May/2003:21:53:00 -0400] "GET /ref/ugh.pdf HTTP/1.1" 302 298 "http://forums.rpghost.com/showthread.php?s=&threadid=4286" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; AT&T WNS5.0)"

h00d0b761273d.ne.client2.attbi.com - - [01/May/2003:21:53:03 -0400] "GET /ref/ugh.pdf HTTP/1.1" 302 298 "http://research.microsoft.com/~daniel/uhh-download.html" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.2.1) Gecko/20030225"

12-232-136-167.client.attbi.com - - [01/May/2003:21:53:11 -0400] "GET /ref/ugh.pdf HTTP/1.1" 302 298 "http://research.microsoft.com/~daniel/uhh-download.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.2.11.0; .NET CLR 1.0.3705)"

Combined Log Format

67.knoxville-03rh15rt-ca.dial-access.att.net - - [01/May/2003:21:53:00 -0400] "GET /ref/ugh.pdf HTTP/1.1" 302 298 "http://forums.rpghost.com/showthread.php?s=&threadid=4286" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; AT&T WNS5.0)"

What is this information?

- host
- username
- date & time
- URL
- transfer speed
- previous link (”refer”)
- browser (and operating system)

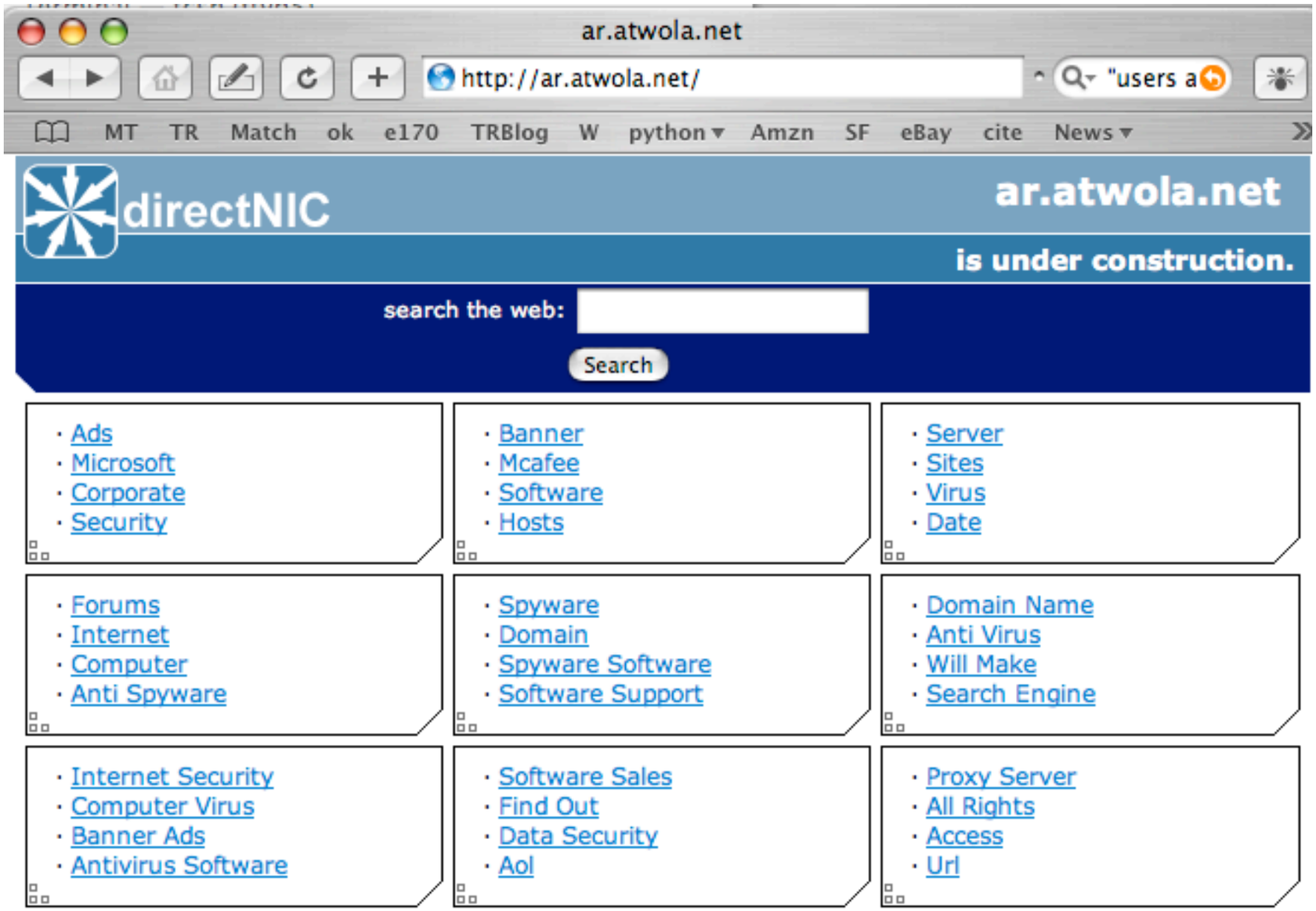
Third Party Image Servers

i.a.cnn.net

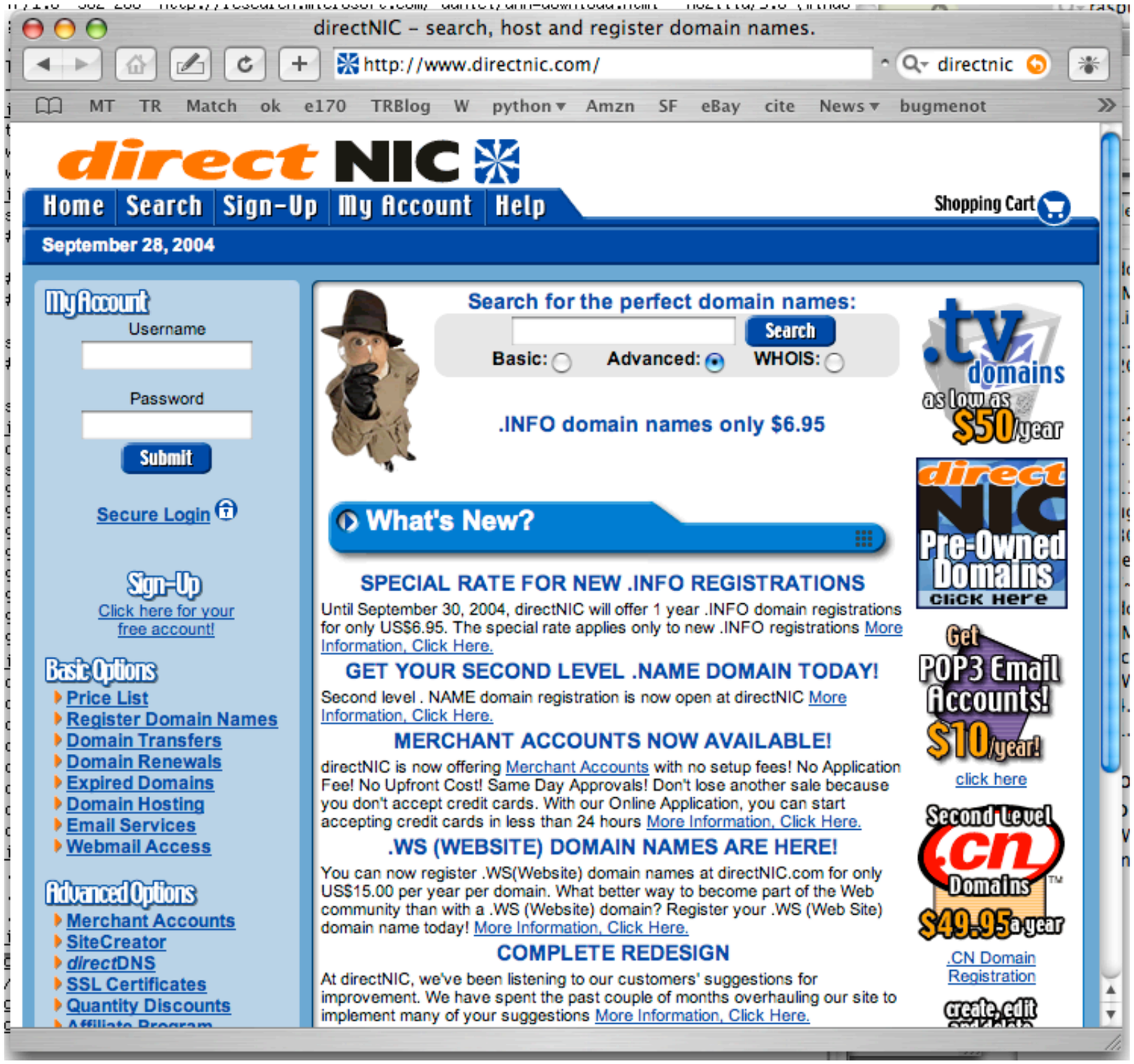
ar.atwola.net

i.cnn.net
width="1"
height="1"

ar.atwola.net



directNIC


directNIC – search, host and register domain names.
http://www.directnic.com/
directnic
MT TR Match ok e170 TRBlog W python Amzn SF eBay cite News bugmenot
direct NIC
Home Search Sign-Up My Account Help
Shopping Cart
September 28, 2004
My Account
Username
Password
Submit
Secure Login
Sign-Up
Click here for your free account!
Basic Options
Price List
Register Domain Names
Domain Transfers
Domain Renewals
Expired Domains
Domain Hosting
Email Services
Webmail Access
Advanced Options
Merchant Accounts
SiteCreator
directDNS
SSL Certificates
Quantity Discounts
Search for the perfect domain names:
Search
Basic: Advanced: WHOIS:
.INFO domain names only $6.95
.tv domains as low as $50/year
direct NIC Pre-Owned Domains click here
Get POP3 Email Accounts! $10/year!
click here
Second Level .cn Domains™ $49.95 a year
.CN Domain Registration
What's New?
SPECIAL RATE FOR NEW .INFO REGISTRATIONS
Until September 30, 2004, directNIC will offer 1 year .INFO domain registrations for only US$6.95. The special rate applies only to new .INFO registrations More Information, Click Here.
GET YOUR SECOND LEVEL .NAME DOMAIN TODAY!
Second level . NAME domain registration is now open at directNIC More Information, Click Here.
MERCHANT ACCOUNTS NOW AVAILABLE!
directNIC is now offering Merchant Accounts with no setup fees! No Application Fee! No Upfront Cost! Same Day Approvals! Don't lose another sale because you don't accept credit cards. With our Online Application, you can start accepting credit cards in less than 24 hours More Information, Click Here.
.WS (WEBSITE) DOMAIN NAMES ARE HERE!
You can now register .WS(Website) domain names at directNIC.com for only US$15.00 per year per domain. What better way to become part of the Web community than with a .WS (Website) domain? Register your .WS (Web Site) domain name today! More Information, Click Here.
COMPLETE REDESIGN
At directNIC, we've been listening to our customers' suggestions for improvement. We have spent the past couple of months overhauling our site to implement many of your suggestions More Information, Click Here.

Browser Information

Cookies

History

Cache

DEMO & DISCUSSION