Is it safe?

How usability and social engineering affect security and privacy in software systems

Gregg Vesonder
AT&T
University of Pennsylvania
Stevens Institute of Technology

©2007 Gregg Vesonder

Marathon Man

Christian Szell: Is it safe?
Babe: You're talking to me?
Christian Szell: Is it safe?
Babe: Is what safe?
Christian Szell: Is it safe?
Babe: I don't know what you mean. I can't tell you something's safe or not, unless I know specifically what you're talking about.
Christian Szell: Is it safe?
Babe: Tell me what the "it" refers to.
Christian Szell: Is it safe?
Babe: Yes, it's safe, it's very safe, it's so safe you wouldn't believe it.
Christian Szell: Is it safe?
Babe: No. It's not safe, it's... very dangerous, be careful.
(from http://wikiquote)

Roadmap

- Preliminaries
- Motivation
- Reality
- On Security
- On Privacy
- Usability
- Getting Personal
- And now …

3

Vesonder's Relevant Bio

- Software for 30+ years
- PhD in Cognitive Psychology - Computer modeling of learning and memory
- 7 years at Bell Labs - Whippany
- 15 years in local loop
- [Bell|AT&T] labs for 27+ years
- "VP R&D" for AT&T's A2B music
- Architecture Reviewer and served software engineering corporate stint at Bell Labs
- Current security projects & a computer center
- Adjunct at University of Pennsylvania and Stevens Institute of Technology

4

News Item: Security

- Security flaws found in MDA computers
- Lack of password control, outdated procedures cited
- Tuesday, March 21, 2006 By SHELBY G. SPIRES
- HuntsvilleTimes Aerospace Writer
- A Defense Department review has cited security flaws with the Missile Defense Agency computer communications networks that link interceptor missiles, sensors and ground-based missile defense ground stations. Among the flaws listed are a lack of computer password control and using two-decades-old security procedures. Huntsville-based contractors, managers and engineers manage, design, test and engineer computer networks within the ground-based missile defense program, which is designed to shoot down enemy missiles in flight. According to the Department of Defense Inspector General's office, Missile Defense Agency (MDA) and Ground-based Mid-course Missile Defense (GMD) computer networks and work policies do not adhere to Pentagon security procedures set in place in 2003. These include restricting access through individual computer passwords and reviewing the computer systems to check if unauthorized users had been using the computer networks. Also, network technicians and managers are not properly trained on Pentagon computer security policies, the report cited. However, a spokesman for the MDA said Monday there was no call for alarm and no security breach with the network had occurred. Defense contractors and military managers design and develop missile defense computer networks in Huntsville, but no Huntsville-specific problems were cited in the report. According to the report, password controls are a concern. Several users can gain access with a single "group" password instead of having individual passwords. This could lead to a security violation of the missile defense network, according to the report, which was issued Feb. 24.

5

News Item: Privacy

This privacy flaw has caused my fiancé and I to break-up after having dated for 5 years.

Basically, we share one computer but under separate Windows XP user accounts. We both use Mozilla Firefox -- well, he used to use it more than I do but now we don't really use it. The privacy flaw is this: when he went to log-in under his dating sites (jdate.com, swinglifestyle.com, adultfriendfinder.com, etc.), Mozilla promptly asks whether or not he'd like Firefox to save the passwords for him. He chose never, obviously. However, when he logged off his user account, and I logged onto my Windows XP account X amount of days later, I decided to use Firefox because … a lot more stable than IE7beta2.

Firefox prompted whether or not I'd like it to save my password for logging into my website. I chose never and changed my mind. I went into the Password Manager to change the saved password option from Never to Always and that's when I saw all these other sites that had been selected as "Never Save Password." Of course, those were sites I had never visited or could ever dream of visiting.

Then I realized who, how and what... Your browser does not efficiently respect the privacy of different users for one system.

- From http://diggdot.us - mozilla bug report

6

Is it Safe?

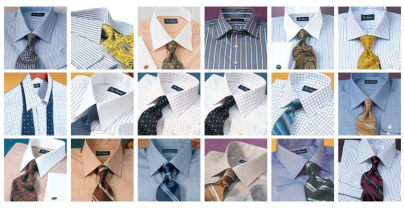
- We were given access to a newish iBook that was purchased on eBay. The iBook of course is not "stuff" for this page but the data left on it is fair game, i.e. it was unambiguously discarded and we got it for free. No cleanup had been done prior to shipping out the machine. As far as we can tell the story goes as follows:
  - Previous owner, let us call him Arthur, is given a Mac laptop and told it is cool and he should "switch"·Possibly with some assistance, Arthur manages to transfer a whole pile of stuff from his old Windows machine's ….·Arthur was however probably unhappy that he could not get his new Mac to play any of his porn collection stored in some Windows Media Format.·Hence Arthur decides that he does not like Macs.·Hence the Mac was sold on eBay, complete with all his data, after only 14 boots (we checked /var/log/system.log*).
  - Credit: Simon Byers "Stuff" - see Other References

7

Unusual?

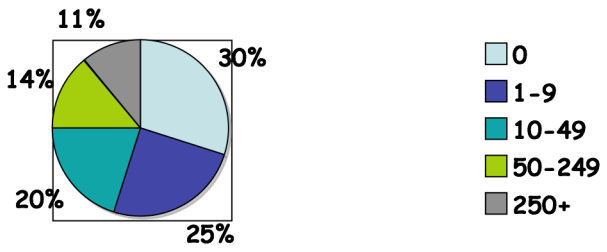
- First P3, a small form factor HP with win98 installed. It is now all happily upgraded to an 800Mhz with 256M Ram and donated to a worthy recipient. On the HD:·Car porn, i.e. pics of cars the pc user will probably never own.·A few mp3s·A few word docs·Pics of scantily clad females in IE cache, ….·Google searches for Maggie Gyllenhaal and other assorted junk.·…·Shown below a montage of cache pics left over from what seems to be some online shopping for shirt/tie combos. …

Credit: Simon Byers "Stuff"



8

Electronic Crimes/Intrusions 2003



9

2003 Losses Due to eCrime

Loss	% of Companies
$10M+	3%
$1M-$10M	5%
$500K-$1M	5%
$100K-$500K	11%
<$100K	26%
Don't Know!	50%

32% did not/could not track losses!

10

Attack Types (CERT)

- Virus/Malicious code 77%
- Denial of Service attack 44%
- Illegal SPAM generation 38%
- Unauthorized access by insiders 36%
- Phishing 31%
- Unauthorized access by outsiders 27%
- Fraud 22%
- Theft of intellectual property 20% …

11

Greatest Cyber Threat

- Hackers 40%
- Current employees 22%
- Former employees 6%
- …
- Terrorists - 1%
- (on to a study, speaking of insiders and outsiders)

12

First

- Any stories you would like to share?
- And there are studies emerging to chronicle what are the sources of the risks for various IP: Inside? Outside?
- For example

13

Movie Production and Distribution

- The issue:
  - 350,000 to 400, 000 illegal movie downloads each day (estimate)
  - Up to $4 billion in lost revenue over two year period
  - Early version of *The Hulk* began circulating two weeks before US theater release date
- Byers, et.al.(2003)

14

Movie Distribution

- 3 periods: prior to theater release, between theater release and DVD release, after DVD release
  - Before theater- critics and judges, also all sorts of studio personnel
  - During theater- cinema employees, movie goers, delivery folks
  - Post DVD- ripping

15

Examples

16

The Study

	Number of samples
Reviewed samples	285
Insider	220 (75%)
Outsider	65 (23%)
Incomplete video editing	4
Watermark or text marker	35 (12%)
DVD quality	223(78%)
Through-air-video	46 (16%)

17

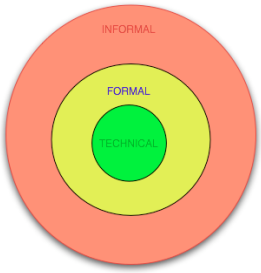
Insider Sources

- Copying in the editing room
- Copying of critics advanced copy
- Copying of promotional or preview screening
- Copying of awards judge
- Through the air recording by a projectionist
- Unauthorized copying of medium at the factory

18

On Security

- Kaufman, et.al., "… how to communicate securely over an insecure medium"
- Garfinkel and Spafford(1991) "A computer is secure if you can depend on it and its software to behave as you expect."
- Dhillon - "Coordination in three's"



19

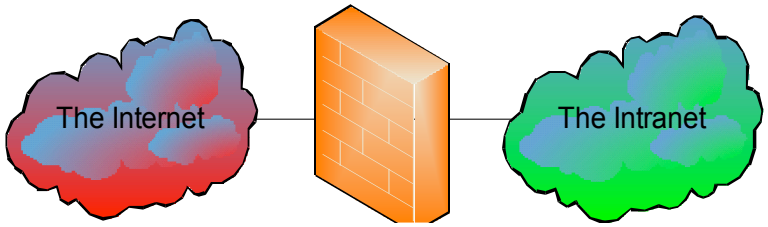
Security Issues

- Copy protection versus none
- Passwords:
  - Use the same one
  - Write them down
  - "remember" them
- Wireless router
- Desktop machine
- (privacy) Take work home
- Being Locked Out!
- … your favorite

Easier to do than NOT to do

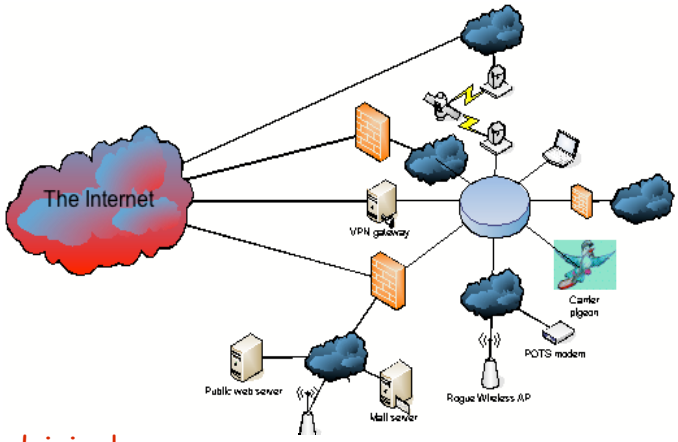
20

The network you think you have…



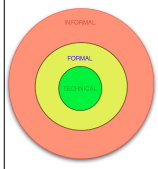
21

The network you *really* have…



Wardriving!

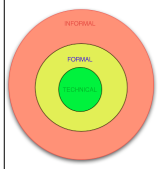
22



Security Controls

- Technical:
  - Supportive: identification, crypto key management
  - Preventive: authentication, authorization, access control enforcement
  - Detection and Recovery: audit, intrusion detection and containment

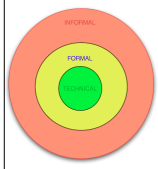
23



Security Controls

- Formal:
  - Preventive: security responsibility assignment, security plans and policies, security awareness training
  - Detection management controls: personnel controls (background checks, clearances, rotation of duties), audits, ongoing risk management
  - Recovery management controls: contingency an disaster recovery plans, incident response capability

24

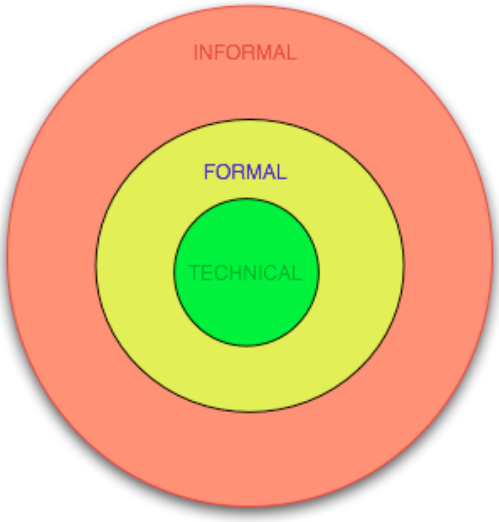


Security Controls

- Informal:
  - Preventive: security awareness program, security training in both technical and managerial issues, develop a security subculture
  - Detection: informal feedback mechanisms (COMMMUNICATION!), reward structures, formal reporting structures ≈ informal social groupings
  - Recovery: ownership of activities, encourage stewardship
  - Beware of social engineering - Kevin Mitnick and Sprint

25

Coordination in 3's



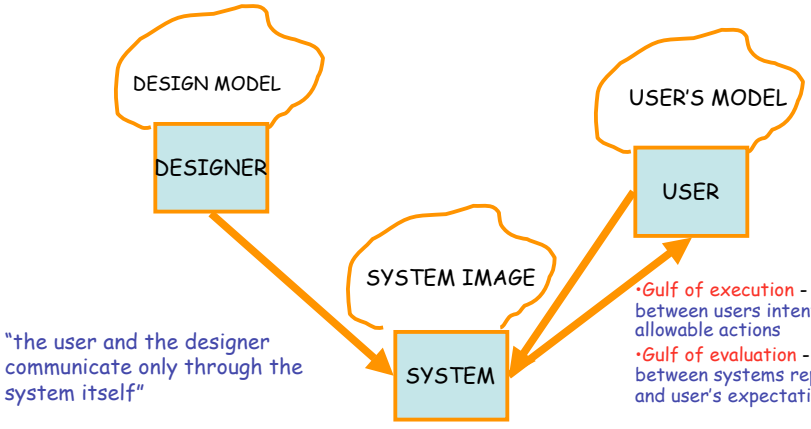
26

Solutions: Security

- Usability and Security have to be considered from the beginning of a project, not at the end
  - Leads to "pseudo-usability"
    - Rapidly dismissing prompts
    - Security by admonition - software admonishes you
  - Strive for security by designation, if possible
    - Allowed set versus acceptable set, in other words,

27

Knowledge in the World and in the Head



"the user and the designer communicate only through the system itself"

•Gulf of execution - mismatch between users intention and allowable actions

•Gulf of evaluation - mismatch between systems representation and user's expectations

The Design Challenge

Norman!

28

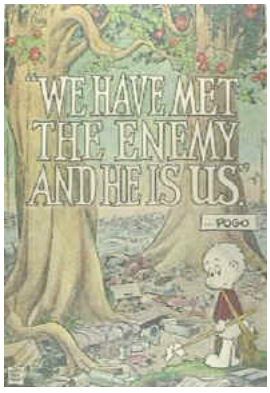
Recall

Garfinkel and Spafford(1991) "A computer is secure if you can depend on it and its software to behave as you expect."

29

Solutions-Security

- Something you know (password)
  - 'WE HAVE MET THE ENEMY…"
- Something you have (smart card)
  - Sometimes combined
- Something you are (retina scan)
  - but



30

Guidelines: Secure Interaction Design (Yee, 2004)

- General Principles:
- Path of least resistance - most natural way, the safest
- Appropriate boundaries - interface draws distinctions that match users expectations

31

Guidelines-2

- Explicit authorization - transfer control, rights explicitly and knowingly
- Visibility - authority decisions abdicated to software should be explicit, something running on my machine
- (& gtv) not an add-on integrated into architecture, design and development

32

On Privacy

- Complying with a person's desires when it comes to handling "his or her" personal information. … the right of individuals to determine if, when, how and to what extent data about themselves will be collected, stored, transmitted, used and shared with others. - Cannon
- From Spin State, "… "Don't you believe in privacy?" Cohen asked sounding exasperated. "Only my own. …" (Li answered)
- "True Names" - Vernor Vinge
- Anonymity is related - AT&T Crowds

33

At Risk

- Money
- Information/Data
- Information/Data integrity
- Time and other resources (computational)
- Privacy
- Confidentiality
- Availability
- Others(?)

"… That equation, simply stated, is: demonstrate trust, and maintain the lifelong value of the customer; break trust, and lose the customer."
--Dr. Ann Cavoukian

34

Privacy by Design

- Privacy should be designed into information management systems, one of the "ilities"
- Privacy Enhancing Technologies and Privacy Aware Technologies (PET and PAT)
- Privacy mantras:
  - Provide prominent disclosures
  - Put users in charge of their data
  - Seek anonymity
  - Recognize less is more when it comes to collecting and managing personal information
  - Construct a policy (what, how, how long, where, ACLs, …) for each bit of data you collect

35

PETs - Degrees of Anonymity

- Helps consumers and companies protect their privacy
- Focus on:
  - Anonymity
  - Pseudonymity
  - Unlinkability - inability to link pieces of related info - observe habits -- your shopper card
  - Unobservability
  - Address privacy - as in ip
  - Location privacy - voip issues
  - Authorization privacy - pseudonymous access to services

36

PATs as an "ility"

- A PAT is a technology that was designed, developed and deployed with privacy in mind - every application today should be a PAT
- Advantages:
  - Increases customer trust
  - Avoids negative press
  - Avoids litigation (international issues)
  - differentiator

37

Privacy Features

- Privacy statement
- P3P integration
- Privacy settings
- Centralized privacy setting management
- Ability to view data to be transmitted
- Documentation of privacy-related data
- Unsubscribe feature
- Access control
- Encryption
- Certification, e.g., Yahoo is TRUSTe certified
- Outsourcing

38

At Home

- Technical, Formal, Informal
- Use a firewall - check all security settings
- Tighten your wireless LAN
- Security awareness
- Dispose of computers and data properly
- Do a security audit - ongoing class project!

39

Home Security Audit Pointers

(from CERT)

- If used for work has your network configuration been vetted by corporate security?
- Do you use regularly updated virus protection software?
- Do you use a home firewall?
- Do you have a home "policy" on unknown or suspicious email attachments?
- Do you have a home policy on unknown or new software?
- How do you retire old hardware? (Byers not CERT)
- Are hidden filename extensions disabled?
- Are all applications (browsers, office) and OS kept up to date with patches?
- Do you turn off computer or disconnect when not in use?
- Do you disable Java, JavaScript and ActiveX at some level?
- Do you make regular backups of important files
- Do you have a boot or emergency disk?

40

References

- http://www.user-agent.org/cgi-bin/stuff - Simon's "Stuff"
- http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf
- Byers, S., Cranor, L., Kormann, D and McDaniel, P. "Analysis of security vulnerabilities in the movie production and distribution process," DRM'03, Washington, D.C., 2003.
- http://www306.ibm.com/ebusiness/ondemand/us/customerloyalty/harriet_pearson_interview.shtml
- S. Singh, The Code Book, Doubleday, 1999, ISBN 0-385-49531-5
- G. Dhillon, Principles of Information Systems Security, Wiley, 2006, ISBN 0-471-45056-1
- Moriarity, C. Spin State, Bantam, 2003.
- Yee, K. "Aligning security and usability" IEEE Security and Privacy, 2004.

Other Resources

- Blog http://vesonder.typepad.com/universe
- Website for notes, resources http://homepage.mac.com/vesonder
- vesonder@mac.com