FSEM 1111 Computer Security – from a Free Software Perspective

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

UNIX commands

1. cp
2. mv
3. rm
4. ln

UNIX commands

1. ping
2. telnet
3. traceroute

TCP/IP Layers

1. Physical Network (Ethernet, PPP, ...)
2. Internet (ARP, IP, ICMP, ...)
3. Transport (UDP, TCP)
4. Application (DNS, HTTP, SMTP, SSH, ...)

SMTP example

1. telnet ariel.cs.du.edu 25
2. MAIL FROM: sender@machine
3. RCPT TO: address@machine
4. DATA
5. Subject: Hello SMTP
6. .

P3P

- Platform for Privacy Preferences Project
- Problem statement: allow WWW-Sites to specify privacy policy precisely and formally

$\Rightarrow$ Humans do not need to read the policy, their browers do!

P3P Architecture

- P3P Advertisements
- P3P Reference File
- P3P Policy File

P3P Advertisements

How can the browser detect P3P and find more P3P information?

- Default location: http://www/W3C/p3p.xml
- HTTP header: P3P: policyref=URL
- HTML header: LINK tag

P3P Reference File

- Which policy is applicable (for a given site)?
- Where is the policy stored (at which URL)?
- When does the policy expire?
- What standard (version) does the policy follow?

P3P Policy File

- Who is collecting the data?
- Who may receive the data?
- Who handles disputes (about policy violations)?
- What data is being collected / accessed?
- Why is the data collected (purpose)?
- How long is the data retained?

P3P Compact Policy

- Part of HTTP P3P header
- Short version of Policy file
- See Privacy textbook, page 159

Does P3P work?

Problems with P3P

- P3P does not discourage excessive data retention
- Having a policy does not mean that it is designed to protect users
- Having a good policy does not mean it is actually implemented or enforced
- Having a 3rd-party for dispute resolution does not mean that it is neutral or effective

What about reading the Privacy Policy?

- Few users bother to read privacy policies
- Even fewer will understand and use P3P
- Based on (flawed) assumptions that users care deeply about privacy for ordinary WWW use
- Fails to address to communicate need for user privacy to developers and managers
- Oversimplifies the problem of privacy

Reputation and Certification Systems

- Idea: know the good and bad vendors

$\Rightarrow$ Users will avoid bad vendors

Examples: Karma on Slashdot, ebay feedback, etc.

Problems with Reputation

- Is the ranking produced in a way that is trustworthy (not easily manipulated)?
- Good reputation determined by past behavior, not future behavior.
- High reputation only attainable by large entities $\Rightarrow$ monopolization

Problems with Certification

- Certification Authority (CA) often commercially bound to certified entity
- CA has interest in process efficiency, not in optimal judgement
- Certification is costly without directly adding value to the product

Midterm

1. This will be a take-home midterm
2. Midterm handed out at the beginning of the next class
3. 20 Points UNIX Shell Programming questions
4. 35 Points Computer Security and Privacy questions
5. DUE: Thursday, 10/11/2007, 3pm
6. Submission format: LaTeX(submit a `.dvi` file)

Questions

?