Software Security: Principles

CS 161: Computer Security
Prof. Vern Paxson
TAs: Jethro Beekman, Mobin Javed, Antonio Lupher, Paul Pearce & Matthias Vallentin
http://inst.eecs.berkeley.edu/~cs161/

January 31, 2013
“Security is economics.”
What does this program do?
What can this program do?

Can it delete all of your files? YES. Why?
“Least privilege.”
Touchstones for Least Privilege

• When assessing the security of a system’s design, identify the *Trusted Computing Base (TCB)*.
  – What components does security rely upon?

• Security requires that the TCB:
  – Is correct
  – Is complete (can’t be bypassed)
  – Is itself secure (can’t be tampered with)

• Best way to be assured of correctness and its security?
  – KISS = *Keep It Simple, Stupid!*
  – Generally, Simple = *Small*

• One powerful design approach: privilege separation
  – Isolate privileged operations to as small a component as possible
  – (See lecture notes for more discussion)
“Ensure complete mediation.”
Ensuring Complete Mediation

• To secure access to some capability/resource, construct a *reference monitor*

• Single point through which all access must occur
  – E.g.: a network firewall

• Desired properties:
  – Un-bypassable (“complete mediation”)
  – Tamper-proof
  – Verifiable
  – (Note, just restatements of what we want for TCBs)

• One subtle form of reference monitor flaw concerns *race conditions* …
procedure withdrawal(w)
  // contact central server to get balance
  1. let b := balance

  2. if b < w, abort

  // contact server to set balance
  3. set balance := b - w

  4. dispense $w to user

TOCTTOU = Time of Check To Time of Use
public void buyItem(Account buyer, Item item) {
    if (item.cost > buyer.balance)
        return;
    buyer.possessions.put(item);
    buyer.possessionsUpdated();
    buyer.balance -= item.cost;
    buyer.balanceUpdated();
}
NO LONE ZONE
SAC TWO MAN POLICY
MANDATORY

CAUTION
DO NOT KEY RTMX IN L/O
EXCEPT IN CASE OF AN
EMERGENCY—MUST BE AT
LEAST 50 FT FROM NSL.
“Separation of responsibility.”
5 Minute Break

Questions Before We Proceed?
“Defense in depth.”
“Company policy: passwords must be at least 10 characters long, contain at least 2 digits, 1 uppercase character, 1 lowercase character, and 1 special character.”
Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.

A second survey found that 79% of people unwittingly gave away information that could be used to steal their identity when questioned.

Security firms predict that the lax security practices will fuel a British boom in online identity theft.
**What a piece of work is a man! how Noble in Reason! how infinite in faculty! in form and moving how express and admirable! in Action, how like an Angel! in apprehension, how like a God!**

-- *Hamlet* Act II, Scene II

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations.

“Psychological acceptability.”
When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

☑ In the future, do not show this message.
When you see a dialog box like this, click 'Yes' to make it go away. If available, click the checkbox first to avoid being bothered by it again.

In the future, do not show this message.
Unable to verify the identity of svn.xiph.org as a trusted site.

Possible reasons for this error:
- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be svn.xiph.org, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the Web site svn.xiph.org?

Examine Certificate...

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this Web site
Unable to verify the identity of svn.xiph.org as a trusted site.
Blah blah geekspeak geekspeak geekspeak.

Before accepting this certificate, your browser can display a second dialog full of incomprehensible information. Do you want to view this dialog?

- View Incomprehensible Information

- Make this message go away permanently
- Make this message go away temporarily for this session
- Stop doing what you were trying to do

[OK] [Cancel]
“Consider human factors.”
“Threat models change.”
Your Windows product must be activated within 7 days. Do you want to activate Windows now?

Yes  No
Wells Fargo Web-enables 6,200 ATMs
The Windows-based infrastructure enables remote upgrades

By Lucas Mearian
March 3, 2005 12:00 PM ET  Add a comment

Computerworld - Wells Fargo & Co. announced this week that it has completed a five-year project to Web-enable its 6,200 ATMs in 23 states. The Windows-based infrastructure is designed to allow Wells Fargo to update and add services such as new languages and envelope-free deposits to its entire network remotely.

Wells Fargo took all "the rational steps you'd take to harden any operating system," such as closing unused ports. But, "the reality is you can't buy a new ATM that runs OS/2. This is where the industry is," he said.
“Threat models change.”

“Design security in from the start.”

(Beware *bolt-on security.*)
CAUTION!
ZOMBIES!
AHEAD!!!

RUN FOR
COLD
CLIMATES

THE END
IS NEAR!
!!!!!!!!!!
TRAPPED IN SIGN FACTORY
“Don’t rely on security through obscurity.”
“Trusted path.”
Soda Hall wiring closet
Protection?
“Use fail-safe defaults.”