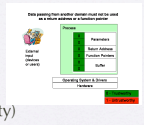
2110413 Computer Security

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

About me



- Born at Chulalongkorn Hospital
- B. Eng, M.Eng (Chulalongkorn University)
- Ph.D. (Michigan State University) -- Scholarship
- At Chula since 1995 (as a student) and 2001 (as a lecturer) and will (probably) retire here.
- Research
  - Computer Architecture
  - Computer Security
  - Embedded Systems
  - Storage Systems

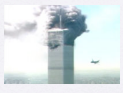
About me

- Security Patents (pending)
  - Secure Bit: Hardware Buffer-Overflow Prevention (2004)
  - Canary Bit: Extension of Secure Bit (2006)
-

Contact

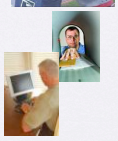
- Office: Eng4 18-18
- email: krerk@cp.eng.chula.ac.th
- homepage: http://www.cp.eng.chula.ac.th/~krerk/
- Office hours: Wednesday & Friday afternoon

Why are we here?



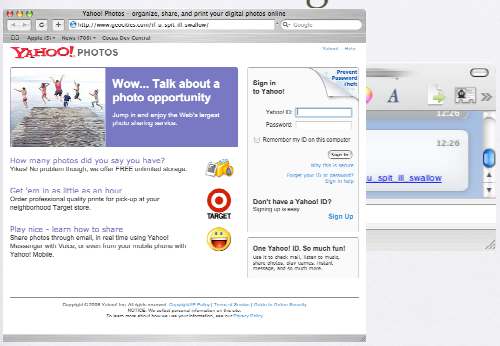
- 9/11
- Computer Worms & Viruses
- Trojan Horses
- Spyware
- Bots Net
- Phishing
- Spam
- Identity Thief
-

Fraud / Identity Theft



- Mailbox theft
  - passwords, account or credit card numbers or other information about others
- Password stolen
  - phishing

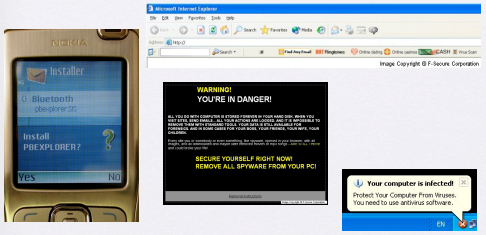
Phishing



Cyber Crime

- Cyber Stalking
  - The use of the Internet, e-mail, or other electronic communications devices to stalk or harass another person.
- Fraud / Identity Theft
  - Identifying and remedying the effects of one of the fastest growing crimes in America and other countries around the world
- Hacking
  - The deliberate and unauthorized access, use, disclosure, and/or taking of electronic data on a computer or other electronic device.

Viruses, Worms, Trojan Horses, Spyware

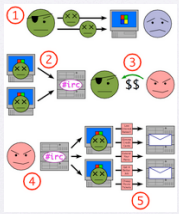


Social Engineer

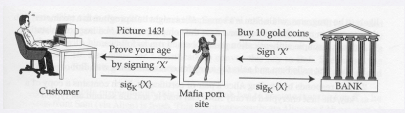
- AOL hack
  - documented by VIGILANTe: "In that case, the hacker called AOL's tech support and spoke with the support person for an hour. During the conversation, the hacker mentioned that his car was for sale cheaply. The tech supporter was interested, so the hacker sent an e-mail attachment 'with a picture of the car'. Instead of a car photo, the mail executed a backdoor exploit that opened a connection out from AOL through the firewall."
- Potential security leaks in our trash
  - "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware."

BotNet

- Bots (short for robot)
  Computers taken over by others.
- Botnet
  Network of bots.
- Can be bought in lots of thousands (millions?)
- Data theft, e.g. keylogging
- Phishing
- Relaying Spam
- Click Fraud
- Hosting (warez, malware, etc.)
- DDoS
-



Mafia-in-the-Middle



- Order?
- "…using crypto keys (or other authentication mechanisms) in more than one application can be dangerous; and letting other people bootstrap their own application security off yours can be downright foolish." Security Engineering by Anderson

Background

- Students should have background in
  - Computer Network
  - Operating Systems, System Programming
  - Database, S[ADE]
  - Programming (C is preferred)
- If you have not taken these, this will be difficult to do well.

Grading

- โครงงาน 45%
- สอบปลายภาคการศึกษา 25%
- บทความ/รายงาน 10%
- การบ้าน 15%
- การเข้าเรียน 5%

Project

- 2-3 persons team (Choose your partners and email me by November 13)
- A team project with both a programming component and a presentation will be expected --- demonstrating an intrusion to the class
- Resource for topics
  - SANS/FBI
  - OWASP

Paper

- Due last day of class
- A 5-10 page paper
- Theme is security analysis of various operating systems using the knowledge learned from this class.
- I will provide a list of topics for you to pick.

Goal

- Create a set of skeptics
- If when you leave this class you have a different way of looking at the world around you, I will have succeeded.

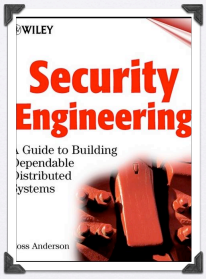
Security

- Computer Security is too broad a topic.
- I know only a small part.
- This course is rather a collaboration among all of us.

Suggested Book

- Security Engineering
- By Ross Anderson

- Wiley, 2001
- ISBN: 0471389226
- Available online in PDF at
- http://www.cl.cam.ac.uk/~rja14/book.html



Suggested Book

from a programmer's viewpoint

- Writing Secure Code, 2nd Edition by Michael Howard and David LeBlanc

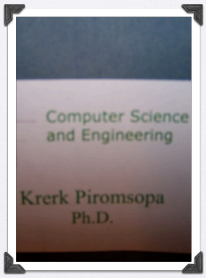
- Microsoft Press, 2002

- ISBN 0-7356-1722-8

Class Material

- Computer Security: The Fundamentals

- A work in progress of Krerk Piromsopa



Ten Security Principles

by various folk
IBM, MS, Albion

Principle 1: Least privilege.

The principle of ***least privilege*** states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

Principle 1: Least privilege.

Impact

If a process is running with elevated privileges (e.g. root or admin) and gets corrupted, more damage can be done.

If a user is running with elevated privileges and is attacked, more damage can be done.

Example: Sony Minidisk application

Principle 2: Defense in depth.

The idea behind ***defense in depth*** is to manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will, ideally, prevent a full breach.

(Well known military strategy.)

Principle 2: Defense in depth.

Impact

Windows Server 2003 changed the search order for DLL's to use system ones first, not duplicate application DLL's. That removed an attack vector.

Later a vulnerability was exploited in Windows to insert DLL's into an application folder, but it didn't work on Server 2003 because of the DLL search order change.

Principle 3: Secure failure

Avoid security problems related to failures. When systems fail in any way, they should not revert to insecure behavior.

Principle 3: Secure failure

Impact

An application fails. What happens next?

If the application was running with elevated privileges does one fail into the operating system with elevated privileges?

If so, attack by overwhelming an application to cause a failure, e.g. segmentation fault.

Principle 4: Secure the weakest link

Security is a chain; ***a system is only as secure as the weakest link***.
One consequence is that the weakest parts of your system are the parts most susceptible to attack.

Principle 4: Secure the weakest link

Impact

Firewalls have been favorite points of attack.

… so are networked printers.

They really are computers and are overlooked.

Principle 5: Compartmentalization

The basic idea behind ***compartmentalization*** is that we can minimize the amount of damage that can be done to a system,
if we break the system up into as many isolated units as possible.

Principle 5: Compartmentalization

Impact

Put a web server in a DMZ and
put your data behind another firewall.

… maybe only a copy of your data
as read-only

… only accept connections
from the web server

Principle 6: Simplicity

The KISS mantra -- "***Keep it simple***, stupid!". Complexity increases the risk of problems; this seems unavoidable in any system. Your designs and implementations should be as straightforward as possible.

Principle 6: Simplicity

Impact

See Microsoft.

Principle 7: Promote

Users generally consider privacy a security concern.
You shouldn't do anything that could compromise the privacy of the user.

And you should be as diligent as possible in protecting any personal information that a user gives you. You can quickly lose the respect of your customers, if they think you handle privacy concerns poorly.

Principle 7: Promote privacy

Impact

- Do I ***need*** their Social Security number?
- Do I need to ***keep*** their credit card number?

…

Principle 8: It's hard to hide secrets

It's incredibly difficult to keep the "secrets" secret.

The most common threat to companies is the "insider" attack, where a disgruntled employee abuses access, … and reveals secrets.

"Security by obscurity": whenever possible, you should avoid using this as your sole line of defense.

Principle 8: It's hard to hide secrets

Impact

All secure encryption algorithms are public.

No one would trust them otherwise.

… only the keys are private.

Principle 9: Don't extend trust easily

Be reluctant to trust your own servers, in case they get hacked.

You should also be reluctant to trust yourself and your organization.

There have been many products from security vendors with gaping security holes

Principle 9: Don't extend trust easily

Impact

The Slammer worm (2003) penetrated a private computer network at Ohio's Davis-Besse nuclear power plant and disabled the safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall.

… a contractor connected to the private network and then dialed into the Internet.

Principle 10: Trust the community

Repeated use without failure promotes trust. Public scrutiny does as well. You get to leverage the experience of others. This principle only applies if you have reason to believe that the community is doing its part to promote the security of components you want to use.

Principle 10: Trust the community

Impact

Again,
all secure cryptographic algorithms are public.

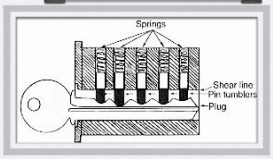
They have been heavily scrutinized by experts.

What is Security?

- "Security: In the computer industry, refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phase that gives a user access to a particular program or system"-----Definition from webopedia.com
- "the state of being secure" with secure defined as "free from risk of loss." ----- Mirriam-Webster Online
-

See the past

- As people formed early communities, the issue of physical security emerged.
- the oldest known lock is a 4,000 year old Egyptian lock



Security

- "***The protection of resources from being accessed by an unauthorized person at a particular time.***"

"**Who** can **do what when**?"