Computer Security

Krerk Piromsopa, Ph.D. @ 2019

Introduction to Computer Security

Chapter I

Krerk Piromsopa, Ph.D. @ 2019

Computer Security

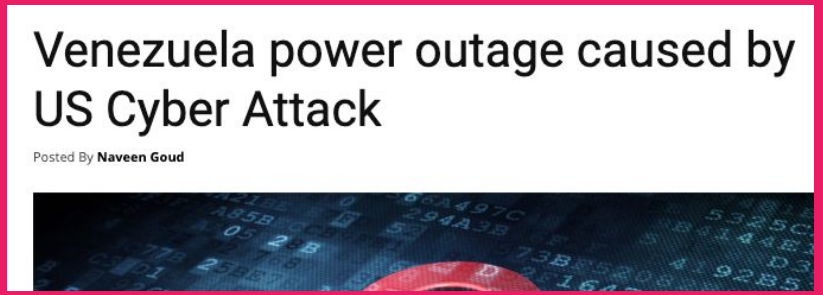
- Why should we learn security?
- Cybercrimes
- What is Security?
  - Ten Principles of Security (as recommended by industries)
- So, what is Security?
- Goal of this class
- Books and Materials for the class.

Why are we here?

- ★ Do you know them all?
  - Computer Worms & Viruses
  - Trojan Horses
  - Spyware
  - Ransomware
  - Bots Net
  - Phishing
  - Pharming
  - Spam
  - Identity Thief
- ★ Most people do not know them.

Facts

Wars in modern day



- Our infrastructure are more vulnerable than you know.
- Your personal life may not be personal.

Slammer worm crashed Ohio nuke plant network
Kevin Poulsen, SecurityFocus 2003-08-19

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power pl
disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that t
protected by a firewall, SecurityFocus has learned.

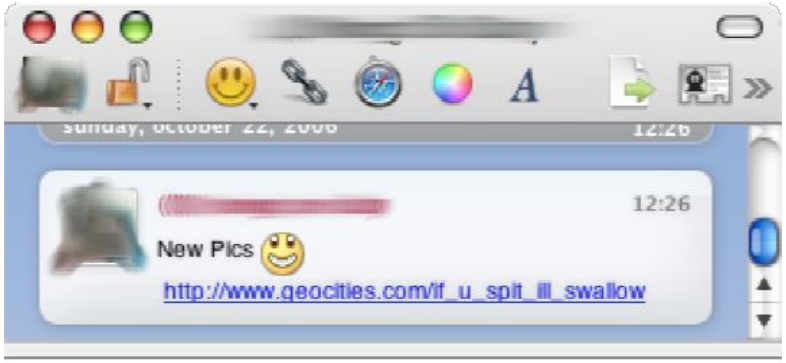
Malicious Software

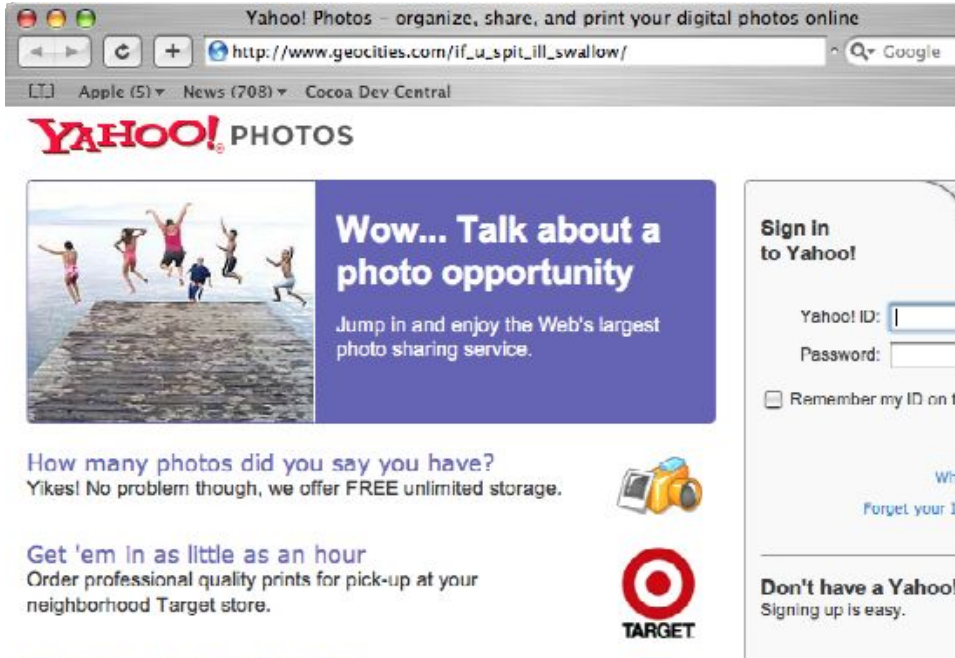
- ★ Malicious Software
  - Computer Viruses
  - Computer Worms
  - Trojan Horses
  - Spyware
  - Ransomware

Morris worm, Internet worm of November 2, 1988, was one of the first computer worms distributed via the Internet.

Phishing

- Can be in any form.
  - Emails
  - Phone
  - Web
  - IM
- What will happen if you typed in your username and password?





Facts

Most banks got hacked every week. However, the bank does not want to pursue any investigation. Why?

How Effective is Phishing? (reported by FBI, 2004)

In 12 months ended 4/04, 57 million reported phish e-mail.

Value of goods & services total $ 1.2B but does not include cost for HW, SW, reputation, etc.

Total $ damage estimated at $50B!

Cyber Crime

- ★ Basically, it is crime that use digital as mediums.
- ★ 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.

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.”

Severity of Cyber Crime

- ★ Similar cases, more serious in time
- ★ Cyber Stalking

In **1985**, a University of Michigan student was charged with interstate transmission of a threat, after writing a fictional account on a computer bulletin board of raping and torturing a named classmate. That case was thrown out after a US District Court ruled that the student **broke no federal law.**

In **2001**, Manish Kathuria was arrested by the New Delhi Police after impersonating Ritu Kohli on the MIRC chat service. The arrest was claimed as India's first case of cyberstalking, with Kathuria being charged under Section 509 of the Indian Penal Code for **"outraging the modesty"** of his victim. Having appropriated her name he "used obscene and obnoxious language", distributing her home telephone number with invitations for callers to "talk dirty".

In **2004**, a South Carolina man was sentenced to **five years of probation, 500 hours of community service and US$12,000 restitution** after pleading guilty to offences under federal stalking law. He had admitted sending dozens of email and fax messages to a Seattle city employee who had broken up with him 14 years previously.

Facts

Thai Computer Law
(2550 B.E.)

You have to look after your devices.

If a friend uses your smartphone to call send bad words about the prime minister, it is your false.

If you share contents that may cause harm to others, it is also your false.

See พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

Advertising/Scam

- ★ No matter where you find classified ads online, you are most likely to find some claims are not true
- ★ Nigerian scam (Why Nigerian?)

Make $2000 or more every week!

I GUARANTEE you will make money within 48 hours, or your money back. No questions asked!

LAGOS, NIGERIA.

ATTENTION: THE PRESIDENT/CEO

DEAR SIR,

CONFIDENTIAL BUSINESS PROPOSAL

HAVING CONSULTED WITH MY COLLEAGUES AND BASED ON THE INFORMATION GATHERED FROM THE NIGERIAN CHAMBERS OF COMMERCE AND INDUSTRY, I HAVE THE PRIVILEGE TO REQUEST FOR YOUR ASSISTANCE TO TRANSFER THE SUM OF $47,500,000.00 (FORTY SEVEN MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS) INTO YOUR ACCOUNTS. THE ABOVE SUM RESULTED FROM AN OVER-INVOICED CONTRACT, EXECUTED COMMISSIONED AND PAID FOR ABOUT FIVE YEARS (5) AGO BY A FOREIGN CONTRACTOR. THIS ACTION WAS HOWEVER INTENTIONAL AND SINCE THEN THE FUND HAS BEEN IN A SUSPENSE ACCOUNT AT THE CENTRAL BANK OF NIGERIA APEX BANK.

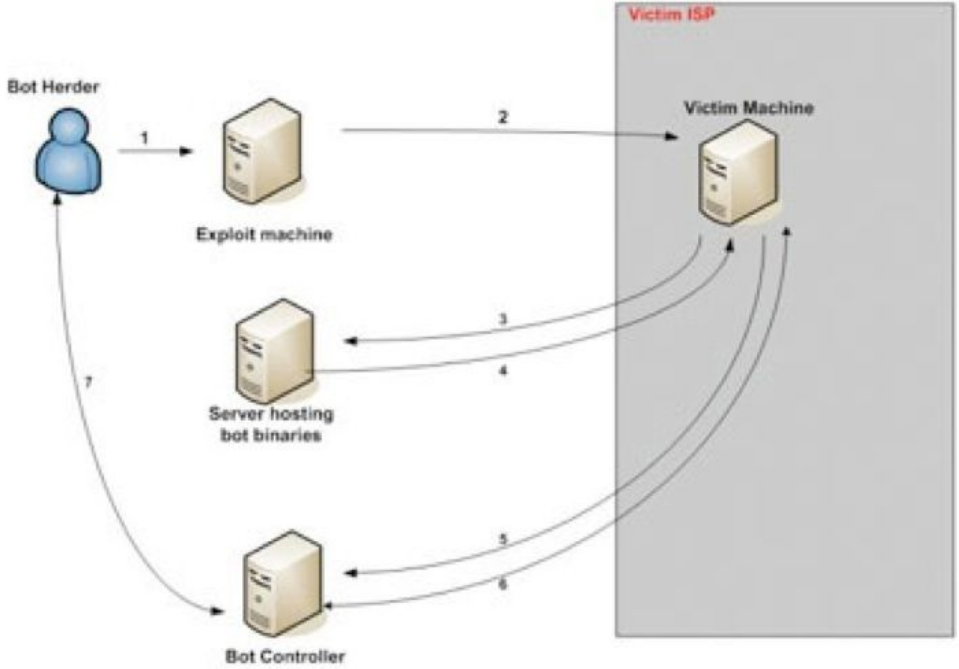
WE ARE NOW READY TO TRANSFER THE FUND OVERSEAS AND THAT IS WHERE YOU COME IN. IT IS IMPORTANT TO INFORM YOU THAT AS CIVIL SERVANTS, WE ARE FORBIDDEN TO OPERATE A FOREIGN ACCOUNT; THAT IS WHY WE REQUIRE YOUR ASSISTANCE. THE TOTAL SUM WILL BE SHARED AS FOLLOWS: 70% FOR US, 25% FOR YOU AND 5% FOR LOCAL AND INTERNATIONAL EXPENSES INCIDENT TO THE TRANSFER.

BotNet

- ★ Bots (short for robot)Computers taken over by others.
- ★ BotnetNetwork of bots.
- ★ Can be bought in lots of thousands (millions?)
- ★ If you can control thousands of computer from a keyboard at your fingertips, what will you do with that power?
  - Data theft, e.g. keylogging
  - Phishing
  - Relaying Spam
  - Click Fraud
  - Hosting (warez, malware, etc.)
  - DDoS

BotNet & DDoS

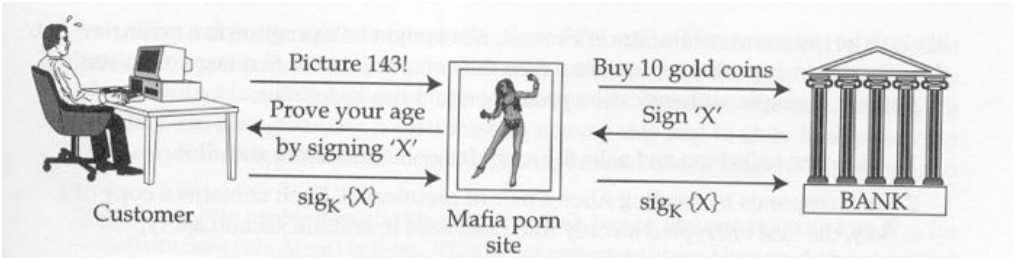
- ★ Hackers typically connect bots to IRC channel.
- ★ The bots can easily be programmed to attack a victic machine.

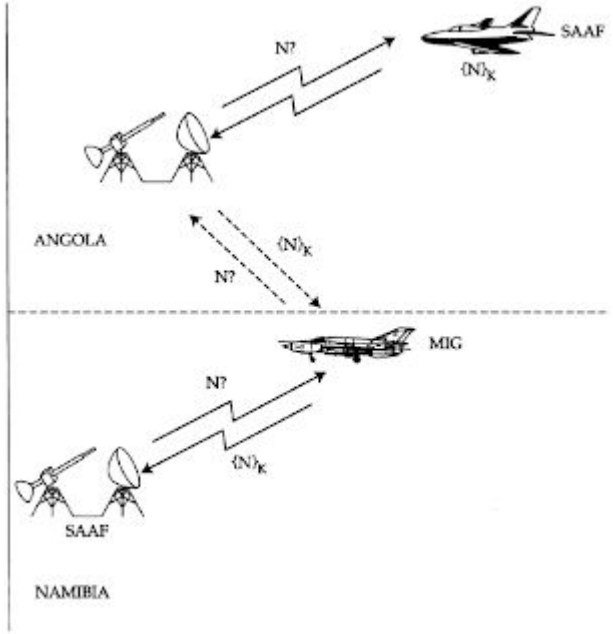


According to shadowserver.org, about 190,000 DDoS attacks were carried out in 2008, “earning” cybercriminals about $20 million. Naturally, this estimate does not include revenues from blackmail, which are impossible to assess.
(Source: https://securelist.com/the-economics-of-botnets/36257/)

Man-in-the-middle attack

- ★ Originally, it is MIG-in-the-middle attack (by Russia).
- ★ Order?





Pictures are taken from Security Engineering by Ross Anderson

Intuitively, user is the first line of defense.

What is Security?

Ten Security Principles

by various folk
(IBM, MS, Albion)

★ Let’s hear what people in the industry are talking about securing a system.

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.

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: Running MS Word as Administrator, a macro virus can wipe out a system.

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.)

To prevent our enemy from capturing a train and getting right to the capital, a track must be crossed by roads every few kilometers.

Principle 2: Defense in depth. (ctd.)

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.

In the past, a segmentation fault will cause a shell to pop up for debugging.

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.

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.

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.

Impact

See Microsoft.

Principle 7: Promote privacy

★ 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.

Impact

Privacy policy

- 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.

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

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.

Impact

Again, all secure cryptographic algorithms are public.

They have been heavily scrutinized by experts.

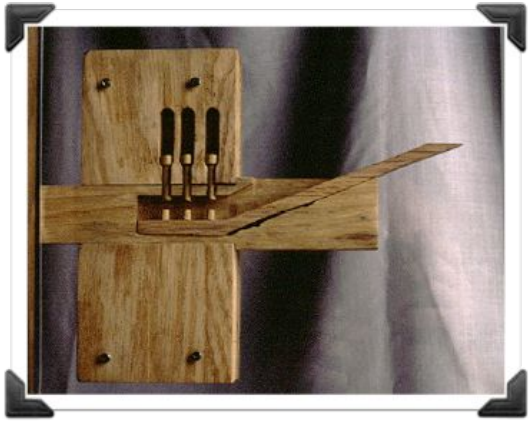
So, What is Security?

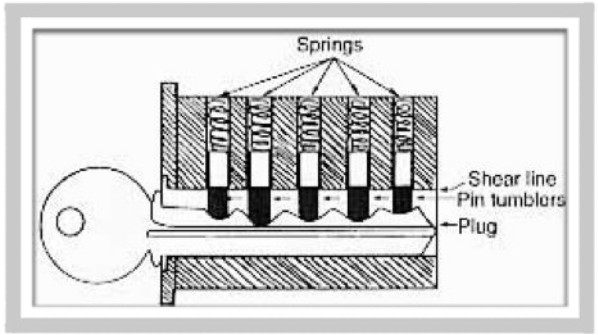
- What do people say?
- “Security: In the computer industry, refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data 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

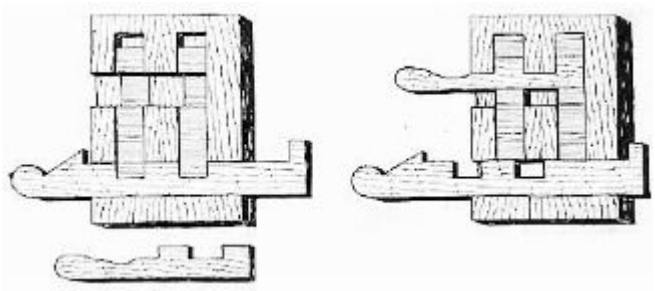
- “the state of being secure” with secure defined as “free from risk of loss.” ----- Mirriam-Webster Online

So, What is Security? (ctd.)

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



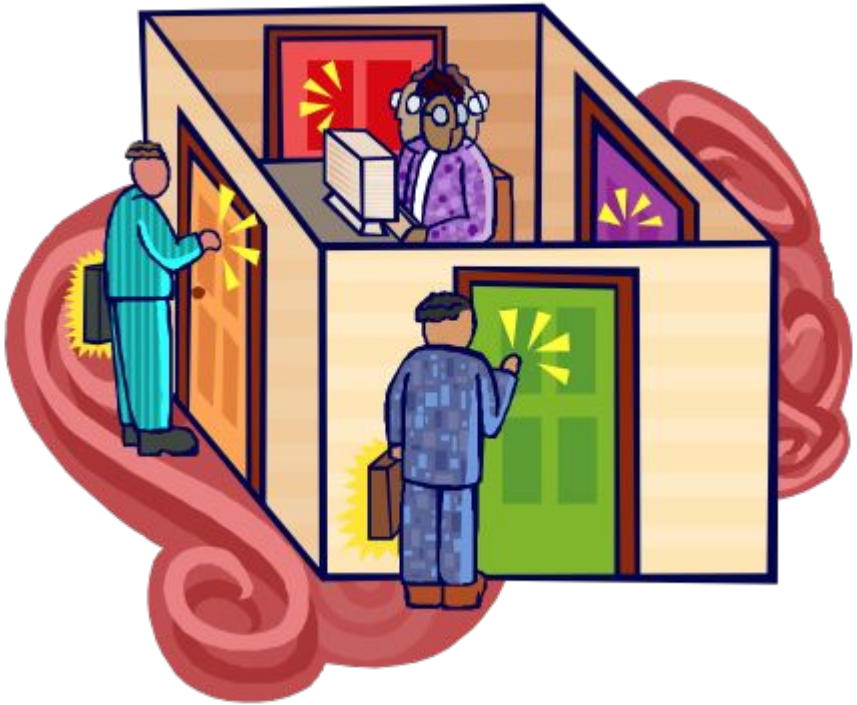




So, What is Security? (ctd.)

★ “The protection of resources from being accessed by an unauthorized person at a particular time.”

★ “**Who** can **do what when**?”



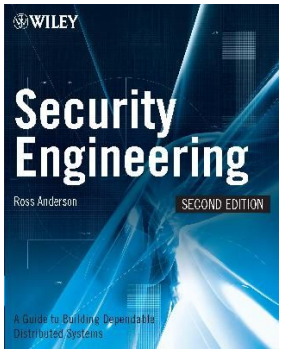
Our Goal

Be skeptical

Goal of this class

Security is too broad a topic. I know only a small part.
This class is rather a collaboration among us.
If when you leave this class you have a different way of looking at the world around you, I will have succeeded.

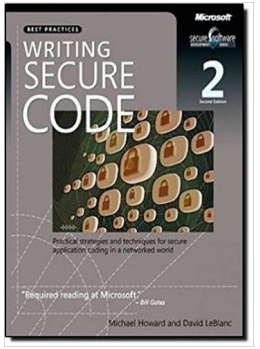
Books and Materials for this class



★ Recommended Reading
  - Security Engineering
    By Ross Anderson
    ISBN-10: 0470068523
    Wiley, 2008

    Available online in PDF
    athttp://www.cl.cam.ac.uk/~rja14/book.html

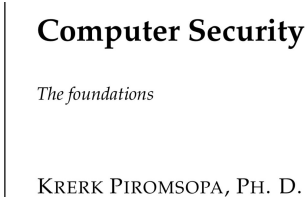
★ This book has summarized the concepts of security quite well in the beginning.



★ Recommended Reading
  - Writing Secure Code, 2nd Edition
    By Michael Howard and David LeBlanc
    ISBN-10: 0735617228
    Microsoft Press, 2002

★ To be a good programmer (security wise), this is a should read.

Books and Materials for this class



- A book by
  Krerk Piromsopa, Ph.D. will be provided.
  Computer Security, The Foundations.

- This is a work in progress.

End of Chapter 1