

Information Security

CS 526

Topic 1





Overview of the Course



How Does Information (In)Security Affect You and Me?

- Anthem Data Breach in Jan 2015
 - Second-largest health insurer in the US (Purdue's health care insurance provider)
 - Data of up to 80 million individuals obtained by hackers
- **Anthem:** *"Cyber attackers executed **a very sophisticated attack** to gain unauthorized access to one of our parent company's IT systems and have obtained personal information... The information accessed may have included names, **dates of birth**, **Social Security numbers**, health care ID numbers, **home addresses**, email addresses, **employment information, including income** data. We have no reason to believe credit card or banking information was compromised."*
- *How did the attack happen?*
- *Why should I be more scared if Anthem serves 5 million individuals instead of 80?*

Emails Like This

 Delete

All  More ▾

 Reply & Delete  Create New

Respond Quick Steps

From: Blackboardlearn <rrounds@purdue.edu>
To: ninghui@cs.purdue.edu
Cc:
Subject: Mandatory Update

Attention,

You have received an Update sent to you through the **Black board** Learning

Please Login below to Reply now.

[Click here to Login](#)

Thank you, The URL: <http://www.african-life.com.zm/wp-content/themes/kallyas/http/bb/mn/login.in.htm>

And This

From: Xerox WorkCentre <Xerox.Device3@cs.purdue.edu>
To: ninghui@cs.purdue.edu; phil@cs.purdue.edu; rcs-bugs@cs.purdue.edu; saw@
 saw@cs.purdue.edu; smb@cs.purdue.edu; spa@cs.purdue.edu; spaf@cs.pur
Cc:
Subject: A new fax has arrived



Message



IncomingFax.zip (99 KB)



Untitled attachment 00924.txt (127 B)

11/21/2012 01:33:42 CST Transmission Record Received from remote ID:
Inbound user ID ninghui, routing code 0
Result: (0/838;0/0) Successful Send
Page record: 1 - 1
Elapsed time: 00:54 on channel 7

Last Sample Email

From: Jean-Pierre Seifert <jeanpierreseifert@helbanoivas.com.br >
To: Ninghui
Cc:
Subject: from: Jean-Pierre Seifert

Greetings Ninghui

<http://weicheng123.com/brief.php?largest=xd9av1tp9fntp1n>

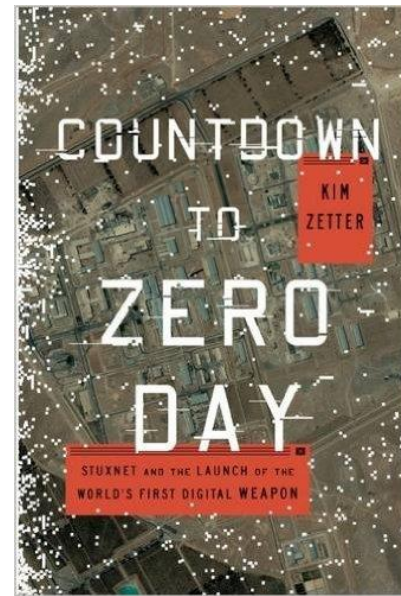
jeanpierreseifert@yahoo.com

Ninghui

Sent from my iPhone

Stuxnet (2010) First(?) Cyber Weapon Used by Nation/State

- Stuxnet: Windows-based Worm
 - Worm: self-propagating malicious software (malware)
- Attack Siemens software that control industrial control systems (ICS) and these systems
 - Used in nuclear power plants, among other factories
- First reported in June 2010, the general public aware of it only in July 2010
- A digital weapon created by nation states
 - Iran confirmed that nuclear program damaged by Stuxnet
 - Sophisticated design, special targets, expensive to develop

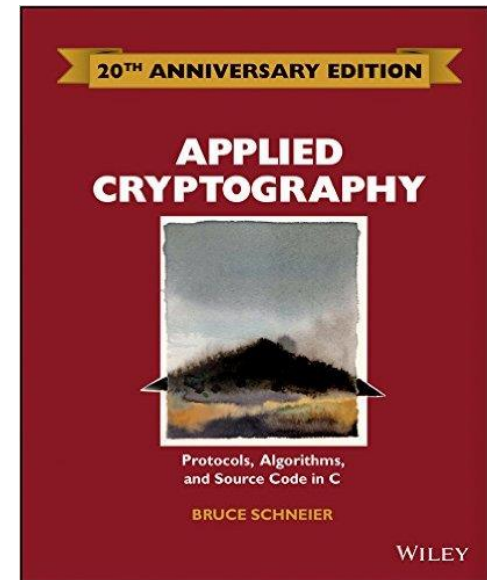
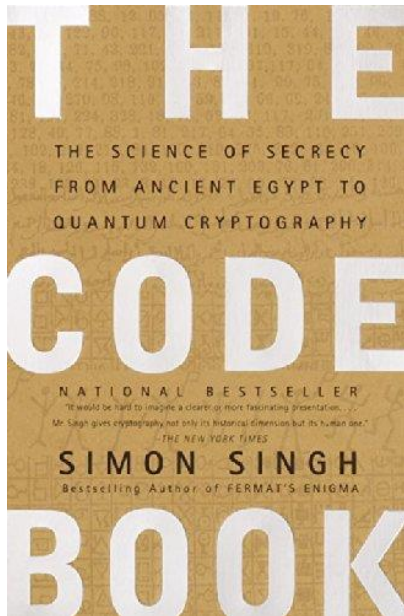


See the Course Homepage

- http://www.cs.purdue.edu/homes/ninghui/courses/526_Fall15/index.html
- Knowledge needed for the course
 - Probability
 - Basic knowledge of algorithms
 - Programming knowledge (for two programming projects)
 - Web (PHP)
 - Low-level (C, some knowledge of assembly)
 - Knowledge of operating systems/networking

Communications

- We are using Piazza.
 - Email me if you haven't received an invitation.
 - Past exams have been posted on Piazza.
- Other books I liked



EMERGENCY PREPAREDNESS – A MESSAGE FROM PURDUE

To report an emergency, **call 911**. To obtain updates regarding an ongoing emergency, sign up for Purdue Alert text messages, view www.purdue.edu/ea.

There are nearly 300 **Emergency Telephones** outdoors across campus and in parking garages that connect directly to the PUPD. If you feel threatened or need help, push the button and you will be connected immediately.

If we hear a **fire alarm** during class we will immediately suspend class, evacuate the building, and proceed outdoors. Do not use the elevator.

If we are notified during class of a **Shelter in Place requirement for a tornado** warning, we will suspend class and shelter in [the basement].

If we are notified during class of a **Shelter in Place requirement for a hazardous materials release, or a civil disturbance**, including a shooting or other use of weapons, we will suspend class and shelter in the classroom, shutting the door and turning off the lights.

Please review the Emergency Preparedness website for additional information.
http://www.purdue.edu/ehps/emergency_preparedness/index.html

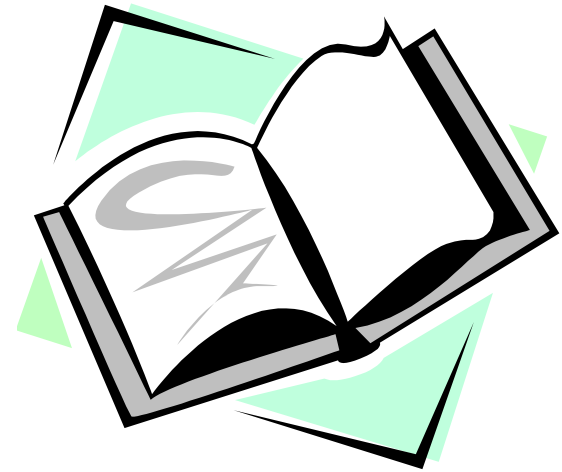
Readings for This Lecture

Required readings:

- [Information Security on Wikipedia](#) (Basic principles & Risk management)

Optional Readings:

- Counter Hack Reloaded
 - Chapter 1: Introduction
- Security in Computing: Chapter 1



What is Information (Computer) Security?

- Security = Sustain desirable properties under intelligent adversaries
- Make the above precise requires making the following two precise
- Desirable properties
 - Understand what properties are needed.
- Intelligent adversaries
 - Needs to understand/model adversaries
 - Always think about adversaries.

Security Goals/Properties (C, I, A)

- Confidentiality (secrecy, privacy)
 - only those who are authorized to know can know
- Integrity (also authenticity in communication)
 - only modified by authorized parties and in permitted ways
 - do things that are expected
- Availability
 - those authorized to access can get access

Which of C, I, A are violated in ..

- Anthem Data Leakage
 - Confidentiality?
 - Integrity?
- Email Phishing/Malware Attacks
 - Integrity?
 - Confidentiality?
- The Stuxnet attack compromises
 - integrity of software systems,
 - availability of some control functionalities,
 - confidentiality of some keys in order to sign malware to be loaded by Windows

Why Do Computer Attacks Occur?

- Who are the attackers?
 - bored teenagers, criminals, organized crime organizations, rogue (or other) states, industrial espionage, angry employees, ...
- Why they do it?
 - fun,
 - fame,
 - profit, ...
 - computer systems are where the moneys are
 - Political/military objectives

Why These Attacks Can Succeed?

- Software/computer/information systems/designs are buggy
 - They are complex, dynamic, and increasingly so
- Users make mistakes
- Some Technological factors
 - Inherent power of computers Von Neumann architecture: stored programs mixing code and data
 - Unsafe program languages

Why Do These Reasons Exist?

- Economical factors
 - Lack of incentives for secure software
 - Security is difficult, expensive and takes time
- Human factors
 - Lack of security training for software engineers
 - Largely uneducated population
 - Security often gets in the way

Security is Secondary

- What protection/security mechanisms one has in the physical world?
- Why the need for security mechanisms arises?
- Security is secondary to the interactions that make security necessary.

Robert H. Morris: The three golden rules to ensure computer security are: (1) do not own a computer; (2) do not power it on; and (3) do not use it.

Information Security is Interesting

- The most interesting/challenging threats to security are posed by human adversaries
 - Security is harder than reliability
- Information security is a self-sustaining field
 - Can work both from attack perspective and from defense perspective
- Security is about benefit/cost tradeoff
 - Thought often the tradeoff analysis is not explicit
- Security is not all technological
 - Humans are often the weakest link

Information Security is Challenging

- Defense is almost always harder than attack.
- In which ways information security is more difficult than physical security?
 - adversaries can come from anywhere
 - computers enable large-scale automation
 - adversaries can be difficult to identify
 - adversaries can be difficult to punish
 - potential payoff can be much higher
- In which ways information security is easier than physical security?

What is This Course About?

- Learn how computers/information systems can be attacked.
- Learn a suite of techniques to prevent attacks and/or limit their consequences.
 - E.g., authentication, access control, various crypto tools, sandboxing, isolation, detection, recovery, etc.
 - No silver bullet; man-made complex systems will have errors; errors may be exploited

Tools for Information Security

- Cryptography
- Authentication and Access control
- Hardware/software architecture for separation
- Processes and tools for developing more secure software
- Monitoring and analysis
- Recovery and response

What is This Course About?

- Learn to think about security when doing things
- Think about
 - Adversary model (capability of the adversary)
 - Desirable properties
 - Trust assumptions (what I am depending upon for the desirable property to hold against certain adversary)
- Learn to understand and apply security principles when designing/building/analyzing systems
 - E.g., least privilege, separation of duty

Ethical Use of Security Information

- We discuss vulnerabilities and attacks
 - Most vulnerabilities have been fixed
 - Some attacks may still cause harm
 - Do *not* try these outside the context of this course

Policies for Homework Cheating

- It is allowed/encouraged to discuss homework problems
- However, if you looks at another student's written or typed answers, or let another student look at your written or typed answers, that is considered cheating.
- If caught for the first time, receive 0 in the assignment. For the second time, receive a failing grade in class.

Coming Attractions ...

- Cryptography: review of probability, terminology of encryption, classic ciphers, one-time pad.
- Readings
 - [Cryptography on Wikipedia](#)

