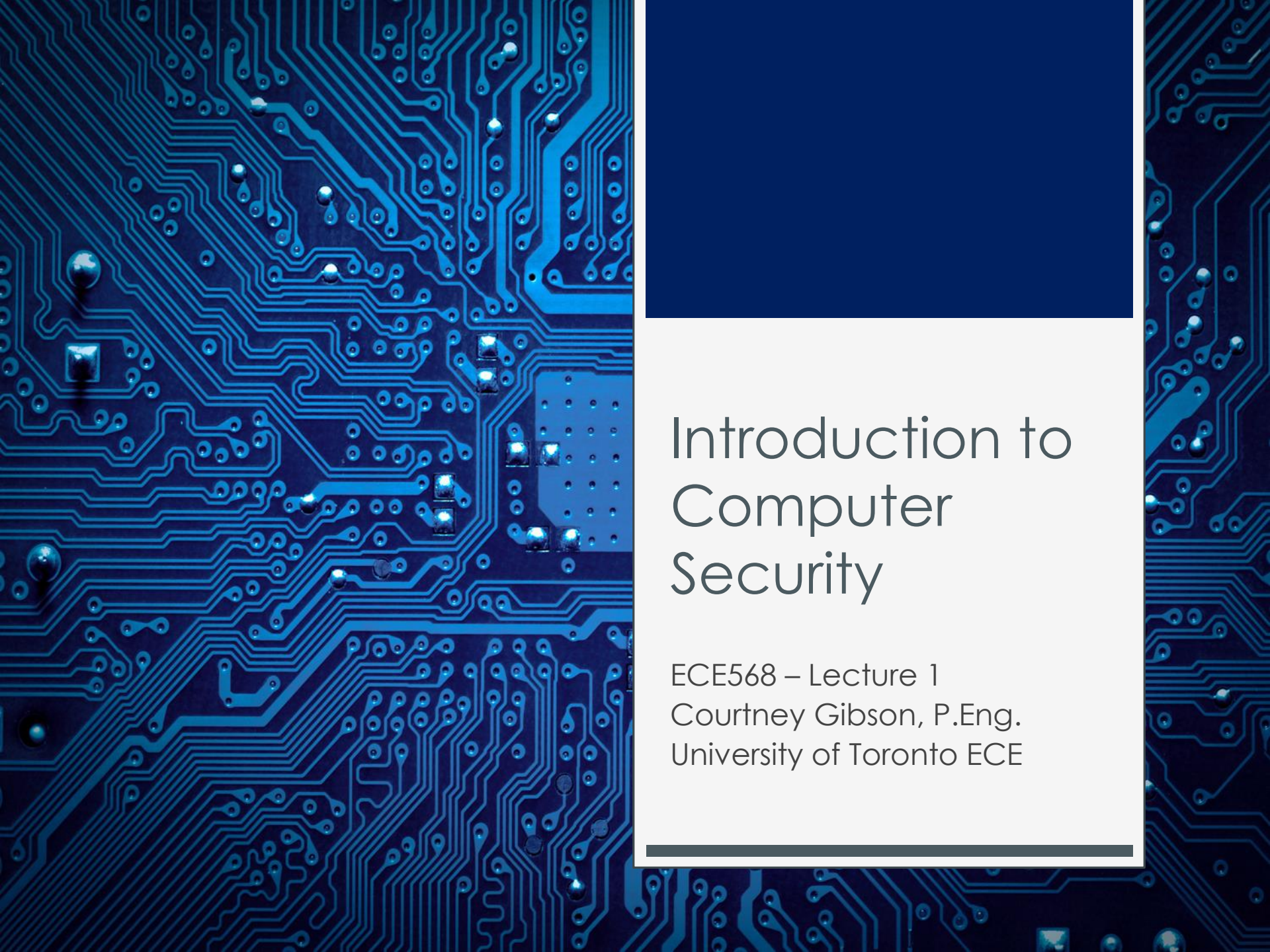


Introduction to Computer Security

ECE568 – Lecture 1

Courtney Gibson, P.Eng.
University of Toronto ECE

Lab Assignment #7: Inheritance

1. Objectives

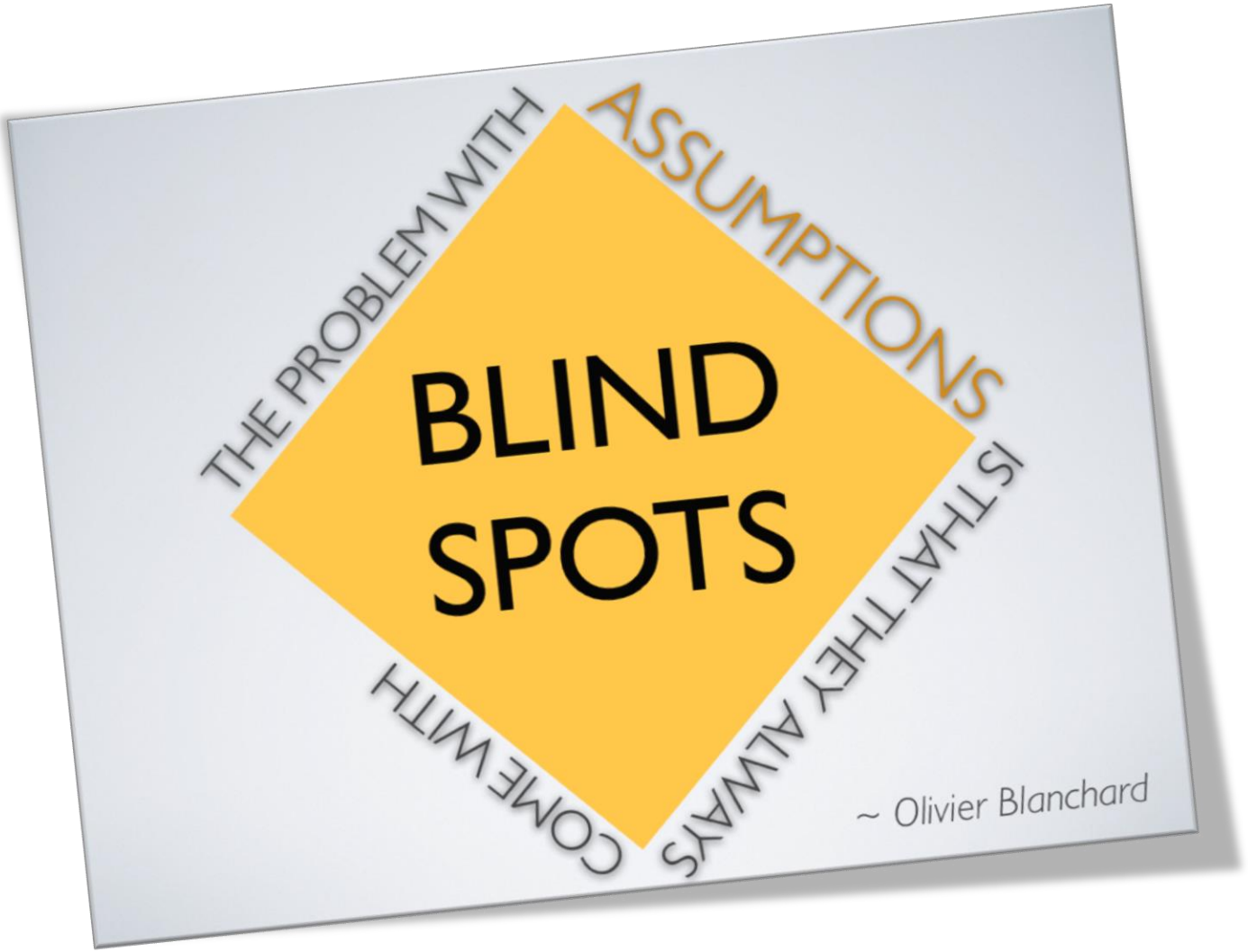
The objective of this assignment is to provide you with practice on the use of inheritance in C++ programming. This will be done in the context of re-implementing the simple student-marks database of Assignment 5 to allow the storage and retrieval of records of any type, not only of type `studentRecord`.

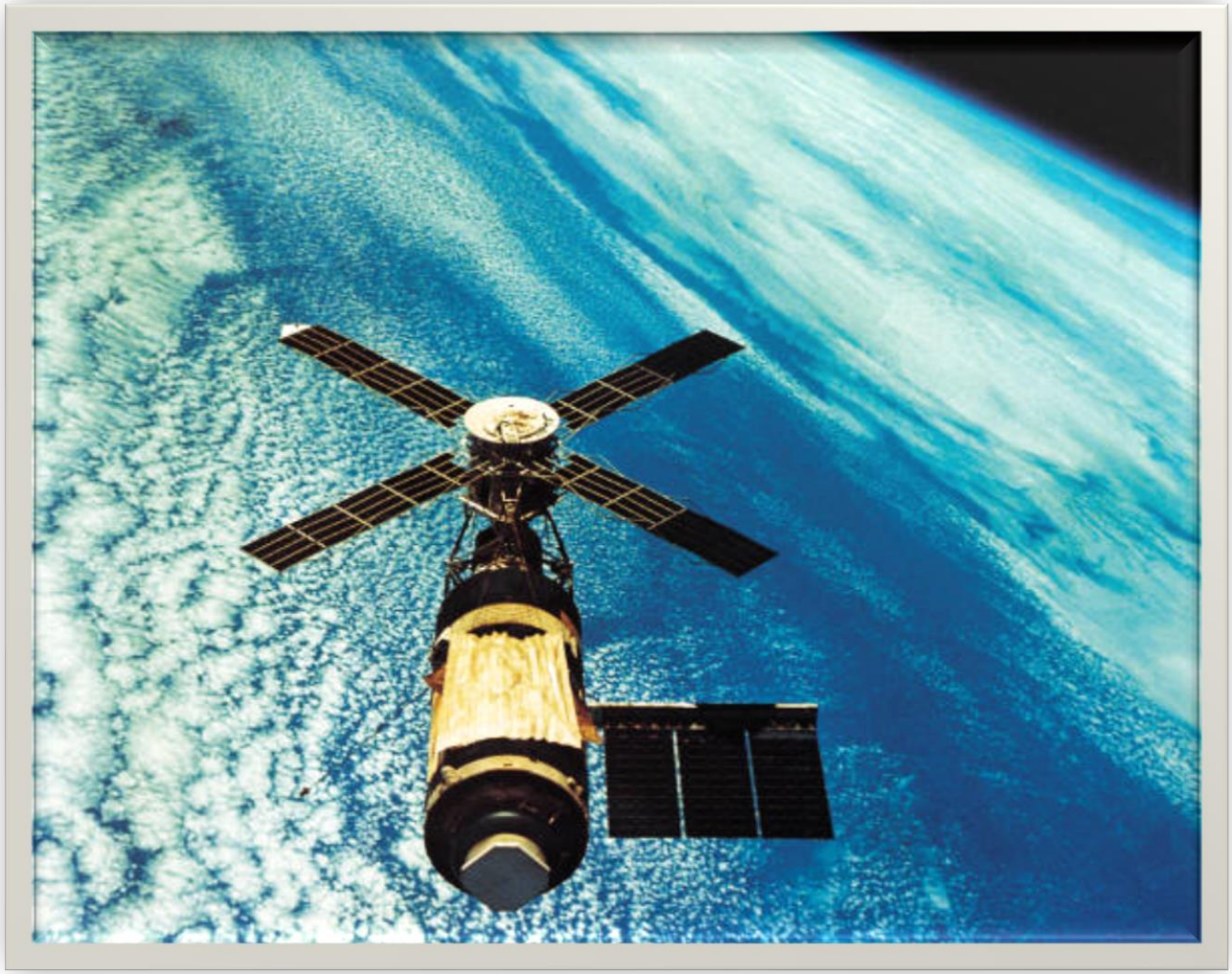
2. Problem Statement

In this assignment, you will implement a simple array-based database to store and retrieve records. In the first part of the assignment, you will implement two classes: `Record` and `DB`. The `Record` class will serve as a base class from which other types of record classes can be derived. The `DB` class will be used to create a database of `Record` objects. In the second part of the assignment, you will design and implement the class `studentRecord`, which is derived from the class `Record`. You will test your implementation with the `Driver` you wrote for Assignment 5. However, your implementation of `Record` and `DB` must work for ***any*** class that is derived from `Record`, even without any knowledge on your part of what the derived class does.

2.1 The `Record` Class

The `Record` class has fields to represent the number (key) of an individual. It also has the


THE PROBLEM WITH
ASSUMPTIONS
IS THAT THEY ALWAYS
COME WITH
BLIND
SPOTS
~ Olivier Blanchard



The New York Times

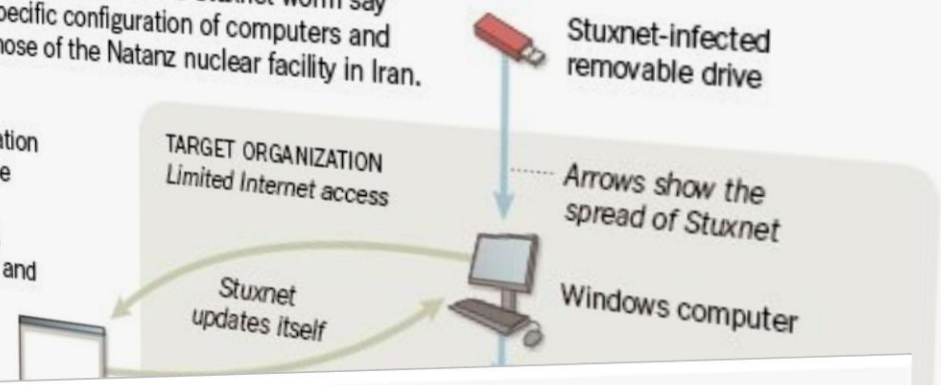
January 16, 2011

How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the



Vulnerabilities give hackers ability to open prison cells from afar

By Sean Gallagher | Published November 7, 2011 8:30 AM

Researchers have demonstrated a vulnerability in the computer systems used to control facilities at federal prisons that could allow an outsider to remotely take them over, doing everything from opening and overloading cell door mechanisms to shutting down internal communications systems. Tiffany Rad, Teague Newman, and John Strauchs, who presented their research on October 26 at the Hacker Halted information security conference in Miami, worked in Newman's basement to develop the attacks that could take control of prisons' industrial control systems and programmable logic controllers. They spent less than $2,500 and had no previous experience in dealing with those technologies.

Photos reveal NSA tampered with Cisco router prior to export

By JR Bookwalter, Routers & storage

Caught with hands in virtual cookie jar

TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station' implants a beacon

“Unauthorized code” in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

by **Dan Goodin** - Dec 17, 2015 11:50 pm UTC

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections," Juniper Chief Information officer Bob Worrall wrote. "Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS."

A separate advisory from Juniper says there are two separate vulnerabilities, but stops short of describing either as "unauthorized code." The first flaw allows unauthorized remote administrative access to an affected device over SSH or telnet. Exploits can lead to complete compromise. "The second issue may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic," the advisory said. "It is independent of the first issue. There is no way to detect that this vulnerability was exploited."

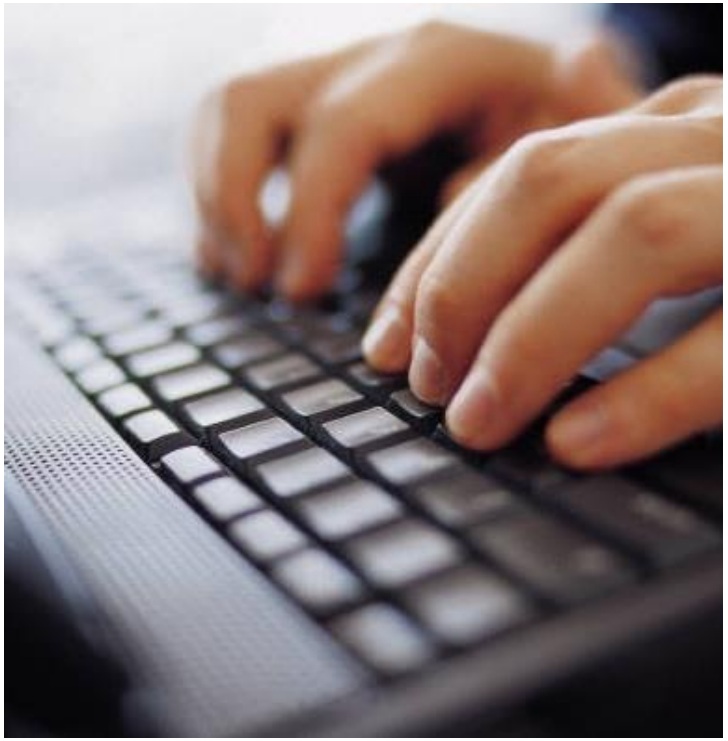
Motivation

How is this relevant to me?

Motivation: User

Software systems are ubiquitous in our daily lives

- Protect your system
- Protect your data
- Identity theft



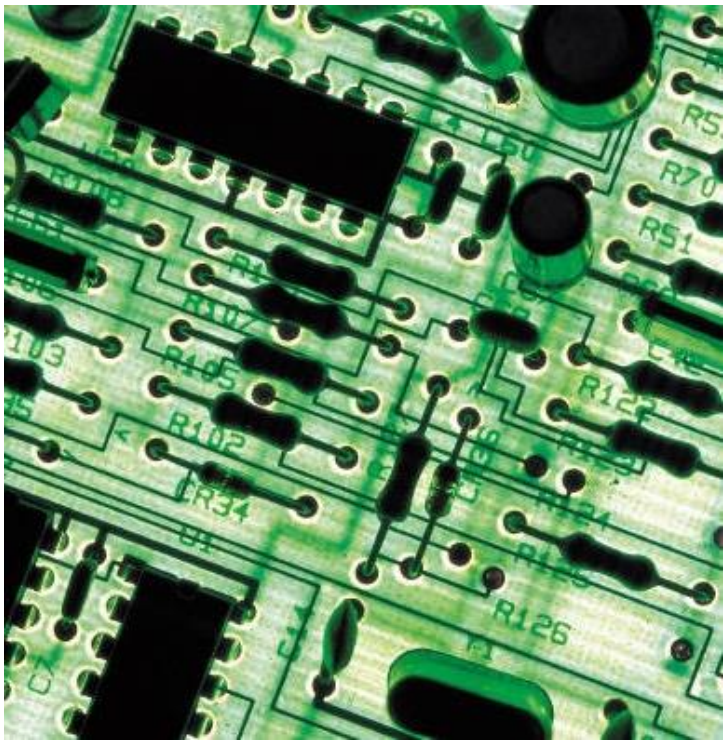

Interac


PayPal

Motivation: Engineer

Security should be a daily consideration in your work

- Challenge your design assumptions
- Understand attackers and identify risks
- Defensive coding



The Wall S

April 26, 2011

Massive Data Breach: Sony

Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

The electronics conglomerate is the latest Japanese company to come under fire for not disclosing bad news quickly. Tokyo Electric Power Co was criticized for how it handled the nuclear crisis after the March earthquake. Last year, Toyota Motor Corp was slammed for being less than forthright about problems surrounding its massive vehicle recall.

The "illegal and unauthorized person" obtained people's names, addresses, email address, birth dates, usernames, passwords, logins, security questions and more, Sony said on its U.S. PlayStation blog on Tuesday.

The shutdown of the

The Wall S

October 12, 2011

PSN Hacked Again: Sony Of

ony has confirmed "Less than one tenth of
other security breach at one percent of our PSN,
popular PlayStation SEN and SOE consumers
ork and warned that may have been affected.
93,000 user accounts There were approximately
been compromised. 93,000 accounts
(PSN/SEN: approximately
60,000 accounts; SOE:
approximately 33,000)
where the attempts
succeeded in verifying
those accounts' valid
sign-in IDs and
passwords, and we have
temporarily locked these
accounts. As a
preventative measure, we
will be sending email
notifications to these
account holders and will
be requiring secure
password resets or
informing"

st breach follows a
hack in April 2011
to the theft of
ddresses and
edit card data
o 77 million

flagged by
amount of
sign-in
to the
sign-in

statement:

Motivation: Employee

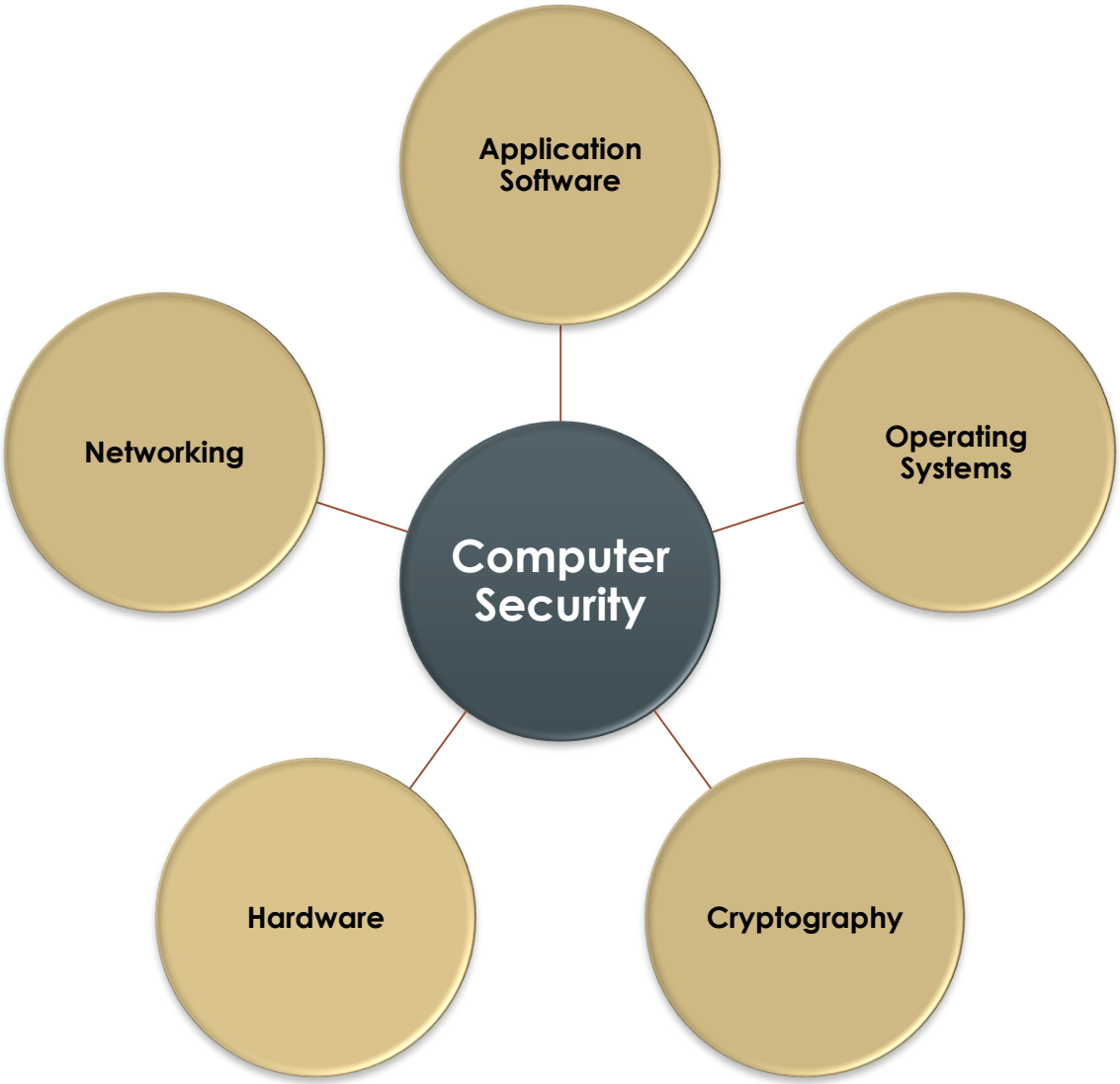
Laws increasingly hold companies accountable for poor security practice

- Protect your company
- Protection of confidential data
- Regulatory requirements

While previous generations of attacks targeted technology such as networks and servers and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses . . . These targeted and personalized attacks are difficult to prevent because they leverage human vulnerabilities and human trust.

We believe it is reasonable to assume, if an advanced attacker targets your company, that a breach is inevitable.

Kevin Mandia, October 4, 2001
Before the Permanent Select Committee on Intelligence, U.S. House of Representatives


Application Software
Networking
Operating Systems
Computer Security
Hardware
Cryptography

Computer Security

Rules and Assumptions

Rules

Like the programs that enforce them, computer systems have rules. Some rules are **explicit** and well thought out; others are **implicit** and based on assumptions.

Assumptions

Security risks occur when our assumptions turn out to be false

- Data
- Input
- User behaviour

Computer Security

Computer security is about understanding a system really well, and questioning the implicit rules

- A **reliable** system does what it is supposed to do
- A **secure** system does what it is supposed to do, and nothing else.

Computer Security

Why is it hard?

Security is a Negative Goal

Our job is to ensure that something **cannot** happen: much harder to measure / verify.

- **Positive goal:** Alice can read the file
- **Negative goal:** Bob cannot read the file

Problem: In what ways might Bob try to access the file? (Not an easy question to answer.)

Identifying the Weakest Link

- Programmers are often not trained to consider their adversaries
- The weakest part of the system will be exploited
- Expect the unexpected

Instructor

Background, Contact Info

Courtney Gibson

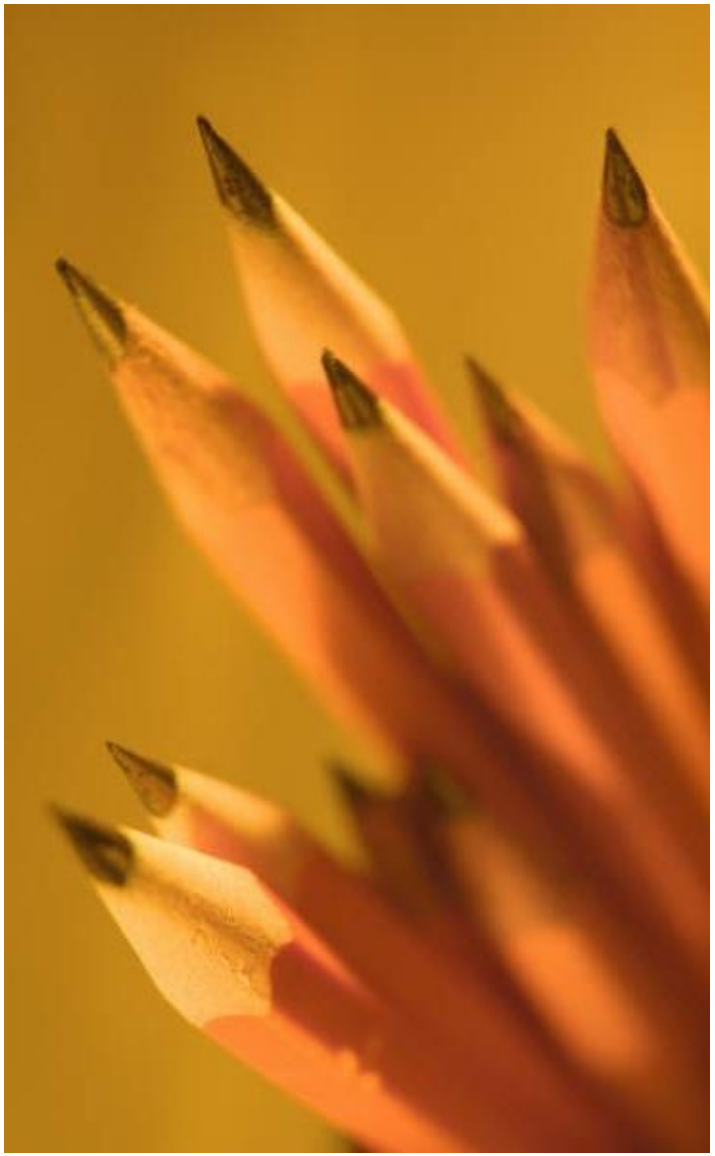
UofT Electrical and Computer Engineering
P. Eng., Adjunct Lecturer

BioConnect
Chief Technology Officer
Chief Information Security Officer

email: gibson@eecg.utoronto.ca

office hours by request

PT371 (Pratt Building)



Course Outline

Major Topics

Course Page

https://q.utoronto.ca/

Syllabus
Lecture Slides
Assignments
Past Tests
Announcements

Course Outline

Section 1: Introduction

- Course introduction
- Quick review: O/S, assembly language, software tools
- Basic principles of computer security
- Confidentiality, Integrity, Availability

Primary Learning Goals:

- Ability to explain the fundamental goals of Confidentiality, Integrity and Availability, and how they each can be applied to creating secure product designs.
- Ability to use basic software debugging tools (e.g., gdb) to analyze program stack behaviour.

Course Outline

Section 2: Software Code Vulnerabilities

- Injection-type attacks: buffer overflows, format strings, double-free, ROP, etc.
- Library attacks: encapsulation, etc.
- Defenses and good programming practice

Primary Learning Goals:

- *Ability to explain and execute the most common attacks against software vulnerabilities, in order to locate design and implementation flaws.*
- *Ability to use appropriate tools and best-practice coding techniques to protect against these types of attacks in your own work.*

Course Outline

Section 3: Cryptography

- Encryption: Symmetric (block/stream ciphers) and Public Key
- Secure key exchange
- Hashes and Signatures: MAC, HMAC, etc.
- Secure Communication Protocols: SSL, VPN

Primary Learning Goals:

- *Ability to select appropriate encryption techniques to meet both the Data Confidentiality requirements and the performance requirements of your software.*
- *Ability to securely exchange cryptographic keys over insecure network channels.*
- *Ability to use hash-based tools to provide Data Integrity and Data Authentication, through the application of MACs, HMACs and digital signatures.*

Course Outline

Section 4: Web Security

- Web authentication, cookies
- Web attacks: Cross-Site Scripting (XSS), CSRF, etc.
- SQL Injection
- Cloud security

Primary Learning Goals:

- *Ability to safely use web cookies to secure secure sessions and end-user data.*
- *Ability to execute the most common web-based attacks, in order to locate design and implementation flaws.*
- *Ability to use appopriate tools and best-practice coding techniques to protect against these types of attacks in your own work.*

Course Outline

Section 5: Access Control

- Access control models
- Hardware Security Modules (HSMs)
- Side-Channels and Covert Channels

Primary Learning Goals:

- *Ability to identify potential sources of side- and covert-channels that could be used to leak information out of both hardware- and software-based systems.*

Course Outline

Section 6: Network Security

- Network-layer security risks: BGP, ARP, DNS, TCP/IP, etc.

Primary Learning Goals:

- *Ability to identify how vulnerabilities in many standard networking protocols could be exploited by a third-party to pose risks to confidentiality, integrity and availability of your software systems.*
- *Ability to use appropriate tools and best-practice techniques to protect your own systems and designs.*

Course Outline

Section 7: Malware

- Viruses and worms

Primary Learning Goals:

- *Ability to identify the mechanisms though which computer viruses and worms propogate, and the risks these may pose to your systems.*

Course Outline

Section 8: Physical Security

- Physical security system design and vulnerabilities

Primary Learning Goal:

- *Ability to explain the most common vulnerabilities and defenses in physical security systems, and relate this to design challenges in digital security designs.*

Optional Texts

Security in Computing

- Pfleeger and Pfleeger

Computer Security: Principles & Practice

- Stallings and Brown

Applied Cryptography, 2nd Edition

- Bruce Schneier

Marking Scheme

- Labs: 25%
- Midterm: 25%
- Final Exam: 50%

The final is “Type C” (single reference sheet), no calculator.

Plagiarism

All labs, assignments and tests are to be completed with your original work. Anything submitted for credit must be something that you (and your lab partner) produced.

What to Expect

Course Covers a Lot of Material

- OS, Networking
- Mathematics of Cryptography

Where You'll Spend Your Time

- Four Labs
- Most of the work will be in the labs: course focuses on practical aspects of security

Labs

Lab 1: Identification of Vulnerabilities, Construction of Attacks

- You will be given some vulnerable programs.
- Your job is to construct attacks that will let you hijack the programs and spawn a command shell.

Labs

Labs 2-3: Network and Web Security

- ~~You will use SSL to write code to securely communicate between a client and a server.~~ (🡐 Lab 2 under revision)
- You will be given a web application. You will craft a series of attacks that exploit vulnerabilities in the application's design.

Lab 4: Single Sign-On