Course Introduction

Michael B. Spring
Information Science and Technology
University of Pittsburgh
spring@pitt.edu
http://www.sis.pitt.edu/~spring

Spring 2015 (15-4)

- Security in E-Business
  - IS 2731
  - CRN: 20485
  - Tuesday 6:00-9:00 Room 405

Contact Information
- Instructor: Michael B. Spring
- Office Location: 701B SIS Building
- Website: http://www.sis.pitt.edu/~spring
- Personal Email: spring@pitt.edu
- Class Email: mbsclass@pitt.edu
- Office Hours: Monday-Friday 8:00-6:00
- Phone: 412-624-9429

Course Expectations

- Prerequisites
  - Familiarity with basic security issues
  - Knowledge of operating systems, particularly Unix
  - Ability to write solid code in C and/or Java

- Preparation
  - Reading and thinking
  - Thinking and “doing” – beyond what I have “done”

- Engagement
  - Experimentation
  - Planning
Course Resources

• The textbook – it is to be read and digested prior to class
  • It has a companion website (in the process of being archived at http://code.google.com/p/browsersec
• The lectures – they will go beyond and around the readings and assignments
  • Lectures will be mounted on www.sis.pitt.edu/~mbsclass – take care that it may require VPN access
• The web and manuals – there is more around than you will ever digest:
  • CERT
  • NIST
  • IETF

Assignments

• There are three focused assignments:
  • PKI lab for Secure email and SSH certificates (10 points)
  • Client side application security (10 points)
  • Server side application security (10 points)
• Quizzes/Exercises: 30 points will be available via unannounced quizzes or assignments. I will determine which based on your efforts
• The instructor reserves 10 points to be awarded based on contributions and efforts
• Final Project of your choosing (30 points)

Submission of Assignments

• Assignments should be submitted to mbsclass@pitt.edu from a pitt email address. The subject should include your name, the course and the assignment. (N.B. Assignments submitted through gmail will be filtered by email security.)
• Care should be taken by students to make sure assignments submitted contain all the necessary information needed for assessment
• Plagiarism will not be tolerated. If the instructor suspects students are submitting non-original material, a grade of 0 will be submitted for the assignment and a failing grade for the course will be considered based on the infraction
Final Project Ideas

- Security Implementation Plans
  - Physical Security
  - Network Security
  - Data Security
- Laboratory Experiments
  - Digital Certificates
  - Cross Browser Vulnerabilities
  - Intrusion detection
  - Honey pot demonstrations

Course Caveats

- This course is conceptually simple and practically hard.
  - Conceptually we need to secure only three things:
    - Employees
      - Maximize confidence in trust
      - Minimize access to information
      - Audit all access
    - Systems
      - Secure all internal systems
      - Harden all publicly accessible systems (both customer and partner)
      - Review all active code for vulnerabilities (both infrastructure and application)
      - Monitor all activity
    - End Users
      - Eliminate them all (only kidding – help them avoid security pitfalls)
  - Practically, the targets and requirements change every day
  - This course is particularly difficult because of the changing nature of the threats and vulnerabilities.

Imperatives for 2731

- Develop an understanding of the vulnerabilities in various operating systems
- Understand how to insure that code for a given application is internally consistent
- Understand what a protocol is – learn how to read standards
- Understand how website security interfaces with network security
- Appreciate the problems associated with physical site security
### OS Vulnerabilities

- The two primary platforms for Web Sites are Unix and Microsoft
  - What are minimal configurations
  - What are the major problem area
  - How do you shutdown services
  - How do you automate intrusion detection
  - What are the primary mechanisms for staying up to date on issues

### Secure Coding

- Be aware of the primary coding vulnerabilities:
  - Buffer overflows
  - Cross site scripting
  - Injection
- Insure that the infrastructure code running on a server is minimally vulnerable
- Be aware of network spoofing vulnerabilities that arise from distributed applications

### Protocols

- In general, a protocol is a set of rules, or a procedure that governs the exchange of information between two processes and the rules for processing that information. (In diplomacy, it defines who is allowed to say what at what point in an interaction.)
- Protocols are defined in standards documents. These include:
  - IP/TCP and IPSEC
  - HTTP and HTTPS
  - DNS and DNSSEC
  - SSL/TLS
- Other standards also impact our ability to secure commerce on the web. These include:
  - Encryption
  - Digests
  - PKI
**Network Security**

- Network security involves those collective mechanisms for insuring that a given site is secured from network attacks. This includes:
  - Mechanisms for insuring authenticated sources
  - Mechanisms for protecting sites from intrusions
- Network security also involves those mechanisms that insure that data being transported is safe

**Physical Security**

- Physical security is as simple as backups and fire protection systems
- It also includes authentication of users who have access to the data
- It includes policies and procedures that insure data is not removed or corrupted

**Why we need the course**

- We wouldn’t need this course if:
  - The internet had been built with security in mind
  - Millions of hackers weren’t looking for someplace to have fun or make money
  - Money was not available to be made by criminals who could access personal data collected by e-businesses
  - People didn’t care about data being stolen electronically
What’s the goal

- Theoretically, we seek to provide CIA:
  - Confidentiality
  - Integrity
  - Availability
- We achieve these goals through:
  - Authentication
  - Access controls
  - Encryption
  - Digital signatures
  - Replication
  - Backup
  - Intrusion detection
  - Redundancy

What are the problems?

- The Network
  - The internet is an open broadcast channel where people can look at everything – the design of Ethernet assumed everyone would look at everything and be good citizens – no looking at other peoples “mail”
  - The internet data packets are such that they can be constructed by anyone – spoofing legitimately generated data
  - The infrastructure is weakly secured allowing third parties to take it over

What are the problems?

- Operating systems
  - Operating systems consist of a complex array of operating system services that are subject to “corruption”
  - Operating systems provide a mechanism that allows privileged processes to create children that by definition are also privileged
What are the problems

- Programmers
  - Programmers tend to be unaware of the ways in which hackers might use inferior coding to gain access to a machine
  - Programmers are people and people can be less than scrupulous about their behavior

What are the problems

- Users
  - Users are not good about their own security
  - Users have fear of what they can’t understand

What are the solutions

- Secure the infrastructure
- Authenticate the end points of the transaction
- Encrypt the data in transit
- Educate the users
Educating Users

• Describe some ways of improving security related to end users – something that might be done by you to make your users better.
• Could be something currently done or something you might propose

A Couple Examples

• Messages to protects against phishing

• Token based confirmation (also IP verification)

• Password strength feedback (also reset reminder)