

Carnegie Mellon University - School of Computer Science – Fall 2007

Web Security, Privacy and Commerce (15-421/08-731)

Draft Syllabus as of September 8, 2007

Instructor: Norman M. Sadeh
Teaching Assistant: Serge Egelman

Important Note: *This is a draft syllabus. Reading material and other details will be finalized during the course of the semester. Please consult the course blackboard for the most up to date version of the syllabus.*

Objective

The objective of this course is to introduce students to the technologies of Web Commerce, Security and Privacy as well as to related business, policy and usability issues.

Content

Over the past ten years, the Web has become an integral part of our daily life, whether at home or at work. This course provides students with an overview of the technologies and practices associated with Web Security, Privacy and Commerce.

Part I - Web Security and Privacy: Internet Security: the big picture, Introduction to Cryptography (e.g. symmetric/asymmetric cryptosystems, MACs, RSA, etc.), digital signatures, key management (e.g. Diffie Hellman Key Agreement), authentication, Internet Security protocols (incl. IPsec, VPNs, SSL/TLS, etc.), certificates & PKI, decentralized trust management, combating semantic attacks, electronic payments, web privacy (concept of privacy, privacy and the law, FTC Fair Information Practices, European Data Protection Directive, etc.). Privacy Enhancing Technologies (including P3P).

Part II – Web Commerce: Internet Marketing, Personalization, Search Technologies, eCommerce business models, Web 2.0, B2B, electronic markets and auctions, web services, P2P, etc

Part III – Mobile Commerce: This part of the course is a series of 3 lectures that looks at Mobile Commerce, revisiting many of the issues covered earlier in the course and looking at what happens when one tries to support Web Commerce on mobile devices such as cell phones.

Prerequisites

15-211 or permission of the instructor

Format

- Lectures (including guest lectures), discussions, and student presentations

Meeting Times and Venue

Tu-Th: 10:30-11:50am - NSH1305

Instructor

Prof. Norman Sadeh

Office Hours: Tu-Th: 3-4pm (Smith 227)

Email: infosec AT cs.cmu.edu (to be activated during the first week of class). Please do not send email to my personal email account.

Teaching Assistant

Teaching Assistant for full semester course:

Serge Egelman (4th year PhD student – COS PhD Program – Sch. of Computer Science)

Office Hours: Mo-Wed: 2-3pm (CIC2222A)

Email: egelman AT cs.cmu.edu

Additional Support Available from Teaching Assistant for the mini-semester course:

Abhishek Guha (2nd year graduate student - INI program)

Office Hours: Mo: 3-4pm, Fr.: 11am-noon (CIC 2312)

Email: rio AT cmu.edu

Grading

- Homework: 15% (3 assignments)
- Class Presentation: 5%
- Midterm: 20%
- Final exam: 15%
- Course project: 45%
- Class participation will be taken into account in assigning final letter grades

Late submission policy (homework assignments & project report): you loose 10% of your grade per late day.

Textbooks & Reading Material

Required Textbooks:

- “E-commerce: Business, Technology, Society”, 3rd edition, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007
- “Web Security, Privacy and Commerce”, 2nd edition, Simson Garfinkel, O’Reilly, 2002.

Optional Textbook (recommended for last few lectures)

- M-Commerce: Technologies, Services and Business Models, Norman Sadeh, Wiley, 2002.

Additional reading material will be provided for many lectures – some required and some optional.

Course Content

Lecture 1 – Aug. 28, 2007

Topic: **Course Overview**

Lecturer: Norman Sadeh

Reading Material : Slides

Venue: NSH 1305

Lecture 2 – Aug 30, 2007

Topic: **Web Security and Privacy: The Big Picture**

Lecturer: Norman Sadeh

Venue: NSH 1305

Reading Material:

- Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 1 & 2 (Ch. 2 will not be covered in class but you should make sure you are familiar with its content)
- E-commerce: Business, Technology, Society”, 3rd edition, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007. Ch. 5

By 5pm on Aug 31, class presentation proposals are due: 1 paragraph, including topic description and team composition – 3 people per team – to be emailed to [infosec AT cs.cmu.edu](mailto:infosec@cs.cmu.edu) (please copy also [rio AT cmu.edu](mailto:rio@cs.cmu.edu))

Homework Assignment #1 out by Aug 31 (topics: Security: General Considerations & Use of Private and Public Keys)

Lecture 3 – Sept. 4, 2007

Topic: **Introduction to Cryptography**

Lecturer: Norman Sadeh

Reading Material :

Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 3

Venue: NSH 1305

Lecture 4 – Sept. 6, 2007

Topic: **Digital Signatures & Key Management**

Lecturer: Norman Sadeh

Reading Material : Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 3 & 4

Venue: NSH 1305

Lecture 5 – Sept. 11, 2007

Topic: **Authentication**

Lecturer: Norman Sadeh

Reading Material: Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 4 and 6.

Venue: NSH 1305

Student Presentation: *Digital Watermarking and Steganography*

Lecture 6 – Sept. 13, 2007

Topic: **Internet Security Protocols**

Guest Speaker: Dr. Paul Drielsma

Reading Material :

- Required: Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 4&5
- Optional: Secure Electronic Commerce”, Warwick Ford and Michael S. Baum, 2nd edition, Prentice Hall PTR, 2001. Section 5.1-5-5

Venue: NSH 1305

Student Presentation: *Intrusion Detection*

Homework Assignment #1 due by 5pm Sept 14

Homework Assignment #2 out by Sept 14 (topics: PKI and Cyber Law)

Lecture 7 – Sept. 18, 2007

Topic: **Certificates & PKI**

Lecturer: Norman Sadeh

Reading Material: Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), Ch. 6 and 7.

Venue: NSH 1305

Lecture 8 – Sept. 20, 2007

Topic: **Trust Management**

Lecturer: Norman Sadeh

Reading Material: to be provided

Venue: NSH 1305

Student Presentation: *CAPTCHAs*

Lecture 9 – Sept. 25, 2007

Topic: **Early Project Presentations**

Lecturer: *Student teams – 10 minutes per team*

Reading Material: none

Venue: NSH 1305

Lecture 10 – Sept. 27, 2007

Topic: **Information Privacy & Web Privacy – incl. legal & regulatory landscape in the US and abroad**

Lecturer: Norman Sadeh

Reading Material:

- E-commerce, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007 – Chapter 9

Venue: NSH 1305

Student Presentation: *VoIP and CALEA*

Homework Assignment #2 due by 5pm on Sept. 28, 2007 – assignments should be turned in using Blackboard.

Homework Assignment #3 out by Sept 28 (topics: Ethical, Social and Policy issues, including Privacy, and Combating Phishing Attacks)

Lecture 11 – Oct. 2, 2007

Topic: **Decentralized Trust Management: Proof Carrying Authorization and the Grey System**

Guest Speaker: Dr. Lujó Bauer

Reading Material: to be provided

Venue: NSH 1305

Student Presentation: *RFID Security*

Lecture 12 – Oct. 4, 2007

Topic: **Combating eCrime with a particular focus on Combating Phishing Attacks**

Venue: **APWG eCrime Research Summit** (in Pittsburgh)

(see <http://www.ecrimeresearch.org/2007/program.html>) - additional details to be provided

Important Note: Students will be given passes to attend the keynote, technical sessions and panels on October 4. You are expected to select and attend one of the following:

- a session consisting of at least 2 refereed paper presentations,
- a keynote presentation, or
- a panel

As part of Homework Assignment #3, you will be expected to provide a summary of the session you attended and answer some questions. You are welcome to attend more sessions if you wish but will not have access to the social events (unless you decide to register for the conference). Additional details will be provided.

Lecture 13 – Oct. 9, 2007

Topic: **Privacy Enhancing Technologies (PETs)**

Lecturer: Norman Sadeh

• Reading Material: Web Security, Privacy and Commerce, Simson Garfinkel, O'Reilly, 2002 (2nd edition), ch. 24

Venue: NSH 1305

Student Presentation: *Multifactor Authentication for the Internet Banking Environment*

Lecture 14 – Oct. 11, 2007

Topic: **Electronic Payments**

Lecturer: Norman Sadeh

Venue: NSH 1305

Reading Material : E-commerce: Business, Technology, Society”, 3rd edition, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007. Ch. 6
Student Presentation: *eBay: Loopholes and Exploits*

Optional Event: October 12, 2007

Topic: **Service Oriented Architectures (SOA)**

We have made arrangements to have IBM staff come to Carnegie Mellon University for a one-day training session on Service-Oriented Architecture. Students are strongly encouraged to attend this event, as it is closely related to the course and is **likely to include material that could help your class project**. At the same time, attendance of this event is optional and material covered as part of the SOA day will not be part of the midterm or final exams (unless also covered in class).

Homework Assignment #3 due by 5pm on Oct 13, 2007 – assignments should be turned in using Blackboard.

MIDTERM EXAM – Oct. 16, 2007

Venue: NSH 1305

Lecture 15 – Oct. 18, 2007

Topic: **Web Commerce: The Big Picture – Including Business Models**

Lecturer: Norman Sadeh

Venue: NSH 1305

Reading Material : E-commerce, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007 – Chapter 1 and 2.

Student Presentation: *Sanitizing User Generated Content on Web 2.0*

Lecture 16 – Oct 23, 2007

Topic: **Search Technologies**

Lecturer: Norman Sadeh

Reading Material: TBD

Venue: NSH 1305

Student Presentation: *Semantic Web*

Lecture 17 – Oct. 25, 2007

Topic: **Mid-semester Project Presentations**

Lecturer: *Student teams – 10 minutes per team*

Reading Material : none

Venue: NSH 1305

Lecture 18 – Oct. 30 , 2007

Topic: **Guest Lecture from Vivisimo**

Lecturer: Raul Valdes-Perez, CEO

Reading Material: TBD

Venue: NSH 1305

Student Presentation: TBD

Lecture 19 – Nov 1, 2007

Topic: **B2B and Electronic Marketplaces**

Lecturer: Norman Sadeh

Reading Material :

- E-commerce, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007 – Chapter 12 and 13

Venue: NSH 1305

Student Presentation: *Biometric Security Techniques*

Lecture 20 – Nov. 6, 2007

Topic: **Auctions at CombineNet**

Lecturer: Dr. William Walsh, CombineNet

Reading Material : TBD

Venue: NSH 1305

Lecture 21 – Nov. 8, 2007

Topic: **Internet Marketing & Personalization**

Lecturer: Norman Sadeh

Reading Material :

- E-commerce, Kenneth C. Laudon and Carol Guercio Traver, Addison Wesley, 2007 – Chapter 7 and 8

Venue: NSH 1305

Student Presentation: *Privacy Issues relating to copyright security measures in recent softwares*

Student Presentation: *Overview of Social Networking Sites – Privacy Issues and Business Models*

Lecture 22 – Nov 13, 2007

Topic: **Peer-To-Peer Technologies and Services**

Lecturer: Norman Sadeh

Reading Material: “Peer-To-Peer Computing”, Milojevic et al., HP Labs, March 2002 – <http://www.hpl.hp.com/techreports/2002/HPL-2002-57.pdf>

Venue: NSH 1305

Student Presentation: *DMCA – Overview, Principles, Controversies and Recent Cases*

Lecture 23 – Nov. 15, 2007

Topic: **The Mobile Internet**

Lecturer: Norman Sadeh

Reading Material : slides

- Optional reading material: M-Commerce: Technologies, Services and Business Models, Norman Sadeh, Wiley, 2002, ch. 4

Venue: NSH 1305

Student Presentation: *XHTML + Voice*

No Lecture on Nov. 20, 2007 – Students to work on their projects

No Lecture on Nov. 23, 2007 – Thanksgiving Break

Lecture 24 – Nov. 27, 2007

Topic: **Mobile Security & Mobile Payment**

Lecturer: Norman Sadeh

Reading Material : slides

- Optional reading material: M-Commerce: Technologies, Services and Business Models, Norman Sadeh, Wiley, 2002, ch. 5

Venue: NSH 1305

Student Presentation: *Cross-Site Scripting*

Lecture 25 – Nov. 29, 2007

Topic: **Mobile Commerce Today and Tomorrow**

Lecturer: Norman Sadeh

Reading Material : slides

- Optional reading material: M-Commerce: Technologies, Services and Business Models, Norman Sadeh, Wiley, 2002, ch. 6, 7 and 8

Venue: NSH 1305

Student Presentation: *WebSpam*

Lecture 26 & 27 – Dec. 4 and 6, 2007

Topic: **Final Project Presentations**

Lecturer: Student Teams

Format: ***20 minute presentation by each team – including prototype demo***

Venue: NSH 1305

Midnight on Friday December 7, 2007 –Final project report to be emailed to [websec AT cs.cmu.edu](mailto:websec@cs.cmu.edu) and [sadeh AT cs.cmu.edu](mailto:sadeh@cs.cmu.edu)

FINAL EXAM – Date and venue TBA