Graduate Course
on

Computer Security

Iliano Cervesato **iliano@itd.nrl.navy.mil**

ITT Industries, Inc @ NRL - Washington DC

http://www.cs.stanford.edu/~iliano/

Scope of this Course

A broad introduction to basic concepts and techniques in computer and network Security

- Information assurance
  - Access control
  - Information flow

  } 1 hour
- Elements of cryptography } 2 hours
- Cryptographic protocols
  - Goals
  - Examples
  - Attacks

  } 7 hours

This Course is **not** about

- Engineering
  - Web sites
  - Computer viruses
  - …
- Countermeasures
  - Intrusion detection
  - Survivability
  - Legal matters
  - …
- Electronic commerce
  - Auctions
  - Electronic cash
  - …
- Other
  - Electronic votation
  - Database security
  - …

Prerequisites

Some familiarity with …

- Networking
- Software Engineering
- Programming languages
- Operating systems

(Computer Science)

- Formal notation
- Mathematical logic
- Number theory

(Mathematics)

… plus

- Interests in solving and creating puzzles
- Curiosity

Outline

- Lecture 1: Information Assurance
- Lecture 2: Shared-Key Cryptography
- Lecture 3: Public-Key Cryptography
- Lecture 4: Authentication Protocols
- Lecture 5: Case Study I: Kerberos V

Outline (cont'd)

- Lecture 6: Case Study II: WEP
- Lecture 7: Specification Languages
- Lecture 8: Intruder Models
- Lecture 9: Automated Verification
- Lecture 10: Beyond Authentication

Readings

- Neal Stephenson, *Cryptonomicon*, 1999

Technical references in each lecture

- Optional
- Enlightening, and some even enjoyable

Acknowledgments

This course includes material from

- Course by Dan Boneh
  - "Introduction to Cryptography and Computer Security"
  - http://crypto.stanford.edu/~dabo/courses/cs255_winter01/
- Course by Martín Abadi
  - "Topics in Security"
  - http://www.cse.ucsc.edu/~abadi/CS290X_F01/home.html
- Course by Paul Syverson
  - "Foundations of Computer Security"
  - http://www.cs.stanford.edu/~iliano/slides/fosad00.ppt
- Slides by Jesse Walker
  - "Overview of 802.11 Security"
  - http://www.cs.umd.edu/~waa/wireless.html

Exam and Homework

- An exercise at the end of each session
- A final exam at the end of the course
  - 1 week to complete (14 Dec. 2001)
  - Solution by email to `iliano@itd.nrl.navy.mil`
  - Grades 1 week later (21 Dec. 2001)

Enjoy!