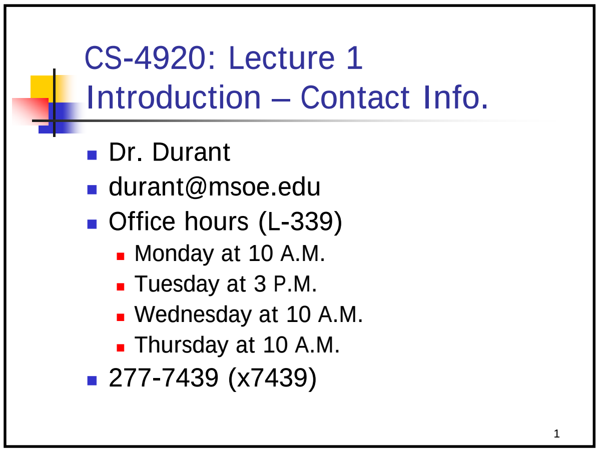
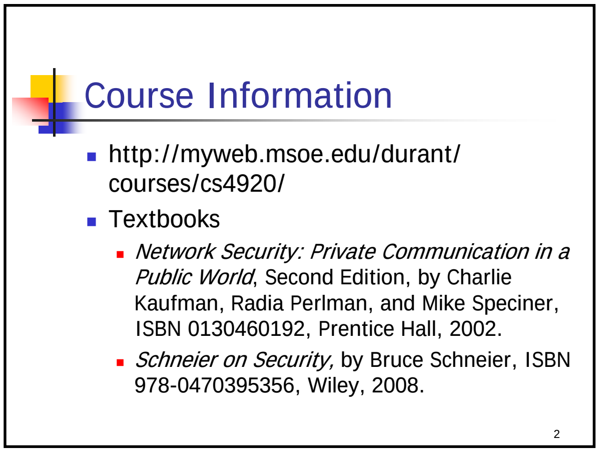


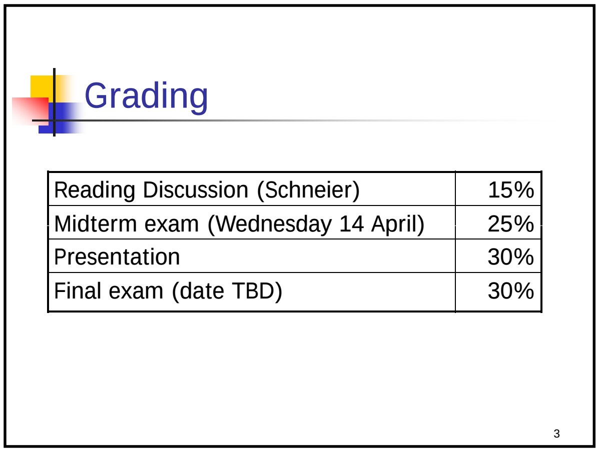
CS-4920: Lecture 1 Introduction – Contact Info.

- Dr. Durant
- durant@msoe.edu
- Office hours (L-339)
  - Monday at 10 A.M.
  - Tuesday at 3 P.M.
  - Wednesday at 10 A.M.
  - Thursday at 10 A.M.
- 277-7439 (x7439)



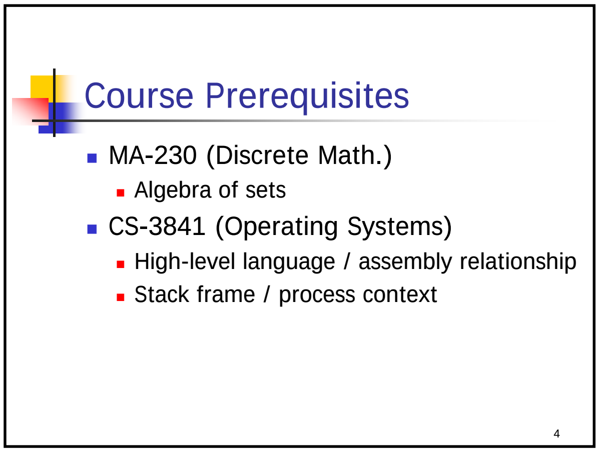
Course Information

- http://myweb.msoe.edu/durant/courses/cs4920/
- Textbooks
  - *Network Security: Private Communication in a Public World*, Second Edition, by Charlie Kaufman, Radia Perlman, and Mike Speciner, ISBN 0130460192, Prentice Hall, 2002.
  - *Schneier on Security,* by Bruce Schneier, ISBN 978-0470395356, Wiley, 2008.



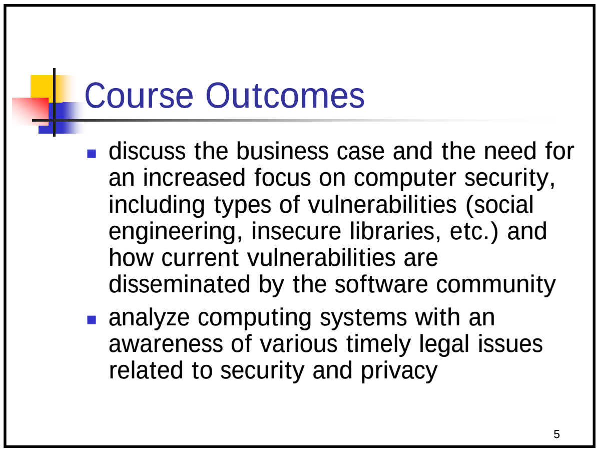
Grading

Reading Discussion (Schneier)	15%
Midterm exam (Wednesday 14 April)	25%
Presentation	30%
Final exam (date TBD)	30%



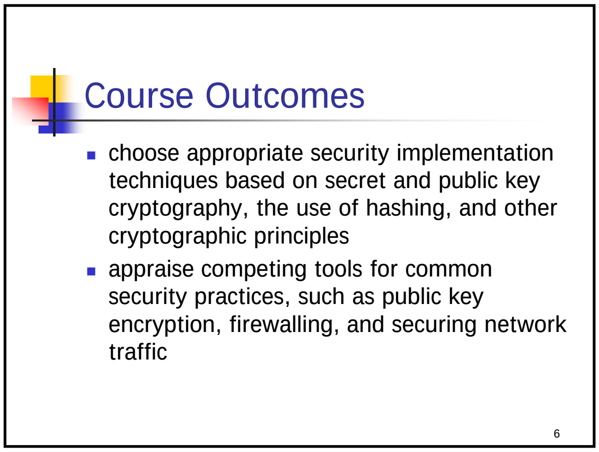
Course Prerequisites

- MA-230 (Discrete Math.)
  - Algebra of sets
- CS-3841 (Operating Systems)
  - High-level language / assembly relationship
  - Stack frame / process context



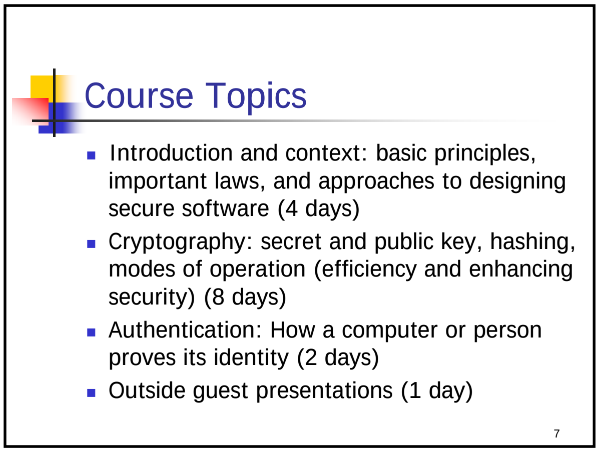
Course Outcomes

- discuss the business case and the need for an increased focus on computer security, including types of vulnerabilities (social engineering, insecure libraries, etc.) and how current vulnerabilities are disseminated by the software community
- analyze computing systems with an awareness of various timely legal issues related to security and privacy



Course Outcomes

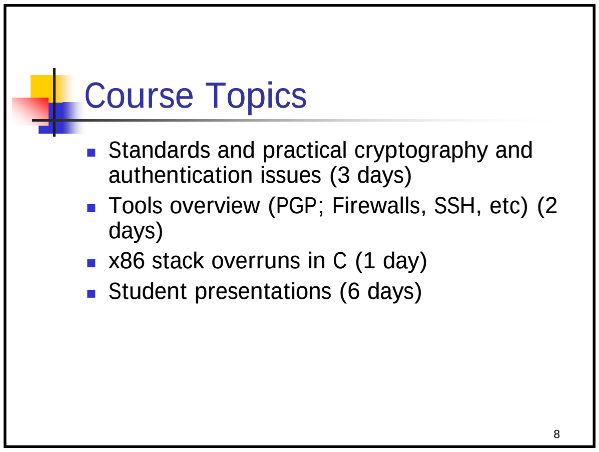
- choose appropriate security implementation techniques based on secret and public key cryptography, the use of hashing, and other cryptographic principles
- appraise competing tools for common security practices, such as public key encryption, firewalling, and securing network traffic



Course Topics

- Introduction and context: basic principles, important laws, and approaches to designing secure software (4 days)
- Cryptography: secret and public key, hashing, modes of operation (efficiency and enhancing security) (8 days)
- Authentication: How a computer or person proves its identity (2 days)
- Outside guest presentations (1 day)

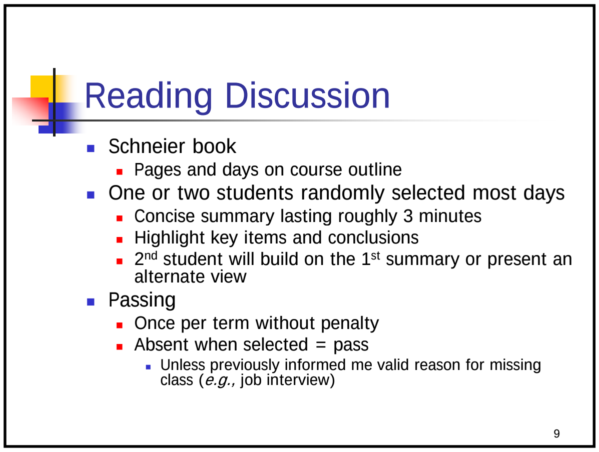
7



Course Topics

- Standards and practical cryptography and authentication issues (3 days)
- Tools overview (PGP; Firewalls, SSH, etc) (2 days)
- x86 stack overruns in C (1 day)
- Student presentations (6 days)

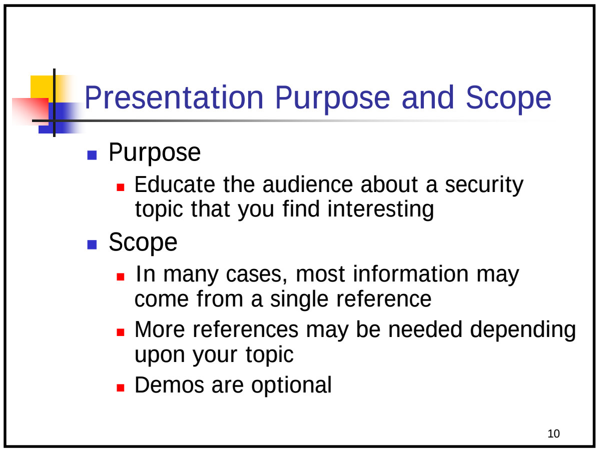
8



Reading Discussion

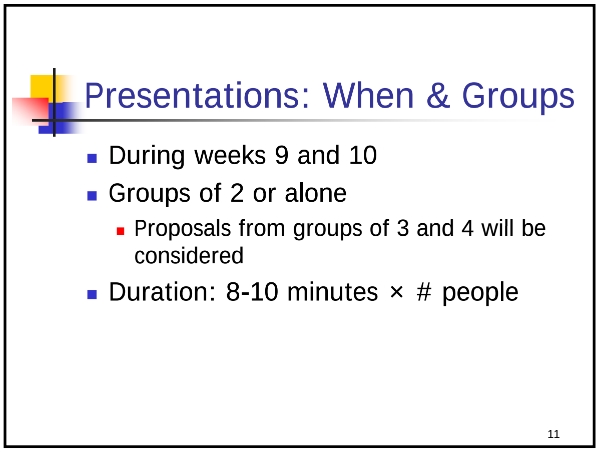
- Schneier book
  - Pages and days on course outline
- One or two students randomly selected most days
  - Concise summary lasting roughly 3 minutes
  - Highlight key items and conclusions
  - 2nd student will build on the 1st summary or present an alternate view
- Passing
  - Once per term without penalty
  - Absent when selected = pass
    - Unless previously informed me valid reason for missing class (*e.g.,* job interview)

9



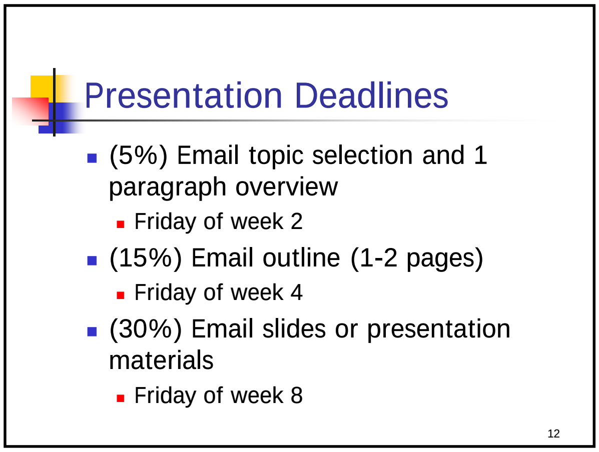
Presentation Purpose and Scope

- Purpose
  - Educate the audience about a security topic that you find interesting
- Scope
  - In many cases, most information may come from a single reference
  - More references may be needed depending upon your topic
  - Demos are optional



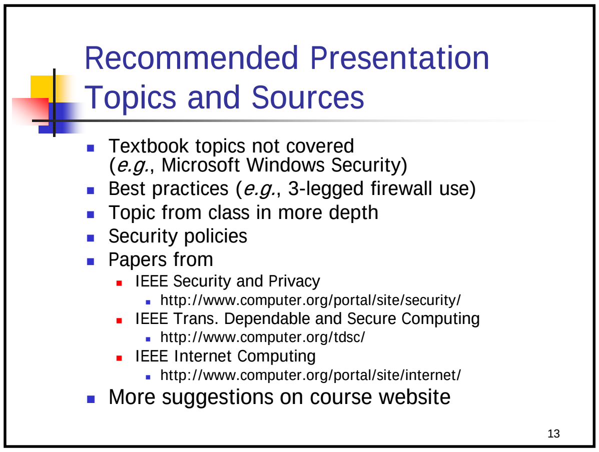
Presentations: When & Groups

- During weeks 9 and 10
- Groups of 2 or alone
  - Proposals from groups of 3 and 4 will be considered
- Duration: 8-10 minutes × # people



Presentation Deadlines

- (5%) Email topic selection and 1 paragraph overview
  - Friday of week 2
- (15%) Email outline (1-2 pages)
  - Friday of week 4
- (30%) Email slides or presentation materials
  - Friday of week 8



Recommended Presentation Topics and Sources

- Textbook topics not covered
  (*e.g.*, Microsoft Windows Security)
- Best practices (*e.g.*, 3-legged firewall use)
- Topic from class in more depth
- Security policies
- Papers from
  - IEEE Security and Privacy
    - http://www.computer.org/portal/site/security/
  - IEEE Trans. Dependable and Secure Computing
    - http://www.computer.org/tdsc/
  - IEEE Internet Computing
    - http://www.computer.org/portal/site/internet/
- More suggestions on course website

13