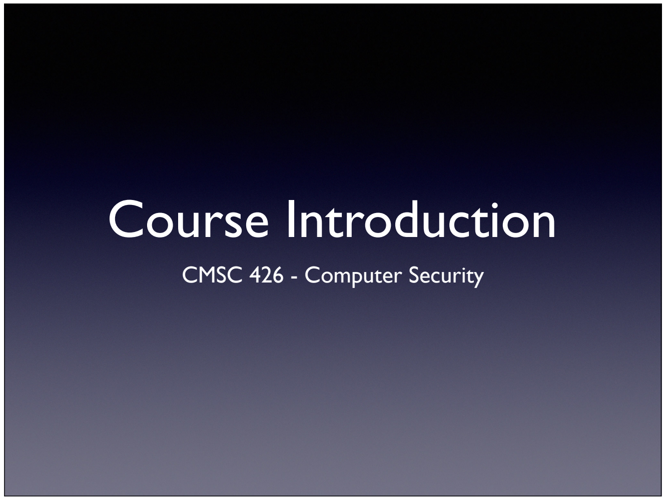
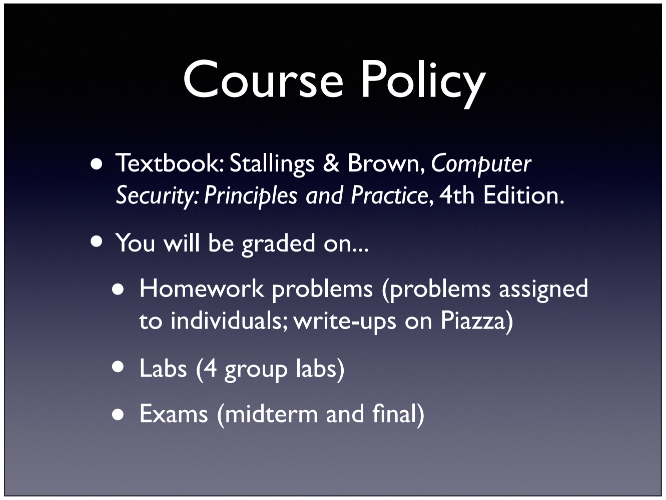


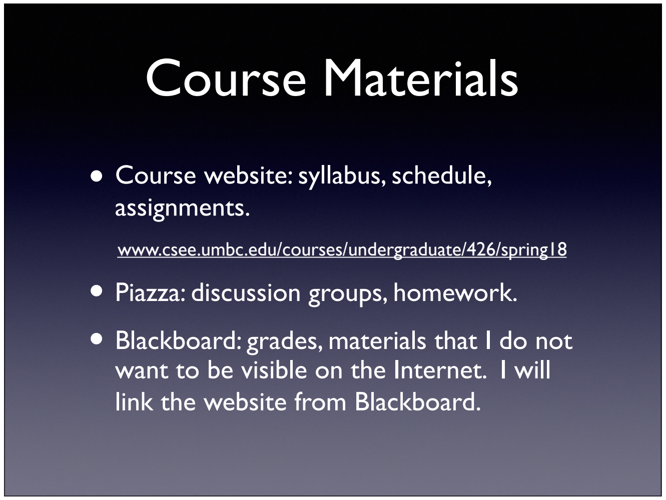
Course Introduction

CMSC 426 - Computer Security



Course Policy

- Textbook: Stallings & Brown, *Computer Security: Principles and Practice*, 4th Edition.
- You will be graded on...
  - Homework problems (problems assigned to individuals; write-ups on Piazza)
  - Labs (4 group labs)
  - Exams (midterm and final)

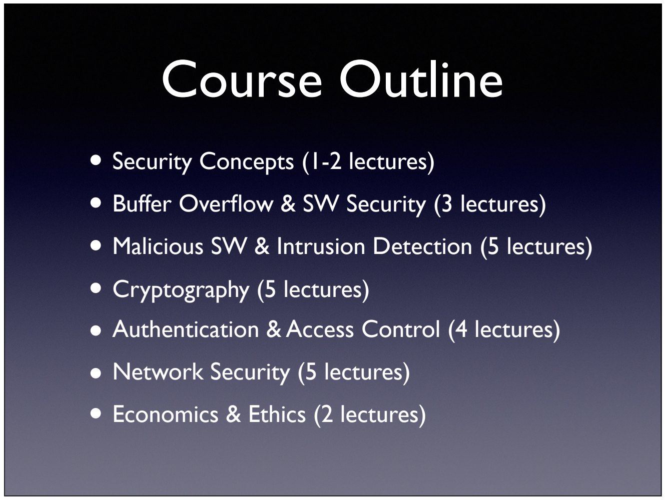


Course Materials

- Course website: syllabus, schedule, assignments.

  www.csee.umbc.edu/courses/undergraduate/426/spring18

- Piazza: discussion groups, homework.
- Blackboard: grades, materials that I do not want to be visible on the Internet. I will link the website from Blackboard.



Course Outline

- Security Concepts (1-2 lectures)
- Buffer Overflow & SW Security (3 lectures)
- Malicious SW & Intrusion Detection (5 lectures)
- Cryptography (5 lectures)
- Authentication & Access Control (4 lectures)
- Network Security (5 lectures)
- Economics & Ethics (2 lectures)

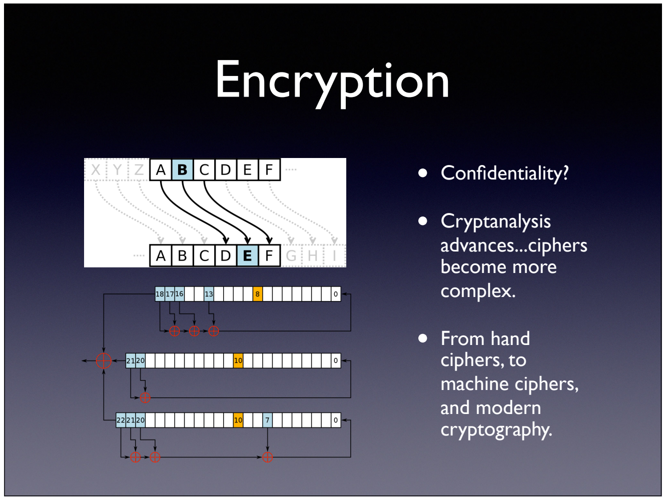
A Brief History of Security Technologies

Culmstock Beacon

- Confidentiality?
- Availability?

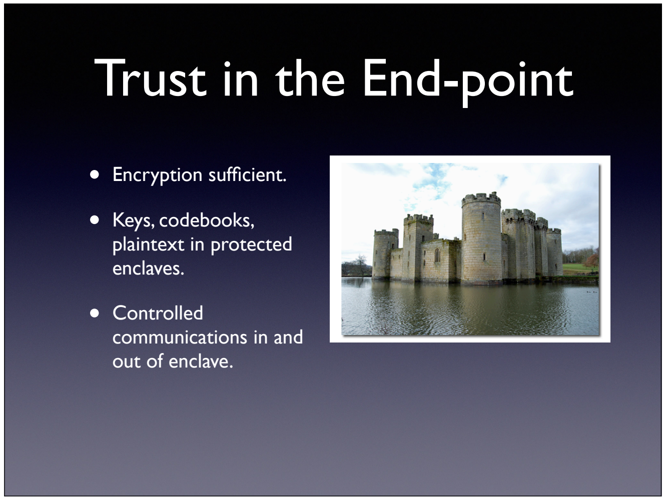
Wax Seal

- Confidentiality?
- Integrity?
- Who or what does a user have to trust?



Encryption

- Confidentiality?
- Cryptanalysis advances...ciphers become more complex.
- From hand ciphers, to machine ciphers, and modern cryptography.

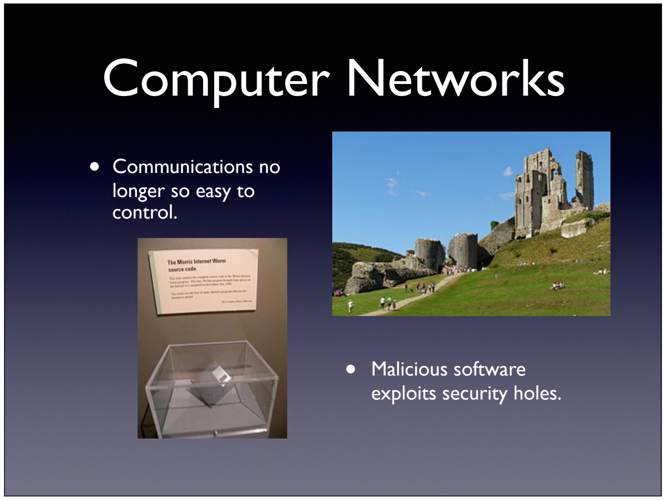


Trust in the End-point

- Encryption sufficient.
- Keys, codebooks, plaintext in protected enclaves.
- Controlled communications in and out of enclave.

Encryption Machines

- SIGSALY - World War II secure voice.
- M-209 - World War II and Korean War tactical encryptor.



Computer Networks

- Communications no longer so easy to control.

The Morris Internet Worm
source code

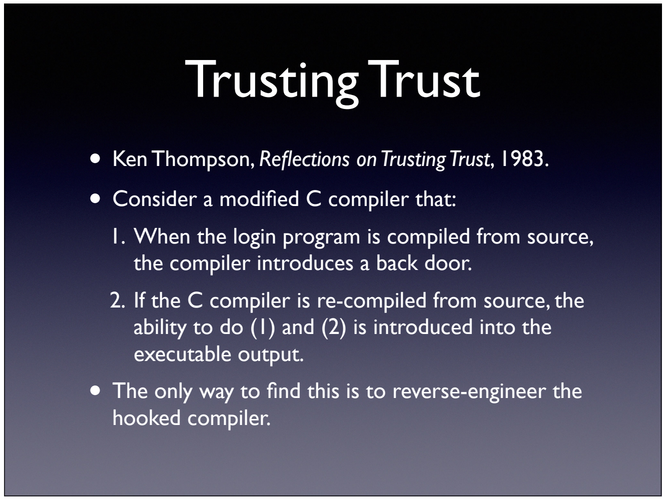
- Malicious software exploits security holes.

Network Security

- Authentication & Access Control
- Firewalls
- VPNs
- Intrusion Detection & Prevention

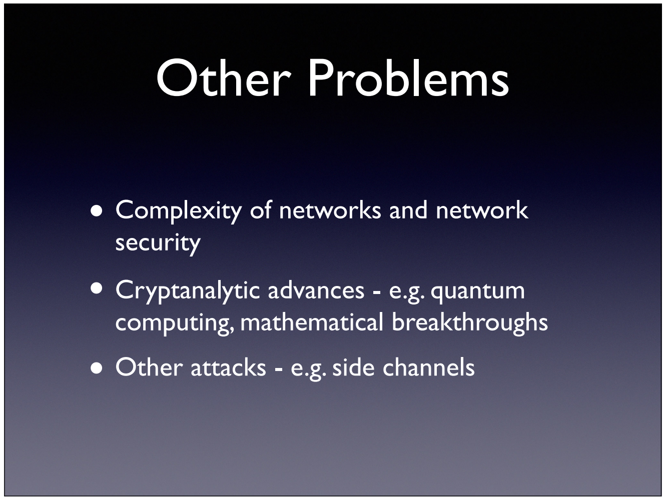
Air Force
Marine Corps
Army
Navy
Doe, Jane Marie
TSGT

How secure can we be?



Trusting Trust

- Ken Thompson, *Reflections on Trusting Trust*, 1983.
- Consider a modified C compiler that:
  1. When the login program is compiled from source, the compiler introduces a back door.
  2. If the C compiler is re-compiled from source, the ability to do (1) and (2) is introduced into the executable output.
- The only way to find this is to reverse-engineer the hooked compiler.



Other Problems

- Complexity of networks and network security
- Cryptanalytic advances - e.g. quantum computing, mathematical breakthroughs
- Other attacks - e.g. side channels

TEMPEST Demo

Next Time: Security Concepts