Welcome to:

Computer Science 356
Systems Security

Spring 2013

Dan Massey

Administrivia

- Website:http://www.cs.colostate.edu/~cs356
  - Syllabus, Outline, Grading Policies
  - Homework and Projects
  - Assignments Already Posted!
- Instructor: Dan Massey
  - Office hours: COMSC 360
    Tues 9-10 am and Thur 3:30-4pm
  - Email: massey@cs.colostate.edu
- Teaching Assistant: Chengyu Fan
  - Office hours: TBA
  - Email: cs356@cs.colostate.edu

Grading and Policies

- Grading
  - 10% Weekly Homework
  - 30% Projects
  - 30% Midterm
  - 30% Final
- Grading Policy
  - No credit for late homework. No exceptions.
  - No late projects. No exceptions.
  - No make-up exams. No exceptions.
    - It is *your responsibility* to check for conflicts for Final Exam and make necessary arrangements.

Workload

- Weekly Reading and Homework Assignments
  - Assigned every Tuesday. Due following Tuesday. (10% of grade)
  - ***Homework 1 is due Tuesday***
- Course Projects
  - Build in hands-on exercises
- Exams
  - Midterm (30% of grade) + final (comprehensive) (30% of grade)
  - In class, closed book, one double-sided cheat sheet allowed

Cheating Policy

- Simple cheating policy
  - Anyone caught cheating will FAIL the CLASS!
  - Regardless of what you cheated in, so think carefully before you cheat.
- Plagiarism – see definition
  - http://writing.colostate.edu/guides/teaching/plagiarism/
- Conflict Resolution web site
  - http://www.conflictresolution.colostate.edu/

Text, Slides, and Projects

- Computer Security: Principles and Practice
  - Second Edition by William Stallings and Lawrie Brown
  - Schedule and lecture slides indicate next topic
  - ***Required to read the material prior to lecture***
- Lecture Slides
  - Posted online after lecture
  - Based on lecture slides by Lawrie Brown

On to the Material!

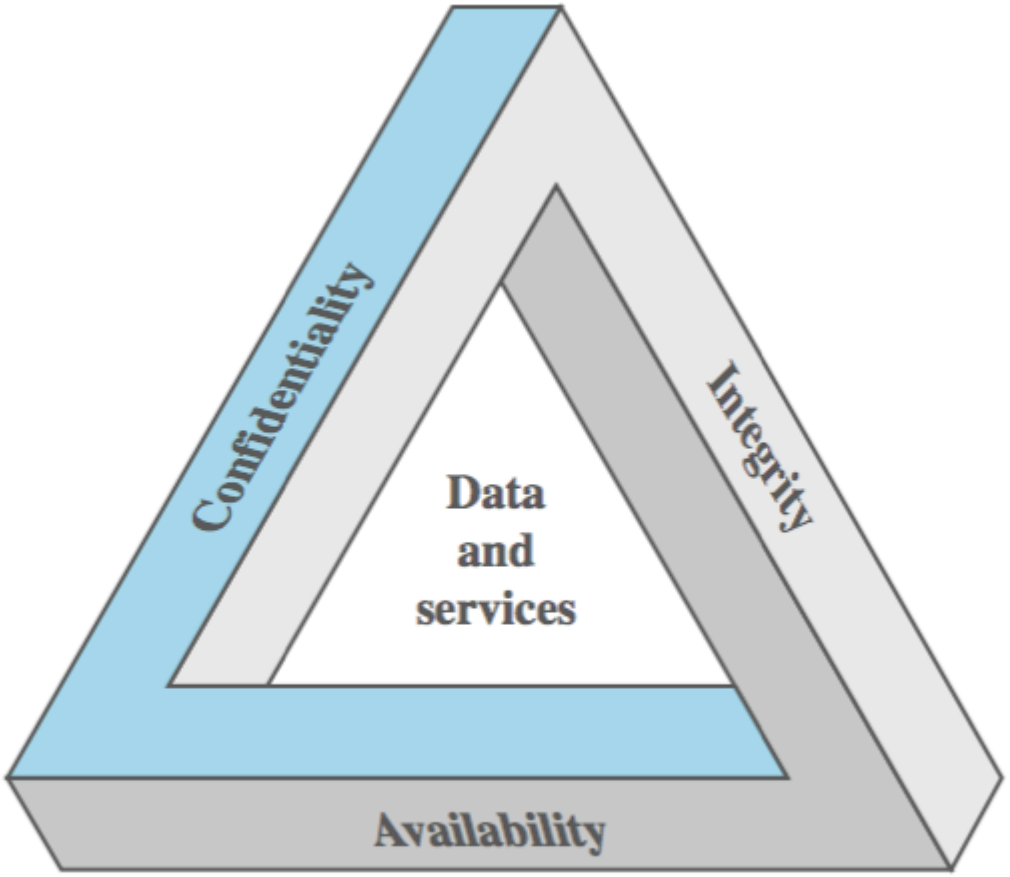
Any questions so far?

Chapter 1
Overview

Overview

Computer Security: protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

Key Security Concepts



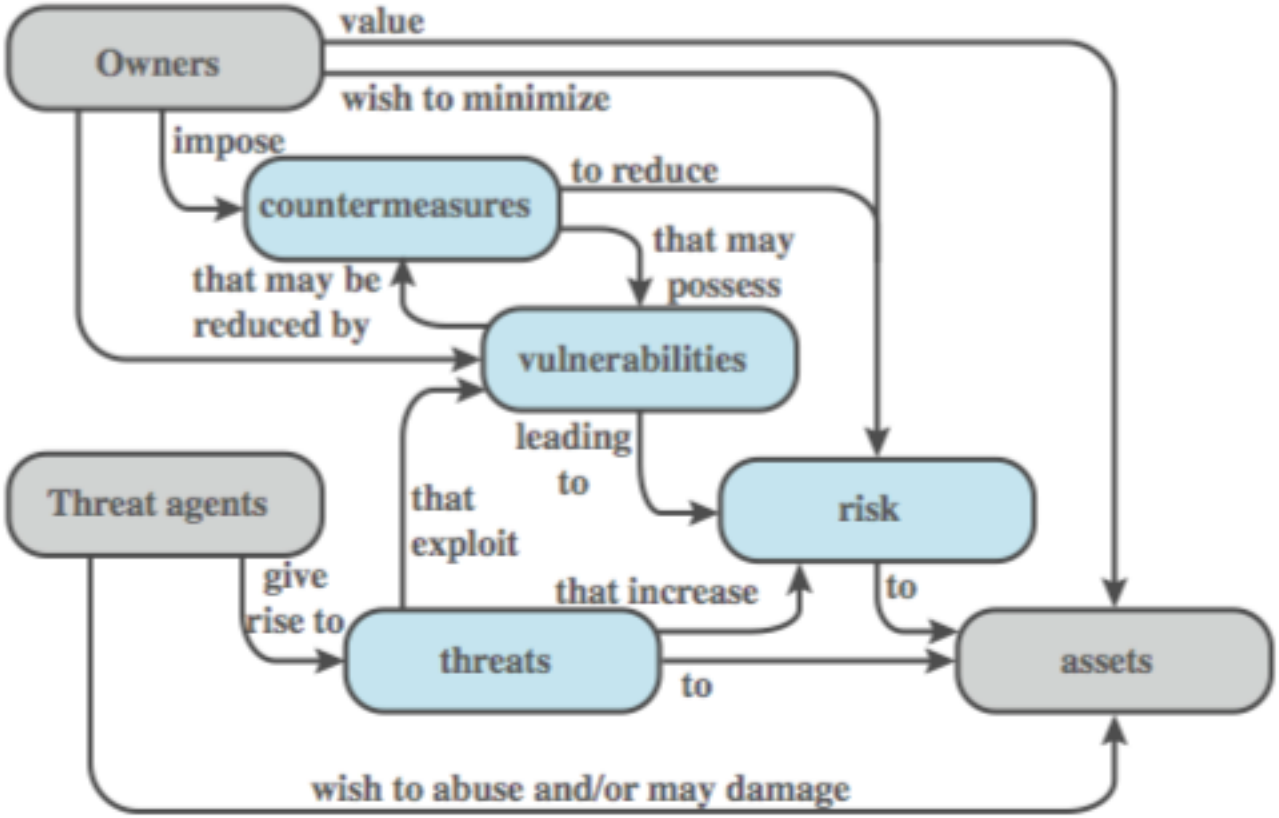
Essential Terminology

- Integrity
  - Guard against improper information modification or destruction
- Confidentiality:
  - Preserve authorized restrictions on information access and disclosure
- Availability
  - Ensure time and reliable access to and use of information
- Authenticity
  - Verifying that users are who they and that the transmission was valid
- Accountability
  - Actions of an entity can be traced uniquely to that entity

Computer Security Challenges

1. Not simple
2. Must consider potential attacks
3. Procedures used counter-intuitive
4. Involve algorithms and secret info
5. Must decide where to deploy mechanisms
6. Battle of wits between attacker / admin
7. Not perceived on benefit until fails
8. Requires regular monitoring
9. Too often an after-thought
10. Regarded as impediment to using system

Security Terminology



Vulnerabilities and Attacks

- System resource vulnerabilities may
  - be corrupted (loss of integrity)
  - become leaky (loss of confidentiality)
  - become unavailable (loss of availability)
- Attacks are threats carried out and may be
  - passive
  - active
  - insider
  - outsider

Countermeasures

- Means used to deal with security attacks
  - Prevent
  - Detect
  - Recover
- May result in new vulnerabilities
- Will have residual vulnerability
- Goal is to minimize risk given constraints

Threat Consequences

- Unauthorized disclosure
  - exposure, interception, inference, intrusion
- Deception
  - masquerade, falsification, repudiation
- Disruption
  - incapacitation, corruption, obstruction
- Usurpation
  - misappropriation, misuse

Network Security Attacks

- Classify as passive or active
- Passive attacks are eavesdropping
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent
- Active attacks modify/fake data
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

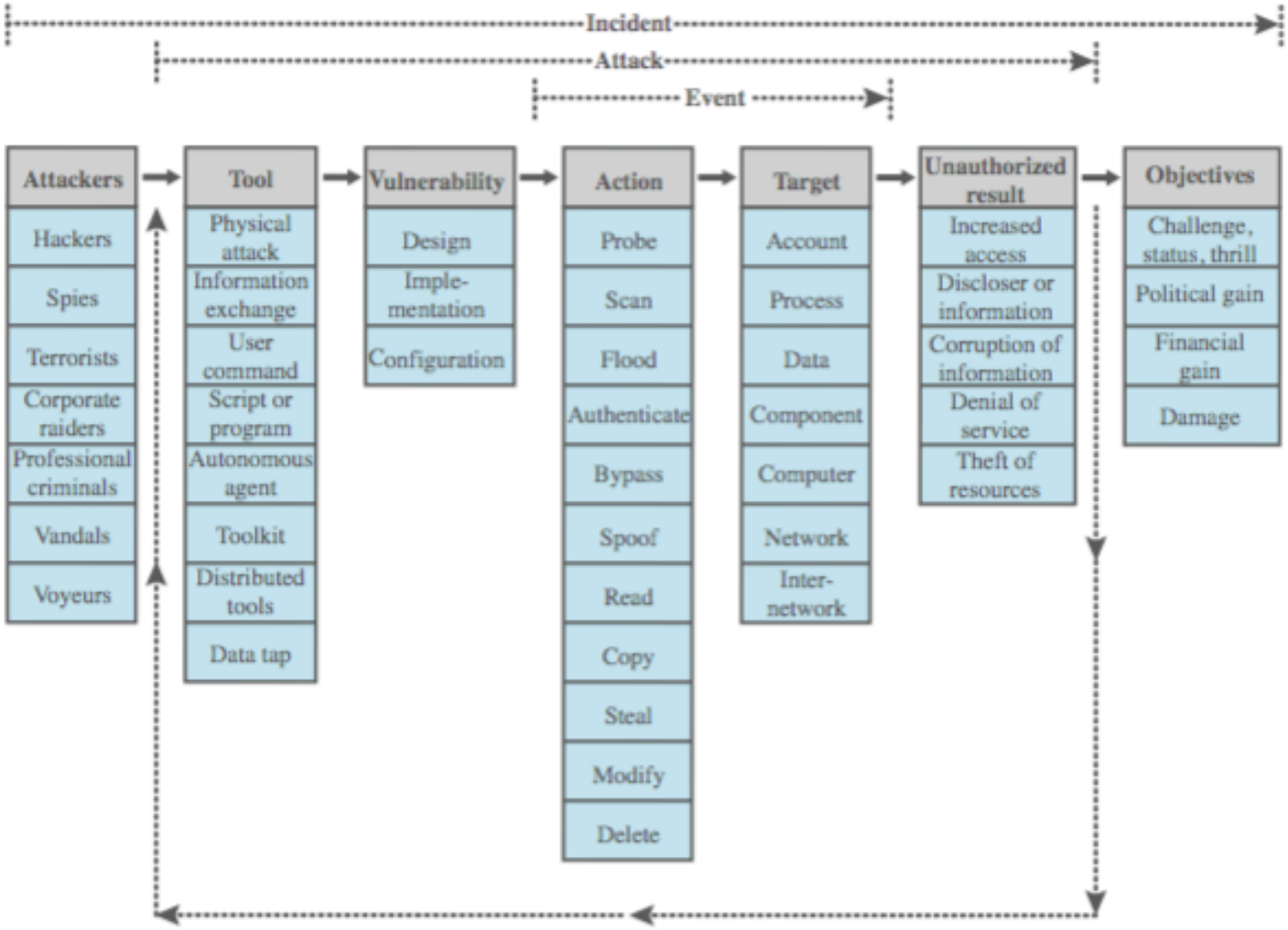
Security Functional Requirements

- Technical Measures:
  - access control; identification & authentication; system & communication protection; system & information integrity
- Management Controls and Procedures
  - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- Overlapping Technical and Management:
  - configuration management; incident response; media protection

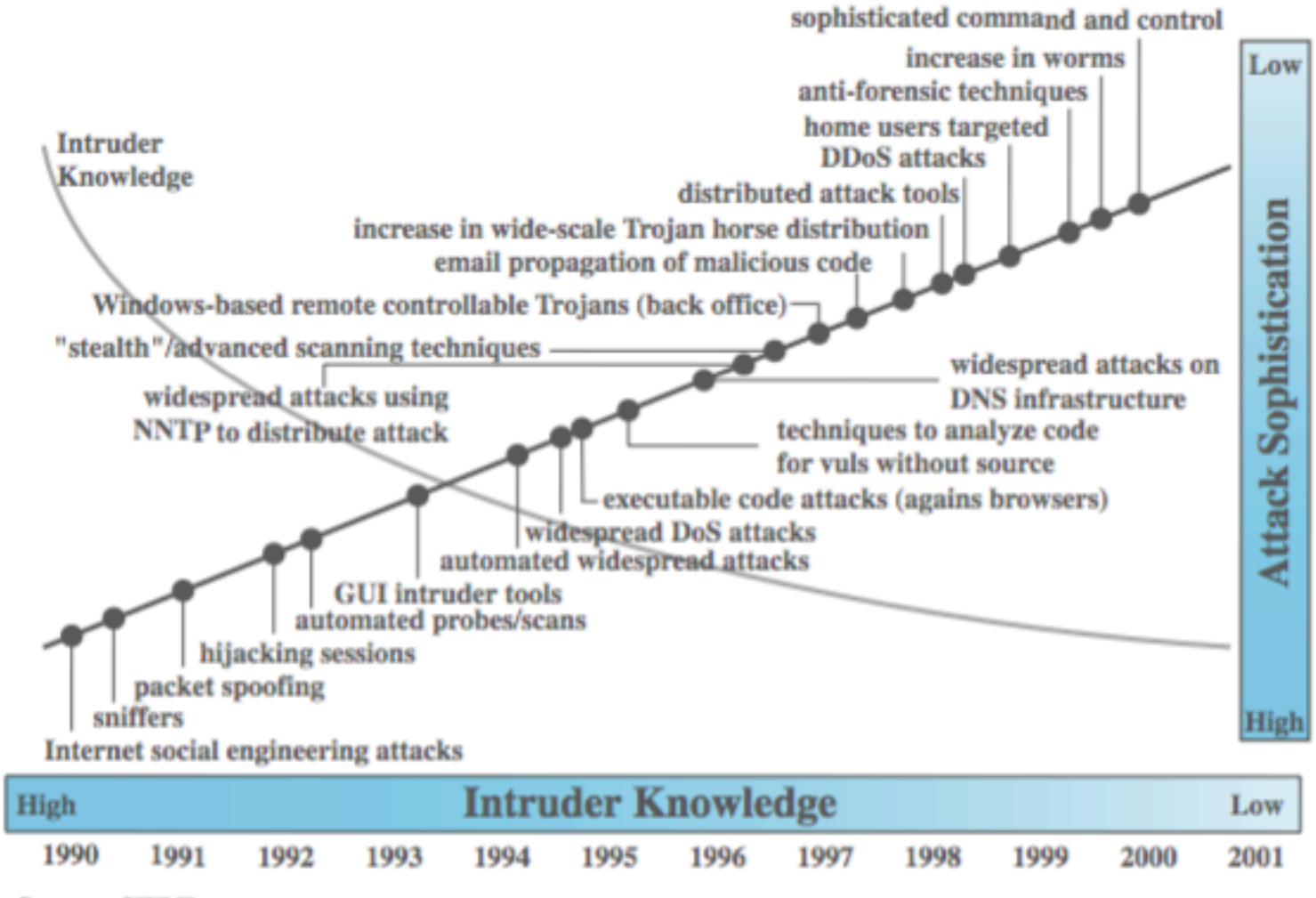
X.800 Security Architecture

- X.800, *Security Architecture for OSI*
- Systematic way of defining requirements for security and characterizing approaches to satisfying them
- Defines:
  - security attacks - compromise security
  - security mechanism - act to detect, prevent, recover from attack
  - security service - counter security attacks

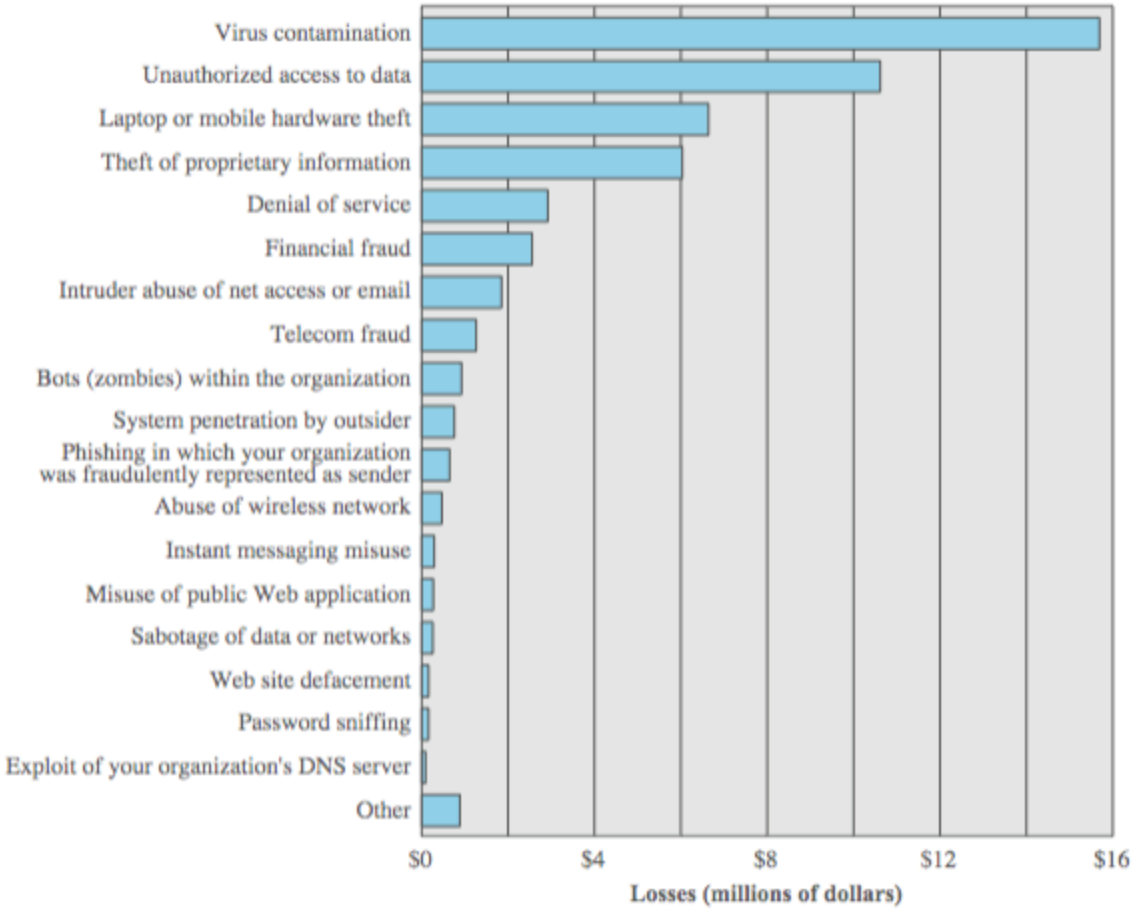
Security Taxonomy



Security Trends

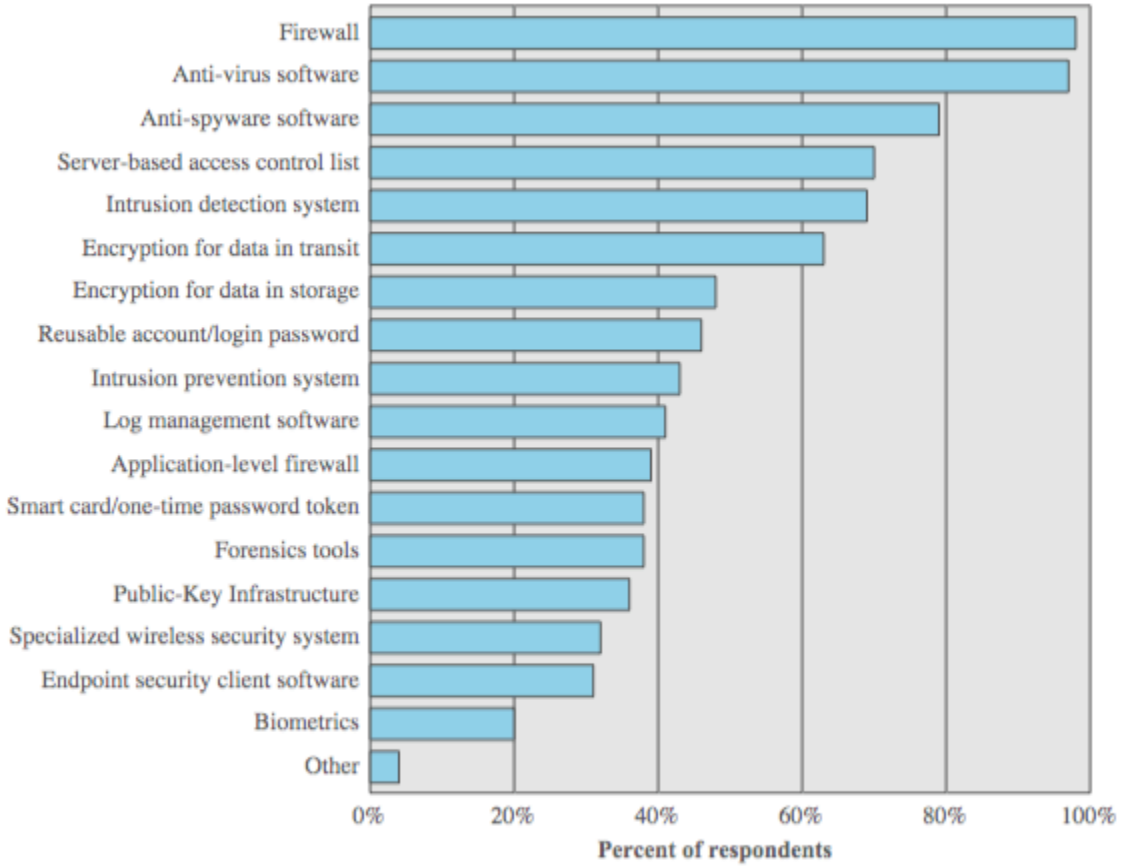


Computer Security Losses



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Security Technologies Used



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Computer Security Strategy

- Specification/Policy
  - what is the security scheme supposed to do?
  - codify in policy and procedures
- Implementation/Mechanisms
  - how does it do it?
  - prevention, detection, response, recovery
- Correctness/Assurance
  - does it really work?
  - assurance, evaluation

Summary

- Security Concepts
- Terminology
- functional requirements
- security architecture
- security trends
- security strategy

What's Next

- Read Chapter 1
  - Lots of terminology, but don't try to memorize every term
    - Recall you get a one page sheet of notes on exam
  - Focus on big picture and recurring concepts
- Homework 1 is Posted on Course Website
  - Due Tuesday Jan 28th
- Next Lecture Topics from Chapter 2
  - Cryptographic Tools

Scope of Computer Security