

Computer Security DD2395

<http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/>

Fall 2011

Sonja Buchegger

buc@kth.se

Lecture 1, Oct. 25, 2011

Introduction

Outline for Today

- About the course
- About computer security

Outline for Today

- About the course
- About computer security

Lectures/Labs

- Course moves from Master's to Bachelor's
- 2011: joint lectures in period 2
- Master's students: labs in period 2
- Bachelor's student: labs in period 3

General Goals

- Learn about security concepts
- Have tools and methods to reason about security
- Spot threats, vulnerabilities
- Know and propose counter-measures
- Present concepts to others

Learning Outcomes

The students should be able to:

- recognize threats to confidentiality, integrity, and availability of systems
- explain the basic computer security terminology and concepts and use them correctly
- find and apply documentation of security-related problems and tools
- analyze small pieces of code or system descriptions in terms of their security
- identify vulnerabilities of such code or descriptions and predict their corresponding threats
- select counter-measures to identified threats and argue their effectiveness
- compare counter-measures and evaluate their side-effects
- present and explain their reasoning to others

People

- Course leader: Sonja Buchegger, buc@csc.kth.se, Osquars Backe 2, 4th floor, room 1437
- Extra lectures given by Torbjörn Granlund, Alexander Baltatzis, Olof Hagsand
- Lab assistants: Oleksandr Bodriagov, Benjamin Greschbach, Guillermo Rodriguez Cano, Meidi Tönisson

Current Info

Check course website regularly for updates!

DD2395 dasakh11

<http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/>

Syllabus: Times and Places

look at schema, course code DD2395

Syllabus: Lectures Content (preliminary)

- Oct. 25, Course administration and introduction to Computer Security [chapter 1]
- Oct. 26, Cryptography [2,20]
- Oct. 31, Authentication [3]
- Nov. 01, Access Control [4]
- Nov. 07, Firewalls [6,9]
- Nov. 10, Web Attacks, OWASP guest lecture, TOP 10 attacks
- Nov. 14, Malware, Denial of Service [7,8]
- Nov. 17, Intrusion Detection [6]
- Nov. 21, Buffer Overflows [11]
- Nov. 24, Social Engineering
- Nov. 29, Models, Multi-Level Security [10]
- Dec. 01, Audits [15], guest lecture by Mårten Trolin
- Dec. 05, Programming/Software Engineering [12]
- Dec. 07, Recap, buffer

Syllabus: Extra Lectures

(termed OVN in the schema)

- Computer architectures: Torbjörn Granlund, Wed Oct 26, 15:00-17:00, E3
- Operating systems: Alexander Baltatzis, Thu Oct 27, 10:00-12:00, Q2
- Computer networking: Olof Hagsand, Tue Nov 1, 13:00-15:00, Q2

Syllabus: Lab Exercises

- ONLY CONCERNS MASTER'S STUDENTS
- See schema for times and rooms
- 4 different exercises
 - 1st: on GnuPG, remote or at CSC, report
 - 2nd: on iptables/firewalls, at CSC
 - 3rd: on web attacks, remote or at CSC
 - 4th: presentation at CSC, report, assess

Exercise 4

- Presentation and demo on computer security topic in a seminar
- Groups of 2-3 students
- Topic distribution on web site
- Group seminars, schedule in schema, signup on course website

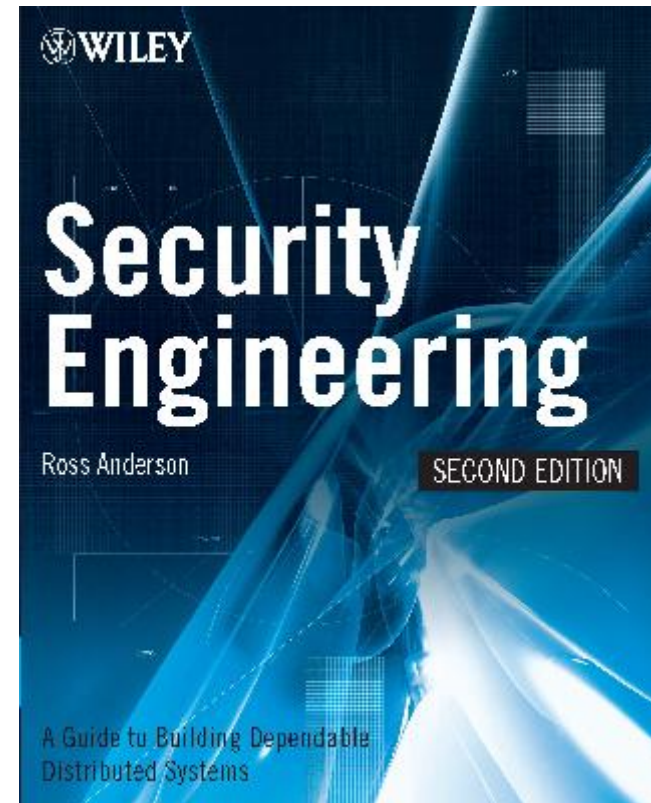
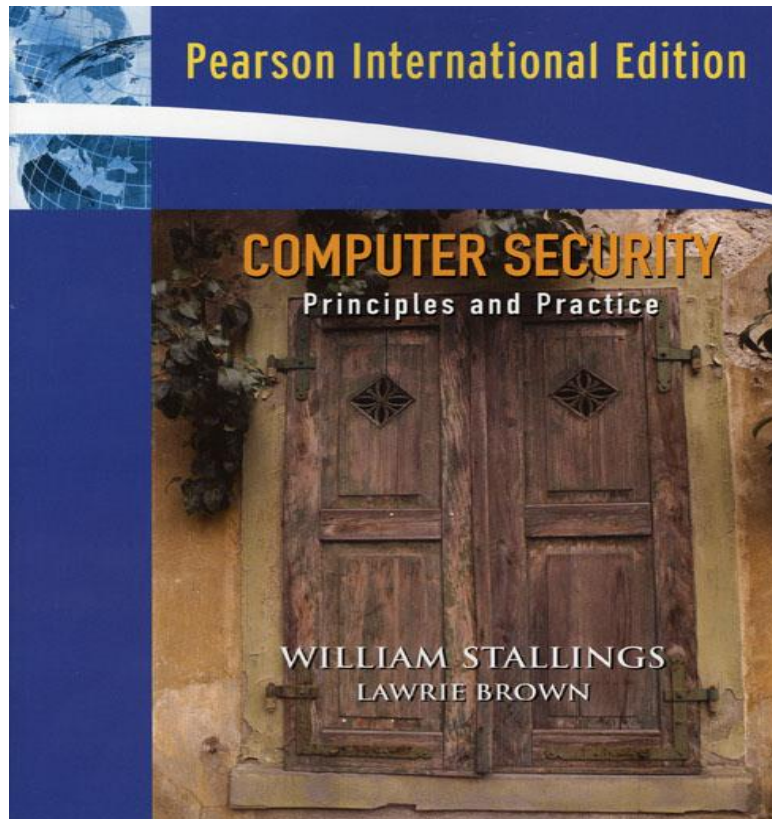
Exam

- January 10, 2012
- Re-exam in June 2012

Assessment, Grades

- 6 ECTS in total, that's about 160 hours of work
- 3 ECTS Exam: A-F
- 3 ECTS Labs:
 - pass/fail, no grades
 - bonus points for exam when handed in early, see lab descriptions

Books



Language

- Course given in English
- Some extra lectures in Swedish
- Questions in Swedish OK

Accounts

- Needed for lab exercises
- Who doesn't have an account and access card?
- Go to the systems group counter, entry floor of Osquars Backe 2

RAPP


- Register for DD2395, if not already
- <https://rapp.csc.kth.se/rapp/>

Next Courses

- Networking Security with Johan Karlander
- Foundations of Cryptography with Douglas Wikström
- Software Security with Dilian Gurov

Course Analysis

- 2010 spring and fall course analyses are available on the course web sites `dasak10`, `dasakh10`
- Some changes: less presentation practice, more written argumentation/peer assessment, more focus on core tasks in labs (gpg, web)

A close-up portrait of Severus Snape from the Harry Potter series. He has long, dark hair and is wearing a dark, high-collared robe. He has a serious, somewhat stern expression. The background is dark and out of focus, with some light reflecting off a surface to the right.

CSC honor code, plus:

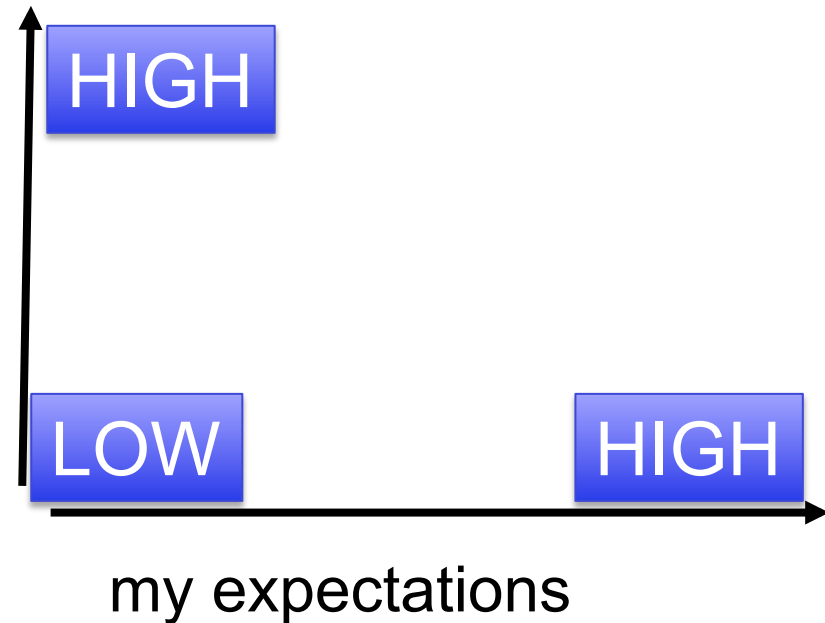
**Defense Against the Dark Arts:
Do not attack a running system
without the consent of the owner
and the users!**

Questions for you:

My most important question
about the course:

my experience, knowledge

My most important question
about computer security:



Questions?

Outline for Today

- About the course
- About computer security

Computer Security

Slides adapted from Lawrie Brown's set of slides
for the course book

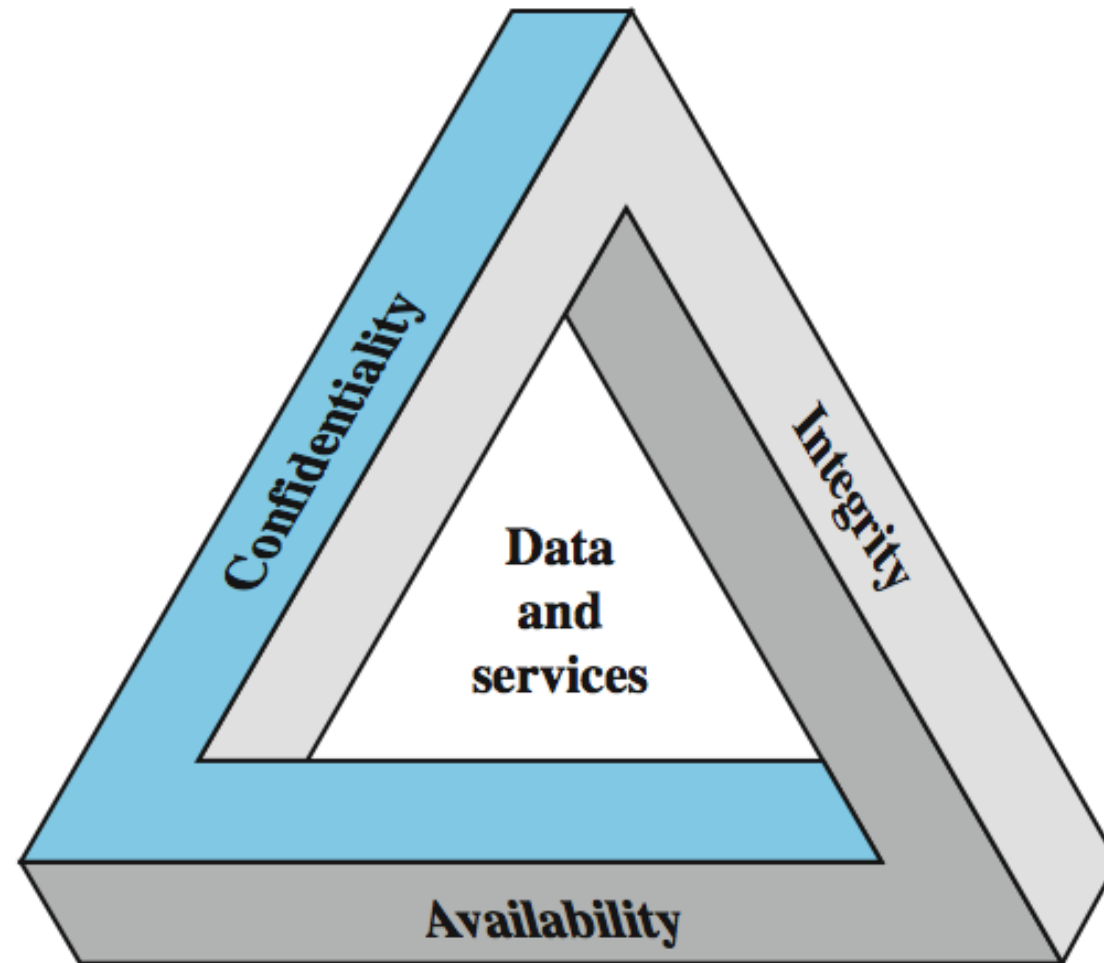
“Computer Security: Principles and Practice”
by William Stallings and Lawrie Brown

Computer Security

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



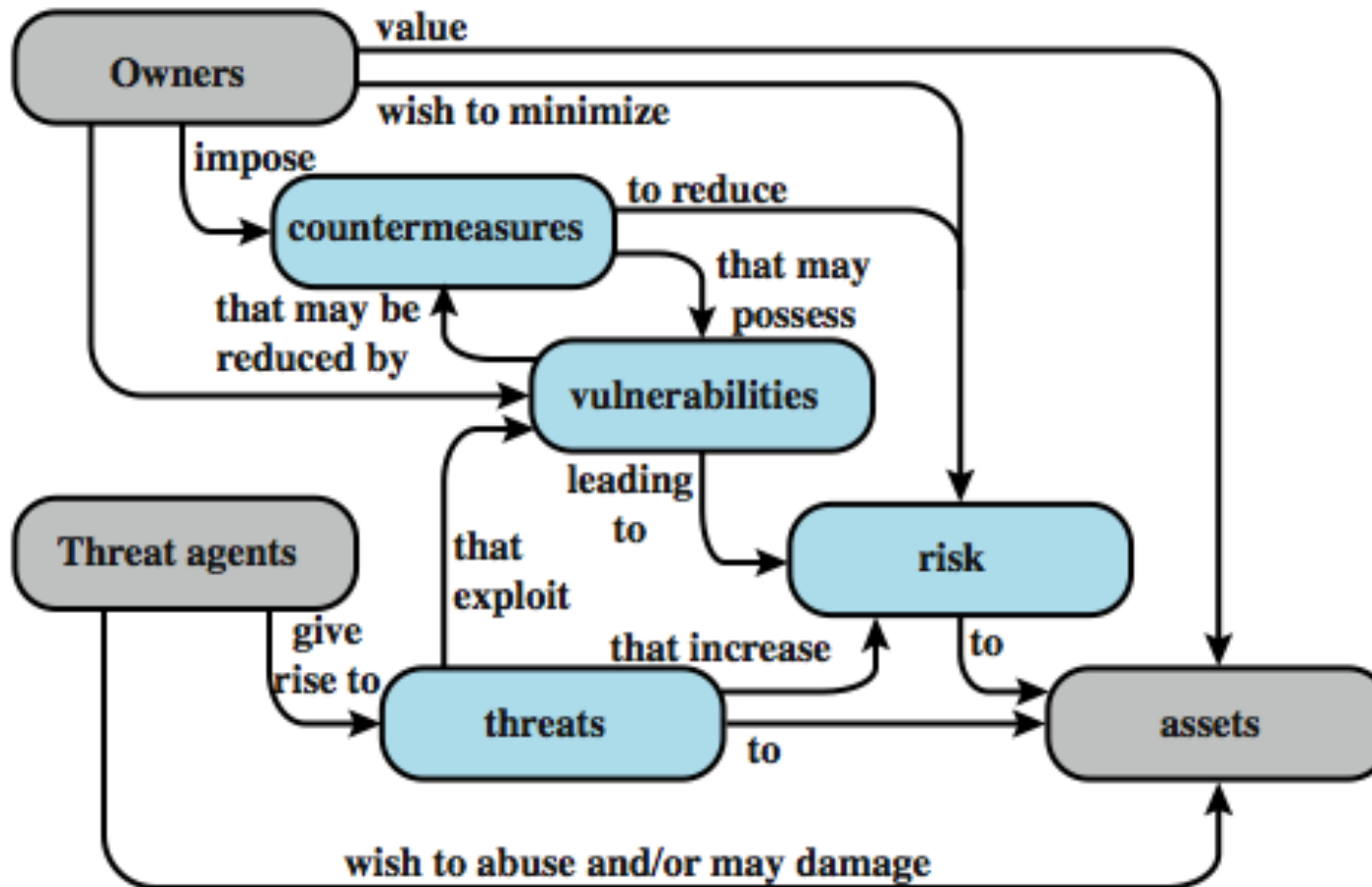
Challenges

- Is security hard to achieve? Why?
- Think about it for 2 min.
- Turn to your neighbor and discuss for 3 min.

Computer Security Challenges

1. not simple in complex systems
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
 - become leaky (loss of
 - become unavailable (loss of
- attacks are threats carried out and may be
 - passive
 - active
 - insider
 - outsider

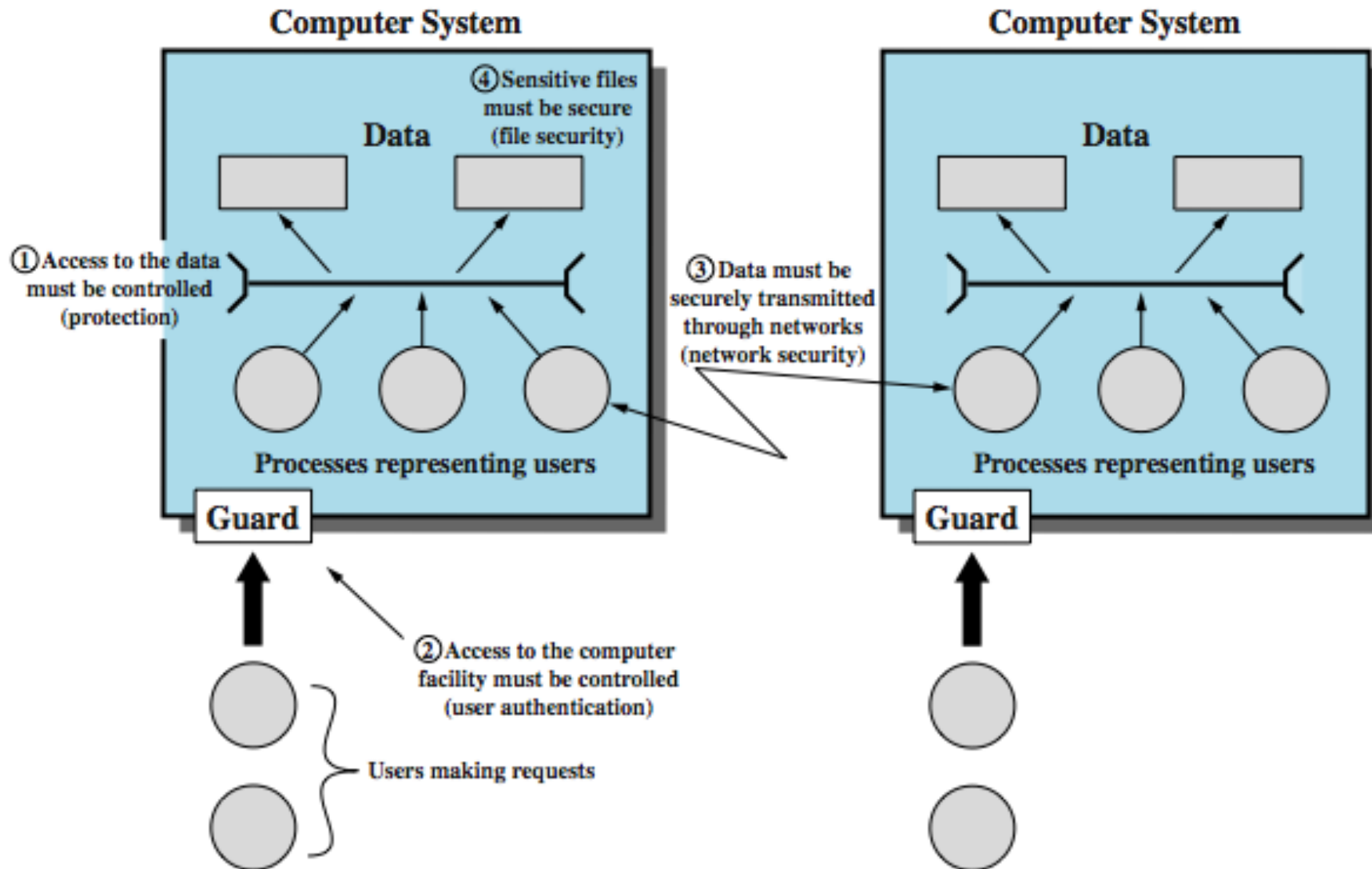
Countermeasures

- 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

Scope of Computer Security



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
- [Networking Security class next term](#)

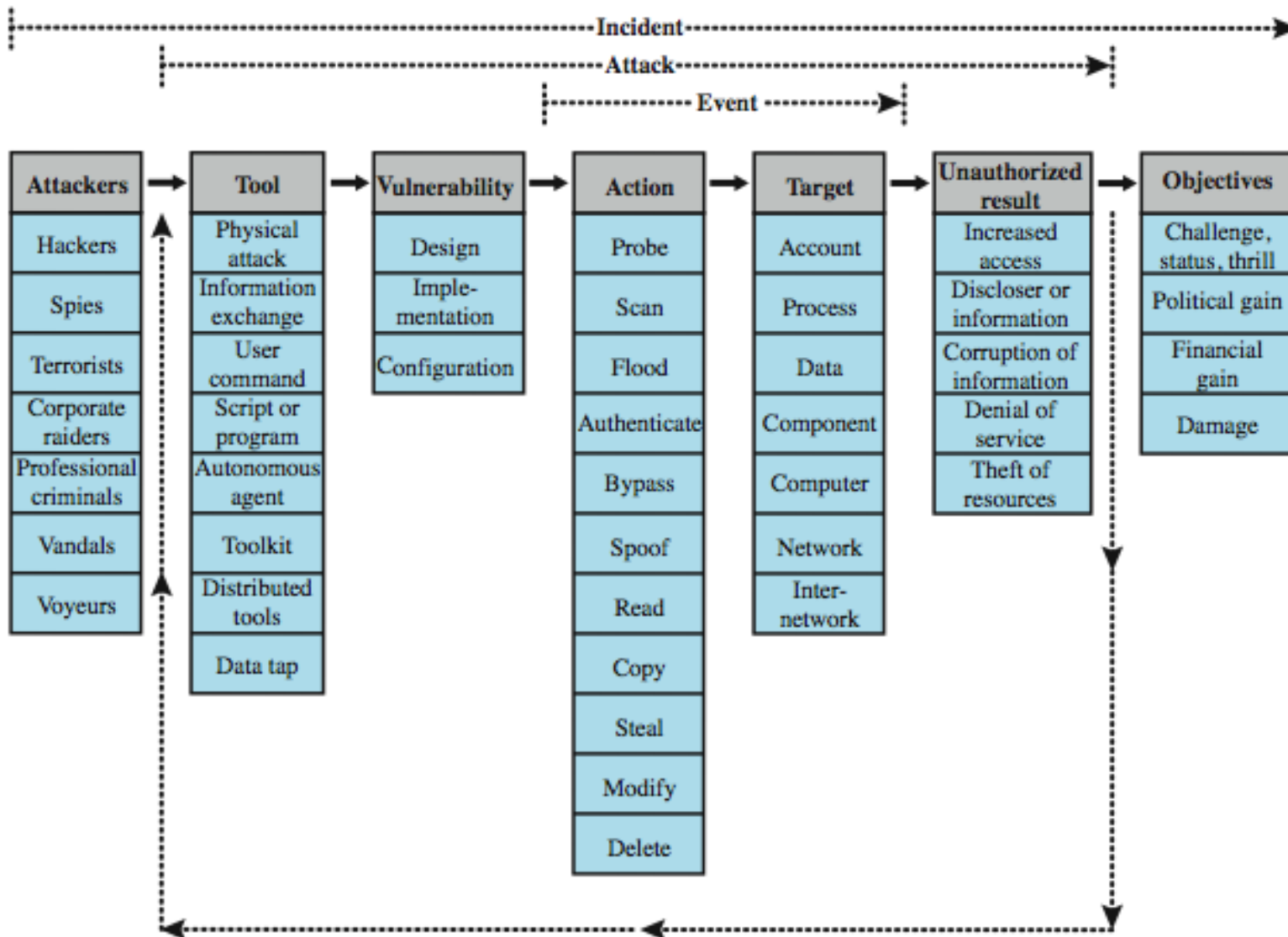
Security Functional Requirements

- 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

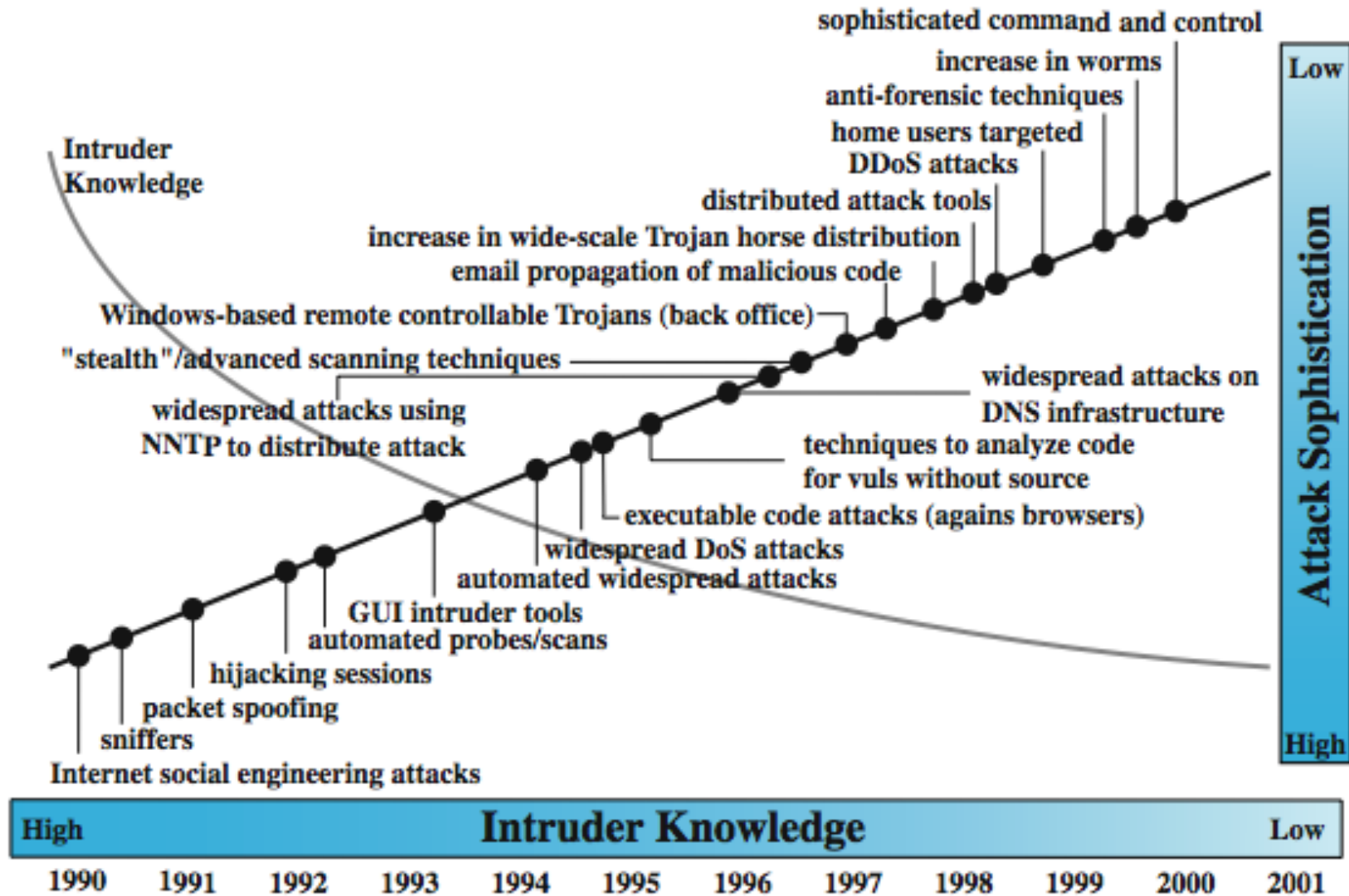
- X.800, *Security Architecture for OSI*
- systematic way of defining requirements for security and characterizing approaches to satisfying them
- defines:
 - security attacks - compromise security
 - security mechanism - act to detect, prevent, recover from attack
 - security service - counter security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

Security Taxonomy

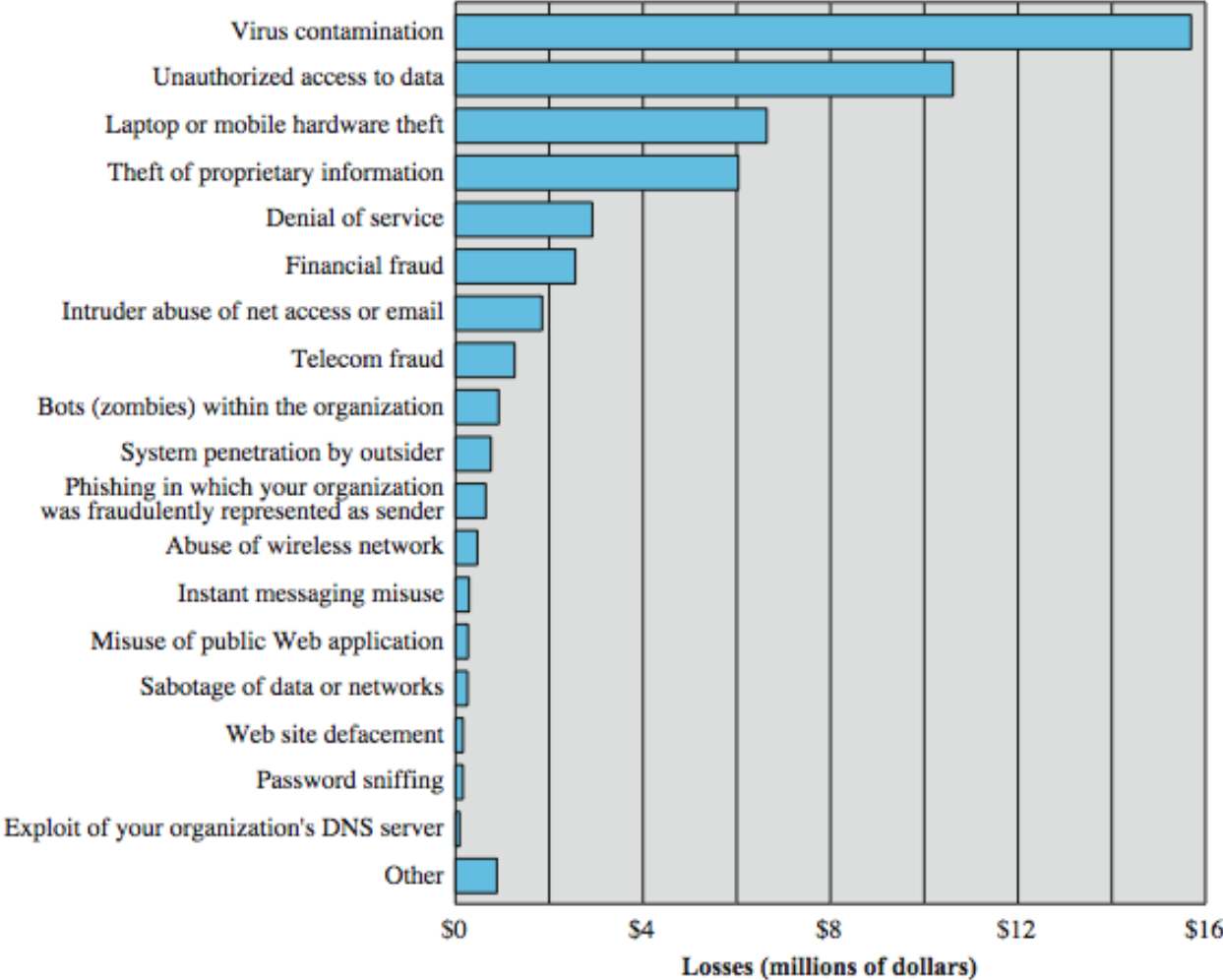


Security Trends

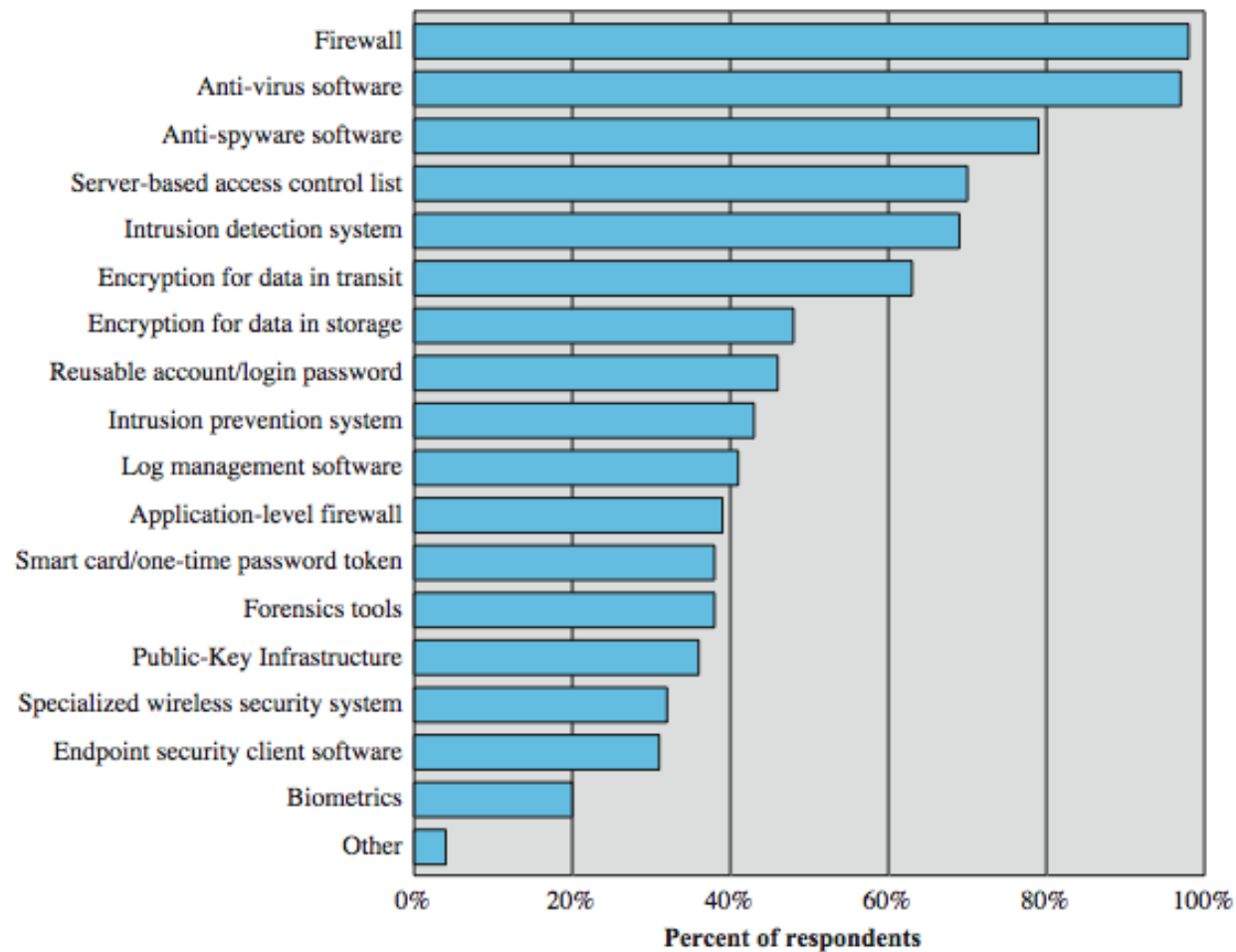
Still true?



Computer Security Losses



Security Technologies Used



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 trends
- security strategy