



CSE331: Introduction to Networks and Security

Lecture 1
Fall 2004



Course Information

- Steve Zdancewic — lecturer
 - Web: <http://www.cis.upenn.edu/~stevez>
 - E-mail: stevez@cis.upenn.edu
 - Office hours: Mon. 3:00—4:00pm,
Tues. 10:00—11:00am
Levine 511
- Baohua Wu — TA
 - E-mail: bauhua@seas.upenn.edu
 - Office hours: TBA
- Course Web Pages
<http://www.cis.upenn.edu/~cse331>



Prerequisites

- Would like to learn network and security fundamentals
- Programming experience (Java)
(CSE 121/115)
- Have not taken TCOM 500 – take CIS 551 instead.



Goals

- Learn networking basics, mainly as they are relevant to security.
(Reduced emphasis on performance.)
- Learn security basics, mainly as they apply to the Internet.



Course Topics

- Networking
 - Communication protocols
 - Ethernet, 802.11
 - Internetworks
 - TCP/IP, Routing
 - Denial of Service, Firewalls
- Security
 - Confidentiality, Integrity, Availability
 - Cryptography & cryptographic protocols
 - Authentication, authorization
 - Virus scanners and related technology



Recommended Reading

- *No required text: instead, articles (mostly from the web) will be provided.*
- **Supplementary reading (available at library):**
 - Security in Computing 3rd edition
Charles P. Pfleeger
 - Computer Networks: A Systems Approach
Larry L. Peterson & Bruce S. Davie
 - Applied Cryptography
Bruce Schneier
- **Slides will be available on the web (PDF)**
 - Linked to from the course schedule page.
- **Material: Slides, Lectures, Articles, HW, Projects**



Assessment

- 7 Individual homework assignments 21%
- Group projects 40%
 - 2 or 3 people per group
 - Programming (in Java)
- In-class midterms 24%
 - Tentatively October 11th (Networks)
 - Tentatively November 15th (Security)
- Final exam 15%
 - Time & place determined by registrar
 - Covers entire course (mostly security)
- Participation (mandatory and subjective) 0%



Course Policies

- No late homework accepted
 - Unless prior permission
 - Emergency
- No collaboration on individual homework
- No individual work on group projects
- Regrades:
 - Only “reasonable” requests
 - Entire homework is regraded
 - Scores may go up or down



Announcements

- Homework 1 is due Sept. 15th
 - Available on the web page
- I will be out of town on Monday Sept. 20th.
 - Class cancelled.



Computer Security

Goal: prevent “bad” things from happening:

- delete or trash files
- crash a system
- deny access to a service
- steal information
- fail to pay for on-line purchase

Similar goals to software engineering.

Difference is in assumptions about “failures”:

- must assume the worst possible case: attacks!



Network Security Concerns

- Confidentiality of transmitted data, such as passwords and credit card numbers.
- Integrity of network information, such as routing tables and DNS bindings.
- Authentication of users who have contact only via the Internet.
- Thwarting Denial of Service (DoS) attacks.
- Aiding security of host systems using firewalls, etc.



Principles of Secure System Design

- **The Protection of Information in Computer Systems**
 - Saltzer & Schroeder 1975
 - <http://web.mit.edu/Saltzer/www/publications/protection/>
- Highly recommended supplementary reading.
 - We will come back to technical parts and related research later in the course.

Privileges

- **Least Privilege:** each principle is given the minimum access needed to accomplish its task.

Examples:

- Administrators don't run day-to-day tasks as root. So `rm -rf /` won't wipe the disk.
- fingerd runs as root so it can access different users' .plan files. But then it can also `rm -rf /`.

- **Separation of Privileges:** dividing privileges among principles is more flexible and robust

TCB

Keep the Trusted Computing Base small.

Trusted Computing Base (TCB):

- the parts of a system that must work correctly to ensure the proper functioning of the system.
- e.g., the OS Kernel & Hardware.

Smaller, simpler systems tend to have fewer bugs and bad interactions.

- so keep the kernel small and simple.

“Small TCB” is a basic principle in *all* software.

Complete Mediation

All access must controlled

- It doesn't help to lock the front door if you leave the back door open.
- Very hard to achieve.
- In practice trade off between value of thing being protected and access.



Security is an ongoing process

- Every system has vulnerabilities
 - Impossible to eliminate all of them
- Systems change over time
 - Security requirements change over time
 - Context of mechanisms changes over time
- Secure systems require maintenance
 - Check for defunct users
 - Update virus software
 - Patch security holes
 - Test firewalls
- ***THERE IS NO SILVER BULLET!***



Software Design

- **Failsafe defaults**

- System should behave securely “out of the box”
- Configuration should be necessary to make the system less secure

- **Open design**

- The security of the system should not rest on the secrecy of its design (or algorithm, or implementation)

Computing Trends

Back in the 1970's, the hardware and kernel were simple, small and relatively trustworthy.

Today, they're HUGE.

- Win2K: >50 Mloc (XP even larger)

Why the growth?

- personal vs. shared computers – protecting users from each other wasn't that important.
- old code never goes away.
- richer set of devices (mice, cd, bluetooth, etc.)
- services (e.g., gui, net, web, suspend, etc.)
- performance – crossing boundaries is expensive.

It's hard to say these are small TCB's.



Further Changes

In the '70s, computing systems were isolated.

- software updates done infrequently by an experienced administrator.
- you trusted the programs you ran.
- physical access was required.
- few things were executable.
- crashes and outages didn't cost billions.

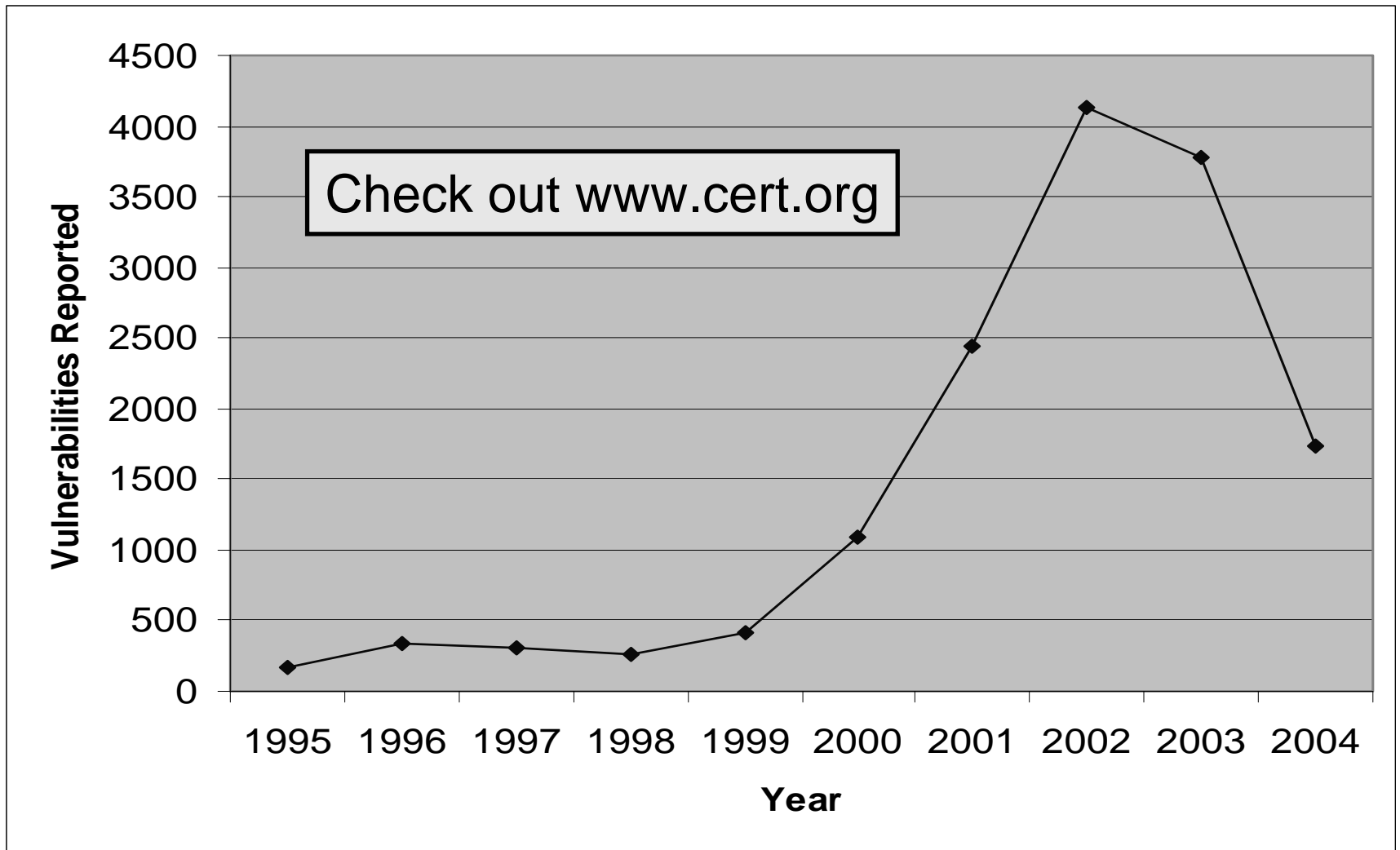
The Internet has changed all of this.

- software is constantly updated – sometimes without your knowledge or consent.
- you have no idea what a program does.
- a hacker in the Philippines is as close as your neighbor.
- everything is executable (i.e., web pages, email, docs).
- we depend upon the infrastructure.

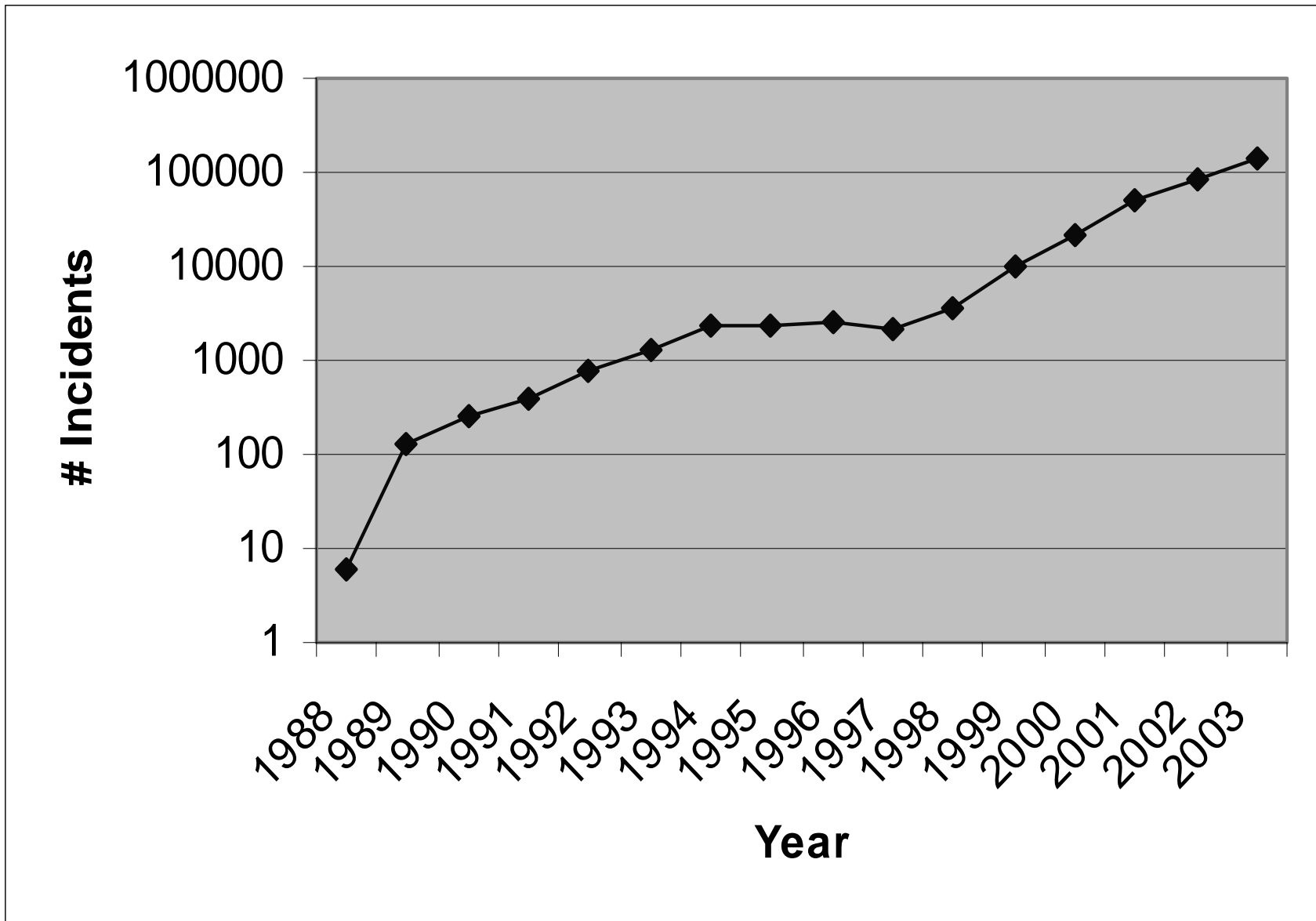
Trends:

Vendors	few	→	many
Media	hard	→	soft
Delivery mechanism	physical	→	electronic
Frequency of installation	seldom	→	always
Size of package	whole thing	→	small pieces
Permanence	persistent	→	ephemeral

CERT Vulnerabilities



CERT Incidents





CERT Status as of 2004

Note: Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported.

Instead, we will be working with others in the community to develop and report on more meaningful metrics, such as the 2004 E-Crime Watch Survey. We welcome ideas and proposals for other collaborations in this area.



Reading Assignment

- ***Security of the Internet***
 - http://www.cert.org/encyc_article/tocencyc.html