Carnegie Mellon
Software Engineering Institute

CERT
Coordination
Center

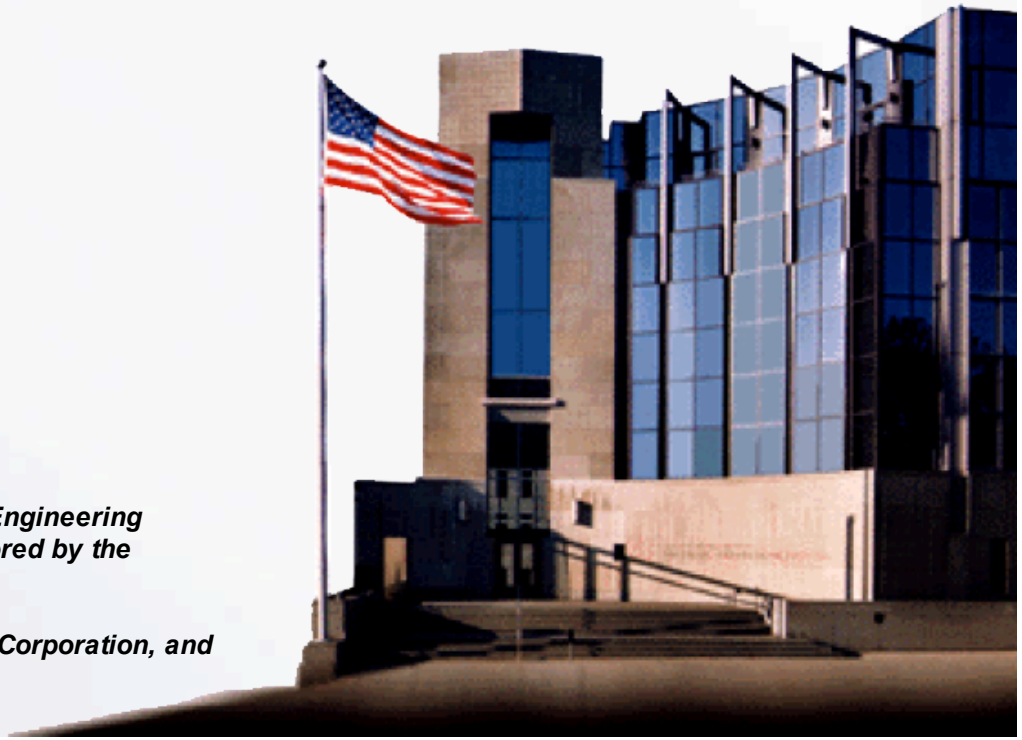
CERT/CC Overview

Attacker motivations, denial of service, vulnerabilities, and malicious code

Presented by: Lucy Crocker, Will Dormann, and Nick Ianelli

March 22, 2005

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890



Agenda

CERT Coordination Center

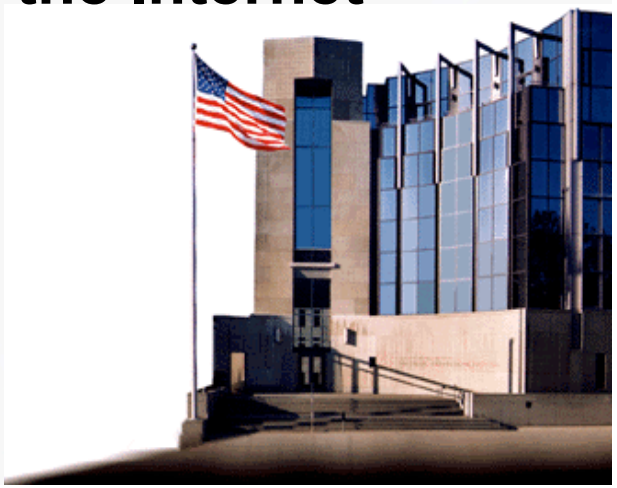
- Overview of CERT®/CC
- Intruders
- Denial of service attacks
- Defining & handling a vulnerability
- Vulnerability trends
- Malware
- Phishing attacks

CERT®/CC Overview

CERT Coordination Center

- CERT®/CC is the center of Internet security expertise. It is located in the Software Engineering Institute operated by Carnegie Mellon University.

- CERT®/CC was established in 1988 on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today.



CERT®/CC Principles

CERT Coordination Center

- **Ensure confidentiality and impartiality**
  - We do not identify victims but can pass information anonymously and describe activity without attribution
- **Provide trusted, unbiased information**
  - We do not sell consulting services or software
  - We do not overstate or understate the risks of vulnerabilities or incident activity
  - We work indiscriminately with vendors

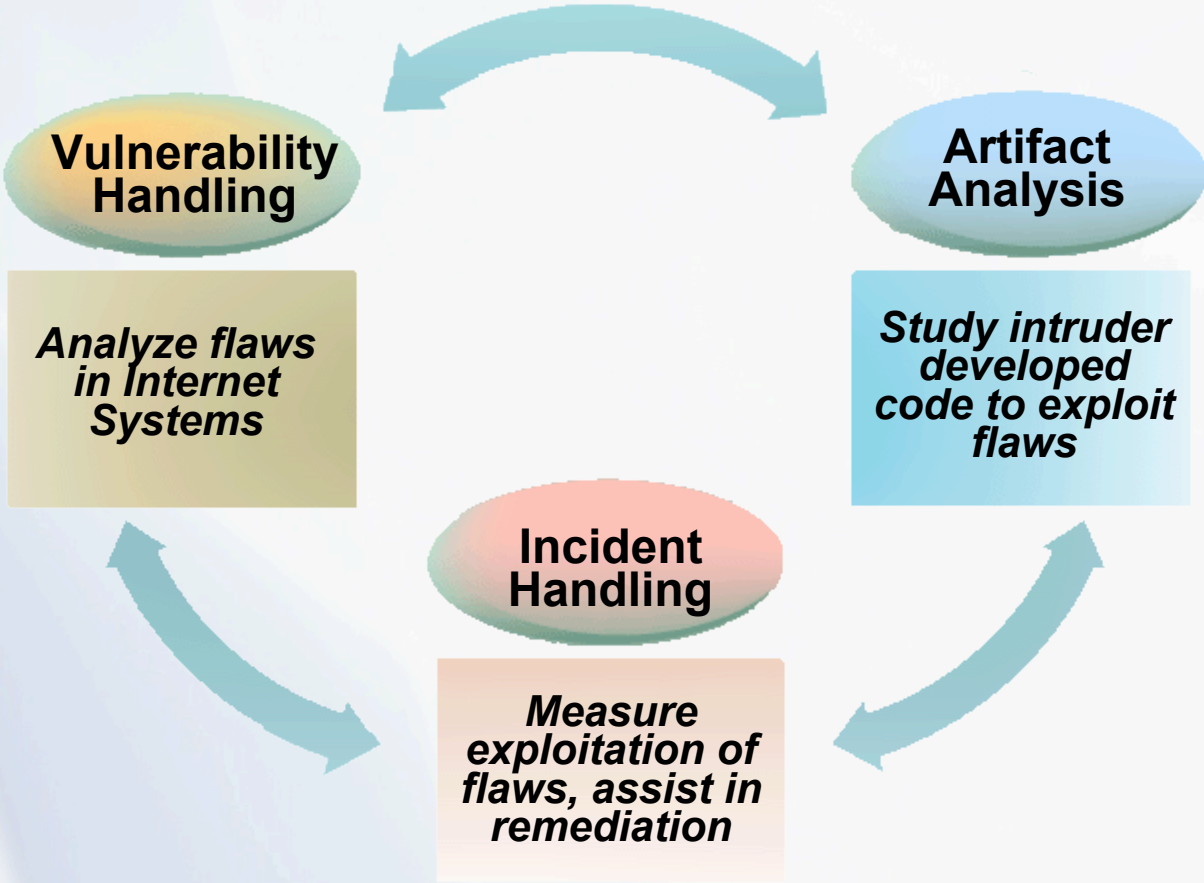
CERT®/CC Mission

CERT Coordination Center

- **Internet Security Threats**
  - Identify
  - Coordinate
  - Remediate
  - Research

CERT®/CC Teams

CERT Coordination Center



Intruders

CERT Coordination Center

- Script kiddies
- Industrial spy
- Insider
- Foreign government
- Criminals
- Organized crime

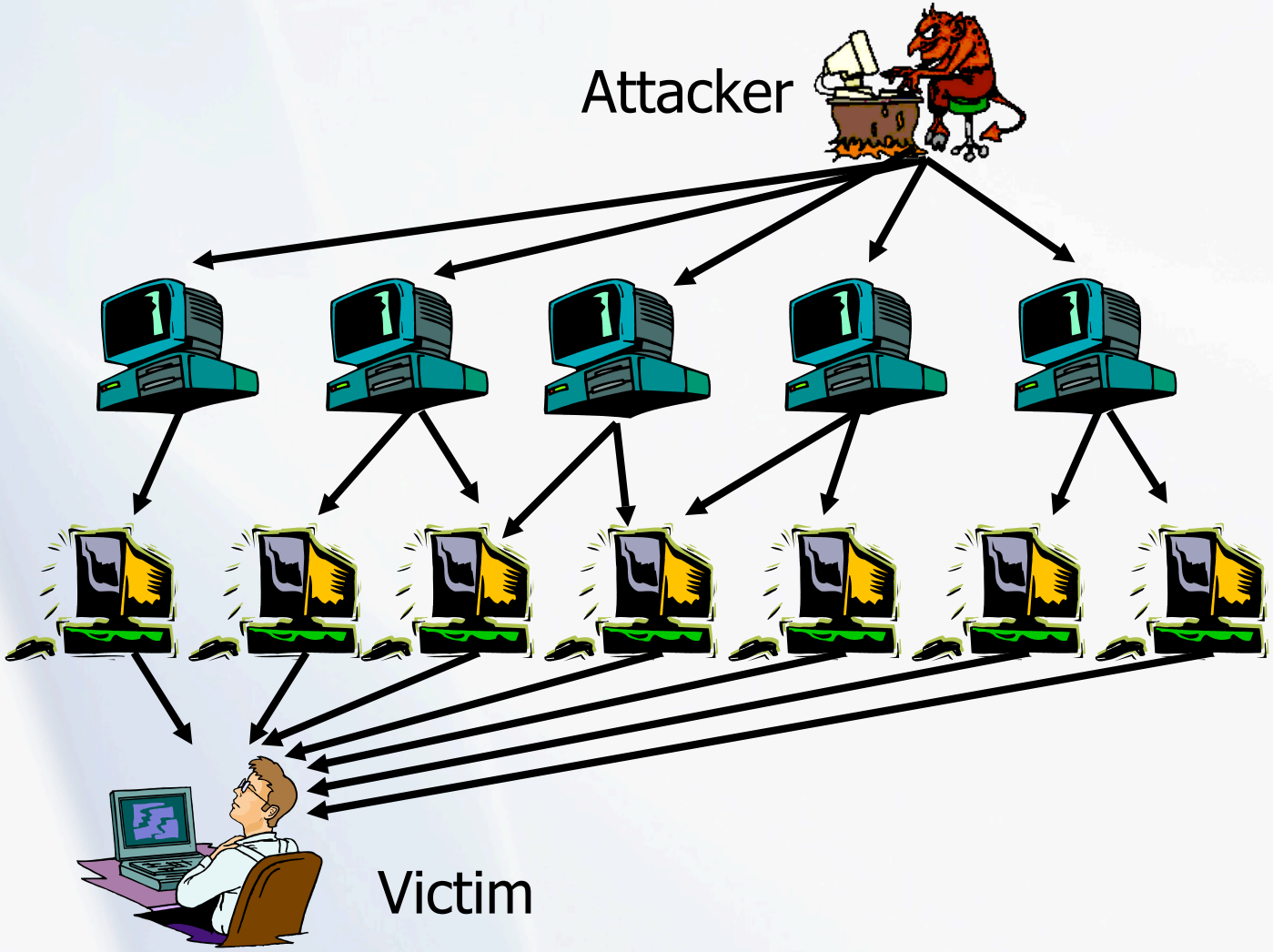
Denial of Service (DoS)

CERT Coordination Center

- **Interferes with normal operation of a service**
- **Common examples:**
  - Vulnerability attack
    Takes advantage of a known vulnerability in software
  - Flooding attack
    Send vast number of messages to consume key resources

Distributed Denial of Service (DDoS)

CERT Coordination Center



What is a Software Vulnerability?

CERT Coordination Center

- **By our definition, a vulnerability**
  - Consists of a set of conditions that when present together:
    - Violates an explicit or implicit security policy
    - Usually caused by a software defect
    - Often results in unexpected behaviour
- **A vulnerability is not a:**
  - Trojan horse, virus, worm, scanner, rootkit

Vulnerability Handling

CERT Coordination Center

- **Receive vulnerability reports**
  - Proactively monitor public sources of vulnerability information
  - Direct reports
- **Verify and analyze reports**
  - Is this really a vulnerability?
  - What is impact of vulnerability?
  - How many systems/types of systems are affected?
  - Are exploits available or in circulation?

Vulnerability Handling (2)

CERT Coordination Center

- **Coordinate with:**
  - Vulnerability reporters
  - Vendors
  - Internet experts
- **Publish information about vulnerabilities and countermeasures**

Vulnerability Disclosure

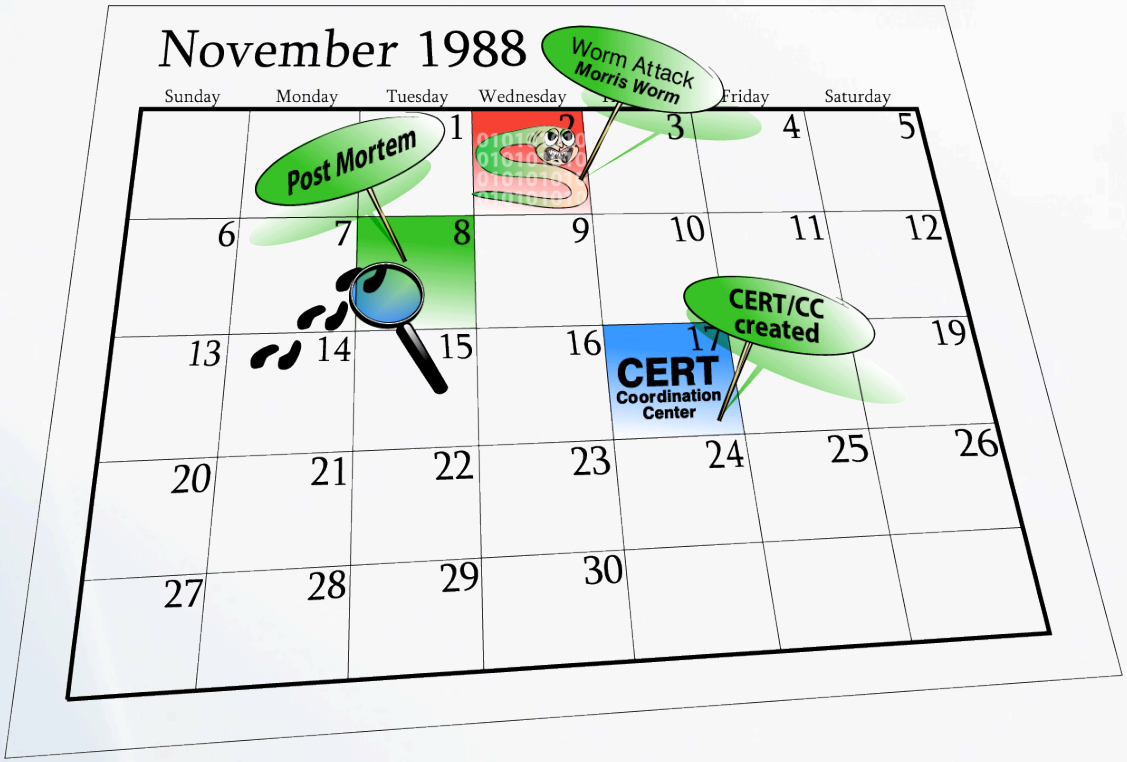
CERT Coordination Center

- **Full disclosure**
  - Full details disclosed to the public
- **Non disclosure**
  - No details disclosed to the public
- **Responsible disclosure**
  - Details are provided to vendor providing the opportunity to make solutions and workarounds available
  - Minimizes the impact of the necessary disclosure of information

Vulnerability Trends

CERT Coordination Center

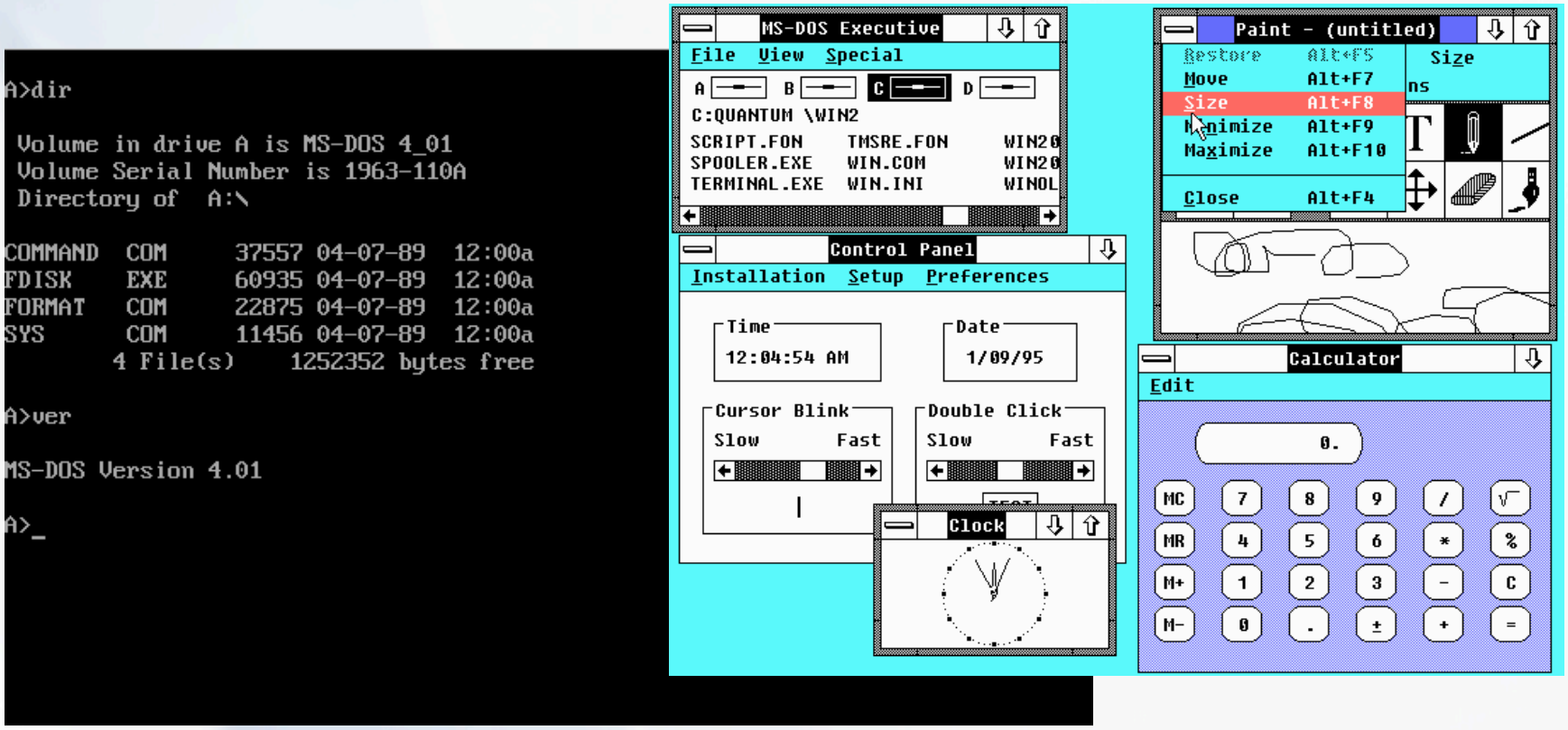
- **The Morris Worm**
  - November 2, 1988
  - Finger daemon
  - Buffer overflow



The Internet in 1988

CERT Coordination Center

- DOS 4.0 and Windows 2.0



The Internet in 1988 (2)

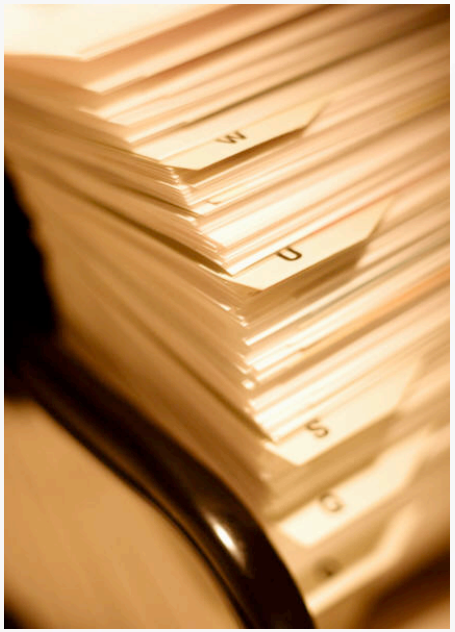
CERT Coordination Center

- 60,000 hosts
- Relatively slow network connections
- Primarily UNIX systems

Finger Daemon

CERT Coordination Center

- Common on UNIX systems
- Listens on TCP port 79
- Answers requests for information about user accounts



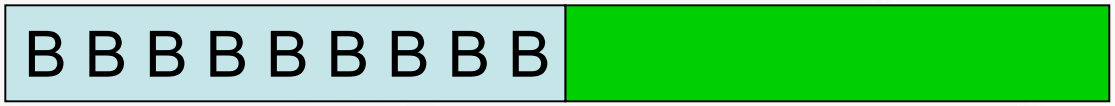
Buffer Overflow

CERT Coordination Center

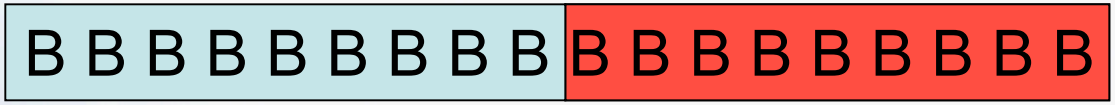
User Input

Fixed Buffer

Adjacent Memory



Memory OK

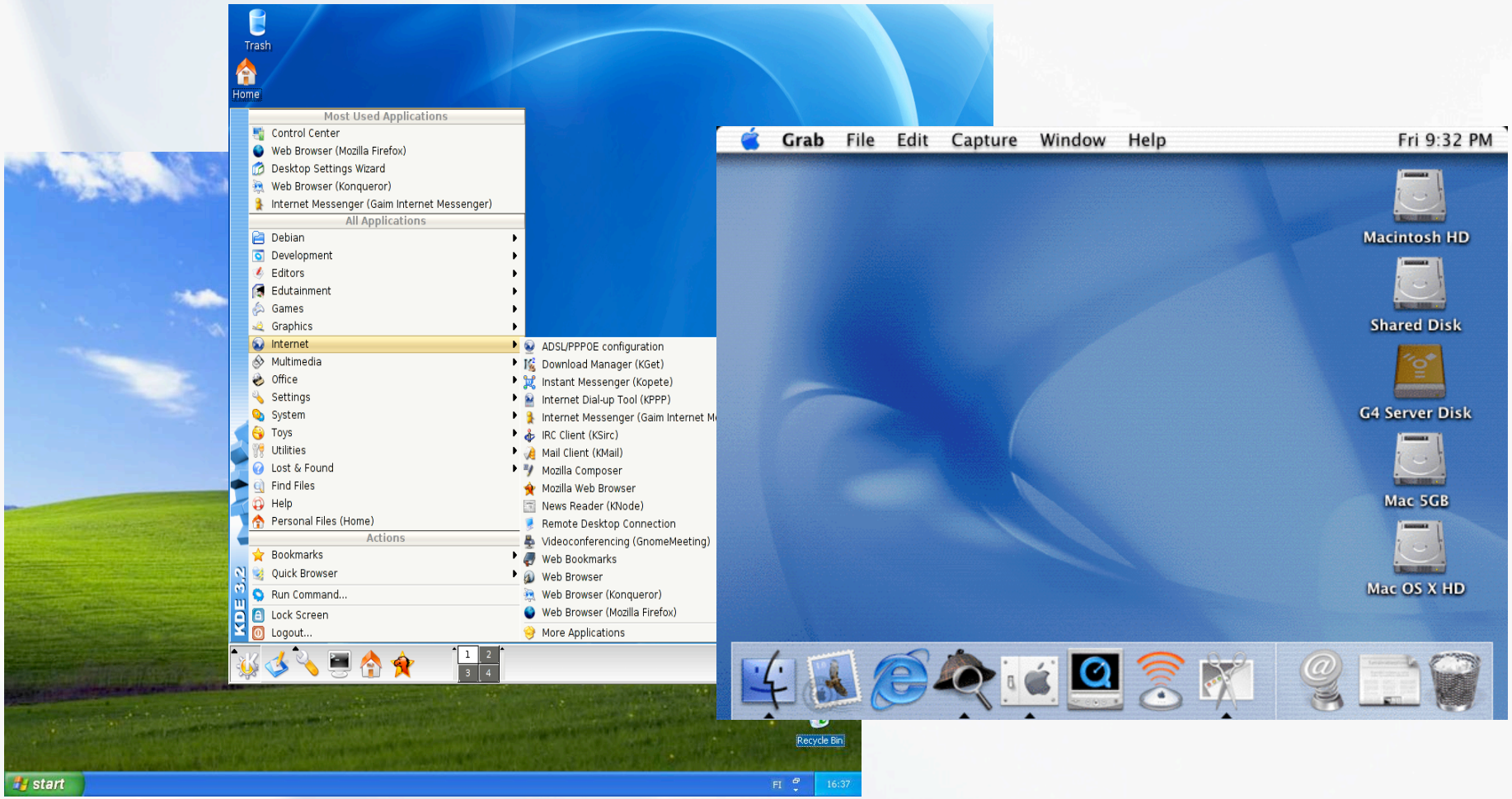


Buffer Overflow

The Internet in 2005

CERT Coordination Center

- **Windows XP, Linux, Mac OS X**



The Internet in 2005 (2)

CERT Coordination Center

Then (1988)

- 60, 000 hosts
- Relatively slow network connections
- Primarily UNIX systems

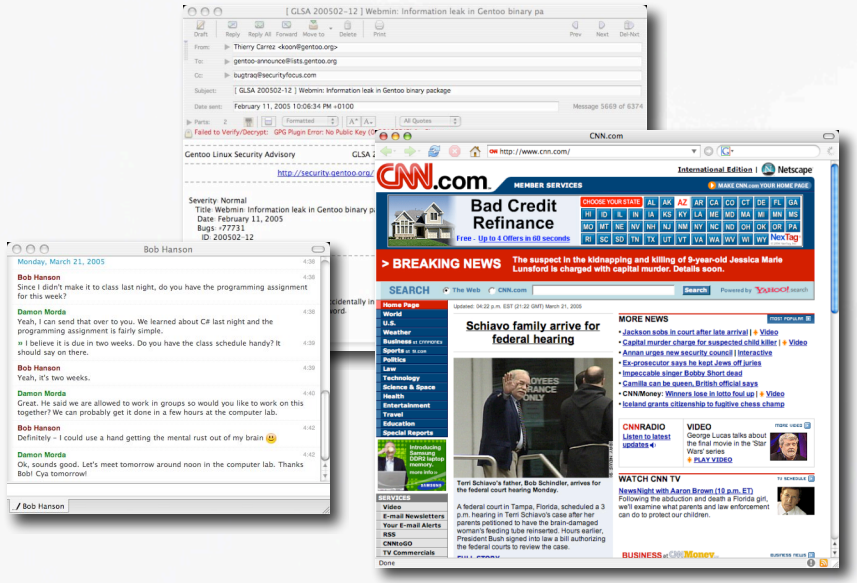
Today (2005)

- Over 300,000,000 hosts
- Broadband connections
- Operating systems with rich Internet features
- Mobile and wireless devices

Vulnerability Trends

CERT Coordination Center

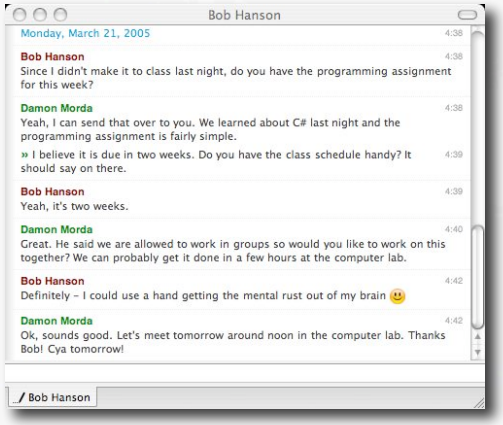
- **Increased client-based vulnerabilities**
  - Instant messaging
  - Web browsers
  - Email applications



Instant Messaging

CERT Coordination Center

- Access to a large number of users
- Social engineering
- Software vulnerabilities



Instant Messaging Case

CERT Coordination Center

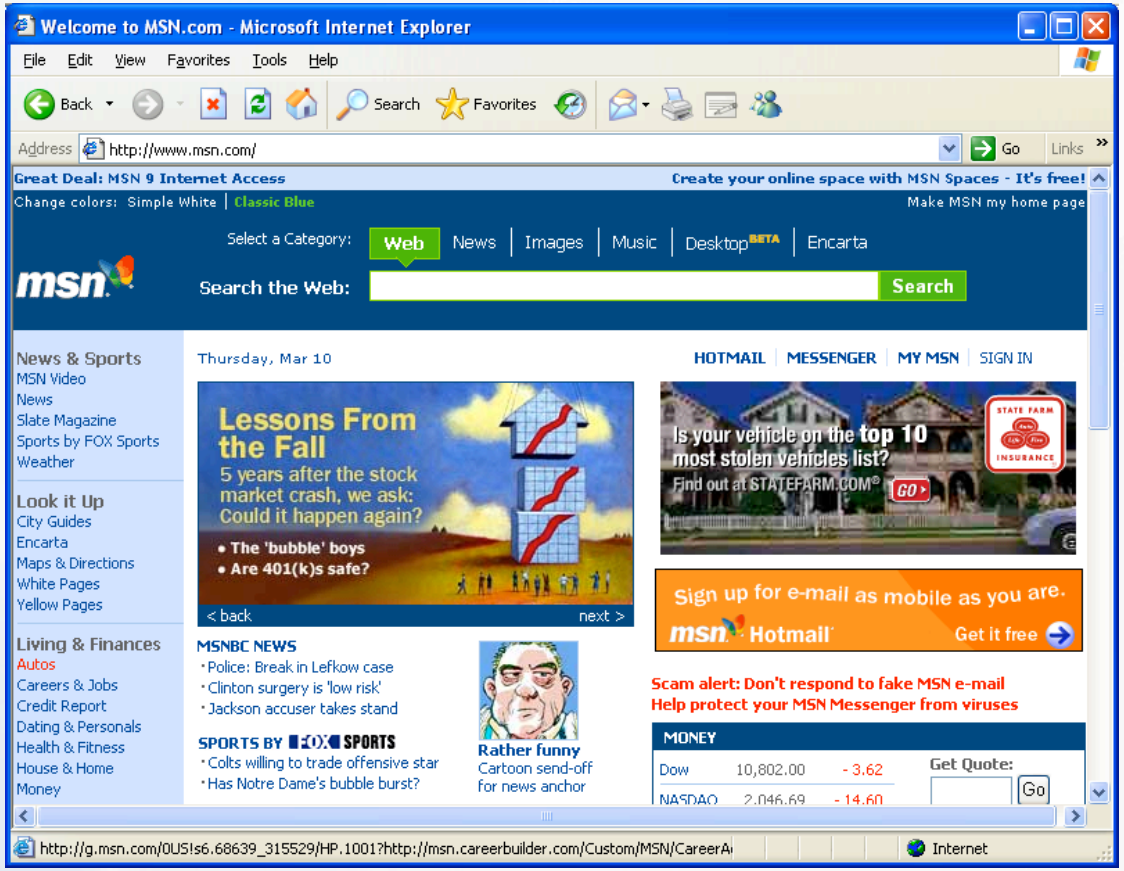
- **February 8, 2005**
  - Microsoft releases security bulletin about MSN Messenger
  - Flaw in PNG processing
- **February 9, 2005**
  - Exploit code released

Web Browsing

CERT Coordination Center

The Modern Web Browser

- Scripting
- ActiveX
- Plug-ins
- Windows Media
- DHTML
- Java



“Drag and Drop”

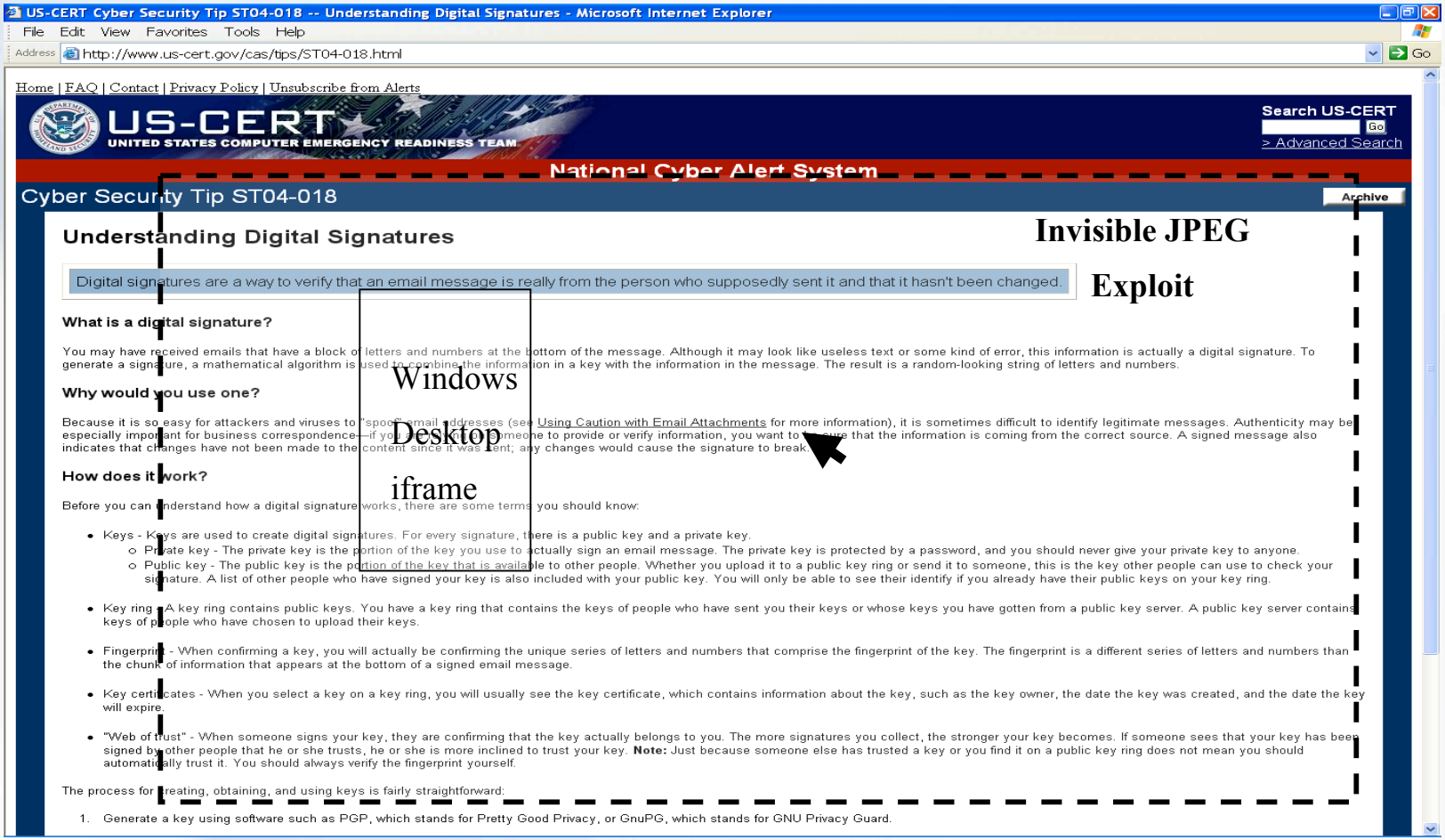
CERT Coordination Center

- **August 18, 2004**
  - Internet Explorer targeted

- **February 25, 2005**
  - New variant targets Firefox 1.0

“Drag and Drop” Vulnerability

CERT Coordination Center



Malware

CERT Coordination Center

- **What is malicious code (malware)?**
  - Malware is a program designed with malicious intentions that attempts to gain resources or information without the end user's consent.

Malware (2)

CERT Coordination Center

- **What are some of the ways malware can get onto someone's computer?**
  - Vulnerabilities in the Operating System (OS) or within the software running
  - Social engineering
  - No Anti Virus (AV) or Anti Adware/Spyware protection

Malware (3)

CERT Coordination Center

- **Common forms of malware:**
  - Worms
  - Viruses
  - Adware/Spyware
  - Bots

Worms and Viruses

CERT Coordination Center

- **Worms**
  - A program that replicates itself without human intervention.
  - Examples: Blaster, Slammer, Nachi/Welchia
- **Virus**
  - A program that replicates itself with human intervention.
  - Examples: Netsky, Bagle, Funlove

Adware/Spyware

CERT Coordination Center

- **Adware**
  - Used by Marketing firms, bundled with popular programs or services
  - Primary purpose, monitor Internet surfing habits and report back to a third party
  - Target based advertising in the form of Pop-up windows
- **Spyware**
  - Personal information stealing for financial gain
    - Key logging, screen captures, sniffing traffic
  - Ability to remotely control the host via a backdoor

Bots

CERT Coordination Center

- **Robot, automate tasks, simulate human behavior**
- **Grouped together to form a Bot Network**
- **IRC is commonly used as the Command and Control (C&C)**
- **Some features include:**
  - Key logging, screen captures, sniffing traffic, port scanning, DDoS, Proxy/Web/FTP/SMTP server…

Phishing

CERT Coordination Center

- Does anyone do any bill pay, shopping or trading online?
- Does anyone know the difference between fishing and phishing?
- Why is phishing being performed?

Phishing Threats

CERT Coordination Center

- **Customer**
  - Financial loss due to fraud
  - Identity theft
  - Time due to fraud remediation
- **Businesses**
  - Financial loss due to fraud liability
  - Potential loss of business due to loss in customer trust
  - Bad publicity

Return on Investment

CERT Coordination Center

- **Why target one Internet browser or OS over another? Why does Microsoft always seem to be in the news?**

- **Internet Explorer holds about 90%* of the browser market share and Microsoft Windows holds about 90%** of the OS market share**

**http://www.websidestory.com/servicessolutions/datainsights/spotlight.html*
***http://www.w3schools.com/browsers/browsers_stats.asp*

What you can do…

CERT Coordination Center

- Defense in depth
- External validation
- User education

What we can do as a community…

CERT Coordination Center

- Secure programming practices
- Two factor authentication
- Reporting of incidents to Law Enforcement (LE)
- Global enforcement of existing laws

Remember….

CERT Coordination Center

- **A famous rapper said it best:**

"It's all about the Benjamins!"

- Puff Daddy '98

Today's intruders are motivated by financial gain, and there are many ways to reach that goal.

CERT®/CC

CERT Coordination Center

Questions & Comments…