



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**

*The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.*

© 2005 by Carnegie Mellon University

Some images copyright [www.arttoday.com](http://www.arttoday.com), Microsoft Corporation, and Google Images



# Agenda

---

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

# CERT<sup>®</sup>/CC Overview



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

---

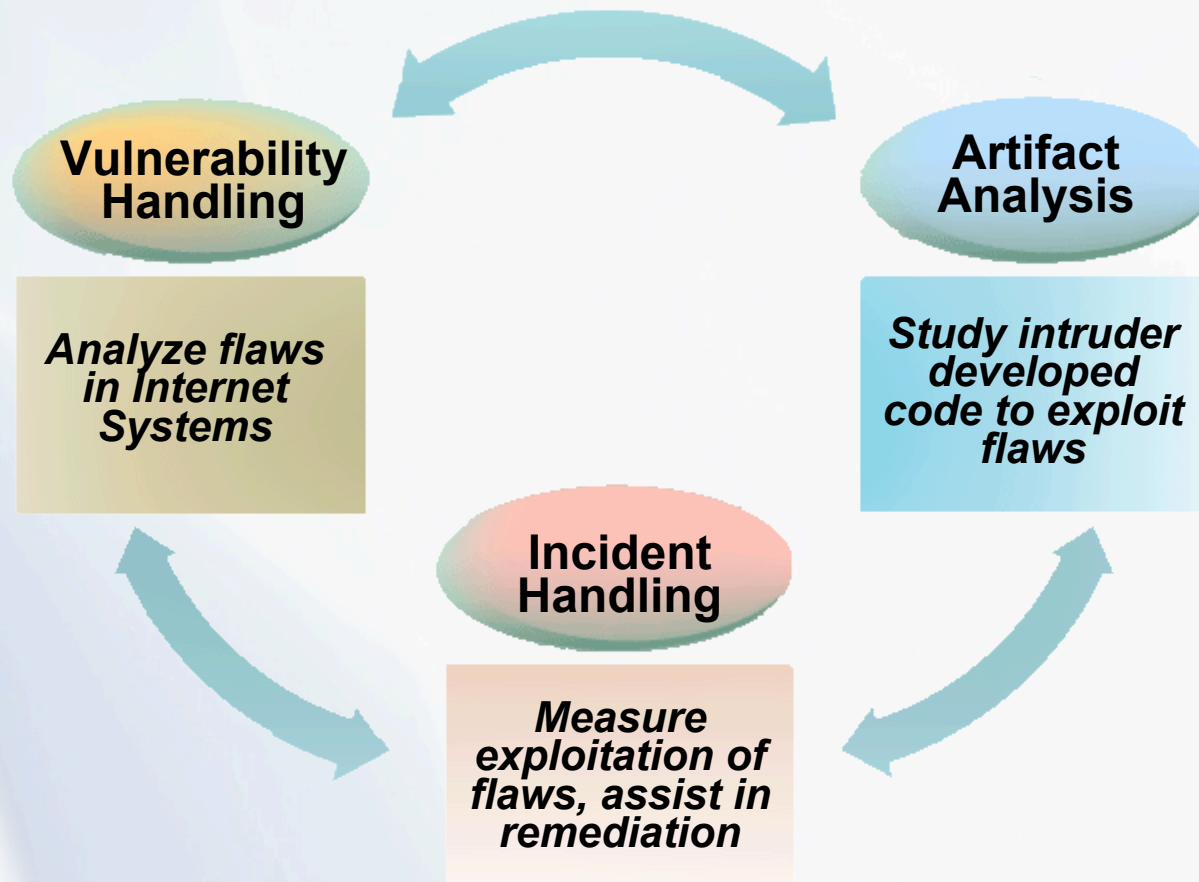
- **Ensure confidentiality and impartiality**
  - We do not identify victims but can pass information anonymously and describe activity without attribution
- **Provide trusted, unbiased information**
  - We do not sell consulting services or software
  - We do not overstate or understate the risks of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



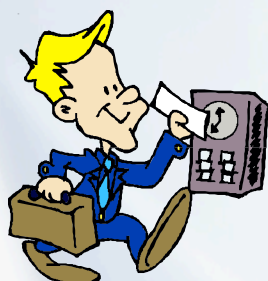
# CERT<sup>®</sup>/CC Mission

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

# CERT<sup>®</sup>/CC Teams



# Intruders



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



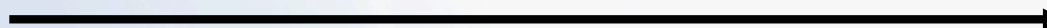
# Denial of Service (DoS)

- **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

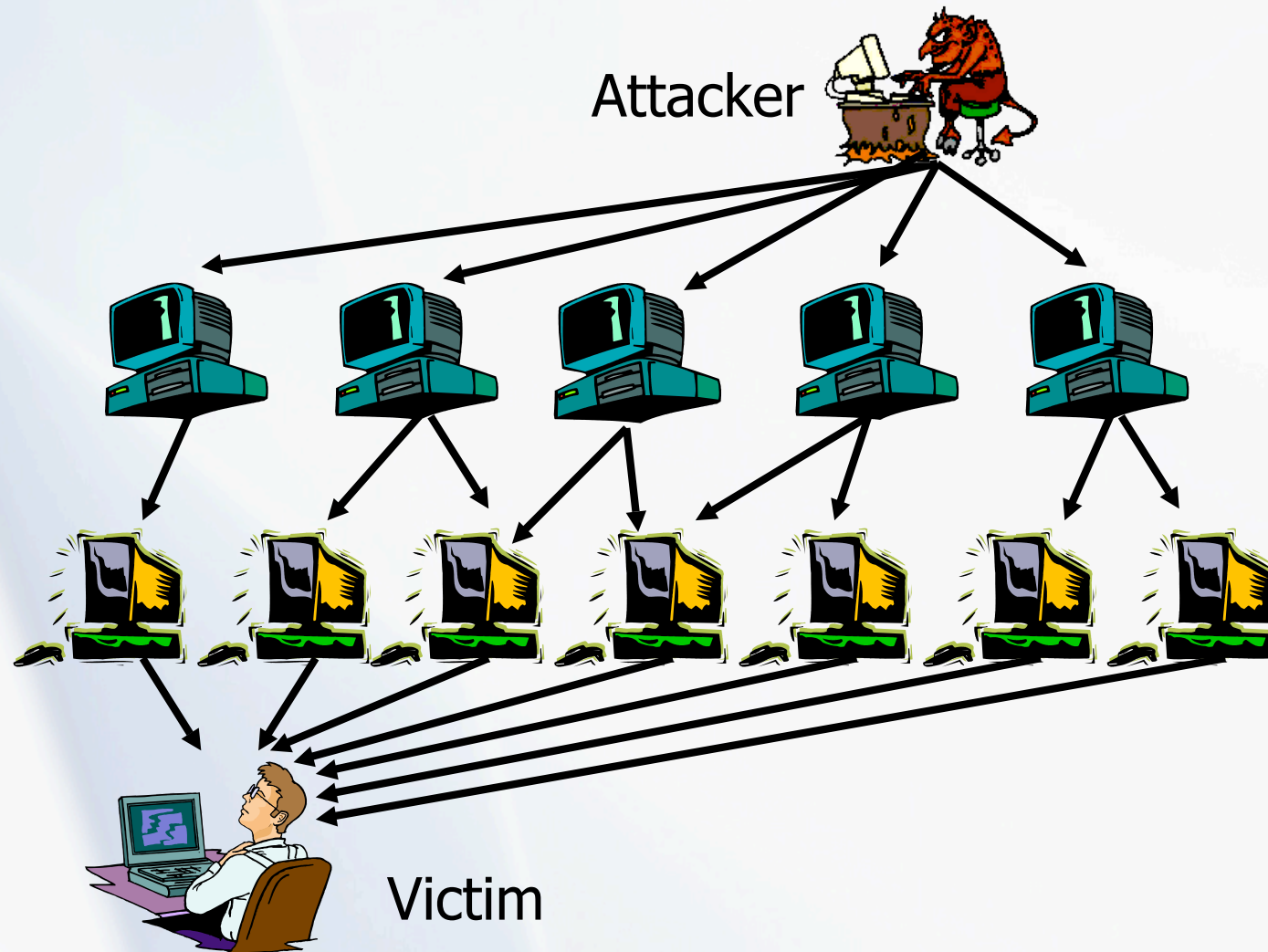
Attacker



Victim



# Distributed Denial of Service (DDoS)



# What is a Software Vulnerability?

---

- **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

---

- **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)

---

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

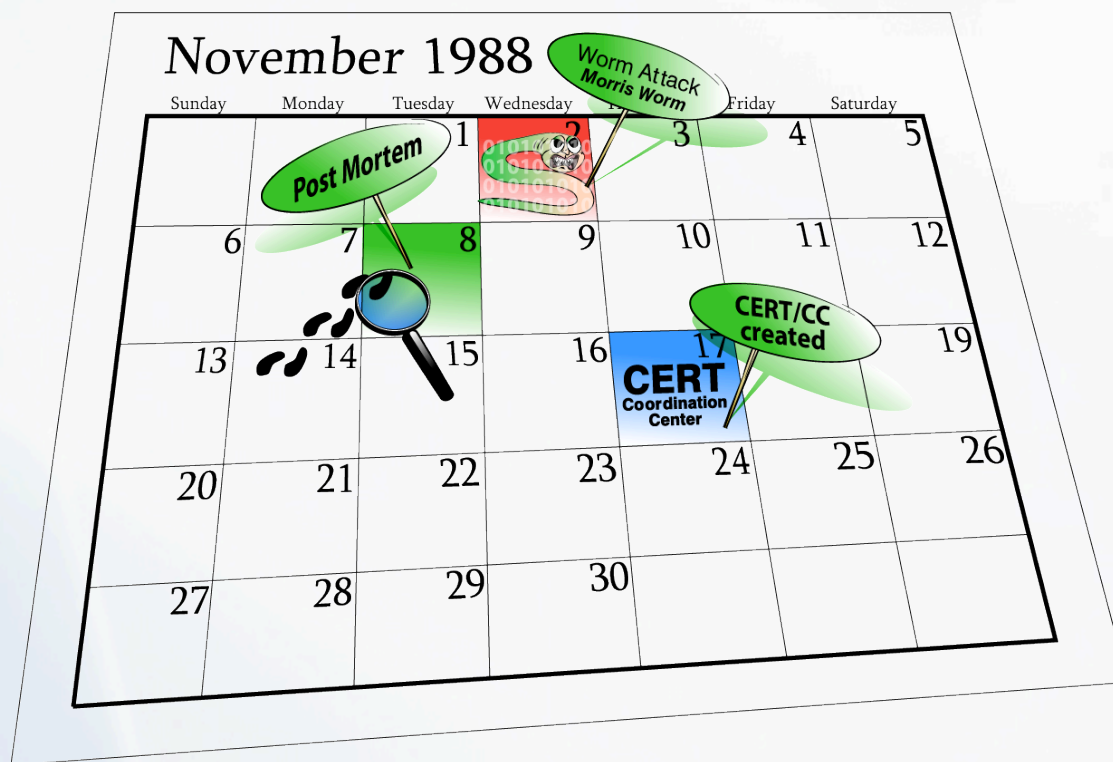
# Vulnerability Disclosure

---

- **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

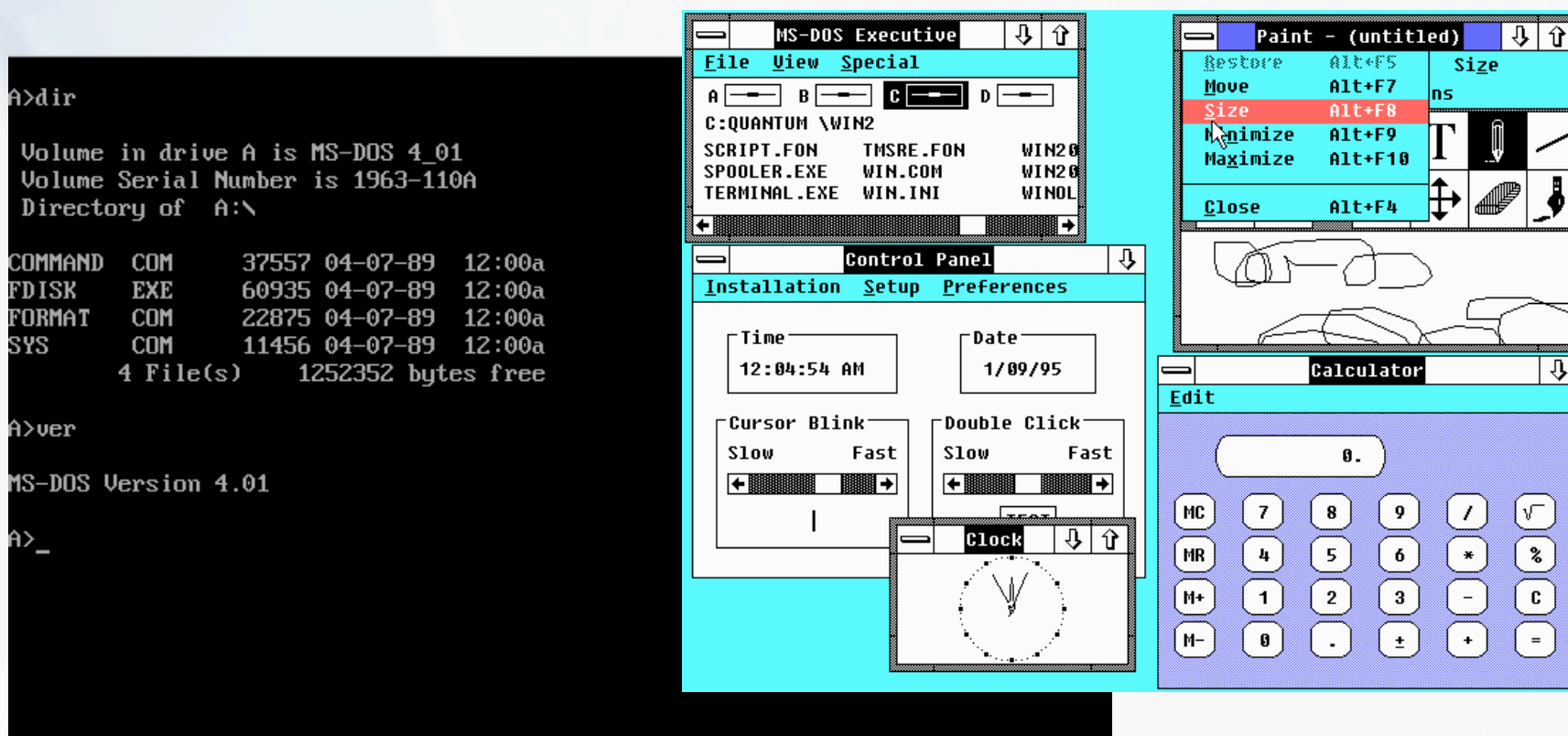
# Vulnerability Trends

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



# The Internet in 1988

- DOS 4.0 and Windows 2.0



## The Internet in 1988 (2)

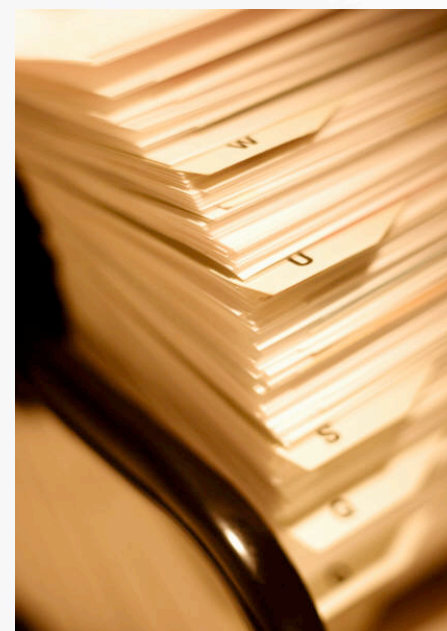
- 60,000 hosts
- Relatively slow network connections
- Primarily UNIX systems





# Finger Daemon

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

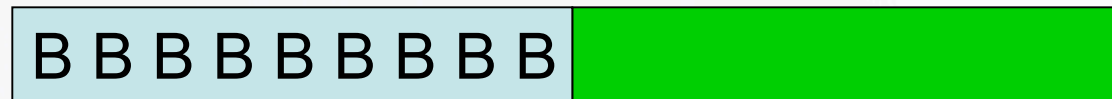


# Buffer Overflow

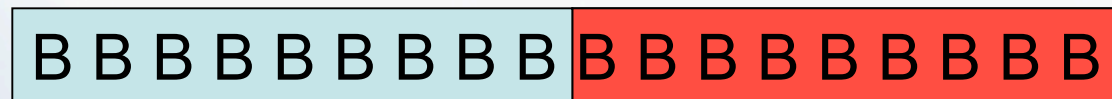
User Input

Fixed Buffer

Adjacent Memory



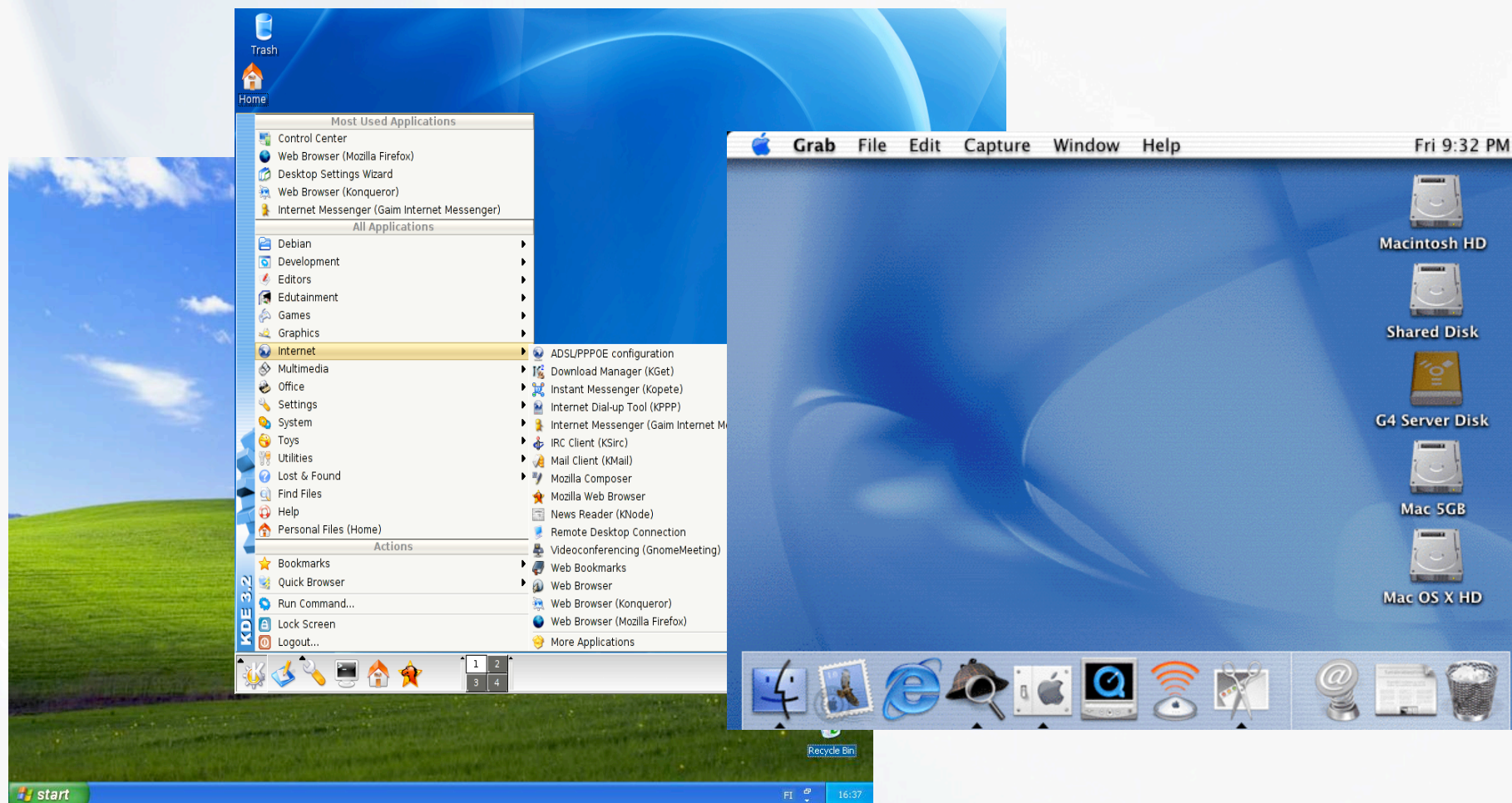
Memory OK



Buffer Overflow

# The Internet in 2005

- Windows XP, Linux, Mac OS X



# The Internet in 2005 (2)

---

## Then (1988)

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

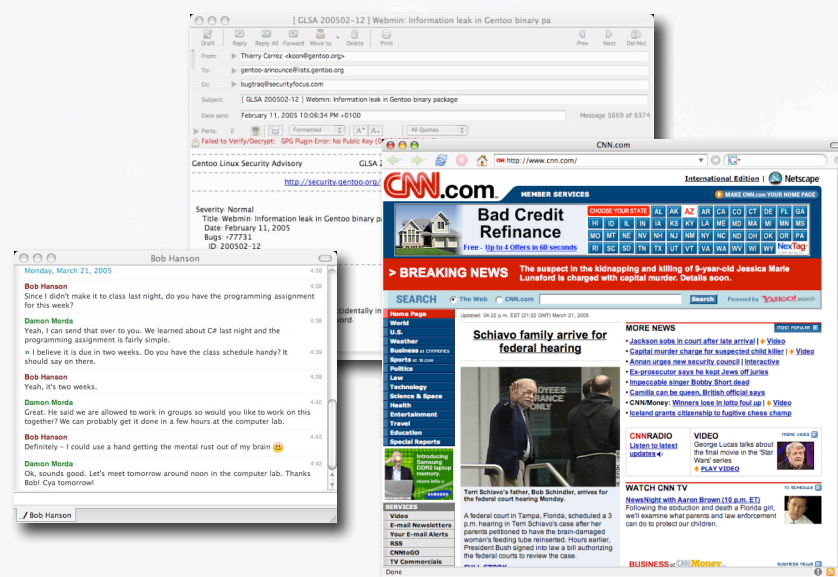
## Today (2005)

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



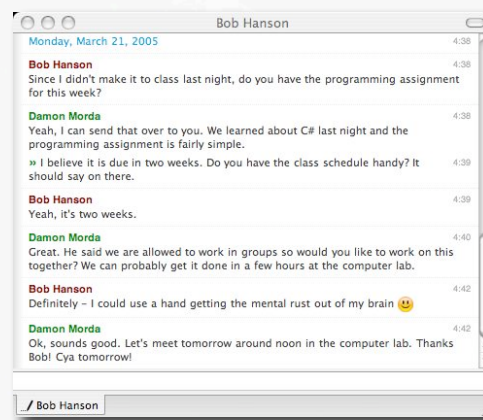
# Vulnerability Trends

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



# Instant Messaging

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





# Instant Messaging Case

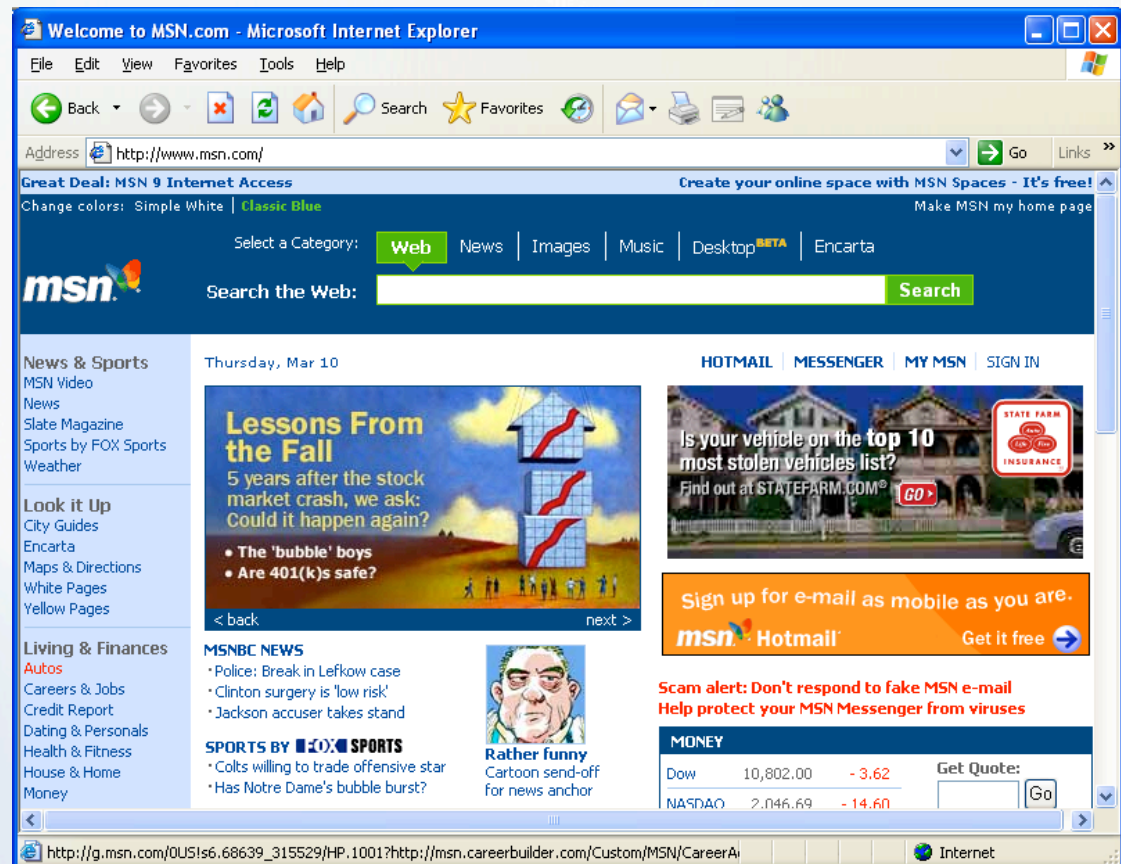
---

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

# Web Browsing

## The Modern Web Browser

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



# “Drag and Drop”

- **August 18, 2004**
  - Internet Explorer targeted
- **February 25, 2005**
  - New variant targets Firefox 1.0



# “Drag and Drop” Vulnerability

US-CERT Cyber Security Tip ST04-018 -- Understanding Digital Signatures - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.us-cert.gov/cas/tips/ST04-018.html

Home | FAQ | Contact | Privacy Policy | Unsubscribe from Alerts

**US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Search US-CERT  
Go  
> Advanced Search

**National Cyber Alert System**

Cyber Security Tip ST04-018

**Understanding Digital Signatures**

Digital signatures are a way to verify that an email message is really from the person who supposedly sent it and that it hasn't been changed.

**Invisible JPEG Exploit**

**What is a digital signature?**

You may have received emails that have a block of letters and numbers at the bottom of the message. Although it may look like useless text or some kind of error, this information is actually a digital signature. To generate a signature, a mathematical algorithm is used to combine the information in a key with the information in the message. The result is a random-looking string of letters and numbers.

**Why would you use one?**

Because it is so easy for attackers and viruses to spoof email addresses (see [Using Caution with Email Attachments](#) for more information), it is sometimes difficult to identify legitimate messages. Authenticity may be especially important for business correspondence—if you receive a message from someone who provides or verifies information, you want to ensure that the information is coming from the correct source. A signed message also indicates that changes have not been made to the content since it was sent; any changes would cause the signature to break.

**How does it work?**

Before you can understand how a digital signature works, there are some terms you should know:

- **Keys** - Keys are used to create digital signatures. For every signature, there is a public key and a private key.
  - **Private key** - The private key is the portion of the key you use to actually sign an email message. The private key is protected by a password, and you should never give your private key to anyone.
  - **Public key** - The public key is the portion of the key that is available to other people. Whether you upload it to a public key ring or send it to someone, this is the key other people can use to check your signature. A list of other people who have signed your key is also included with your public key. You will only be able to see their identify if you already have their public keys on your key ring.
- **Key ring** - A key ring contains public keys. You have a key ring that contains the keys of people who have sent you their keys or whose keys you have gotten from a public key server. A public key server contains keys of people who have chosen to upload their keys.
- **Fingerprint** - When confirming a key, you will actually be confirming the unique series of letters and numbers that comprise the fingerprint of the key. The fingerprint is a different series of letters and numbers than the chunk of information that appears at the bottom of a signed email message.
- **Key certificates** - When you select a key on a key ring, you will usually see the key certificate, which contains information about the key, such as the key owner, the date the key was created, and the date the key will expire.
- **“Web of trust”** - When someone signs your key, they are confirming that the key actually belongs to you. The more signatures you collect, the stronger your key becomes. If someone sees that your key has been signed by other people that he or she trusts, he or she is more inclined to trust your key. **Note:** Just because someone else has trusted a key or you find it on a public key ring does not mean you should automatically trust it. You should always verify the fingerprint yourself.

The process for creating, obtaining, and using keys is fairly straightforward:

1. Generate a key using software such as PGP, which stands for Pretty Good Privacy, or GnuPG, which stands for GNU Privacy Guard.

# Malware

- **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)

---

- **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)

---

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

# Worms and Viruses

---

- **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

---

- **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

- **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

- 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

---

- **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

---

- **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](http://www.w3schools.com/browsers/browsers_stats.asp)*

# What you can do...

---

- **Defense in depth**
- **External validation**
- **User education**

# What we can do as a community...

---

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

# Remember....

---

- 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.**

## Questions & Comments...

