RAMAIAH
Institute of Technology

Chapter 1: Running With Scissors

Mrs.Shubha Malige
Asst. Professor
Department of CSE (AI&ML), CSE (Cyber Security)
MSRIT, Bangalore

Agenda

- **Running with Scissors**
- **Gauging the Threat**
- **Security Concepts**
- **Development Platforms**
- **Strings**
- **Character Strings**
- **Common String Manipulation Errors**
- **String Vulnerabilities and Exploits**

Running with Scissors

- The W32.Blaster.Worm
  - Discovered on August 11, 2003.
  - Infected unpatched system connected to the Internet without user involvement.
  - At least eight million Windows systems have been infected by this worm [Lemos 04].
  - Economic Damage > $500M$

The W.32 Blaster Worm

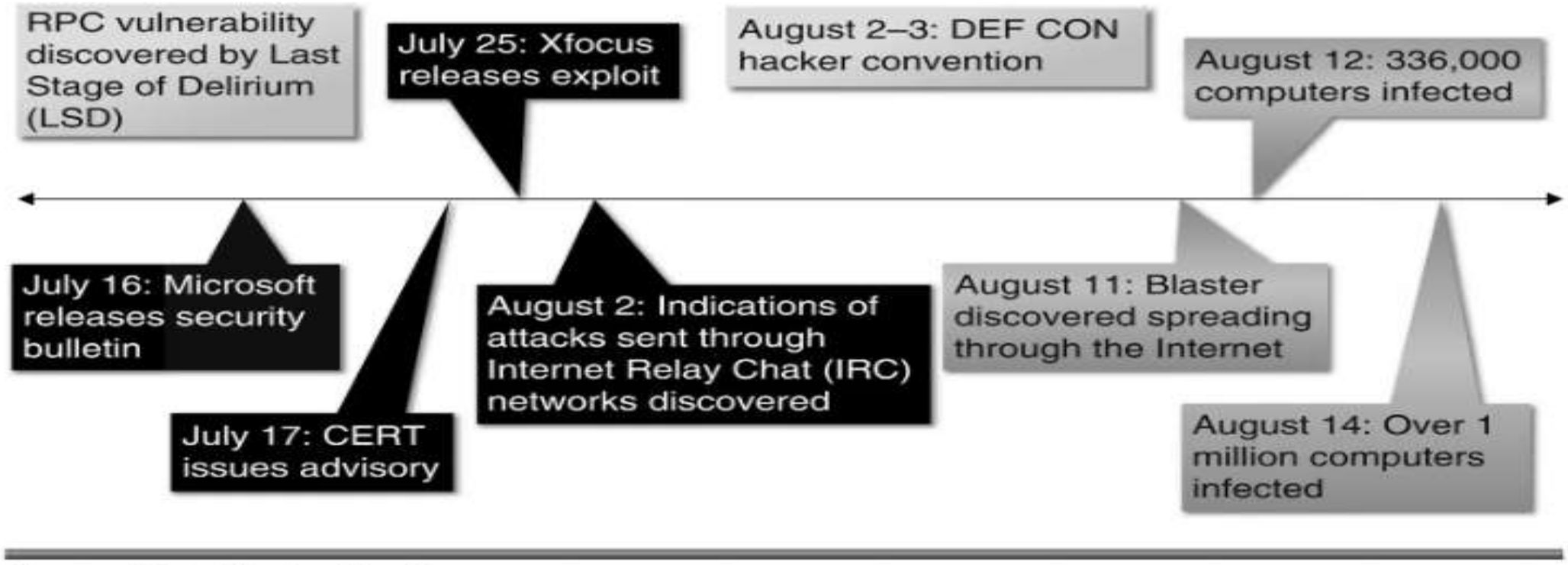


Figure 1.1 Blaster timeline

The W.32 Blaster Worm

- Blaster:
  - Checks to see if the computer is already infected.
    - Adds "windows auto update" = "msblast.exe" to registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Runs when Windows starts.
  - Generates a random IP address.
  - Attempts to infect the computer with that address.
  - Sends data on TCP port 135 to exploit the DCOM RPC vulnerability on either Windows XP or Windows 2000.

Gauging the threat

- The risk of producing insecure software systems can be evaluated by
  - Looking at historic risk.
  - The potential for future attacks.
- Historic risk can be measured by
  - Looking at the type.
  - Cost of perpetrated crimes.
- The potential for future attacks can be partially gauged by:
  - Evaluating emerging threats.
  - The security of existing software systems.

What is the Cost?

- Based on conservative projections, about 100,000 new software vulnerabilities will be identified in 2010 alone.
- The number of security incidents worldwide will swell to about 400,000 a year, or 8,000 per work week [Berinato 04].

Table 1.1 Judgment on Coverage of Cost Categories by Known Estimates*

Type of Cybercrime	Global Estimate ($ million)	Reference Period
Cost of Genuine Cybercrime		
Online banking fraud	320	2007
Phishing	70	2010
Malware (consumer)	300	2010
Malware (businesses)	1,000	2010
Bank technology countermeasures	97	2008–10
Fake antivirus	22	2010
Copyright-infringing software	150	2011
Copyright-infringing music, etc.	288	2010
Patent-infringing pharmaceutical	10	2011
Stranded traveler scam	200	2011
Fake escrow scam	1,000[a]	2011
Advance-fee fraud		2011
Cost of Transitional Cybercrime		
Online payment card fraud	4,200[a]	2010
Offline payment card fraud		
Domestic	2,100[a]	2010
International	2,940[a]	2010
Bank/merchant defense costs	2,400	2010

What is the Cost?

Who is the Threat?

- Threat is a person, group, organization, or foreign power that has been the source of past attacks or may be the source of future attacks.
- Threats include:
  - Hackers
  - Insiders
  - Criminals
  - Competitive Intelligence Professionals
  - Terrorists
  - Information Warriors.

Hackers

- Motivated by curiosity and peer recognition from other hackers.
- Write programs that *expose vulnerabilities* in computer software.
- The methods used to disclose these vulnerabilities varies from a policy of responsible disclosure to a policy of full disclosure.

Insiders

- The threat comes from a current or former employee or contractor of an organization.
- Has legitimate access to the information that was compromised.
- Do not need to be technically sophisticated to carry out attacks.
- Technically sophisticated insiders can launch attacks with immediate and widespread impact.
- Technical insiders can cover their tracks.

Criminals

- Common crimes include:
  - Auction fraud,
  - Identity theft.
  - Extortion.
- Phishing
  - Lure victims to fake website to gather account data.
- Pfarming
  - Exploit DNS vulnerabilities to redirect web traffic to malicious site.

RAMAIAH
Institute of Technology

Corporate Spies

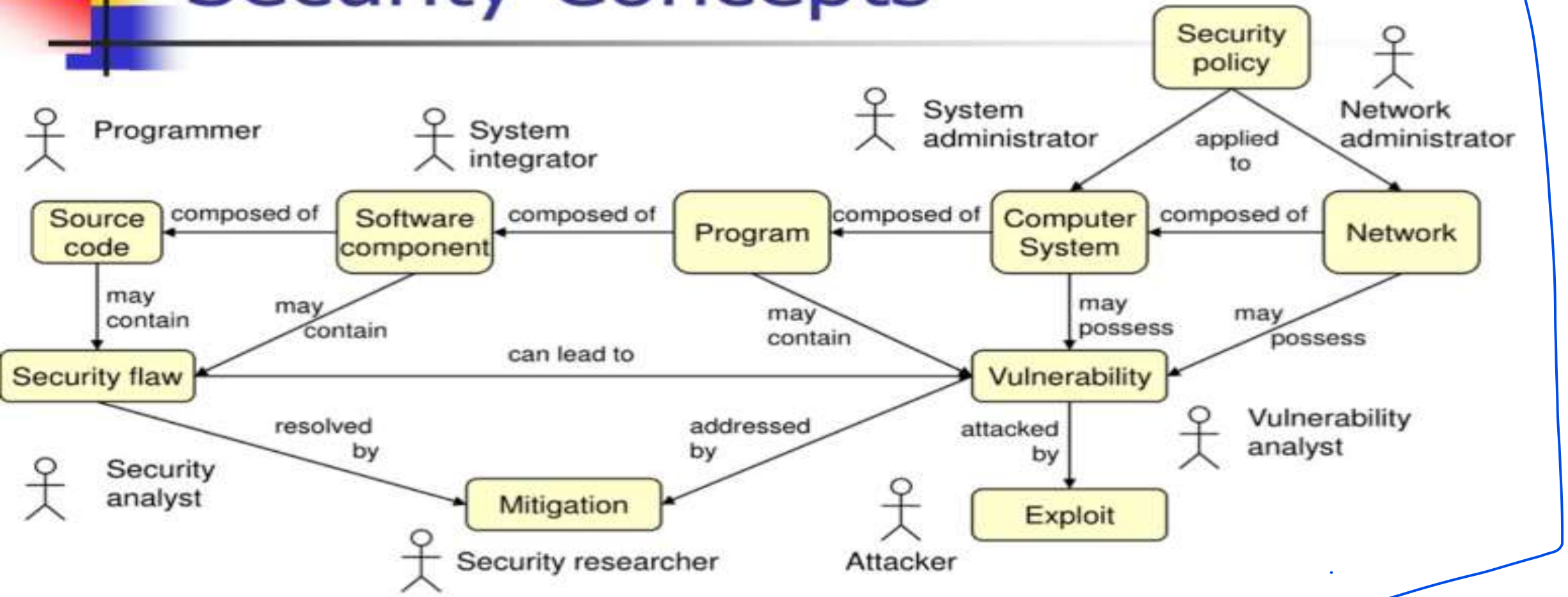
- Corporate spies:
  - Call themselves *competitive intelligence professionals.*
  - Have their own professional association—the Society for Competitive Intelligence Professionals (SCIP).
  - May work from inside a target organization, obtaining employment to steal and market trade secrets.
  - Conduct other forms of corporate espionage.

- Cyber-terrorism can be defined as unlawful attacks or threats of attack against computers, networks, and other information systems to intimidate or coerce a government or its people to further a political or social objective [Denning 00].

Information Warriors

- Eight nations have developed cyber-warfare capabilities comparable to that of the United States.
- More than 100 countries are trying to develop them.
- Twenty-three nations have targeted U.S. systems.

Security Concepts



RAMAIAH
Institute of Technology

Security Concepts

- *Computer security* is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks [Howard 97].
- A *programmer* is concerned with properties of source code such as correctness, performance, and security.
- A *system integrator* is responsible for integrating new and existing software components to create programs or systems that satisfy a particular set of customer requirements.
- *System administrators* are responsible for managing and securing one or more systems including installing and removing software, installing patches, and managing system privileges.

RAMAIAH
Institute of Technology

Security Concepts

- *Network administrators* are responsible for managing the secure operations of networks.
- A *security analyst* is concerned with properties of security flaws and how to identify them.
- A *vulnerability analyst* is concerned with analyzing vulnerabilities in existing and deployed programs.

RAMAIAH
Institute of Technology

Security Concepts

- A *security researcher* develops mitigation strategies and solutions and who may be employed in industry, academia, or government.

- The *attacker:*
  - Is a malicious actor who exploits vulnerabilities to achieve an objective.
  - These objectives vary depending on the threat.
  - The attacker can also be referred to as the adversary, malicious user, hacker, or other alias.

RAMAIAH
Institute of Technology

Security Policy

- A Security Policy is a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

RAMAIAH
Institute of Technology

Security Flaws

- **Software Defects:**
  - A software defect is the encoding of a human error into the software, including omissions.

Security Flaw:

- A *security flaw* is a software defect that poses a potential security risk.
- Eliminating software defects eliminate security flaws.

RAMAIAH
Institute of Technology

Vulnerabilities

- *Vulnerability*
  - set of conditions that allows an attacker to violate an explicit or implicit security policy.
  - Not all security flaws lead to vulnerabilities.
- *Security flaw*
  - can cause a program to be vulnerable to attack.
- Vulnerabilities can also exist without a security flaw.

RAMAIAH
Institute of Technology

Exploits

- Exploit:
  - Proof-of-concept exploits are developed to prove the existence of a vulnerability.
  - Proof-of-concept exploits are beneficial when properly managed.
  - Proof-of-concept exploit in the wrong hands can be quickly transformed into a worm or virus or used in an attack.

RAMAIAH
Institute of Technology

Mitigation

- **Mitigation:**
  - *Mitigations* are methods, techniques, processes, tools, or runtime libraries that can prevent or limit exploits against vulnerabilities.
  - At the source code level, a mitigation might be replacing an unbounded string copy operation with a bounded one.
  - At a system or network level, a mitigation might involve turning off a port or filtering traffic to prevent an attacker from accessing a vulnerability.

C and C++

- C and C++:
  - Popular programming languages.
  - The vast majority of vulnerabilities that have been reported to the CERT/CC have occurred in programs written in one of these two languages.

What is the problem with C?

- Short term solutions:
  - Educating developers in how to program securely by recognizing common security flaws and applying appropriate mitigations.
- Long term solutions:
  - Language standard, compilers, and tools evolve.

Legacy Code

- A significant amount of legacy C code was created (and passed on) before the standardization of the language.
- Legacy C code is at higher risk for security flaws because of the looser compiler standards and is harder to secure because of the resulting coding style.

RAMAIAH
Institute of Technology

Operating Systems

Microsoft Windows:- Microsoft Windows family of operating system products, including Windows 7, Windows Vista, Windows XP, Windows Server 2003, Windows 2000.

Linux: Linux is free Unix Derivative created by Linus Torvalds with the assistance of developers around the world.

Other Languages

- Many security professionals recommend using other languages, such as Java.
- Adopting Java is often not a viable option because of:
  - Existing investment in C source code,
  - Programming expertise,
  - Development environments.
- Another alternative to using C is to use a C dialect, such as Cyclone [Jim 02].
- Cyclone is currently supported on x86 Linux, and on Windows using Cygwin.

Compilers

- Microsoft's Visual C++ is the predominant C and C++ compiler on Windows platforms.
- Visual C++ includes
  - Visual C++ 6.0
  - Visual C++ .NET 2002
  - Visual C++ .NET 2003
  - Visual C++ 2005 Beta1 and Beta2
- The GCC compilers are the predominant C and C++ compilers for Linux platforms.