Viruses, Trojan Horses, and Worms

- Some software is a security risk, often all called “viruses”, but there are 3 different classes:
  - **Viruses**
    - program or code that **replicates**; i.e., infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium
    - most only replicate, but many do a large amount of damage
  - **Worms**
    - program that **makes copies of itself**; for example, from one disk drive to another, or by copying itself using email or another transport mechanism and spreads through a network
    - some worms run over several computers; others communicate among themselves over the network
    - may do damage and compromise the security of the computer
    - may be malicious or may take up system resources, causing a slowdown in performance

---

Some material adapted from Web 101 Copyright © 2007 Pearson Education, Inc. Publishing as Pearson Addison-Wesley

See Symantec Security Response Glossary

---

Viruses, Trojan Horses, and Worms

- Some software is a security risk, often all called “viruses”, but there are 3 different classes:
  - **Trojan horses**
    - program that slips into a computer under the guise of another program but **neither replicates nor copies** itself
    - often, someone emails you a Trojan Horse, e.g., a game that when you run it, you also run the Trojan horse
    - a Trojan horse does not email itself
    - causes damage or compromises the security of the computer, e.g., could record your keystrokes or allow someone to access your computer

---

See Symantec Security Response Glossary
What are the risks?

- **Client-side Vulnerabilities:**
  - C1. Web Browsers
  - C2. Office Software
  - C3. Email Clients
  - C4. Media Players

- **Server-side Vulnerabilities:**
  - S1. Web Applications
  - S2. Windows Services
  - S3. Unix and Mac OS Services
  - S4. Backup Software
  - S5. Anti-virus Software
  - S6. Management Servers
  - S7. Database Software

- **Security Policy & Personnel:**
  - H1. Excessive User Rights and Unauthorized Devices
  - H2. Phishing/Spear Phishing
  - H3. Unencrypted Laptops and Removable Media

- **Application Abuse:**
  - A1. Instant Messaging
  - A2. Peer-to-Peer Programs

- **Network Devices:**
  - N1. VoIP Servers and Phones

**All systems at risk!!**

What actions can be taken?

- **How do you know your computer is infected?**
  - There is no particular way
  - Be aware of any unusual or unexpected behaviors

- **If your computer gets infected with malicious code, there are steps you can take to recover.**
  - The fastest and easiest way to detect and remove malicious programs from your computer is to run a virus removal program on a regular schedule.
  - Companies like [Symantec](https://www.symantec.com), [McAfee](https://www.mcafee.com), and others provide virus removal tools
What actions can be taken?

- **Minimize the damage**
  - if you have access to an IT department, contact them immediately
  - if you are on your home computer or a laptop, disconnect your computer from the internet
    - prevents access to your computer to perform tasks such as locating personal data, manipulating or deleting files, or using your computer to attack other computers.
- **Remove the malicious code**
  - use anti-virus software, update the virus definitions (if possible), and perform a manual scan of your entire system
  - reinstall your operating system, usually with a system restore disk and install all of the appropriate patches to fix known vulnerabilities

Take control & secure your computer

- **Use antivirus software and keep it updated**
  - scan files on computer, disks, CDs, email and downloaded files
  - if you need to work without a virus scanner, you should manually scan each file before opening or executing it
- **Keep bootable disks out of your drive unless you are actively working with the files on the disk**
  - Some viruses can hide on the boot sector on a disk
  - These are triggered when the computer starts up and accesses the disk
- **Use a firewall on your home computer (especially if you use a broadband connection)**
- **Encrypt all files that contain sensitive information or store them offline on removable media**
E-Mail Viruses

- E-mail is the number one source of computer viruses
  - attachments are the most common culprit
  - some attachments contain scripts
    - a script is a small program written in a scripting language (e.g. Visual Basic)
  - Microsoft Word documents are a popular source of viruses
- Mailers that render (html) messages into Web-like displays are susceptible to script attacks
  - some messages contain scripts
  - if the script is automatically executed, it can cause harm
- You can take precautions:
  - configure your mailer to not open attachments automatically
  - configure your mailer to not display html automatically
  - save attachments and scan them first
  - don’t open a document that contains a macro

Threats

- CERT
  - Microsoft - Multiple Vulnerabilities November 9, 2010
  - Oracle Multiple Vulnerabilities October 14, 2010
  - Microsoft - Multiple Vulnerabilities October 12, 2010
  - Adobe Reader and Acrobat Affected by Multiple Vulnerabilities October 6, 2010
  - Adobe Flash Vulnerabilities September 20, 2010
- McAfee
  - Global Threat Level = “Elevated”
    - Critical Security-related updates have been released by multiple vendors (Microsoft, Adobe, Oracle, VMWare).
    - "Low" malware activity observations around the PWS-Zbot, FakeAlert and Pinkslipbot families. October 18, 2010
Threats

- Some threats can contain a blend of different types of attacks
- W32/Nimda worm (2001)
  - spread through a variety of means (via email, open network shares and browsing of compromised web sites) exploiting vulnerabilities in Microsoft Windows and backdoors left by Code Red II and Sadmind worms
- Conficker (2009)
  - spreading through low security networks, memory sticks, and PCs without current security updates
  - infects nearly 20 million Microsoft server systems running everything from Windows 2000 to Windows Vista and Windows Server 2008, including French air force, Royal Navy warships and submarines, Sheffield Hospital network, UK Ministry of Defence, German Bundeswehr all affected
  - Microsoft has allocated $250,000 to identify its creator

Denial-of-service attack

- Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack)
  - an attempt to make a computer resource unavailable to its intended users.
  - common method of attack involves saturating the target (victim) machine with external communications requests
- Denial-of-service attacks are considered violations of the IAB’s Internet Proper Use Policy
  - also commonly constitute violations of the laws of individual nations
Summary of Threats

- **AdWare, Spyware**
  - displays commercial advertisements, mostly a nuisance, but also can install tracking software
  - monitors usage and/or keystrokes and sends data to remote user, dangerous
- **Pharming**
  - redirects valid URLs to bogus sites, dangerous
- **Phishing, Spear Phishing**
  - emails requests for personal information, dangerous
- **Rootkit**
  - undetectable modifications to the OS that permit remote, surreptitious access to your computer, very dangerous
- **Spam**
  - unsolicited e-mail, low (unless you open an attachment)
- **Dangerous**
  - Trojan Horse, Virus, Worm

Some material adapted from Web 101 Copyright © 2007 Pearson Education, Inc. Publishing as Pearson Addison-Wesley

Computer and Information Security

**Security Goals**

- **Confidentiality**
  - Concealment of information or resources
- **Integrity**
  - Trustworthiness of data or resources
- **Availability**
  - Ability to use information or resources

Adapted from COM 260 slides developed by S. Jane Fritz St. Joseph's College
Why do we need security?

- Increased reliance on Information Technology:
  - e-mail, e-banking, e-commerce, e-trading, etc.
  - Supply chains, services architectures
  - Critical infrastructure
  - Finance and markets
  - Healthcare
  - Research
  - Defense
  - Entertainment

Security Concerns

- Damage to any IT-based system or activity can result in severe disruption of services and losses
- Systems connected by networks are more prone to attacks and also suffer more as a result of the attacks than stand-alone systems (Reasons?)
- Concerns such as the following are common
  - How do I know the party I am talking on the network is really the one I want to talk?
  - How can I be assured that no one else is listening and learning the data that I send over a network?
  - Can I ever stay relaxed that no hacker can enter my network and play havoc?

Adapted from COM 260 slides developed by S. Jane Fritz St. Joseph's College
### ISO 7 Layer Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application How application uses network</td>
</tr>
<tr>
<td>6</td>
<td>Presentation How to represent &amp; display data</td>
</tr>
<tr>
<td>5</td>
<td>Session How to establish communication</td>
</tr>
<tr>
<td>4</td>
<td>Transport How to provide reliable delivery (error checking, sequencing, etc.)</td>
</tr>
<tr>
<td>3</td>
<td>Network How addresses are assigned and packets are forwarded</td>
</tr>
<tr>
<td>2</td>
<td>Data Link How to organize data into frames &amp; transmit</td>
</tr>
<tr>
<td>1</td>
<td>Physical How to transmit “bits”</td>
</tr>
</tbody>
</table>

### OSI Network Stack and Attacks

- **Application**
  - Sendmail, FTP, NIS bugs, chosen-protocol and version-rollback attacks
  - RPC worms, portmapper exploits
  - SYN flooding, RIP attacks, sequence number prediction
  - IP smurfing and other address spoofing attacks
  - WEP attacks

- **Presentation**
  - Network port scanning is an information gathering process, and when performed by unknown individuals it is considered a prelude to attack

- **Session**
  - A SYN synchronization packet is sent to a receiving application, which acknowledges receipt of this packet with a SYN/ACK, to which the sending application responds with an ACK. In a SYN flood attack, the hacker sends a large volume of SYN packets to a victim.

- **Transport**
  - A key recovery attack on WEP intercepts a number of packets to recover the secret key.

- **Network**
  - A smurf program builds a network packet that appears to originate from another address (spoofing) and contains a ping message that is addressed to an IP broadcast address; the echo responses to the ping message are sent back to the “victim” address.

- **Data Link**

**Only as secure as the single weakest layer...**
Attacks, Services and Mechanisms

- **Security Attack**: Any action that compromises the security of information.
- **Security Mechanism**: A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service**: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Attacks

- **Interruption**: This is an attack on availability
  - Disrupting traffic
  - Physically breaking communication line
- **Modification**: This is an attack on integrity
  - Corrupting transmitted data or tampering with it before it reaches its destination
- **Interception**: This is an attack on confidentiality
  - Overhearing, eavesdropping over a communication line
- **Fabrication**: This is an attack on authenticity
  - Faking data as if it were created by a legitimate and authentic party

Figure 1.1 Security Threats
Threats and Attacks

- Attack - an assault on system security - an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.
- Threat - a potential for violation of security or a possible danger that might exploit a vulnerability
  - Disclosure – unauthorized access to information
  - Deception – acceptance of false data
  - Disruption - interruption or prevention of correct operation
  - Usurpation - unauthorized control of some part of a system

Friends and enemies: Alice, Bob, Eve

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Eve (intruder) may intercept, delete, add messages

**Passive Attacks:** Eve reads Alice’s message to Bob or analyzes traffic between Bob & Alice

**Active Attacks:** Eve masquerades as Alice and sends messages to Bob
Authentication

- Alice sends the message, "I am Alice," to Bob
- Bob chooses a nonce, $R$, and sends it to Alice
- Alice encrypts the nonce using Alice and Bob's symmetric secret key, $K_{A-B}$, and sends the encrypted nonce, $K_{A-B}(R)$ back to Bob.
- the fact that Alice knows $K_{A-B}$ and uses it to encrypt a value that lets Bob know that the message he receives was generated by Alice. The nonce is used to insure that Alice is "live."
- Bob decrypts the received message. If the decrypted nonce equals the nonce he sent Alice, then Alice is authenticated.
Who might Bob, Alice be?

... well, real-life Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

The language of cryptography

plaintext message

plaintext

ciphertext

ciphertext, encrypted with key \( K_A \)

\( m = K_R(K_A(m)) \)

Alice's encryption key

Bob's decryption key

encryption algorithm

decryption algorithm
Types of Cryptography

- Crypto often uses keys:
  - Algorithm is known to everyone
  - Only “keys” are secret
- Symmetric key cryptography
  - Involves the use one key
- Public key cryptography
  - Involves the use of two keys

Symmetric key cryptography

- Bob and Alice share same (symmetric) key: $K_S$
- Key is knowing substitution pattern in mono alphabetic substitution cipher
- Q: how do Bob and Alice agree on key value?
Public key cryptography

<table>
<thead>
<tr>
<th>Alice</th>
<th>plaintext message, m</th>
<th>encryption algorithm</th>
<th>ciphertext $K_B^+(m)$</th>
<th>decryption algorithm</th>
<th>plaintext message $m = K_B^-(K_B^+(m))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>$K_B^+$ Bob's public key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$K_B^-$ Bob's private key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Privacy

- An important issue today
- Individuals feel
  - Uncomfortable: ownership of information
  - Unsafe: information can be misused
  - (e.g., identity thefts)
- Enterprises need to
  - Keep their customers feel safe
  - Maintain good reputations
  - Protect themselves from any legal dispute
  - Obey legal regulations
Definition

- Privacy is the ability of a person to control the availability of information about and exposure of him- or herself. It is related to being able to function in society anonymously (including pseudonymous or blind credential identification).
- Types of privacy giving raise to special concerns:
  - Political privacy
  - Consumer privacy
  - Medical privacy
  - Information technology end-user privacy; also called data privacy
  - Private property

Data Privacy

- Data Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.
- The most common sources of data that are affected by data privacy issues are:
  - Health information
  - Criminal justice
  - Financial information
  - Genetic information
Data Privacy

- The challenge in data privacy is to share data while protecting the personally identifiable information.
  - Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in aggregate form.
  - The idea of sharing the data in aggregate form is to ensure that only non-identifiable data are shared.

- The legal protection of the right to privacy in general and of data privacy in particular varies greatly around the world.

Data vs Information

- Protecting information means to protect not only the data directly representing the information.
- Information must be protected also against transmissions through:
  - Covert channels
  - Inference
    - It is typical of database systems
    - It refers to the derivation of sensitive information from non-sensitive data
### Inference - Example

- Assume that there is a policy stating that the average grade of a single student cannot be disclosed; however statistical summaries can be disclosed.
- Suppose that an attacker knows that Carol is a female CS student.
- By combining the results of the following legitimate queries:
  - Q1: SELECT Count (*) FROM Students WHERE Sex = 'F' AND Programme = 'CS'
  - Q2: SELECT Avg (Grade Ave) FROM Students WHERE Sex = 'F' AND Programme = 'CS'
  - The attacker learns from Q1 that there is only one female student so the value 70 returned by Q2 is precisely her average grade.
Technologies with Privacy Concerns

- Biometrics (DNA, fingerprints, iris) and face recognition
- Video surveillance, ubiquitous networks and sensors
- Cellular phones
- Personal Robots
- DNA sequences, Genomic Data

Approaches

- Anonymization Techniques
  - Have been investigated in the areas of networks (see the Anonymity Terminology by Andreas Pfitzman) and databases (see the notion of k-anonymity by L. Sweeney)
- Privacy-Preserving Data Mining
- P3P policies
  - Are tailored to the specification of privacy practices by organizations and to the specification user privacy preferences
- Hippocratic Databases
  - Are tailored to support privacy policies
- Fine-Grained Access Control Techniques
- Private Information Retrieval Techniques
Privacy vs Security

- Privacy is not just confidentiality and integrity of user data
- Privacy includes other requirements:
  - Support for user preferences
  - Support for obligation execution
  - Usability
  - Proof of compliance