Welcome to Section 10

Computer Security

By: Imran Afzal
www.utclisolutions.com

Types of Security Breach

- **Data**
  - Steal
  - Corrupt
  - Remove
- **Application**
  - Apache webserver
  - Database
  - Financial applications
- **Operating System**
  - Filesystem corruption
  - System failure
  - Process management
- **Hardware**
  - Attack on CPU, Memory, etc.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- Distributed denial-of-service (DDoS) attack
- Hacking
- Malware
- Pharming
- Phishing
- Ransomware
- Spam
- Spoofing
- Spyware
- Trojan Horses
- Wi-Fi Eavesdropping
- Viruses
- Worms

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Distributed denial-of-service (DDoS) attack**
  - when a hacker put a network of zombie computers (other people computers) to attack or destroy a specific website or server. That increase in the volume of traffic overloads the website or server causing it to be slow or server shuts down completely

- **Hacking**
  - When someone gains unauthorized access to a computer.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Malware**
  - Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware

Consequences:

- Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information
- Reformat the hard drive of your computer causing you to lose all your information
- Alter or delete files
- Steal sensitive information
- Send emails on your behalf
- Take control of your computer and all the software running on it.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Pharming**
  - It points you to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website

Consequences

- Convince you that the site is real and legitimate by spoofing or looking almost identical to the actual site down to the smallest details. You may enter your personal information and unknowingly give it to someone with malicious intent.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Phishing**
  - Fake emails, text messages and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from you

Consequences

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action
- Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Ransomware**
  - Ransomware is a type of malware that restricts access to your computer or your files and displays a message that demands payment in order for the restriction to be removed. The two most common means of infection appear to be phishing emails that contain malicious attachments and website pop-up advertisements

Consequences

There are two common types of ransomware:

- Lockscreen ransomware: displays an image that prevents you from accessing your computer
- Encryption ransomware: encrypts files on your system's hard drive and sometimes on shared network drives, USB drives, external hard drives, and even some cloud storage drives, preventing you from opening them.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Spam**
  - Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people

Consequences

- Annoy you with unwanted junk mail
- Create a burden for communications service providers and businesses to filter electronic messages
- Phish for your information by tricking you into following links or entering details with offers and promotions
- Provide a vehicle for malware, scams, fraud and threats to your privacy.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Spoofing**
  - This technique is often used in conjunction with phishing in an attempt to steal your information. A website or email address that is created to look like it comes from a legitimate source. An email address may even include your own name, or the name of someone you know, making it difficult to discern whether or not the sender is real

Consequences

- Spends spam using your email address, or a variation of your email address, to your contact list
- Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Spyware**
  - Software that collects personal information about you without you knowing. They often come in the form of a ‘free' download and are installed automatically with or without your consent. These are difficult to remove and can infect your computer with viruses.

Consequences

- Collect information about you without you knowing about it and give it to third parties
- Send your usernames, passwords, surfing habits, list of applications you've downloaded, settings, and even the version of your operating system to third parties
- Change the way your computer runs without your knowledge
- Take you to unwanted sites or inundate you with uncontrollable pop-up ads.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Trojan Horses**
  - A Trojan horse may not be a term you're familiar with, but there's a good chance you or someone you know has been affected by one. A malicious program that is disguised as, or embedded within, legitimate software. It is an executable file that will install itself and run automatically once it's downloaded

Consequences

- Delete your files
- Use your computer to hack other computers
- Watch you through your web cam
- Log your keystrokes (such as a credit card number you entered in an online purchase)
- Record usernames, passwords and other personal information.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Viruses**
  - Most people have heard of computer viruses, but not many know exactly what they are or what they do. Malicious computer programs that are often sent as an email attachment or a download with the intent of infecting your computer, as well as the computers of everyone in your contact list. Just visiting a site can start an automatic download of a virus

Consequences

- Send spam
- Provide criminals with access to your computer and contact lists
- Scan and find personal information like passwords on your computer
- Hijack your web browser
- Disable your security settings
- Display unwanted ads.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

- **Wi-Fi Eavesdropping**
  - WiFi eavesdropping is another method used by cyber criminals to capture personal information. Virtual "listening in" on information that's shared over an unsecure (not encrypted) WiFi network.

Consequences

- Potentially access your computer with the right equipment.
- Steal your personal information including logins and passwords.

By: Imran Afzal
www.utclisolutions.com

Types of Security Threats

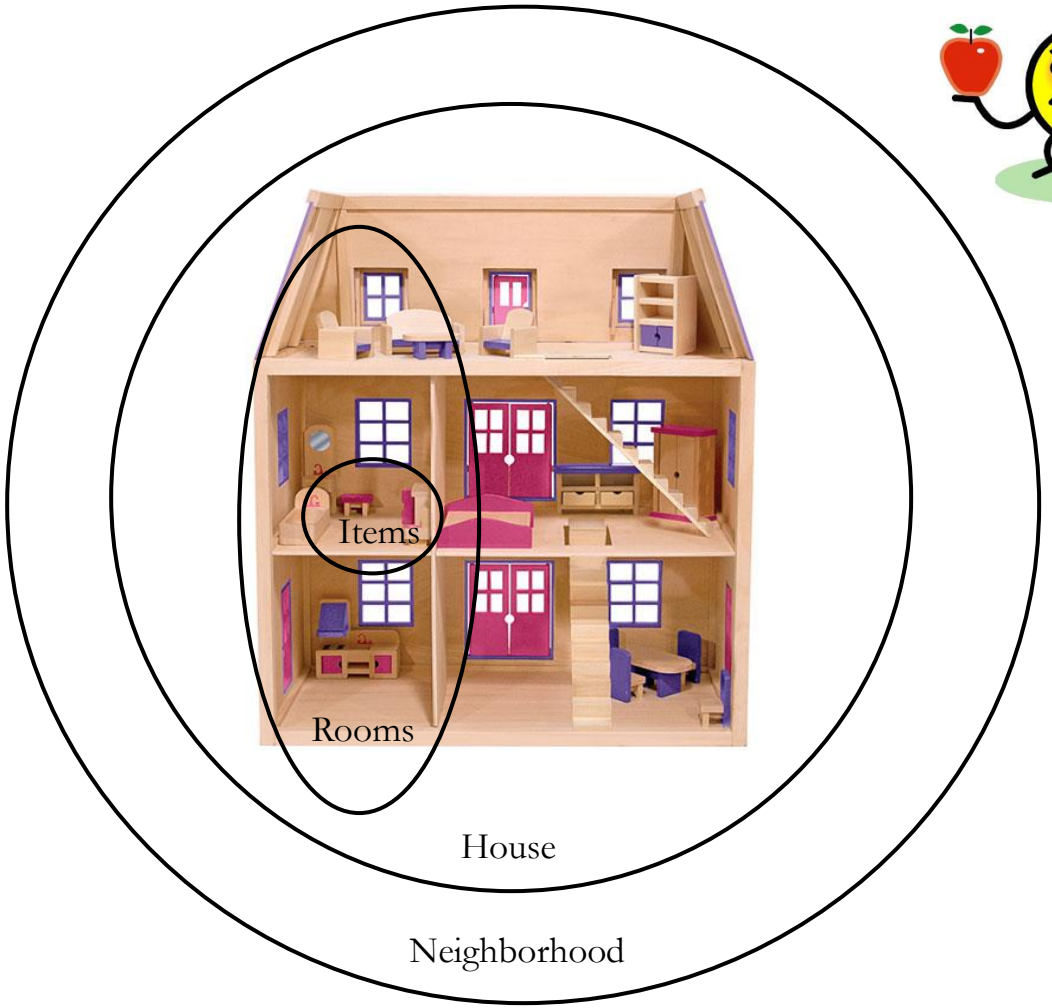
- **Worms**
  - Worms are a common threat to computers and the Internet as a whole. A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, doesn't damage or alter the hard drive and propagates by sending itself to other computers in a network – whether within a company or the Internet itself.

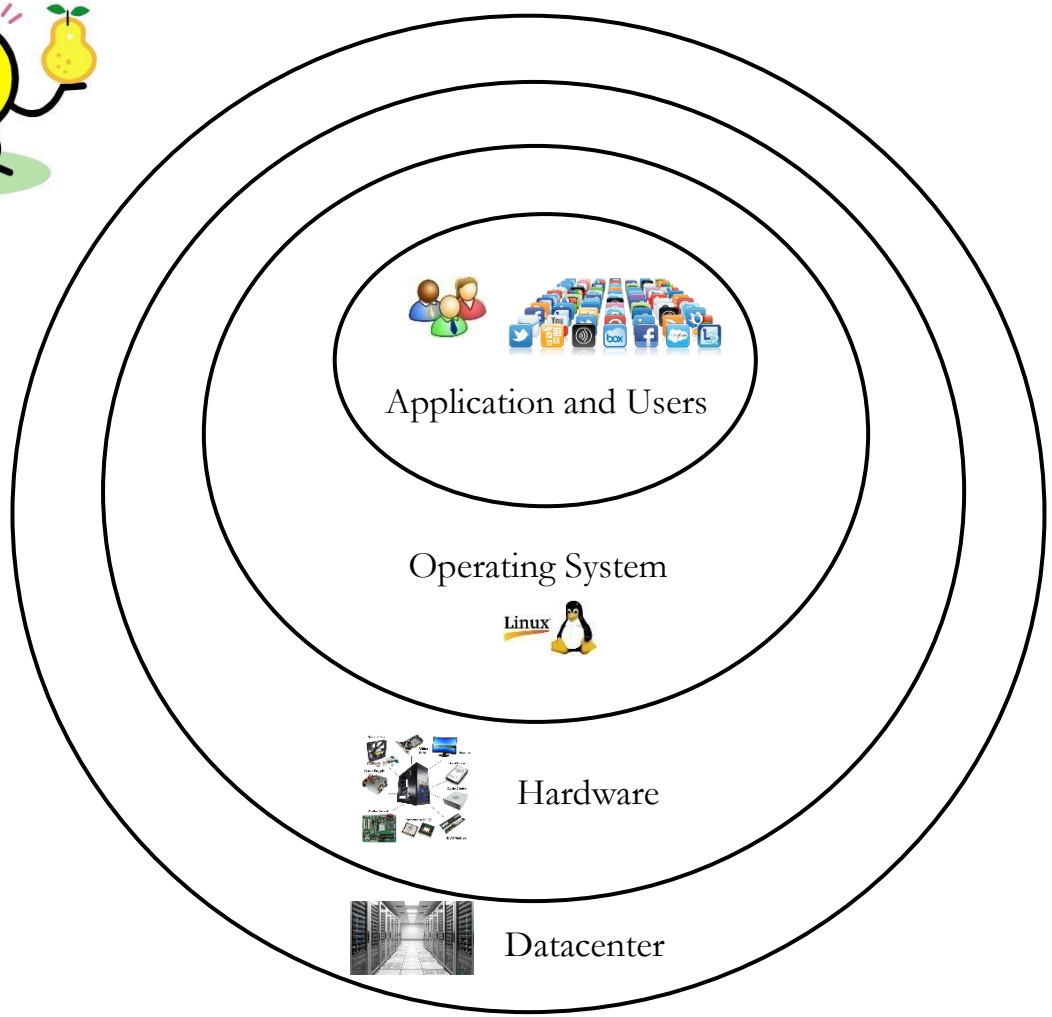
Consequences

- Spread to everyone in your contact list
- Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies enormous amounts of lost revenue.

By: Imran Afzal
www.utclisolutions.com

Comparing House Security with Computer Security





By: Imran Afzal
www.utclisolutions.com

Securing All Operating Systems

- Tiered environment (e.g)
  - Linux → Solaris/Oracle → Windows
  - Windows → Linux → Solaris/Oracle

Security Implementation Tools

- Manual security configuration
  - User Accounts
  - File Systems
  - System access
  - System security (system configuration files)
  - OS network layer security

- Automate through scripts
  - Create a script
  - Copy over or access over network
  - Execute one by one on each server

- Deployment tools (Ansible, puppet. Etc.)
- 3rd part security software (e.g. McAfee) – Not for all security measures

By: Imran Afzal
www.utclisolutions.com

Physical Server Security

- **Security Levels at physical location**
  - Datacenter
  - Floor
  - Cage
  - Rack
  - Server

- **Security Levels at virtualization**
  - Virtualization management software access
  - VM management access (reboot, shutdown etc.)
  - VM OS level access

Application and Database Encryption

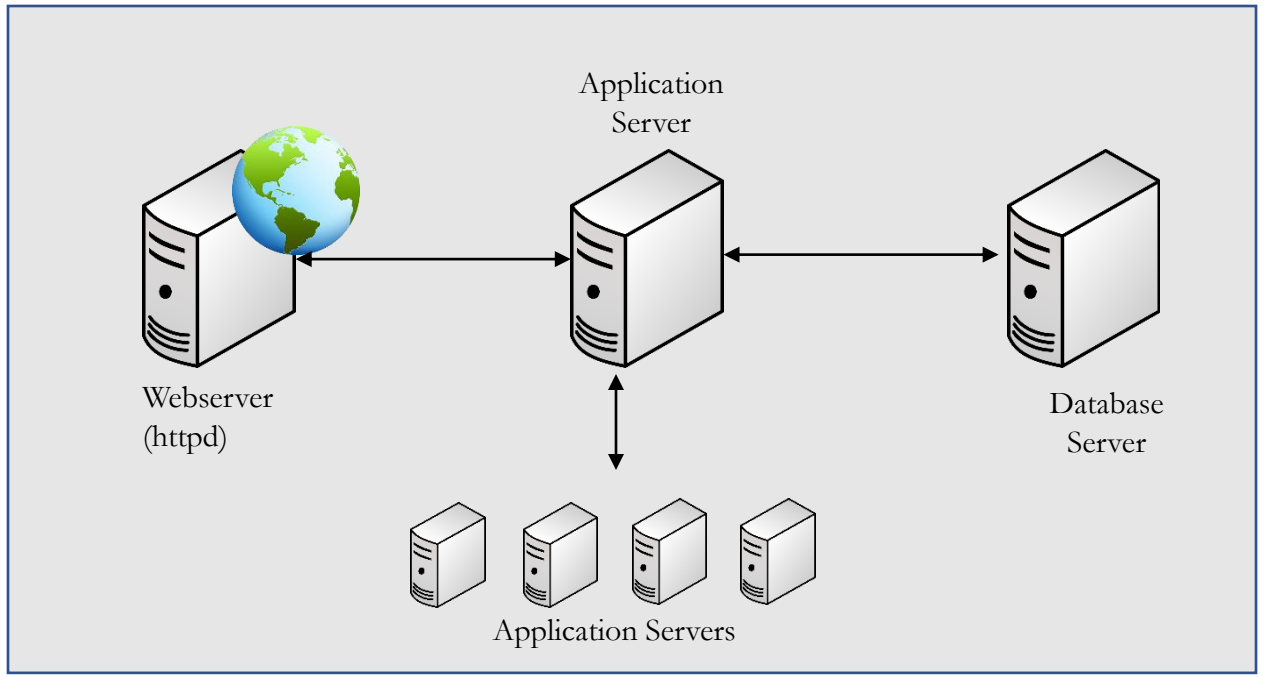
- What are the applications and database?

Hardware →

Operating System →

Applications/DB →

Users



By: Imran Afzal