Type of Security Threats and its Prevention

Piyush Bhatia[1] Rahul Sehrawat[2]
[1,2]Department of Information & Tehnology
[1,2]Maharishi Dayanand University

Abstract— Security is a branch of computer technology known as information security as applied to computers and networks. The objective of online security includes protection of information and property from theft, corruption, or threats attack, while allowing the information and property to remain accessible and productive to its intended users. The term online system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The basic aim of this article is to Prevention against unauthorized security Attack and Threats.

Keywords: Security Threats, Introduction, Types of Security, Prevention, Detection

I. Introduction

Computer technology is more and more ubiquitous; the penetration of computer in society is a welcome step towards modernization but society needs to be better equipped to grapple with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficulty for the security professionals in order to catch hackers. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information.

The recent research is focused on bringing quality security training combined with rapidly changing technology. Online networking security is to provide a solid understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems.

II. Why Is Computer Security Necessary?

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

III. Common Online Security Threats

Online Computer security threats are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm. Arm yourself with information and resources to safeguard against complex and growing computer security threats and stay safe online. There are some common Threats to attack the system.

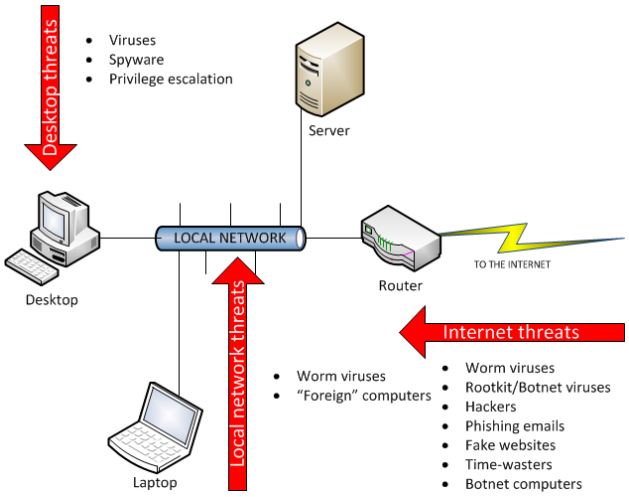


Fig. 1: Online Threats

A. *Virus Threats*

Threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process

B. *Spyware Threats*

A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We've amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

C. *Hackers*

People, not computers, create computer security threats and malware. Hackers are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism. What scams are they using lately? Learn how to combat dangerous malware and stay safe online.

D. *Phishing Threats*

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Internet Based Attacks While your computer is connected to the Internet it can be subject to attack through your network communications. Some of the most common attacks include:

- Bonk – An attack on the Microsoft TCP/IP stack that can crash the attacked computer.
- RDS_Shell – A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges.
- Win Nuke – An exploit that can use NetBIOS to crash older Windows computers.

E. *Viral Web Sites:*

Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well-

known web sites and can have similar web addresses to the sites they are imitating. Users who visit these sites often inadvertently download and run a virus or Trojan and CA

F. Spyware, Adware and Advertising Trojans

Spyware, Adware and Advertising Trojans are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software on to your computer. They are often included within programs that you can download free from the Internet or that are on CDs given away free by magazines. Spyware doesn't usually carry viruses but it can use your system resources and slow down your Internet connection with the display of ads. If the Spyware contains bugs (faults) it can make your computer unstable but the main concern is your privacy. These programs record every step that you take on the Internet and forward it to an Ad Management Centre which reviews your searches and downloads to determine your shopping preferences. The Ad Management Centre will build up a detailed profile of you, without your knowledge, and can pass this on to third parties, again without your knowledge. Some Spyware can download more serious threats on to your computer, such as Trojan Horses.

G. Unsecured Wireless Access Points:

If a wireless access point, e.g. an ADSL (Broadband) Router, hasn't been secured then anyone with a wireless device (laptop, PDA, etc.) will be able to connect to it and thereby access the Internet and all the other computers on the wireless network.

H. Bluesnarfing:

The act of stealing personal data, specifically calendar and contact information, from a Bluetooth enabled device.

I. Social Engineering

Tricking computer users into revealing computer security or private information, e.g. passwords, email addresses, etc., by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response.

J. Microsoft Office Document Metadata

The average Microsoft Word, Excel, etc. document includes hidden metadata with details of who created it, who has worked on it, when it has been amended and quite possibly the text of all those changes as well. Viewing a Word document in a text editor can reveal the metadata in plain text at the start and finish of the document.

IV. How to Secure the System

There are basic three methods to secure the system from online security attack.

A. Prevention

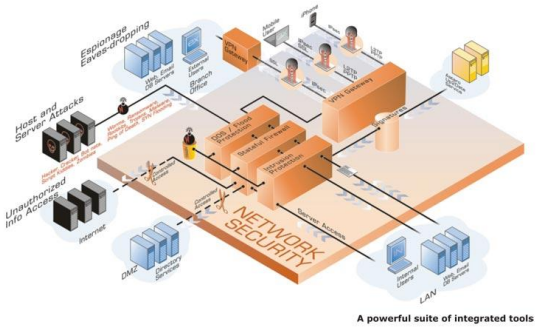
If you were to secure your house, prevention would be similar to placing dead bolt locks on your doors, locking your window, and perhaps installing a chain link fence around your yard. You are doing everything possible to keep the threat out.

B. Detection

You want to be sure you detect when such failures happen. Once again using the house analogy, this would be similar to putting a burglar alarm and motion sensors in the house. These alarms go off when someone breaks in. If prevention fails, you want to be alerted to that as soon as possible.

C. Reaction

Detecting the failure has little value if you do not have the ability to respond. What good does it to be alerted to a burglar if nothing is done? If someone breaks into your house and triggers the burglar alarm, one hopes that the local police force can quickly respond. The same holds true for information security. Once you have detected a failure, you must execute an effective response to the incident.



V. Prevention From Attacks And Threats

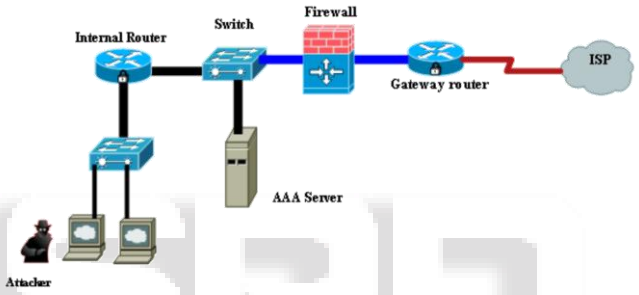


Fig. 3: Router with firewall configuration

The various ways to prevent from attacks and threats are as follows:

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading
- Using Caution with USB Drives
- Securing Wireless Networks

VI. Prevention from Email and Communication

The various ways to prevent from emails and other communication means are as follows:

- Using Caution with Email Attachments
- Reducing Spam
- Using Caution with Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying safe on social Network Sites.

VII. Use Safe Browsing

In order to browse safely one must keep in mind the following points:

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Usage of Private Browsing
- Deleting History
- Reviewing End-User License Agreements

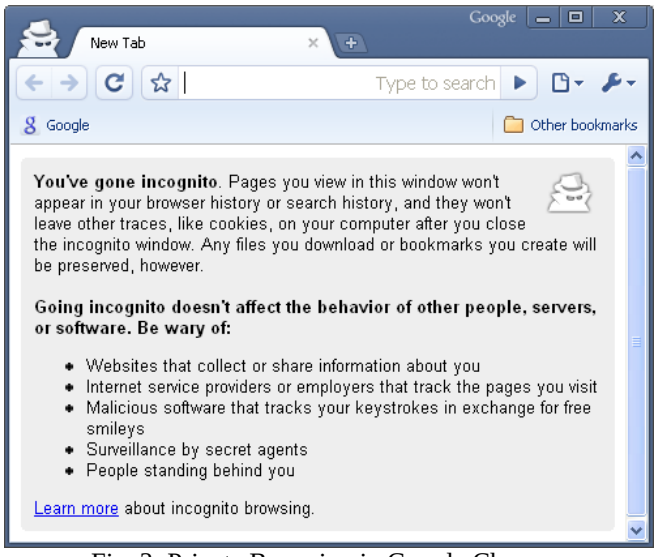


Fig. 3: Private Browsing in Google Chrome

In order to browse safely one must keep in mind the following points:

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Usage of Private Browsing
- Deleting History
- Reviewing End-User License Agreements

VIII. PRIVACY CONTROL

- Protecting Your Privacy
- Effectively Erasing Files
- Supplementing Passwords

IX. TIPS FOR SECURING THE SYSTEM FROM ATTACKS

Below are a few tips that are used for securing the system from attacks

- Install and Use Anti-Virus Programs
- Use Care When Reading Email with Attachments
- Install and Use a Firewall Program
- Make Backups of Important Files and Folders
- Use Strong Passwords
- Use Care When Downloading and Installing Programs
- Install and Use a Hardware Firewall
- Install and Use a File Encryption Program and Access Controls
- Safeguard your Data
- Real-World Warnings keep you safe online.
- Real-World Warnings keep you safe online.
- Keeping Children Safe Online

REFERENCES

[1] Auerbach Publishers (a division of Warren Gorham & Lamont). Data Security Management.Boston, MA. 1995.
[2] British Standards Institute. A Code of Practice for Information Security Management, 1993.
[3] Caelli, William, Dennis Longley, and Michael Shain. Information Security Handbook. New York, NY: Stockton Press, 1991.
[4] Fites, P., and M. Kratz. Information Systems Security: A Practitioner's Reference. New York, NY: Van Nostrand Reinhold, 1993.
[5] Garfinkel, S., and G. Spafford. Practical UNIX Security. Sebastopol, CA: O'Riley & Associates, Inc., 1991.
[6] Institute of Internal Auditors Research Foundation. System Auditability and Control Report.

