CIS 483 Term Paper

Michael Colliver

Jake Ellis

Threat Detection

**Intro:**

According to Webster’s dictionary the definition of a threat is “An expression of intention to inflict evil, injury, or damage”. This means a threat can be physical, emotional, or even digital. Throughout this document we will be discussing the physical and digital threats and the proper techniques to prevent them.

The scope of this document encompasses intrusion, anomalies, weather, and new challenging threats. For each threat, we will discuss several different types of prevention and detection techniques such as Firewall, Anti Virus, and Secure Computing.

Intrusion detection is a large aspect of threat detection because most people, without realizing it, have some sort of intrusion detection on their computers. According to Infonetics Research the top ranked Intrusion Prevention system (IPS) companies are Cisco, McAfee, Juniper and IBM, although there are many different options. These companies produce systems with the intention of blocking Worms, Trojans, Viruses and exploits against application and OS vulnerabilities.

First we will address the types of threats that may occur to any type of computer prior to discussing the detection and prevention techniques. The most basic digital threats are the Virus, Worm, Trojan, Spyware, Adware, and Rootkits. All of these can be “infect” a computer through corrupt files, downloads, or malicious web pages.

**Body:**

The Virus is a malicious program that is designed to spread from one computer to another in order to interfere with computer operations. A virus is commonly spread through downloads, email and other types of communication. A user must act upon a virus in order for it to spread. This means that a user must open an attachment from an email or download a file from a webpage in order for the virus to access the computer. Once this occurs, the virus attaches itself to an executable program and is able to interfere with operations and, using the computer’s directory, send itself out to other computers.

A Worm is very similar to the Virus although it is a self-replicating and self-contained program. This means that the worm does not need to attach itself to an executable program to broadcast itself. This can be very dangerous because many times the user does not even know the worm is causing damage to the computer until it is too late.

A Trojan Virus is named after the “Trojan Horse” used by the Greeks in the Trojan War for its similar hidden attack strategy. The Trojan Virus disguises itself as a harmless program or file but once it is executed it actually begins to harm to a user’s computer. Trojan Viruses can arrive in all sorts of ways but a very common source is email. Emails that contain headers like “You have won!!!!” often get user’s attention and curiosity drives them to click on a fun game which actually executes the release of a Trojan Virus through out the computer. The Virus will then begin deleting files, changing settings, or even crash the entire system depending on their intentions.

Spyware is a program usually hidden in downloads or pop-ups throughout a webpage that will gather the user’s information such as downloads, personal information, and other information that can be used to track browsing habits. Many times spyware is only used to record the types of browsing a user does so the webpage is able to display ads that are more appealing to the user. Although in other cases, Spyware has the ability to hijack the browser and change settings, go to unwanted web pages, and even make unwanted long distance calls.

Adware is very similar to Spyware because it is usually unknowingly downloaded to the user’s computer with the intent to display unwanted advertisements. These ads can come in the form of banners across the screen, pop up messages, or basic ads on the web page. Most of these are nothing more than a nuisance that appear when you least expect it.

A Rootkit is very different from any of the previous threats we have discussed. A Rootkit’s objective is not to spread and cause a disruption for the user. Instead, the goal is to access all possible files that are affiliated with the user’s computer, which allows an outside attacker access to all of those files. The attacker can read any and all documents on the computer even private data. This can be devastating for a company with classified information or large amounts of client data that could be sold for millions of dollars.

Lastly, we begin to move away from the digital threats and move towards physical threats. Many of these can be very obvious even to non-technological people such as theft and weather damage although they should not be ignored. Theft is very common among laptops and other hardware devices such as keyboards, mice, headphones, monitors, and more. Weather threats are much harder to prevent because of the unpredictability although there are some preventative measures businesses can take depending on their geographical location. The most common weather threats are flooding, tornados, hurricanes, and earthquakes.

Now that we have explained the different types of threats we will begin discussing how to detect and prevent each type.

1. Intrusion Detection
   1. Firewalls - filters traffic to a computer and helps control the activities of Internet facing activities.

Anti Virus - provides protection from Virus, Worm, Spyware, Adware, and Rootkit infections.

* 1. Secure downloading
  2. Secure Computing
  3. No-script

1. Anomaly Detection
2. Weather detection
   1. Tracking weather
   2. Planning accordingly by location
3. Hybrid Systems – anomaly and signature detection strategies
4. New challenges
   1. Biological detection systems
   2. Biological threats (illness, toxins)
5. Prevention techniques
   1. Intrusion
   2. Anomaly
   3. Hybrid
   4. Other – Hidden object detection (X rays)

**Work cited**

Techsupportalert.com

Sans.org