Abhishek Honmute
111803055
Div 1 Batch B2
Cyber Security
Assignment 1

Literature Survey of Latest Trends in Cyber Security

I. Hypervisor-assisted dynamic malware analysis

Paper link: Click here

This paper proposes a method for dynamic malware analysis classified as a hypervisor-based malware analysis method. In the proposed method, the system call monitoring component is located within the guest OS and consequently, no intervention of the hypervisor is required during the system-call monitoring and analysis. As a result, the performance overhead is kept to a minimum. Though completely handled in the guest context, the monitoring component is fully transparent to the guest OS.

System Description:

The system described in this paper consists of four components:

1. **Boot application:** For installing the component in the guest system.
2. **Hypervisor:** The hypervisor is responsible for installing the monitoring component and protecting it from detection and modification.
3. **Monitoring component:** The monitoring component, in turn, is responsible for system call intercepting and recording. A special sandbox configuration file determines the system's recording format.
4. **Process behaviour analyzer:** The process behaviour analyzer is responsible for analyzing the output of the monitoring component.

Operation:

The boot application, during the boot phase, obtains the configuration file from the disk, initializes a hypervisor, and returns to the original OS bootloader. The hypervisor remains in the main memory and continues its operation even after the application terminates.

The hypervisor maps a monitoring component into the address space of the guest OS, and the latter intercepts all system calls and records only those that belong to the monitored process. The hypervisor then protects the monitoring component from detection and modification.

Process behaviour analyzer:

The process behaviour analyzer receives two parameters as input: (1) a sandbox configuration file, and (2) a dump file containing the recorded system calls.

Evaluation:

In the experiment, they tested the system in three scenarios :

1. without a hypervisor
2. with a hypervisor and disabled monitoring component
3. with a hypervisor and enabled monitoring component

They used three benchmark tools

1. PCMark 10 – Basic Edition
2. PassMark Performance Test 9.0
3. Novabench 4.0.3

Result suggests that the hypervisor degrades the performance by no more than 5%, and the monitoring component degrades the performance by, at most, an additional 1%.

Conclusion:

Compared to current hypervisor-based systems, their system uses a novel approach in which a specially crafted monitoring component is injected into the address space of the guest OS. The hypervisor protects the monitoring component from detection and modification. They have shown that because the entire handling is done within the guest context, the performance overhead is negligible.

II. A Review on Cyber Security and the Fifth Generation Cyberattacks

Paper Link: Click Here

This paper presents the significance of cyber security along with the various risks that are in the current digital era. The analysis made for cyberattacks and their statistics shows the intensity of the attacks. Various cyber security threats are presented along with the machine learning algorithms that can be applied to cyberattack detection. The need for the fifth generation cybersecurity architecture is discussed.

Cyber Attack Statistics:

The number of unique cyber attacks in 2018 are found to be 47% more than in the previous year. In that, 99.9% of attacks were happened due to packages downloaded from third-party app stores. Many companies have spent hefty money repairing ransomware attacks. Professionals Security Report Survey says that 76% of organizations experienced a phishing attack in the past year and 49% of organizations experienced a DoS attack in the past year.

Over 300 apps in the google play store contained malware and were downloaded by over 106 million users.

Cyber Security Threats:

The main goal of cyberattacks is to gain access, damage or disable the target system. The goal can be achieved by applying various attacks on the target system. Several cyberattacks exist and even evolve day by day.

Some of the threats are listed here:

1. Malware
2. Phishing
3. Man-in-the-middle Attack
4. Cryptojacking
5. Denial-of-service Attack
6. SQL Injection
7. Zero-Day Exploit
8. Spam

Some of the fifth-generation cyber-attacks include Andromeda, AdvisorsBot, Cerber, CNRig, Cryptoloot, Fireball, HiddenMiner, Iotroop, Nivdort, NotPetya, RubyMiner, Trickbot, WannaCry, WannaMine, Ransomeware, adultSwine, and cryptocurrency attacks. These are sophisticated attacks that cause severe damage.

Moving to Fifth Generation Cyber Security Architecture:

Current cyber security architectures are outdated are the most common cause of unavailability and security issues that lead to failure and create vulnerable loopholes. So there is a need for the fifth generation that include cloud infrastructure and the internet of things through businesses can avoid a single point of failure by providing the necessary strength to maintain the operation and security under any conditions. In this way, having the right architecture upon which the entire security infrastructure operates is the only way to ensure to prevent fifth-generation cyberattacks.

Conclusion:

In the past few decades, cyber attacks have become more advanced and sophisticated and have evolved rapidly due to advancements in technology. These fifth-generation attacks are called mega attacks as they are as it large-scale and fast-moving attacks. Still, many companies are using older cyber security architecture. So they need to upgrade their system to the fifth generation cyber security architecture to counter the fifth-generation attacks.

III. CYBER SECURITY AND MOBILE THREATS: THE NEED FOR ANTIVIRUS APPLICATIONS FOR SMART PHONES

Paper Link: Click Here

Smartphones have become an integral part of today's human life. Their use has been increased exponentially in the past few decades. But they are a breeding ground for cyber attacks. Unlike personal computers, they don't have features like firewalls, antivirus software and proper encryptions. Attackers are using these loopholes to their advantage.

One of the major cyber-attacks on smartphones is the 2011 Valentine's Day Attack. It was a picture sharing application that sent premium-rate text messages from a user's phone. This example shows us the importance of cyber security in smartphones.

Challenges With a Mobile Browser:

Due to the small screen size of smartphones, URLs in the bowsers are not completely visible and hence can easily redirect users to malicious websites. Also, one research showed that SSL certificates are more difficult to find on smartphones than on computers.

Also, the touch screen is one of the causes for users visiting the wrong websites. Attackers hide the malicious link under the attractive images so that users can easily click on it. Hence they use the touch screen feature to redirect users to wrong website.

Common mobile device OS:

Apple created IOS operating system for iPhone first. Then it was used for iPod Touch and IPad too. IOS have specifically different applications than android phones. Apple app store both automatically and manually tests the apps before making it open to iPhone users. The code of IOS is not publicly open which makes it a little more secure than Android phones.

Android Platform:

Android is an open-source and most used operating system in the world. However, this open-development feature also poses challenges to securing sensitive user data and protecting users from malicious attacks, such as phishing applications that are usually sent to users to trick them into providing their financial information and credentials while accessing malicious websites.

Malware attacks on Phones:

One of the famous malware attacks on smartphones is the "Zeus-in-the-Mobile" attack. It attempted to bypass the two-factor authentication to steal the bank credentials and gain access to the user's bank account.

Analysis of the study of smartphone security :

Smartphones contain most of the user's personal data. But people don't pay much attention to the security of their smartphones. Hence they are more prone to cyber-attacks. According to a study attacks on smartphones will increase by 44% each year.

Conclusion:

In order to establish a policy of cyber security, it will take a collaborative effort from a variety of officials in various disciplines in society. Each official brings a specific set of knowledge to the issue of cyber security and has a potential role in establishing the different set of functions that are needed to create a general intra-and international cyber security standard Ultimately, a decentralized approach is the best way to make cyber security an interconnected, coordinating mechanism that benefits the society as a whole.