International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

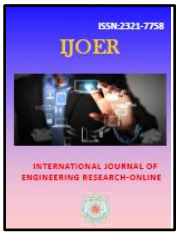
Vol.6., Issue.5, 2018
Sept-Oct.,

RESEARCH ARTICLE

ISSN: 2321-7758

A COMPRAHENSIVE STUDY ON EMERGING THREATS IN CYBERSECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES

ABDULHAKIM H.S BAROUD
Department of Computer Science
Baniwaleed University, Baniwaleed, Libya
hakembaroudcontact@gmail.com



ABSTRACT
Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. The development of more innovative and effective malware defense mechanisms has been regarded as an urgent requirement in the cyber security community. We then discuss new attack patterns in emerging technologies such as social media, Cloud computing, smartphone technology, and critical infrastructure. Finally, we describe our speculative observations on future research directions.
Keywords : Cyber security, cloud computing, smart phone, cloud computing, cybercrime

Introduction

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Cyber attacks become more attractive and potentially more disastrous as our dependence on information technology increases. According to the Symantec cybercrime report published in April 2012, cyber attacks cost US$114 billion each year Victims of cyber attacks are also significantly growing. Based on the survey conducted by Symantec which involved interviewing 20,000 people across 24 countries, 69% reported being the victim of a cyber attack in their lifetime. Symantec calculated that 14 adults become the victim of a cyber attack every second, or more than one million attacks every day.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing.

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent

Why cyber attacks flourish? It is because cyber attacks are cheaper, convenient and less risky than physical attacks. Cyber criminals only require a few expenses beyond a computer and an Internet connection. They are unconstrained by geography and distance [2]. They are difficult to identity and prosecute due to anonymous nature of the Internet.

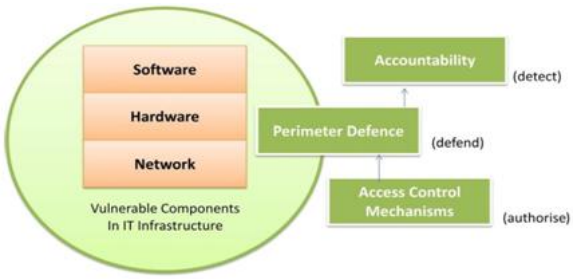


Fig. 1: Vulnerabilities and defense strategies in existing systems.

Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace. Malware refers to a broad class of attacks that is loaded on a system, typicallywithout the knowledge of the legitimate owner, to compromise the system to the benefit of an adversary. Some exemplary classes of malware include viruses, worms, Trojan horses, spyware, and bot executables. Malware infects systems in a variety of ways for examples propagation from infected machines, tricking user to open tainted files, or alluring users to visit malware propagating websites. In more concrete examples of malware infection, malware may load itself onto a USB drive inserted into an infected device and then infect every other system into which that device is subsequently inserted[3].

To give more defined access to certain internal re-sources, the access control mechanisms have been used in conjunction with the perimeter defense mechanism. On top of perimeter defense and access control, accountability is added to identify or punish for any misbehaviors, as represented in Fig. 1. We then discuss the pros and cons of the most representative defense mechanisms that have been used in these layers.
Malware evolves through time capitalizing on new approaches and exploiting the flaw sin the emerging technologies to avoid detection. We describe a number of new patterns of malware attacks present in the emerging technologies. In choosing emerging technologies for illustration, we focus a few that have changed the way we live our daily life [4]. These include social media, cloud computing, smartphone technology, and critical infrastructure. Realizing its potential to connect millions people at one go, adversaries use social media accounts to befriend unsuspecting users to use as vehicles for sending spam to the victim's friends while the victim's machine is repurposed into a part of botnet. Cloud computing paradigm allows the use of computer resources like utilities where the users pay only for the usage without having to set up any upfront expense or

requiring any skills in managing complex computing infrastructure. The growing trove of data concentrated in the cloud storage services is now attracting attackers. In June 2012, attackers compromised Distributed Denial of Service (DDoS) mitigation service on CloudFlare by using flaws in AT&T's voicemail service for its mobile users; similarly, Google's account-recovery service for its Gmail users. There is also growing concerns in cyber threats to critical infrastructure such as electricity grids and healthcare systems to use in terrorism, sabotage and information warfare. Apart from investigating exploitations through unique characteristics in the selected emerging technologies, we also discuss general malware attack patterns appear in them to understand the methods and trends of the new attacks [5].

Malware as attack tool

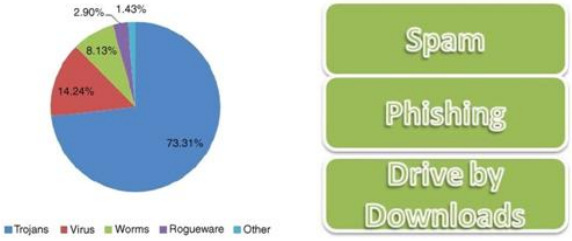


Fig. 2. Types of malware and mediums to spread them.

In early days, malware was simply written as experiments often to highlight security vulnerabilities or in some cases to show off technical abilities. Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. For example, malware is often used to target government or corporate websites to gather guarded information or to disrupt their operations. In other cases, malware is also used against individuals to gain personal information such as social security numbers or credit card numbers. Since the rise of widespread broad band Internet access that is cheaper and faster, malware has been designed increasingly not only for the stealth of information but strictly for profit purposes[6].

In 2009, Trojans were reported to have made up 60 percent of all malware. In 2011, the number has jumped up to 73 percent. The current percentage indicates that nearly three out of every four new malware strains created in 2011 were Trojans and shows that it is the weapon of choice for cyber criminals to conduct network intrusion and data stealing.

	Hardware	Software	Network
Common attacks	▪ Hardware Trojan ▪ Illegal clones ▪ Side channel attacks (i.e. snooping hardware signals)	▪ Software programming bugs (e.g. memory management, user input validation, race conditions, user access privileges, etc.) ▪ Software design bugs ▪ Deployment errors	▪ Networking protocol attacks ▪ Network monitoring and sniffing
Examples of countermeasures	▪ Tamper-Resistant Hardware (e.g. TPM) ▪ Trusted Computing Base (TCB) ▪ Hardware watermarking ▪ Hardware obfuscation	▪ Secure coding practice (e.g. type checking, runtime error, program transformation, etc.) ▪ Code obfuscation ▪ Secure design and development ▪ Formal methods	▪ Firewall ▪ Intrusion prevention and detection ▪ Virtual Private Network (VPN) ▪ Encryption

Fig. 3. Common attacks and examples of countermeasures in existing system.

Malware authors use a number of different intermediaries to spread malware to infect a victim's system. Traditionally, spam , phishing and web download have been the most comm only used mediums for the purpose.

Spam refers to sending irrelevant, inappropriate and unsolicited messages to thousands or millions of recipients. Spam has turned out to be a highly profitable market since spam is sent anonymously with no costs involved beyond the management of mailing lists.

Phishing is a way of attempting to acquire sensitive information such as username, password or credit card details by masquerading as a trustworthy entity. Most phishing scams rely on deceiving a user into visiting a malicious web site claiming to be from legitimate businesses and agencies.

Drive-by Downloads concerns the unintended downloads of malware from the Internet and have been increasingly used by the attackers to spread malware fast. Drive-by downloads happen in a variety of situations; for example, when a user visits a website, while viewing an email message by user or when users click on a deceptive pop-up window. However, the most popular drive-by downloads occur by far when visiting websites.

TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

Web servers

The threat of attacks on web applications to extract data or to distribute malicious code

persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications.

Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information.

APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise).

Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which needto be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity.

Exploiting existing vulnerabilities

Once malware is carried out to the victim's system, cyber criminals could utilize many different aspects of existing vulnerabilities in the victim's system further to use them in their criminal activities. We examine most commonly exploited existing vulnerabilities in hardware, software, and network systems. The summary of the common attacks in the hardware , software and network layers are present edalong with the examples of countermea sures.

Hardware

Hardware is the most privileged entity and has the most ability to manipulate a computing system. This is the level where it has the potential to give attackers considerable flexibility and power to launch malicious security attacks if the hardware is compromised. Among different types of hardware misuse, hardware Trojan is the most hideous and common hardware exploits. The hardware Trojans are malicious and deliberately stealthy modification made to electronic devices such as Integrity Circuits(IC) in the hardware. The hardware Trojans have a variety of degrees which cause different types of undesir able effects.

Software defects

A software bug is the common term used to describe an error, flaw, mistake, or fault in a computer program such as internal OS, external I/O interface drivers, and applications. Cyber attacks utilize the software bugs in their benefits to cause the systems to behave unintended ways that are different from their original intent. The majority of cyber attacks today still occuras are

sultofex ploiting software vulner abilities causedby software bugandde signflaws.

Emerging threats

Cyber attacks on cyberspace evolve through time capitalizing on new approaches. Most times, cyber criminals would modify the existing malware signatures to exploit the flawsexistinthe new technologies. In other cases, they simply explore unique characteristics of the new technologies to find loopholes to inject malware. Taking advantages of new In- ternet technologies with millions and billions active users, cyber criminals utilize these new technologies to reach out to a vast number of victims quickly and efficiently. We select four such up and coming technology advancements which in- clude: social media, cloud computing, smartphone technology, and critical infrastructure, as illustrative examples to explore the threats in these technologies [8]. We discuss unique characteristics of each of these emerging technologies and analyze a number of common attack patterns present edin them, as summarized in Fig.4.

Common characteristics	Common attack patterns
• Millions and billions of active users • Became part of our daily life • No geographical boundaries • Accessed 24/7 from anywhere at anytime • Services are available via Internet connection using Web Browsers • Services offered by many different devices such as mobiles and tablets	• Increased Attack through Web Browser • Increased attacks through social engineering websites • Increasing attacks coming from non-PC-based devices (e.g. mobiles, tablets, VoIP) • Increasing number of more organized attacks through botnet • Increasing number of attacks through the attackers with internal knowledge (i.e. insider threats)

Fig. 4. Emerging Technologies: Their common characteristics and common attack patterns.

ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

CYBER SECURITY TECHNIQUES

Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

Authentication of data

The documents that we receive must always be authenticated be before downloading that is itshould be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:
DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world

Don't be a bully on the Internet.

- Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords. Never try to send any kind of malware to other's systems and make them corrupt. Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

Future research direction

With the tremendous growth in the Internet availability and the advancement of Internet enabled devices, an increasing number of populations use the Internet in all wakes of their lives, often exposing highly sensitive personal information without realizing the consequences of data misuse.

Focus on privacy

In recent years, privacy has become a critical issue in the development of IT systems with the widespread of networked systems and the Internet. Now, the Internet is used in all wakes of our lives demanding increasing volume of personal information to be entered in the cyberspace. According to JP Morgan's annual report, global ecommerce sales has been increased at an annual rate of 19.4% reaching $963 billion sales by 2013. This increase in online shopping suggests that the Internet users are becoming more comfortable sharing their sensitive financial information, such as credit card numbers and shipping addresses [17,18].

The goal of privacy-aware security is to enable users and organizations to better express, protect, and control the con-fidentiality of their private information, even when they choose to (or require to)share it with others. One stream of research in this field concerns with the way data is accessed and disclosed while protecting privacy. A number of researches are conducted to investigate how to selectively disclose the data, how to protect the data that are shared by people, and how to sanitize the data.

There is no doubt that the Internet has been a social phenomenon that has changed, and continues to change how humans communicate, businesses work, how emergencies are handled, and the military operates among many other things. Despite the Internet's critical importance, some portions of the Internet is fragile and the constantly under incessant attacks that range from software exploits to denial-of-service. One of the main reasons for these security vulnerabilities is that the Internet architecture and its supporting protocols were primarily designed for a benign and trustworthy environment, with little or no consideration for security issues [19-21].

Conclusions

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light eachday, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

Popular social networking sites like Facebook, Twitters and others have been increasingly used as delivery mechanisms to get unsuspecting users to install or spread malware.

More organized attacks through the use of botnets have been reported. As the impact of such damage is much bigger than individual attacks, there is a growing concern to thwart botnets. Recent statistics also show there is an increasing number of cyber attacks tailored to a specific system, for example command and control system, using inside knowledge and personnel.

References

[1]. http://shibboleth.internet2.edu/

[2]. Australian Parliament the report of the inquiry into Cyber Crime,http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf.

[3]. www.it2trust.com/pdf/Aladdin.SafeWord_PO_SafeWord.pdf, last accessed: June2013.

[4]. Cardenas, T. Roosta, G. Taban, S. Sastry, Cyber security basic defenses and attack trends, Fujitsu Lab., http://www.flacp.fujitsulabs.com/~cardenas/ Papers/Chap4v2.pdf, last accessed: June2013.

[5]. DHS S&T, Roadmap for cybersecurity research, Jan. 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf, last accessed: June2013.

[6]. Annual Emerging Cyber Threats Report, Georgia TechInformation Security Center, http://www.gtisc.gatech.edu/,lastaccessed: June2013.

[7]. Internet Security Threats Report.Symantec, http://www.symantec.com/threatreport/,lastaccessed:June2013.

[8]. S.E.Goodman, H.S.Lin(Eds.), Toward a Safe rand More Secure Cyber space, TheNat'l Academics Press,2007.

[9]. R.C.Newman, Computer Security: Protecting Digital Resources, first edition, Jones& Bartlett Publishers, February 20, 2009.

[10]. B.W.Lampon, Privacy and security–Usablesecurity: how to getit, Commun. ACM 52 (11) (2009)25–27.

[11]. A.Haeberlen,P.Kouznetsov,P.Druschel,Practicalaccountabilityfordistributedsystems,in:SOSP2007,pp.175–188.

[12]. M.Tehranipoor,C.Wang,IntroductiontoHardwareSecurityandTrust,Springer,2011.

[13]. TrustedComputingGroup,TPMMain,Part2,TPMStructures,Specificationversion1.2.Revision94,2006.

[14]. TrustedComputingGroup,TPMMain,Part3,DesignPrinciples,Specificationversion1.2.Revision94,2006.

[15]. B. Beckert, R. Hähnle, P.H. Schmitt (Eds.), Verification of Object-Oriented Software: The KeY Approach, Lect. Notes Comput. Sci., vol. 4334, Springer, Heidelberg,2007.A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

[16]. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

[17]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.

[18]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518,

[19]. "Study of Cloud Computing in HealthCare Industry "IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[20]. CIO Asia, September 3rd, H1 2013: Cyber security in Malaysia by Avanthi Kumar.