Cybersecurity and Emerging Threats in Cybersecurity

Vijay Ramalingam, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - r.vijay@galgotiasuniversity.edu.in

ABSTRACT: Cybersecurity is a widely used term with highly diverse, frequently subjective, and occasionally uninformative definitions. Disrupting force processes in national security and the economy can be disastrous. The challenge of meeting safety and quality compliance on operations, given the complexity of widely distributed assets and the inter-dependence between computing, communication and power infrastructures. In recent years a cyber security standard is set by the North American Electric Reliability Corporation (NERC), which demands compliance by the utility with cyber security control systems. This standard identifies various cyber related vulnerabilities in control systems and recommends multiple corrective measures (e.g. best practices). A systematic information security analysis of critical infrastructure is stated in this article. The following four main components propose a framework for monitoring and data acquisition: 1) real-time monitoring; 2) identification of anomalies; 3) effect analyzes; and 4) methods for mitigating. Furthermore, an attack-tree methodology is developed for impact analysis. In order to predict processes, the situation, and leaf-level flaws, the attack-tree model based on power system control networks determines the system's opponents. The insecurity of the leaf is central to port testing or password intensity evaluation methodology. In the framework for controlling the power plant, the measurement of vulnerabilities is based on conditions of former cyber security and the vulnerability indices are assessed.

***KEYWORDS: Attack tree, Cybersecurity, Defense systems, Power system control, Security vulnerability*.**

INTRODUCTION

In scholarly and mainstream literature the word "cybersecurity" became a concept that has treated the issue generally in a specific way. Based on the analysis of literature discussed in this paper, the term is commonly used and has extremely flexible meanings, context-dependent, often subjective and, often, insightful. There are little publications on the sense of the word and the way it is placed in various contexts. The lack of the predominantly technical view of cyber security, while separating disciplinarians that should act together to resolve complex cyber security challenges, can potentially impede technological and scientific advances in the field of multi-dimensional Internet security. There are a wide range of technical solutions, for example, that promote cyber security. However, these solutions alone do not solve the problem; there are several examples and substantial scholarly research demonstrating the cultural, fiscal, financial, political and other aspects of society inextricably associated with information security efforts[1].

Nowadays everyone is increasingly dependent on computer networks and information technology technologies for our culture, economy and vital infrastructure. If our reliance on information technologies increases, cyber threats become more attractive and even more destructive. Cyberattacks cost $114 billion per year according to the cybercrime study released by Symantec in April 2012. The overall cost of cyber breaches will be staggering US$ 385 billion if the time taken by businesses seeking to rebound from cyber threats were counted. Cyber-attack victims are also increasing substantially. During their lives 69 percent reported becoming victims of a cyber threat, based on a study by Symantec, which interviewed 20,000 people from 24 countries. Every second, or more than a million attacks each day, Symantec estimated that 14 adults are victims of a cyber-attack[2].

Why is there a flourishing cyber-attack? Cyber-attacks are more cost-effective, easy and less dangerous than physical attacks. In addition to computers as well as the Internet, cybercriminals require only few expenses. Geography and distance are unconstrained. Due to the anonymity of the Internet, they are difficult to identify and prosecute. Since IT attacks are so enticing, the amount and severity of cyber-attacks is projected to continue to rise (Figure 1).

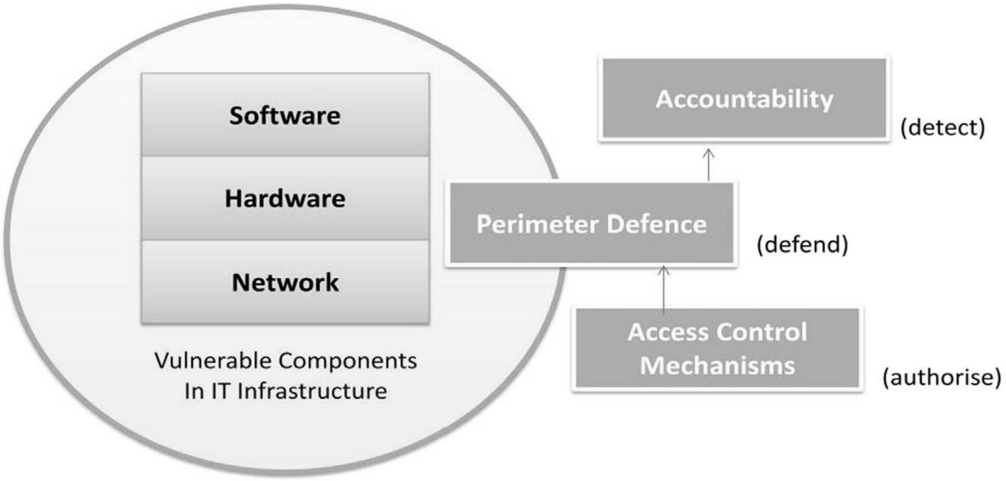

Figure 1: Vulnerabilities and defense strategies in existing systems.

Cyber security concerns about the comprehension of the issues surrounding various cyber-attacks and defense strategies (i.e. countermeasures) that preserve the privacy of digital technology and accessible data.

The word secrecy is used to deter unauthorized parties or programs from divulging information. Integrity is the term used to prevent unauthorized change / deletion. Quality is the term used to guarantee that information services are accessible as needed, and that individuals are willing to collect, store and process information. Most information security analysts agree that ransomware is the primary option for malicious devices to infringe cyberspace defense efforts. Malware is a broad class of attacks which are loaded on a system to compromise the system to the benefit of the enemy, usually without the knowledge of the legitimate owner. Exemplary malware types include viruses, worms, cheetah, spyware, and executable bot. Across a number of ways, malware infects devices, such as propagating compromised computers, exploiting users to access spotted files or enticing users to visit malware websites[3].

Malware may load itself to a USB drive inserted in an infected device for more concrete example malware infections. This malware can infect every other system that the device is later inserted into. Malware can spread from embedded systems and computational logic devices and equipment. In short, malware can be inserted everywhere in the life cycle of the system. Malware victim can include end-user systems, servers, network devices (e.g. routers, switches, etc.) and process control systems (e.g., SCADA). Today's Internet has great concern over the proliferation and sophistication of rapidly growing malware numbers[4].

Malware attacks have traditionally occurred at a single surface point among hardware, software, or network level using existing vulnerabilities in design and implementation at each level. The perimeter defense strategy was primarily used to put a wall outside of all internal resources to protect everything inside against undesirable intrusion. Instead, it protected every asset. In particular, firewall and Antiviral Software installed in intrusion detection systems is used in most of the perimeter defense mechanisms. Any traffic from outside will be intercepted and checked for malware not entering the internal resources. This perimeter model has been accepted generally because securing one perimeter is much easier and apparently cheaper than securing a large number of applications or a large number of internal networks. The access management systems have been used in combination with the perimeter security system to provide more specified access to unique internal re-sources. However, as malware progresses and increases the complexity, the collective efforts of the perimeter security policy have become largely ineffective. Malware that has always grown appears to always find ways to fully bypass the perimeter defense. The three distinct layers of existing information systems in hardware, software and network layers are described in great detail [5].

Malware grows over time, taking advantage of innovative methods to prevent detection and leveraging vulnerabilities of emerging systems. A variety of new forms of malware attacks in emerging technologies are identified. In selecting emerging illustrative technologies, it focus on a few that have changed our daily lives. These include social media, cloud, smartphone and vital infrastructure and discuss the unique characteristics of each new technology and how malware takes advantage of the unique characteristics to grow. As many people report about their events, share news and make friends, social media, for example, like social networking sites and bloggers now form an integral part of our life. Once opponents understand their ability to bind millions of people at once, social media accounts act as unwitting users for sending spam to friends of the victim once the network has been transformed to a botnet portion. Cloud computing paradigm permits the use of computer resources such as utilities in which users only pay for their uses without the need for an upfront costs or skill in the management of complex computing infrastructure[6].

The growing amount of data in cloud storage attracts assailants now. By using flaws in AT&T voicemail service for its mobile users, attackers compromised Distributed Denial of Service (DDoS) mitigation on Cloud flare, in June 2012, similarly, Google's account recovery service for its users. A major rise in mobile malware was recently experienced by the development of 2 billion smartphones by 2015. For example, there was a global increase in the number of single malware detections for Android 17 times last year in 2012. Critical infrastructures such as electricity grids and health systems to be used in terrorism, sabotage and warfare are also facing growing concerns about cyber threats. They further analyze general dynamics of malware attacks to explain the techniques and developments of the latest attacks, in addition to analyzing exploitations through special characteristics in the chosen emerging technologies[7].

LITERATURE REVIEW

The World Economic Forum sees cyberattack threats as one of the world's top five global risks today. The main roles of economies in nations worldwide are constantly threatened by cyber threats. There is a growing risk of critical infrastructures attacking, disrupting critical services, and causing a wide range of damage. Cyber defense: Safety of essential Cyber Assault and Cyber Warfare systems discusses the global cyber threat environment and address the approaches employed by governments and businesses to defend against such risks. The book explores how the risk of cybersecurity can be calculated and assessed. It discusses the several cost factors involved and describes the findings of many significant industry-based economic analyses of health breaches in several countries. The book ends with an insight into future cyber safety trends. It discusses the potential impacts of transformation changes across the industry, such as virtualisation, social media, cloud computing, structured and unstructured data, big data and analytics of data[8]. The problems for those who use the internet and computers used to be cyber-security and attacks. However, the problems are increasing to anyone who does not even directly use them. The society depends on networks and computers progressively and heavily. They are no longer closed in a cyber space and interact with sensors and actuators in our real world. These networks are often named CPS, IoT / E (The Internet of Things / All), Business 4.0, Digital Internet, M2 M etc. Such devices are often accessible to consumers. Regardless of what they are labeled, utilizing all of these devices will have a huge effect on our daily lives and adequate countermeasures must be taken to minimize the risks. This paper explores public protection as a leading example of electronic physical defense of sensitive infrastructures of ICS (Industrial Control Systems). Instead IoT protection for users is clarified as a potential dimension of it[9].

METHOD

Design:

Malware as attack tool

In the early days, malware was written simply as tests mostly to demonstrate flaws in security, or in some situations to show off technical capabilities. Malware today is mainly used to capture confidential data, political, or company details to benefit others. Malware, for example, is often used to target government or corporate websites to collect guarded information or to disrupt their operations. In other cases, malware is also used to gain personal information against individuals, such as social security numbers or credit card numbers. With the advent of more inexpensive and quicker ubiquitous broadband Internet service, malware has been increasingly developed not only for intelligence protection but specifically for profit purposes. For instance, most common malware has been developed to take control of user computers for black market manipulation, such as sending email spam or tracking user's web surfing habits and showing unsolicited ads. In 2012 a total of 26 million new malware was identified based on the Anti-Phishing community report.

According to this study, as the number grew spectacularly Trojans continued to account for much of the threats in terms of malware counting. Trojans allegedly made up 60 percent of all malware in 2009. The figure shot up to 73 per cent in 2011. The current percentage suggests that approximately three out of four new strains of malware generated in 2011 were Trojans which reveals that it is the weapon of choice for cyber criminals to perform infiltration into the network and steal data. Malware authors use a number of different intermediaries to infect a victim's system by spreading malware. Spam, phishing, and online access have historically been the most widely used mediums for this purpose (Table 1).

Table 1: Common attacks and examples of countermeasures in existing system.

	Hardware	Software	Network
Common attack	• Hardware Trojan • Illegal clones • Side channel attack(i.e. snooping hardware signals)	• Software programming bugs (e.g. memory management, user input validation, race conditions, user access privileges etc.) • Software design bugs • Development errors	• Network protocol attacks • Networking monitoring and sniffing
Examples of Counter measures	• Tamper-resistant Hardware(e.g. TPM) • Trussed 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 • Encryption

Spam has turned out to be a highly profitable market since spam is transmitted anonymously, with no costs involved beyond managing mailing list. Spammers are numerous because of such a low barrier to entry, and the volume of unsolicited mail has grown enormously. The projected spam messaging figure for the year 2011 is around seven trillion. This number covers the cost of reduced efficiency and theft, as well as the additional power required to accommodate the spam. Today email spam is the most widely recognized form of spam. According to the Message Anti-Abuse Working Group report, spam was transmitted between 88–92 per cent of email messages in the first half of 2010[10].

Phishing is a means of attempting to obtain personal information like username, password or credit card data by masquerading as a trustworthy person. Most phishing scams focus on tricking a user into visiting a fake website pretending to be from reputable corporations and agencies. Unsuspecting user enters private information on the malicious website which is then exploited by malicious offenders afterwards. Many phishing methods use a form of technological manipulation intended to make a connection appear to belong to a real entity, such as a well-known bank, in an email (and spoofed website. Misspelled URLs or sub-domains are common techniques phishers use. The technical report Anti-Phishing reported that in 2011, there was a noticeable pattern among phishers to mask their motives by preventing the use of obvious IP hosting to host their false login pages. The phishers instead preferred hosting on a compromised domain to avoid detection. It is stated that the number of phishing URLs featuring the spoofed company name in the URL decreased by 16 per cent. These combined trends show how phishers become more informed and knowledgeable about the traits of a typical phish as users adapt.

E Dvownloads is concerned with unintended downloads of malware from the Internet, and attackers have increasingly used it to spread malware quickly. Drive-by-downloads occur in a number of situations; for example , when a user visits a webpage, sees a user's email address, or taps on a tricky pop-up button. However, when visiting websites, the most popular drive-by downloads do occur by far. Various types of malware have infected a growing number of web pages. In 2008, 11 million variants of malware were discovered, according to the Osterman Research survey, and 90 percent of this malware comes from hidden downloads from popular and often trusted web sites. A user must first access the compromised site before a request is made. In order to get the user to access a malicious website, attackers will send spam mails containing links to the website. When a suspicious user visits the web, malware is downloaded from the victim's machine and installed without user's knowledge. For example, the infamy Storm worm uses its own network to send spam emails with links to such pages of attack.

Exploiting existing vulnerabilities

If ransomware is deployed to the victim's network, cyber criminals may then use several various facets of known vulnerabilities in the victim's system and use them throughout their illegal activities and analyze current vulnerabilities in hardware, applications, and network networks which are most widely exploited. This is followed by discussion of existing efforts proposed to mitigate negative impacts from the farms. The summary of common attacks in hardware, software and network layers will be presented along with countermeasure examples.

Instrument Used

Hardware is the most powerful entity, and the most capable of controlling a computer machine. That is the point that, if the hardware is hacked, it has the ability to allow attackers tremendous flexibility and strength to initiate destructive attacks. Compare with software-level attacks where there are many security patches, intrusion detection tools, and anti-virus scanners to periodically detect malicious attacks, many of the hardware-based attacks are able to escape such detection. Taking advantage of lack of tool support in hardware detection, it has been reported that the hardware-based attacks are on the rise. Hardware trojan is among the most hideous and common hardware vulnerabilities among various forms of hardware misuse. Trojan hardware is aggressive and intentionally stealthy alteration made in the hardware of electronic devices such as Integrity Circuits (IC). Trojans hardware has a number of degrees that induce different forms of unintended results. A Trojan hardware may allow a module for error detection to accept inputs which should be rejected. A Trojan could insert more buffers into the chip's interconnections and thus consume more power, which in turn could quickly drain the battery. In more extreme situations, Trojans with Denial-of - Service (DoS) are blocking a task or resource from running.

A DoS Trojan can cause the target module to exhaust scarce resources such as bandwidth, battery power, and computation. It may also physically kill, disable, or change the configuration of the computer, for example, allowing the processor to miss the interrupt from a specific peripheral. Illegal hardware clones are a source of hardware-based abuse when the chances of illegally counterfeited hardware that to produce malicious backdoor or hardware Trojans. With a recent phenomenon in IT businesses aiming to minimize their IT expenditures by exporting and purchasing off untrusted hardware from web platforms, the chance to manufacture unauthentic hardware has improved.

An author explores how today's IT outsourcing paradigm has led to the increased possibility of exporting fabricated hardware parts from untrusted factories abroad. Likewise, it is often pointed out that IT firms frequently buy untrusted equipment from internet auction platforms or resellers such as chipsets and routers, which in effect can contain dangerous hardware-based Trojans. Not only are these activities troublesome because The com- panies run on the compromised hardware with possible backdoor access, it also raises the probability that the initial configuration and the specifics of internal device states will be exposed to unauthorized workers. Side channel attacks occur when opponents gain information about the internal states of a system by examining device physical information such as power consumption, electromagnetic radiation, and timing of data in and out of the CPU. Via the outcome of these side channel attacks confidential data can be leaked. A method has been published in that it explores a variety of ways the hidden key leaked by the cryptographic algorithm as a result of radio frequency analysis.

A series of techniques were proposed to thwart hardware-level attacks. Due to its criticality as an entry point to overall system security, manipulator resistant hardware devices have become an important consideration. Trusted Platform Module (TPM) provides cryptographic primitives and protected storage along with the functionality for remote servers to exchange tamper-resistant evidence. The term Trusted Computing Base (TCB) has been specified to refer to parts of a system, the collection of all components of hardware and software, which are essential to the overall system protection. The TCB must not contain any internal glitches or flaws, because that may jeopardize the security of the entire network. To ensure TCB's security, an exhaustive and thorough analysis of its code base is performed through computer-assisted software audit or system verification. In a watermarking hardware, the ownership information is embedded and concealed in a circuit description which prevents illegal counterfeiting of the host product. Equipment Obfuscation is a method for altering the explanation or configuration of electronic hardware in order to intentionally mask its features.

These methods are used to keep adversaries from accessing the original template or the falsification

/Clone important hardware components, such as IC units. Some countermeasures to count against side channel attacks include introducing noise so that physical information cannot be displayed directly, filtering certain parts of physical information, and making / blinding any correlation between input data and side channel emissions.

Software defects

A software bug is the common term used to describe a computer program error, flaw, mistake, or fault, such as internal OS, external I / O interface drivers, and applications. Cyber-attacks use the program vulnerabilities as their advantages to allow the programs to behave suddenly different ways from their original purpose. Most cyber-attacks still occur today because of the exploitation of software vulnerabilities caused by software bug and design flaws. Software-based usage occurs when certain software stack and interface features are exploited. As a result of manipulating memory processing glitches, user input authentication, race constraints, and user access rights, most common program flaws exist. Attackers commit memory protection breaches to change the contents of a memory location. Buffer overload is most excellent procedure. The buffer overload happens when a system tries to store more data than it was designed to retain in a buffer. Since buffers are generated to contain a finite amount of data, the additional information that overflow into adjacent buffers, corrupting or overwriting the valid data stored therein.

It allows attackers to interfere with existing code in the process. Validation of inputs is the method of ensuring that input data meets certain laws. Incorrect validation of data can result in contamination of the data as seen in SQL injection. SQL injection is one of the most well-known techniques in a website software which exploits a program bug. An intruder injects SQL commands from the web form to either modify the content of the database or leak data base information to the attacker, such as credit cards or passwords. Adversary exploits a flaw in a process where process output is critically and unexpectedly dependent upon the timing of other events.

The time of check to use time is a error triggered by device adjustments between testing a condition and processing the effects of the check. It's also called race condition error exploitation. Privilege confusion is an act of exploiting a bug by gaining high access to resources which are normally protected against an application or user. As a result, opponents with more privileges are performing unauthorized actions such as accessing protected secret keys.

A number of projects have been initiated in the programming community, which are dedicated to increasing safety as a major goal. The primary concern of these projects is to provide new ideas in an attempt to create a secure computing environment not only to help fix inherent common set of security flaws. In a secure coding practice based on code review, software engineers identify common programming errors that lead to vulnerabilities in software, establish standard secure coding standards, educate software developers and advance the state of practice in secure coding. Techniques are developed in a language-based, secure coding practice to ensure that programs can be relied upon not to breach important security policies. The methods which are most commonly used include analysis and transformation. A well-known method of analysis is "value testing" in which the software detects any insecure object types before running the program. Another well-known form of program transformation is the addition of runtime checks where the program is implemented in a manner that prevents any policy-violating transformation from happening. Code obfuscation is a method of producing source or computer code which has made it impossible for humans to comprehend. Sometimes, programmers intentionally obfuse code to hide its intent or logic in order to avoid reverse engineering possibilities.

It has also been suggested a safe design and development process which provides a series of design techniques allowing for efficient inspection that a piece of device part is free from any possible defects from its original design. Although not straightforward approaches, formal methods provide the ability to explore the design comprehensively and identify complicated vulnerabilities to security. Tools and techniques for promoting the inspection of mission-critical safety properties have been developed. These methods and strategies help turn higher-level health targets into a list of radioactive properties to be tested for.

Network infrastructure and protocol vulnerabilities

The early network protocol has been developed to support completely different environment that is in much smaller scale today and often does not function properly in many situations that are used today. Weaknesses of network protocols become difficult because the networking infrastructure is open to both system operators and users. The system administrators, for example, do not use an efficient encryption scheme, do not apply recommended patches on time or forget to apply security filters or policies. One of the most common network attacks is by exploiting the limitations of the Internet Protocol (IP), Transmission Control Protocol (TCP) or Domain Name System commonly used network protocols. The IP is the network layer’s primary protocol. It provides the details required to route the packets between network routers and computers. The original IP protocol had no mechanism for checking the authenticity and privacy of the transmitted data. This caused the data to be intercepted or altered when transmitted between two computers over an unknown network. IPSec has been developed to provide encryption of IP traffic to prevent this problem. IPSec has been used as one of the main technology in many years to create a virtual private network that creates a secure channel over the Internet between a remote computer and a trusted network (i.e. company intranet).

TCP sits on top of the IP to efficiently relay the packets (i.e., retransmit missing packets) and controlled packet delivery. SSL was originally developed to provide end-to - end security between two computers that sits over the transmission control protocol (TCP), as opposed to only layer-based protocol. SSL / TLS for secure Web pages is commonly used with http to form https. The Domain Name Server (DNS) is the protocol that translates the human-readable host names into the IP addresses of the 32-bit Internet Protocol. Essentially it works as an Internet directory book telling routers to which IP address to direct packets when the user provides a URL. Due to the lack of authentication of DNS replies, an attacker may be able to send malicious DNS messages to impersonate an Internet server. Another major preoccupation with DNS is its availability. Because a successful attack on the DNS service would create a significant disruption of communication on the Internet, DNS was the target of several Denial-of - Service (DoS) attacks.

Cryptography is an essential tool for protecting data that is transmitted between users by encrypting the data so that the data can be decrypted only by users with appropriate keys. Cryptography is the most commonly used data-protection tool.

A 2007 survey commissioned by Computer Security Institute showed that 71 per cent of businesses used encryption in transit for their records. In addition to defending the advanced attackers of today who exploit the shortcomings of current cryptographic algorithms, a variety of steps are on the rise. Recently, the United States National Institute of Standards and Technology (NIST) announced the discontinuation of SHA-1 and the adoption of the 2012 Advanced Hash Standard (ASH). The ability to use identity-based encryption is an aggressive research agenda for applications involving high-speed encryption to stop using sluggish 2048 bit RSA key duration along with the trusted certifying authority's impractical participation.

Quantum cryptography is an emerging technology in which two parties generate shared, secret cryptographic key material simultaneously using the transmission of quantum light states. Today, professional adversaries use a sophisticated technique that disguises malicious traffic payloads which look more like legitimate traffic payloads. Moreover, in order to measure and even simulate the volatility added to data sets, the vast amount of data flow on high bandwidth networks requires modern computational techniques. This challenge has created a new research area where network practitioners and the visualization community need the combined skill sets to capture network traffic with better visualization technique. Network experts with in-depth domain knowledge in networking systems will then analyze the visual presentation of the data.

Emerging threats

Cyber assaults on cyberspace grow, capitalizing on emerging techniques over time. Cyber criminals would most of the time modify existing malware signatures to exploit the flaws in the new technologies. In other cases, they are simply exploring unique features of the new technologies to find loopholes for malware injection. Taking advantage of emerging Internet technology and millions and billions of active users, cyber criminals use these latest technologies to easily and efficiently reach out to a large number of victims. They choose four such up-and - coming developments in technology that include: social media, cloud computing, mobile technology, and sensitive infrastructure, as illustrative examples to illustrate the risks in those technologies and discuss the unique characteristics of each of these emerging technologies and analyze, as summarized in Fig, 3 a number of common patterns of attack presented in them.

Social media

Online media, including Facebook and Twitter, have seen rapid growth over the past few years. Twitter has more than 450 million active user accounts as of the end of 2012, although the figure increases exponentially in Facebook reaching almost 1 billion people. Social networking sites were very popular for most young generations and became the preferred method of communication. Typically, each of these social media websites provides tools where users share their personal information (i.e. name, address, and gender, date of birth, music and film preference), photographs, stories, and links. Attackers use social media craze as a new medium to launch insidious attacks. By the end of 2008, more than 43,000 malicious files relating to social media sites were included in the Kaspersky Lab collection. A research released by Sophos, an IT technology and data privacy agency, has reported an unprecedented rise in attacks against social media website users. Roughly 60 per cent of users of social networks have received spam, according to their study. Because of unrestricted access to the users profile, attackers may also obtain corporate and company secrets knowledge. In Sophos' study, about 60 % of companies are worried that their workers share too much information through social networks, while about 66% of companies agree that using social networks presents a significant challenge to enterprises (Table 2).

Table 2: Emerging Technologies: Their common characteristics and common attack patterns.

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 • Service are available via Internet connection using Web Browser • Services offered by many different device such as mobiles and tablets	• Increased attack through browser • Increased attacks through social engineering • Increasing attacks coming from non PC based device • Increasing number of more organized attacks through • Increasing number of attacks through the attackers with internal knowledge

Koobface worm, which spreads via social media sites in 2009, is notably the best known malware case which uses social media sites to proliferate. Taking advantage of its zombie arsenal, the Koobface botnet automates the creation of new social media accounts that are used to friend unsuspecting users, spamming in turn enticing links that are redirected to malware. Victims who are prey to the attacks on social engineering witness their own social networking accounts turning into vehicles to send spam to friends of the victim, while the machine of the victim is repurposed into a zombie. Thomas and Nicol built a zombie emulator that was able to infiltrate the botnet of Koobface and identified fraudulent and compromised social network accounts that were used to distribute malicious links to over 213,000 users of the social network generating over 157,000 clicks. They found the ineffectiveness of new blacklisting systems that social network providers provide to remove dangerous viruses from the most popular blacklisting systems. They claimed that such blacklisting services only identify 27 percent of threats and take an average of 4 days to respond, while finding that 81 percent of Koobface 's spam visitors occur within the first 2 days of posting a message, rendering most social networking users unprotected. Another common malware attack happens when a small number of Twitter or Facebook accounts are used which are not legitimate or are not in use. The efforts of cyber criminals to appear as trustworthy users are becoming much more sophisticated. Then the criminals trick users into "friendly" or follow them on the social network site and click on their status updates which often lead to malicious websites.

In another study it is illustrated that after clicking for content on "trending" topics via Twitter, a large number of malware was spread. Also researched was the interpretation of social network networks and applications for distributing malware using Facebook mock-up facilities.

Due to the centralization of massive amounts of user data, the intimacy of personal information gathered and the availability of up-to - date data that is consistently tagged and formatted, social networking sites have also raised the stakes for privacy protection. This makes social networking sites an enticing option for a number of organizations attempting to collect vast volumes of user data, some for benign reasons and others for sinister ones. Extracting data in most cases breaches the expectations of users regarding privacy. It has been explored to protect private data of users kept in social networking service providers. Lucas et al proposed a Facebook application for the encryption and decryption of sensitive data using JavaScript on the client side. This architecture means that data never enters social network service providers in an unencrypted manner that prohibits them from monitoring and storing the information that users share over the network.

Privacy sensitivity related problems and software have also been introduced which can allow users to configure their privacy settings more intuitively. Fang and LeFevre have suggested for example a safety wizard. The wizard iteratively asks the user to add privacy "labels" to selected friends and uses this information to construct a classifier using a machine learning algorithm that can be used to automatically grant rights to the other friends of the user. The rationale for the concept stems from the assumption that actual users formulate their privacy habits, which friends will be able to see what content, based on the tacit collection of rules that they collection and regularly use with other groups.

DISCUSSION

Within malware found in the evolving technologies is mentioned above, a variety of rising trends emerge. Increased Assault by Web Browser – Using mobile browsers usually allow the services offered by new technologies. Web browsers are arguably one of the most commonly used apps offering the inter-face for users to conduct a wide variety of tasks linking them to outer world. Therefore web browsers are becoming increasingly important tool for millions of computer users today. Web browsers contain a number of vulnerabilities as with any other piece of software. Such vulnerabilities are used by the attackers to gain control of the user's device, capture user information, erase the data, and use the infected user machine to target other computers. In 2008, 11 million variants of malware were discovered, according to the Osterman Research survey, and 90 percent of this malware comes from hidden downloads from popular and often trusted web sites.

Some of the common attacks that exploit the security of the browser are through extensions, often also called "plug-in" or "add-on" languages and scripting such as JavaScript or VBScript. Extensions are reusable components of software that can be plugged into a browser to provide a new functionality or customize the user experience. Anyone, even with a little train of experience and software development, can develop an extension and many unsuspecting users can freely download it. Such extensions often contain software bugs that greatly increase the attack surface to be exploited by the attackers. The ability to run a scripting language such as JavaScript or VBScript enables authors of a web page to add significant features and interactivity to a web page. Attackers can abuse this same capability though. Cross-site Scripting (XSS) is a well-known vulnerability to exploit scripting language. XSS allows malicious script injection into web pages by attackers. The malicious code is executed as naive clients access the web sites to conduct destructive operations on the user's computer.

Most common defense mechanism against vulnerabilities of web browsers is done by means of strengthened user authentication to ensure that only authorized users access the webpage. The filtering of content is another common technique used to detect any malicious scripts embedded in web pages. Few plugins or plugin extensions may be programmed to deactivate per-domain client-side scripts to make server protection tougher. The Internet by its very nature provides anonymity. Many Internet-based attacks have grown substantially to exploit such Internet nature. A requirement has been raised not only for users to authenticate to a server but also for the server to authenticate itself to users in such a way that both parties are assured of the identity of the others. To address this requirement, the technique called "mutual authentication" has gained a popularity. Some of the mutual certification techniques studied today include password authenticated key exchange (PAKE), Dynamic Security Skins (DSS) and Trusted Computing Group (TCG) remote certification.

CONCLUSION

This study centered on two facets of the information system: understanding flaws in evolving systems, and new challenges in progressing telecommunications and IT. Through new technologies, such as social media, cloud storage, mobile apps, and vital infrastructure, rising vulnerabilities have been found, frequently taking advantage of their specific features. They identified the characteristics of each digital technology and the various ways in which malware is circulating in these new technologies. Instead, ir will address common set of trends of general attack found in the evolving technologies. For example, because most of these new technology provide services online, some of the recent attacks are increasingly leveraging browser protection by malware concealed within plugins or bugs to access sensitive data in scripting languages. Adversaries also move their fighting ground from a laptop to other devices to prevent detection, including smart phones, tablet PCs and VoIP. With the growing number of mobile users and the sophistication of mobile applications, mobile malware has risen sharply in the last few years especially. Scams which use social engineering are on the increase. Increasingly popular social networking platforms such as Facebook, Twitters and others have been used as distribution channels to get unwitting users to install or propagate malware. More coordinated attacks were documented through the use of botnets. Since the effect of such disruption is much greater than individual attacks, the thwarting of botnets is a growing issue. Latest figures also indicate that there are growing numbers of cyber threats targeted to a particular system, using within information and resources, for example, and command and control systems.

We also outlined potential future paths for the project. When more and more people are communicating over the Internet, it has been proposed to consider all levels of users including both experts and non-experts of computer technology, and to establish security measures relating to their degree of trust. Many security experts have stressed the preservation of user privacy as an important future research to be carried out as the quantity of personal information over the Internet has expanded rapidly in recent years. Instead of simply attempting to fix a specific problem on current Web and computer networks, more innovative approaches to seeing "a larger picture" or looking "outside the box" have been proposed, as some evidence suggests that digital technology’s capacity is exhausted and no longer scale well using traditional incremental methods. Developments of secure internet and trustworthy systems for the next generation have been suggested as important research areas for looking to the future. As an important issue to be addressed in the future, the development of global identity management and traceback techniques to enable adversaries to be tracked.

REFERENCES

[1] European Union Agency for Cybersecurity (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. 2017.

[2] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, “Cybersecurity protection for power grid control infrastructures,” *Int. J. Crit. Infrastruct. Prot.*, 2017.

[3] J. D. Moteff, “Critical infrastructures: Background, policy, and implementation,” in *National Critical Infrastructure Policy: Background and Select Cybersecurity Issues*, 2016.

[4] J. Payette, E. Anegbe, E. Caceres, and S. Muegge, “Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects,” *Technol. Innov. Manag. Rev.*, 2015.

[5] H. Wang, N. Lau, and R. M. Gerdes, “Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis,” *Hum. Factors*, 2018.

[6] S. Muegge and D. Craigen, “A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks,” *Technol. Innov. Manag. Rev.*, 2015.

[7] M. Domínguez, M. A. Prada, P. Reguera, J. J. Fuertes, S. Alonso, and A. Morán, “Cybersecurity training in control systems using real equipment,” *IFAC-PapersOnLine*, 2017.

[8] T. A. Johnson, *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. 2015.

[9] K. Kobara, "Cyber physical security for Industrial Control Systems and IoT," *IEICE Trans. Inf. Syst.*, 2016.

[10] G. Wen, W. Yu, X. Yu, and J. Lü, "Complex cyber-physical networks: From cybersecurity to security control," *J. Syst. Sci. Complex.*, 2017.