Emerging cyber security technology research paper sample

Law, Security

Abstract

The enhancement of cyber-attacks that is being experienced at enterprise, national and international level is worrying. This trend has resulted in the increase of funding for the research and study of cybersecurity technologies. Threats occurring on the organization’s assets are experienced daily due to change and improvement of technologies that are developed frequently. Computer security is an important aspect of any organization and government agency. With the advancement in computer technologies, there are advanced attacks that are targeted at computer systems which are thought to contain vital information. Computer hackers are doing all they can to break into computer systems in order to gain information. There are technologies that are being used to counter these attacks. Various governments are doing all they can to ensure that the systems are safe. Attackers are becoming more and more sophisticated and utilize highly sophisticated techniques to compromise critical information infrastructure that supports networks and information flow. In order for the attacks to be successful, attackers are devising new mechanisms of promoting anonymity and evading detection. This paper will focus on the technologies that are used in countering cyber attacks and the role that the federal government is doing to alleviate these attacks.

Introduction

Network security is a process of ensuring that digital data of an organization are protected. This process is aimed at protecting the confidentiality, maintain the integrity and ensure that there is availability of data to all

stakeholders (Brinkley and Schell 1995). This means that the unsecure system can bring denial of services and access to data. Confidentiality and integrity of data can also be lost if network security is breached. It is imperative that the network of an organization is protected, from threats and vulnerabilities, to be able to maximize the potentials of a network. There is a formidable challenge in evaluating potential malicious attacks, threats, and vulnerabilities to a network security because of the large scale of modern enterprise networks and a many vulnerability that are found in the software applications. Malicious threat is an event that when it takes place it causes the system to fail. It can also be described as a potential cause of an unwanted incident which may cause harm or damage the system or an organization. A malicious attack is an event or sets of actions that are directly aimed at causing harm to a target system. There are actions that are planned and well thought and they are driven by political, illegal or malevolent motives.

When President Bush signed the e-government Act of 2000, the main intention was to have a more 24/7 government. The aim was to have many operations going on without the need to wait for some services to restart after being stopped overnight. Security was an issue when this act was signed but it was not at the rate and magnitude that it deserves today. before information would be moved and accessed online, there would have been vetted so that the information system that was deployed would have been efficient and secure. Ten years of this movement, there are still a lot of movements that are being experienced where government agencies and private enterprises are moving their information online. The pace at which

information was moved online was not at par with the pace at which security is improved and enhanced. Governments did not take into consideration the need to spend more on cyber security. This was not the case as the US government is learning the hard way in the current cybersecurity threats that is being seen. There is a serious cybersecurity attacks hat have been experienced in the recent past like the recent attacks by Anonymous to FBI and Homeland Security systems. This made two government agencies handling cyber-security issues. There are proposals that have been made by the Congress to the effect that the government should control SCADA systems. This proposal makes one wonder how this will be possible and yet the government is not able to protect her own systems.

It was in the year 2009 that the cyber attacks were used by the US to attack nuclear computer systems network of Iran. This was ordered by President Obama and used Stuxnet worm. There are many cyber attacks that have been experienced by Iran on their nuclear computer network systems.

Emerging cybersecurity technologies

There are new cyber attacks that have emerged. One example is Advanced Persistent Threats (APT); these threats have changed the way cyber attacks are undertaken. They have also changed the countermeasures as this has made it difficult to prevent them from attacking information systems. It has been found out that an APT which makes use of targeted code which leverages zero-day vulnerability is difficult to mitigate with the use of intrusion detection systems and with the use of anti-viruses. The issue with this is that after the malware has been detected, it will be hard to determine

for how long that malware has been attacking the system. Another issue with the handling of the APT is that it is hard to determine if he malware that has been discovered is the entire attack that has been in the system. With APT, there could be leveraged multiple malware tools that enable the APT to gain access to the system. With cyber security attacks being a major concern for both national and international entities, cybersecurity has been considered to be a critical issue of concern than it has been in the past. There is a lot of funding towards the handling of the cybersecurity threats and information.

Moving target technologies

This is one of the technologies that has been developed to counter cyber attacks. With this technology, the surface area of the attack is increased so that the cost of the attack for the attacker will be increased. It will also decrease the chances of the attacker hitting the target system. The vulnerabilities of the attack will eventually be decreased. One problem that is being experienced by many systems is that these systems are static. With this feature, the attacker has all the time to track and strategies on the best way in which to undertake the attack. With the use of moving target technology, the network will constantly change the configurations and the values of the environment. One way in which this can be achieved is by changing the IP addresses of the organization, changing the Operating Systems, changing the ports, and also changing the protocols that are being used in the organization. After all these changes have been made, the attacker will not have consistent scans when they scan the system. The moving target technology is also useful in the fact that it will reduce the area

that is known to the attacker so that they will have less area of attack. One challenge that is experienced with the use of this technology is that it will be hard to maintain the network that is operated when the changes are made in the system. There is also the cost factor which issues of concern. One real-world example where this technology is being used is JumpSoft subscription. With this, JumpSoft Company has created a defense package that will enable companies subscribe to enable moving technology mechanisms in their systems. The subscription is known as JumpCenter. This package enables organizations to make use of reactive and adaptive systems of automation to decrease the surface area of the attacks. The concept that JumpCenter and moving technology makes use in this process is to ensure that the costs for undertakimg thaattack will be enormous for the attacker. The risks will also be increased. JumpCenter makes sure that the network is kept operational. This is achieved by deploying this at the application layer. This is because the application layer is exploited with ease by making use of the regular vendor releases. Another reason for the choice of the application layer is that JumpCenter considered that the application can ground the business if it is attacked. It was made as secure as possible. Attacks from trusted hosts can be minimized by administrators through implementation of hierarchical or one time password and data encryption techniques. Users and administrators can protect themselves and their networks by installing firewalls that block outgoing packets with source addresses that differ from the IP address of the user’s computer or its network.

Remote agent technologies

There is also the use of remote agents which are known to monitor the network. They are also referred to s mobile agents. It is important to monitor a network actively so that patches can be updated to mitigate the network against the modern cyber attacks. It is evident that a network which is not monitored is reactive and will not be effective with regard to today's cyber attacks. In addition to this is the fact that larger networks are difficult to be manually monitored by network administrators. This is because they are made up of many nodes that enable the connections. With the use of remote gents, the network security assessment and monitoring can be done from remote agents or servers without having to travel to the premise. The cost is also minimized. The most important point to note in this aspect is that remote agents are able to run the testing of the network without the use of unsecured firewall protocols.

There are many organizations which use network monitoring based on SNMP. They can sometimes make use of scripts which are built and used in situations where there is tedious and intensive monitoring that is to be done. The use of SNMP monitoring and script are not that effective and will require a network administrator who will do through the logs in order to ascertain that proper monitoring has been undertaken.

With these challenges faced in network monitoring agents, there were a group of students from the University of Minnesota who developed a mobile agent monitoring system with the use of the Ajanta mobile agent system. This system is able to filter information in the system and alter some functionalities of a system.

Real-time forensic analysis

The use forensic tools in criminal processes and procedure has proved to be handy hen handling criminal activities. It is one method that has been adopted by many agencies when looking for information. This relates to network monitoring. The slight difference is that with this method is that it takes an investigative approach so that there is a maintenance of situation awareness. in this respect, there is continuous monitoring of the network. Another difference is that with network monitoring, the agent will monitor the network and if there is a threat, it will take the necessary corrective or preventive action to prevent it. With forensic analysis, if there is a threat, it will reproduce the threat and analysis the action that the threat takes. This is the analysis that is taken by the process. A network forensic analysis tool prepares the network for forensic analysis and ensures that it is easy to monitor and identify the threats to the network. It is important to note that the information that is found from the forensic analysis rakes can be used as background data for other data and processes.

There are other uses of forensic analysis. One practical use of forensic analysis is with healthcare sector. Because the healthcare sector falls under Health Insurance and Portability and Accountability Act, it is required that the information that is passed in the works undergo some form of monitoring. Although all the information in the forensic analysis tool may not be required, it is better and preferable to have more information than has little information when undertaking legal processes. With the use of network forensic analysis tool, it is possible to recover network data when all other methods of data recovery have failed.

Threats evolve every single day. As new threats emerge companies such as WebCenter need to develop dynamic mechanisms of combating and mitigating them. In order to continuously monitor the evolicution of new attacks and develop mechanisms to prevent and mitigate its effects, periodic review of the threats should be carried out. These reviews examine and assess the evolution schemes of new threats and the target areas as well as a weak point. This is done through collaborative involvement of the concerned parties in research institutions, conferences, trainings and seminars. These events have the advantage over individual reviews because it involves many stakeholders with different versions of vulnerabilities and solutions. Collaborative learning is essential in this era of the internet revolution due to the emerging challenges posed by widespread computer applications.

The role of the federal government in implementing these technologies

Role of the federal government in support of Moving technology

The federal government has been seen to be supporting the implementation of these emerging technologies for cyber threats. One way in which this was evident is in January 2011 where the Presidential Council of Advisors on Science and Technology undertook the sponsorship of the work of Networking and Information Technology Research and Development. There has been the identification of emerging technologies on cyber threats by Networking and Information Technology Research and Development. They have enhanced the development of current technologies when mitigating threats. One of the technologies identified by Networking and Information

Technology Research and Development is moving technology. The support that is seen to come from government in the enhancement of moving technology and other cyber security threats mitigation efforts is seen to be an effort by the government to enhance security in both private and public entities. One example in which this can be seen is that the government, through the Air Force Office of Research was given a grant of one million US dollars. If the military reactive position is changed regarding cyber attacks, then security would be forgotten.

Federal Remote agent technologies

The government is known to have large and complex computer networks. Many military computer networks cut across many countries. The interest of these networks is to all people and residents of the countries with which the networks cross. There is heavy investment in monitoring networks that span many countries. The for the support of the networks is for the benefit of everyone who is involved in the whole process.

Federal Government support in real-time forensic analysis

The federal government supports real-time forensic analysis because of the fact that the federal courts and the criminal justice process. The police has also been seen to use computer forensics in nearly, all operations.

Government's role in policy making

Apart from the technologies that are being formulated for use in emerging cyber threats, there is a lot of effort that is done by the government in terms of developing policies. Formulation of security policies is important because

policies serve as guidelines for the use, access, storage and transfer of information between related parties. Policy formulation processes outlined the mechanisms in which information should be retrieved, used, and stored, and the personnel that are authorized to use it. This controls the flow of information to the wrong persons thereby reducing the risks of misuse and modification. Information in the digital age is vulnerable to numerous attacks originating from different sources. Attacks such as viruses, malware, and spyware among other degrade the quality and integrity of information.

Conclusion

With the advancement in computer technologies, there are advanced attacks that are targeted at computer systems which are thought to contain vital information. Computer hackers are doing all they can to break into computer systems in order to gain information. There are technologies that are being used to counter these attacks. Various governments are doing all they can to ensure that the systems are safe. Attackers are becoming more and more sophisticated and utilize highly sophisticated techniques to compromise critical information infrastructure that supports networks and information flow. There is a formidable challenge in evaluating potential malicious attacks, threats, and vulnerabilities to a network security because of the large scale of modern enterprise networks and a many vulnerability that are found in the software applications. Malicious threat is an event that when it takes place it causes the system to fail. It can also be described as a potential cause of an unwanted incident which may cause harm or damage the system or an organization. A malicious attack is an event or sets of

actions that are directly aimed at causing harm to a target system. There are actions that are planned and well thought and they are driven by political, illegal or malevolent motives. Collaborative learning is essential in this era of the internet revolution due to the emerging challenges posed by widespread computer applications.

References

Barker, W. C. (2011). E-Government Security Issues and Measures. In H. Bidgoli, Handbook of Information Security (pp. 97-107). Hoboken: John Wiley & Sons.

Bhatti, R., LaSalle, R., Bird, R., Grance, T., & Bertino, E. (2012, June). Emerging trends around big data analytics and security: Panel.
In Proceedings of the 17th ACM symposium on Access Control Models and Technologies (pp. 67-68). ACM.

Casey, E. (2011). Handbook of digital forensics and investigation. Burlington: Academic Press.

Stolfo, S. J., Creamer, G., & Hershkop, S. (2006, May). A temporal based forensic analysis of electronic communication. In Proceedings of the 2006 international conference on Digital government research (pp. 23-24). Digital Government Society of North America.

Tripathi, A., Ahmed, T., Pathak, S., Carney, M., & Dokas, P. (2002). Paradigms for mobile agent based active monitoring of network systems. In Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP (pp. 65-78). IEEE.

U. S. Securities and Exchange Commission. (2011). 2010 Annual FISMA

Executive Summary Report. Washington D. C.: U. S. Securities and Exchange Commission.