IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 07, February 2019)

Analysis and Design of a Model for Cyber Security

Hemantkumar Narayanbhai Patel
Research Scholar
Mewar University, Chhitorgarh,
Rajasthan (India)

Dr. Chandikaditya Kumawat
Professor of CSE
Mewar University, Chhitorgarh,
Rajasthan (India)

Dr. Jigar Patel
Director
Kalol Institute of Management,
Kalol, Gujarat, (India)

Abstract –**The dynamic character of the contemporary society is regarded as a result of alarming alterations in social environment. Introduction of new cultural traits into society bring new social changes. Present society is dominated by a complex culture of networking and information. The Information Technology Revolution has brought many changes in the social structure. Cybercrime is the product of technological development. Social networking has become so predominant in our lives because we all are living in Network Society. We are in touch with the world constantly. Although, a massive literature has been generated on Cybercrime and Social networking sites, still ambiguity persists on the impact of technology and social networking sites on society because still the effect is in the infancy stage and much needs to be done. Indian society has a dearth of relevant literature on cybercrime and social networking sites. It is also noted that very few studies have been conducted and reviewed on adolescent's use of social networking sites in Indian context. The studies which are conducted on the effects of these sites on adolescents provide a mixed stand. The following chapter Research Strategies explains various objectives, tools and techniques used in the study conducted on adolescents. While some cyber security incidents have occurred at nuclear power plants, crossing the imaginary boundary between IT and PCS and shutting down reactors, so far the potential for damaging a nuclear reactor appears theoretical.**

Keywords – **Cybercrime, Cyberspace, IT, Neuromancer, PCS.**

I. Introduction

First coined by William Gibson [1] in his 1984 novel Neuromancer, the term Cyberspace is a popular descriptor of the virtual environment in which activity of internet takes place. The term cyberspace has become so common that it seems to dominate the thinking of people who consciously or subconsciously feel that they are entering a place which has new meanings, dimensions and purposes. Internet has created new public spaces and communities. These spaces and communities are known as virtual because they are no longer linked with place or time. However, they have common interests in social, cultural and psychological realms. They are based on Computer-mediated-Communication (CMC) and Human Computer Interaction (HCI).This has led to the emergence of Network Society. The Primary condition to be a part of virtual community is a network connection and a desire to be a part of a wider community called as Virtual Community.

Virtual Community is a combination of individuality and sociability in modern Network Society. [2]

Reflecting social anxieties about this surprisingly new phenomenon, the early studies which attracted the most attention were those that focused on pathological internet use and addiction Young (1998)[3], but as sociology delved deeper into cyberspace, some very basic questions became apparent. Do traditional concepts and theories suffice in our understanding of online behaviour? Do we have to modify these theories? Do we need to develop new ones? These questions arise out of the recognition that cyber space as a sociological realm is quite different from face to face environment. Geographical boundaries are transcended. Everything is recordable and no boundaries of privacy exist. Social interactions can be synchronous, asynchronous, or something in between. Under complete anonymity, people become more disinherited than usual, or they might experiment with different identities. Sensory experience is expanded to multimedia experiences with highly creative fantasies. All these features of online space are characteristic of contemporary society i.e. network society.

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time but the basic crime ideas remain same. The significant change in modern time is on increase in personal computing power in a globalized communication network. The networked technology has become more than simply a force multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed. Internet is a set of social practices; it is the kind of purpose to which we put the internet that creates the possibility of criminal and deviant activities. The internet provides the means to link up the many and diverse networks already inexistence. Since commercialization of the internet during the mid-1990s it has grown manifold. Even though majority of worldwide total internet connections are located in developed countries, the fact is that these are growing at a very fast rate in developing countries too. An Unequal access also follows along existing lines of social exclusion within individual countries and factors such as employment, income, education ethnic disability are reflected in the patterns of internet use (Castells 2002) [4]. These inequalities point out the social characteristics behind the emergence of cybercrime and cybercriminals. Thomas and Loader 2000[5] conceptualize cybercrime as those Computer Mediated Activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. This definition reflects an important difference between crime (acts explicitly prohibited by law and hence illegal) and deviance (acts that reach informal social norms and rules, hence considered undesirable Objectionable). However it is worthwhile that crime and deviance cannot always be strictly separated in criminology. The boundaries between the criminal and deviant are socially negotiated and have become a recurrent feature of contemporary developments around the internet. Some criminologists argue that cybercrime is not a new type of crime but is same as non-virtual crime; it just uses new tools and techniques, while some others say that cybercrime is radically different and focuses on social structural features of the environment.

The objectives of the present study are:

1. To analysis the cyber security using various sources.
2. To identify and classified security holes with vulnerabilities assessment.
3. Design and validate a model for cyber-attacks.

II. Cybercrime: A Conceptual Perspective

Theorists of the internet agree that cyberspace makes possible near and instant interactions between individuals who are spatially distant, which creates possibility for new forms of association which in turn gives rise to cybercrime and cyber deviance. Cybercrime, in simple terms, is a crime that is facilitated or committed using a computer, network or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. It can take place on the computer alone, or in other virtual or non-virtual locations. It is recognized that current legal definition of cybercrime varies drastically between jurisdictions. A practical definition of a cybercrime is offered by Kshetri, (2010) [6]. According to him, Cyber Crime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations. Examples of cybercrime include denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber terrorism, and cyber extortions. It is evident that organized criminal organizations use cybercrime extensively to collaborate and connect with their vast network which is spread across globe. The synergy between organized crime and the internet has thus increased the Insecurity of the digital world.

Following are the common motives behind cyber-crimes:

1. Monetary Profit Like many offline crimes, cyber-crimes are also motivated by the desire for financial gain.
2. Political Motive Internet is used by extremist and radical groups for propaganda, to attack the websites and network of their opposite groups.
3. Sexual Impulses Sexually deviant behaviour is illegal and is considered harmful. People view porn sites to fulfil their immoral desires and needs.
4. Entertainment many cybercrimes are done for fun and enjoyment unlike other cybercrimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both a means and an end.
5. Emotional Motivators Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. Revenge is much better planned than anger and it could be more dangerous because cybercriminal has more time to think and plan his tracks which often reduces the possibility of being caught.

III. Proposed Model to Prevent Cyber Attacks

The cyber-attack simulator was initially developed using the ARENA software. This development resulted in a model with basic network editing capabilities and a reasonable level of attack specification capabilities. Although this ARENA model has proved that the concept of simulating cyber-attack is plausible, the new features desired for the model, such as working with XML data, are beyond the limitations of ARENA. The desire to overcome such limitations has since motivated the development of an independent simulation model that can be appropriately configured to implement features that are not possible with the ARENA simulator. This new model includes a customized interface specific to the development of network structures and attack scenarios, a series of input and output options, and more detailed features in defining the networks and attack scenarios.

The model was developed using the object-oriented programming language Java. Java has many desirable characteristics in modeling realistic environments. Java is also a cross-platform programming language that only requires the JRE (Java runtime environment) to run a java program on any platform. The remainder of this section discusses the primary intentions of the model, provides a background of the development environment used, and presents the structure of the modeling elements.

Demonstrating Intents and Model Overview:

The overall goal of developing this cyber-attack simulation model is to create an application that can generate valid intrusion detection system alerts in a virtual network representative of a real private network. With the cyber-attack simulator, a user can create or load a specific network topology, specify the vulnerabilities of the network create and run attack scenarios, and view sensor alert data produced. Several inputs and outputs are necessary to the functionality of the simulator. A diagram depicting the types of inputs and outputs is displayed in Figure 1.

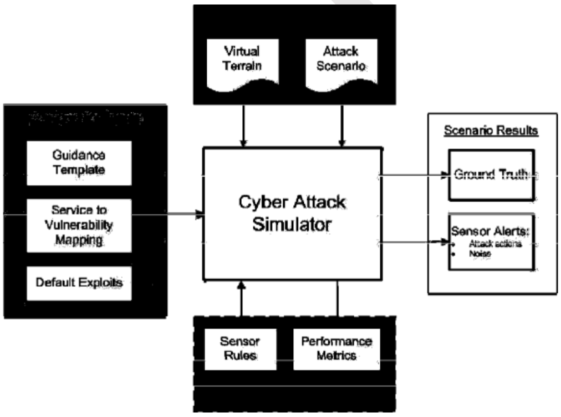

Figure 1: Cyber Attack Simulator Functionality

As is shown in Figure, the simulator consists of three primary categories of inputs and outputs: configuration inputs, XML imports and exports, and scenario results. A sensor management add-on, developed by McConky in 2007 is also shown.

The configuration inputs include data that is loaded from files as the simulator is opened. The guidance template file is a directed graph that indicates what sequence of stages can be used in an attack and what categories of exploits are included in each stage. This information is used when attacks are generated based on a set of parameters. Another file includes the service to vulnerability mappings, which maps a machine service to a set of vulnerabilities through the use of service IDs and vulnerability IDs.

This effectively indicates what exploits can be executed on a machine that is running a certain service. The default exploits file loads a database of known exploits (also referred to as available actions) that the simulator can choose and filter from. This database of actions is used by the simulator when creating the individual steps of an attack as well as when creating the noise (or false-positives) that occurs during an attack scenario.

The XML imports and exports allow for structured XML documents to be created by or interpreted by the simulator. These documents can also be created by and interpreted by other applications, providing a means by which the simulator can interface with these applications. A document that is commonly used by the information fusion tools in development is the Virtual Terrain XML document. This document depicts the detailed structure of a network, whether the network is real or virtual. Figure shows how the virtual terrain document is used among different applications. The cyber-attack simulator specifically can read in a network model from the virtual terrain or create a virtual terrain document from a network that has been modeled. Therefore, applications that make use of the alert data generated by the simulator can also be provided with the entire structure of the network used to generate the data. Also, an additional XML document depicting the set of attacks in an attack scenario can be created by or read in by the simulator. The scenario results include data that is generated during an attack scenario run and output into text files. A ground truth file lists all of the attack-based actions that occur, along with details such as the attack that the action belonged to, the source and destination of the attack, and the success or failure of the action. A set of sensor alert files list all of the IDS alerts generated by sensors placed in the network model.

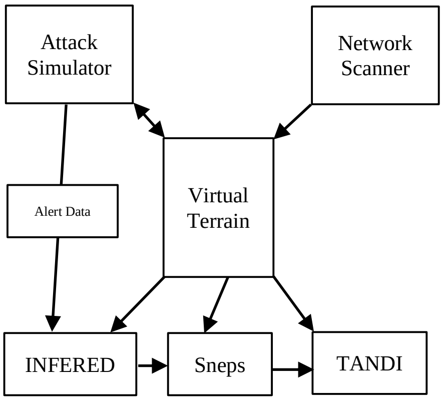

Figure 2: Integration of Virtual Terrain

These IDS alerts correspond to both attack-based actions and noise-based actions. Lastly, the sensor management add-on includes the appropriate functionality to define rules for the manner in which sensors handle the alerts generated. A fusion engine queue is modeled, and alerts are sent to this queue as defined by the sensor rules. Performance metrics are generated for purposes of comparing the sensor rules.

IV. Conclusion

People rely on technology for many needs. However, it is noted that abuse of technology has given rise to a new variant of crime online i.e. cybercrime. Emergence of virtual society has associated risks with it. It is characterized by instant communication with anonymity, deception and disguise. Various theoretical explanations provide an answer to an in-depth curiosity about use and abuse of technology and how it has given rise to cybercrime. The classical theorists relate emergence of crime to the development of science and technology. The modern theorists, on the other hand discuss the effect of technology on contemporary society which they characterize as risk society, encouraging anomie, dehumanization. The postmodern theorists see the world as hyper real and virtual, full of simulations and technological intensities facilitating spatial interactions and providing anonymity to cybercrime. Cybercrime has serious impact on society in the form of psychological disorder, social disorganization and economic losses. Even though all people suffer from its ill effects, the most vulnerable group is adolescent and youth.

Cyber security should never be neglected. In fact, it should be accorded with utmost importance. These days when security across the Internet is getting more serious, it is just appropriate if you would aim not to be victimized by cyber criminals and cyber threats. Cybercrimes and risks could be avoided if you know how Cyber security is essentially about managing future risk and responding to current and past incidents and attacks.

Reference

[1] Gibson, William (1984), Neuromancer, Pg.4, Ace Hardcover, New York.

[2] Network Society-The term network society was coined in Norwegian by Stein Braten in his book Modelleravmenneskeogsamfunn (1981). Later the term was put to use in Dutch by Jan van Dijk in his book De Netwerkmaatschappij (1991) (The Network Society) and by Manuel Castells in The Rise of the Network Society (1996).

[3] Young, Kimberly (1998), Internet Addiction: The Emergence of a new clinical Disorder, Cyber Psychology and Behavior, Volume 1- No.3, Pg. 237-244.

[4] Castells, Manual and PekkaHimanen (2002), The Information Society and the Welfare State: The Finnish Model.), Pg 208-23, Oxford UP, Oxford.

[5] Thomas, Douglas and Loader Brian (2000), Cybercrime Law Enforcement, Security and Surveillance in the Information Age, Pg 8,Routledge, London.

[6] Kshetri, Nir (2010), The Global Cybercrime Industry, Pg 3, Springer, New York.

[7] www.gov.uk/government/publications/information-security-breaches-survey-2014

[8] 'When Vulnerabilities are Exploited: the Timing of First Known Exploits for Remote Code Execution Vulnerabilities', Tim Rains, 17 June 2014, http://blogs.microsoft.com/cybertrust/2014/06/17/when-vulnerabilities-are-exploited-the-timing-of-first-known-exploits-for-remote-code-execution-vulnerabilities

[9] Brenner,W.Susan (2010), Cybercrime:Criminal threats from cyberspace. Greenwood Publishing group, Westport.

[10] Furnell, Steven (2002), Cybercrime : Vandalizing the information society,Addison-Wesley, Boston.

[11] Arquilla, John and Ronfeldt, David and Monice, Santa (2001), Networks and Netwars : The future of Terror, Crime and Militancy. C.A :Rand.

[12] Rege, Aunshul (2009), Whats love got to do with it? Exploring online dating scams and identity. International Journal of Cyber Criminology, Vol.3(2) , 494-512.

[13] Kluver, Randolph and H., K.C. and Yang, C.C. (2003), Asia.com : Asia Encounters the Internet, Routledge Curzon, New York.

[14] Ahn, John (2011). The Effects of Social Network sites on Adolescents, Social and Academic Development : Current theories and Controversies. Journal of the American Society for Information Science and Technology, 62(8), 1435-1445.

[15] Ahn, John (2012). Teenagers Experiences with Social Network Sites : Relationships to Bridging and Bonding Social Capital. The Information Society : An International Journal, 28(2), 99-109.