ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security

Jeffy Mwakalinga and Stewart Kowalski

Department of Computer and Systems Sciences, Stockholm University, 16440 Kista, Sweden

Summary
This paper presents an analysis of ICT crimes using the adaptive information security systems model. There is a desire of being able to identify potential ICT victims so that measures could be taken to protect them. We briefly describe the crime theories, the top ten crimes, and the desire to have crime proofing products. We then describe the adaptive model for information security systems, and the architecture and the socio-technical system for analyzing ICT crimes. The analysis of the ICT crimes is presented. Finally, we present recommendations on how to improve on how to improve ICT security.

Key words:
Socio-technical, deterrence, prevention, detection, response

1. Introduction

ICT crime resulted when some hackers understood that they could make money out of hacking. The early hackers were creative programmers and scientists in the 1960s that were mostly from MIT and Stanford University [20]. The early hackers were much respected and they started computer companies and include people like Steve Jobs and Gordon Moore [19]. The hackers started getting ideas of using hacking for criminal activities in the 1980s because of the film 'war games' [19]. According to Paulsen [19], this film inspired the mini-boom in amateur hacking. A wave of law breaking teen hackers came up in the years after this film in contrast to the original MIT hackers who were not breaking laws [19].

ICT crime is part of the techno crime involving crimes against computers, or committed with computers, cybercrimes, and crimes involving credit cards, automated telling machines, and crimes against digital rights properties [11]. The results of these crimes have given birth to new techno laws, techno security, and techno police. There are a number of theories to explain the general crime [14]. The first one is a traditional explanation called environmental theory. The theory is based on the effect of biology and heredity on criminal behavior in humanity. The second traditional theory is called personal theory. This theory is based on the effect of upbringing on behavior of individuals.

Manuscript received March 5, 2011
Manuscript revised March 20, 2011

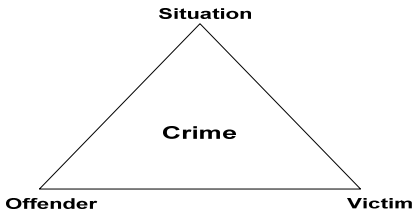

Figure 1: The model for opportunity theory [14].

The modern theory on crime explanation is called opportunity theory. According to this theory, for a crime to occur there must be a situation, an offender, and a victim as shown in Figure 1 [14].

Today we have a situation where ICT criminals have made hacking a business with models, supply chains, and pillars of business [17]. Paul Otellini, the Intel CEO, announced recently that security has become the third pillar of business together with networking and power consumption [17]. For the hacking industry the pillars of their business is supply chains, optimization, and automation [17]. The supply chain comprises different groups of hackers with different roles. Optimization is done by effectively using the compromised resources and tools for command and control. The hacker groups compete against each other by removing competitors' tools in a compromised computer. For example, a tool kit called the Spy Eye first removes the Trojan called Zeus before making an installation is a compromised zombie computer [17]. Automation is achieved with attack templates and kits, botnet army, search engines to find potential targets. In this way, a hacker could make a complete attack with just a few mouse clicks [17]. The next section presents the top ten Internet crimes in the USA in 2009.

1.1. The Top ten Internet Crimes

The Internet Crime report for 2009 reported 336 655 Internet crimes reported in USA that year [10]. The top ten most common Internet crime complaints are briefly described [10]. The first crime is the category of FBI scams with 16.6% of the total crimes. In this fraud, a victim receives an e-mail supposed to be coming from the FBI director. In the e-mail, it appears that FBI is trying to

get something, like money or identity information, from the victim.

Another type of scams is when a sender uses threatening methods to make a victim part with money. A victim receives an e-mail and the sender claims that the message was sent by a gang to assassinate the victim because of some offense against the gang. The victim is asked to send a certain amount of money within 72 hours to the sender or die if the victim does not do that. The next crime in the top ten Internet crimes is the non-delivery of merchandize, 11.9%, in which the victim bought something but it never arrived. The next crime is called advanced fee fraud, 10.4 %. It is an incident where a victim is promised to receive a huge amount of money if the victim helps to transfer a huge sum of money from the sender. The victim is to pay some kind of expense fee before the transfer. The next crime is identity theft, 10.3%, an incident where someone steals an identity or identity information. Overpayment fraud, 7.9%, is a crime in which a seller of an item advertizes on the Internet. The purchaser gives to the seller a counterfeit cheque that has an excessive amount than that agreed. The seller is asked to deposit the cheque and wire back the excessive amount immediately to the buyer but the cheque bounces at the bank and the wired amount is never returned. Miscellaneous consumer frauds are different types of frauds where victims are asked to send money where nothing is bought or sold. Spam, 4.8%, is unwelcome mass distributed e-mails. Credit card fraud, 4.5%, is a crime where someone is charging goods or services to victims' credit cards. Auction fraud, 4.3%, occurs during online auction transactions. Computer damage, 3.5%, is a crime that occurs because of intrusions or some kind of hacking to victims' computers.

1.2 ICT Crime Prevention Efforts

The main concern is how to prevent or reduce crime? Experiments show that some crimes could be reduced by modifying the opportunity for committing a crime in the design or built environment [14]. In Canada and USA, street crime prevention is done through environmental design [14]. In Europe, street crime prevention is done by reducing crime and fear of crime by designing out crime, which implies reducing crime through urban planning and architectural design [14]. In efforts to prevent ICT crime, the European Telecommunications Standards Institute comments that

"*The European Commission services believe that European standardization in this area will contribute significantly to crime proofing products or services. One possible solution would be the development of a check list of factors to be taken into account at an appropriate stage in the product/service development process that will increase general crime prevention and contribute to the protection of citizens*" [3].

The aim of product proofing, as suggested by European commission services, is to prevent an offence, lower the impact of an offence, increase the ability to detect an offence, and establish responses to an offence [3]. The European commission services suggest five main keys [3] in this regard. The first key is intelligence, which involves gathering necessary information on a crime. The second key is to be able to intervene by using generic principles. The third key is to encourage crime proofing at the implementation stages during manufacturing of products and systems. The fourth key is to involve organizations and individuals as crime proofers. The last key is to assess the impact of the crime proofing measures.

The International and European police have a special section for dealing with ICT crime. The international police (Interpol) have set a special section that gathers intelligence information including strategic reports and operational reports to help member states [11]. Interpol presents a checklist of IT crime prevention on what to consider in different areas of an organization [18]. For instance, in the management responsibilities one should consider whether an information security policy exists and whether the all management staff knows the contents in it. Other areas include whether there is an information-training plan. Also whether there initiative to create security architecture, and whether there is an initiative to create a security plan. The European Union police (Europol) also support member states police departments in exchanging experiences and best practices in the fight against cross-border crimes [11].

The second chapter describes the adaptive information security systems model. Chapter 3 presents the analysis of the crimes. Chapter 4 describes the recommendations. Chapter 5 presents the conclusion.

2. The Adaptive Information Security Systems Model

The adaptive information security systems model was developed to minimize the gap between what we can do with ICT and what we can control with ICT. This is because one of the systemic problems with ICT is that it is a double-edge sword and it could be used for constructive and destructive purposes [12]. The model is based on the Systemic-Holistic approach [4], Immune system [13], the Security by Consensus model [1], and the Socio-Technical system [1] as outlined in Figure 2.

2.1 Critical Sub Systems

The model consists five critical systems the deterrence, prevention, detection, response, and recovery [2]. This is analogous to Millers critical systems in every living system [7]. According to Miller, 19 critical systems must be present in every living system for it to survive in different environments [7]. We believe that there are critical systems that should be present in every model for adaptive information security systems in analog to living systems. We identified the critical systems that should be present in every framework for adaptive information security systems. The critical functions are based on the value-based chain. Kowalski developed the Value-based chain for security [2] from the Value chain model [8]. The Value chain model was first established by Porter to describe the concept of value adding activities in a company [8]. The Value chain model was aimed at maximizing value creation at minimum costs.

2.2 Critical Systems in the Immune System

The value-based chain functions are also present in the immune system. The Immune system consists of three main layers. These include the surface barriers, the innate immune system and the adaptive immune system [16]. The surface barriers are the first line of defence, like firewalls, against infection and include the mechanical (skin), the chemical (enzymes), and the biological (potential hydrogen (pH)) barriers. The surface layer of defence acts as a deterrence and prevention systems. The innate immune system is the second layer of defence. This layer consists of specialized white blood cells that detect and respond to foreign cells. All the cells belonging to a human body are labelled as 'self'. The foreign cells are identified as 'non-self'. The surface of a cell has antigens which tell an immune system if the cell belongs to the body or not [16].

If the cell is a 'non-self', it will be destroyed by the immune system. The third layer of defense is the adaptive immune system. The adaptive immune system has the ability to detect and remember new foreign cells and creates immunity to prepare the body for future challenges. We apply these futures by providing adaptability measures in our model as described in the next section.

2.3 The Architecture

The architecture for implementation consists of the components as outlined in figure 3. The first component is the system manager. This is the only component that has access to all the components. The system manager creates rules, identities, goals, and security policies of operations and monitors the behaviour of all the components in the security framework.

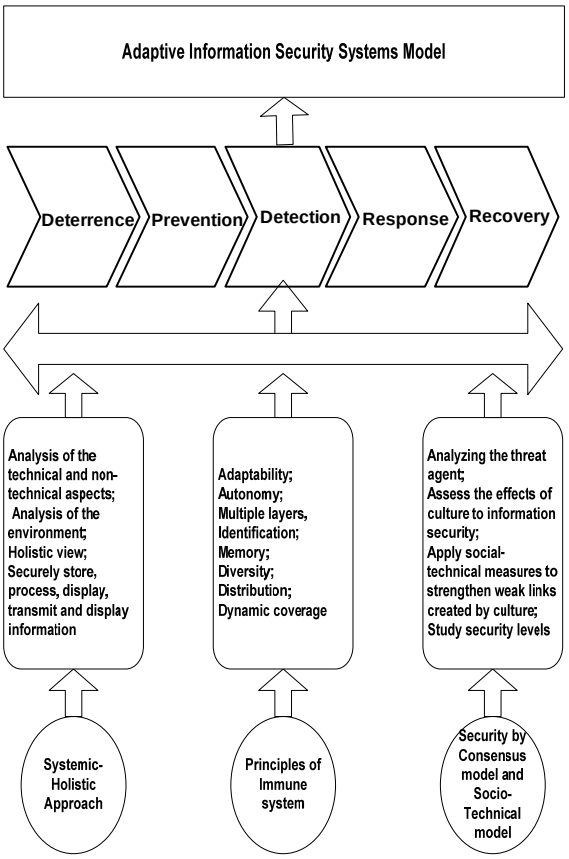

Figure 2: The adaptive information security systems model

The system manager activates the security framework and initializes all the components of the framework. The second component of the architecture is the integrated security system. This component performs identity management and provides security services.

The immune system uses cells to protect the body. The adaptive model uses software agents to provide security services. All components request specialized software agents for providing security services from the software agents' creator. The software agents are generated based on the existing knowledge of adapting principles of the immune system [13] and cybernetic feedback mechanisms [4]. This knowledge is stored in the gene libraries. The DNA combines the genes to form different solutions the way children combine Lego blocks to form different solutions.

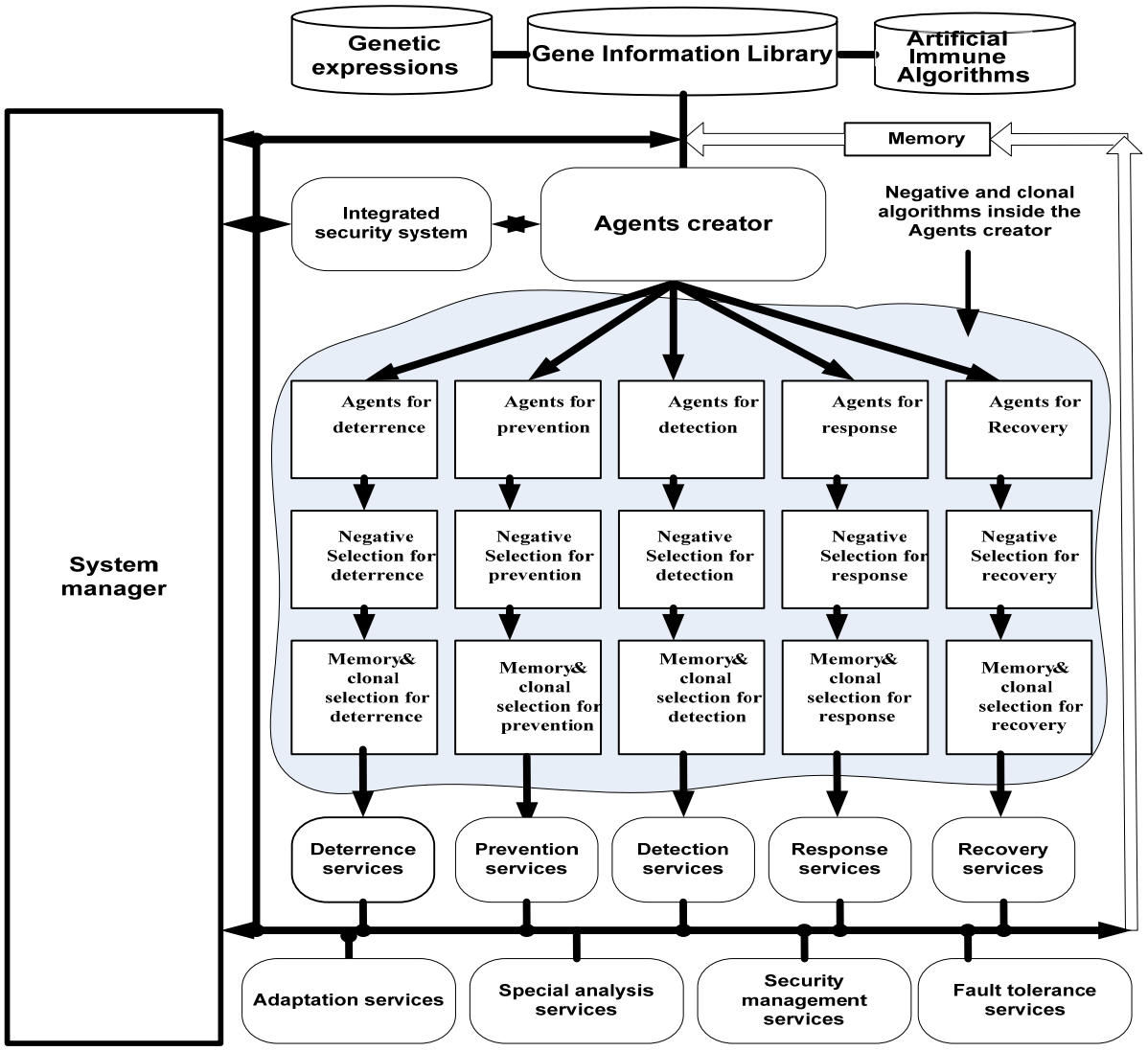

Figure 3: The architecture of the adaptive information security system

The gene libraries provide information for the agents' creator. The bone marrow, in the immune system, contains a gene library and this library is called the DNA [16]. The DNA rearranges the genes to form future B-cells. After the rearrangement of B-cells, they are tested by the negative selection algorithm [16]. If the B-cells pass the test, they will be allowed to monitor in the body.

In our architecture the software agents' creator represents the immune system's bone marrow. The software agents' creator forms software agents by combining genetic expressions using the artificial immune algorithms as outlined in figure 3. The agent creator applies the existing knowledge to form different normal and abnormal profiles for the sub-systems deterrence, detection, prevention, response, and recovery. The agent creator applies the Negative selection algorithm to test the agents [16]. The agents' creator equips software agents with specialized principles for the deterrence, prevention, detection, response, and recovery systems. The software agents that pass the test are trained before released into the real environment. The performance of agents is monitored and recorded. The software agents provide security services to all the components of the architecture. The software agents that perform successfully according to the specified policy are cloned using the clonally selection algorithm [16]. The

agent creator applies these principles to improve the next generation of software agents.

3. Analysis of Cases

We made an autopsy of 41 ICT crime cases [5]. We applied the Socio-Technical system [1] as outlined in Figure 4.

3.1 The Socio-Technical System

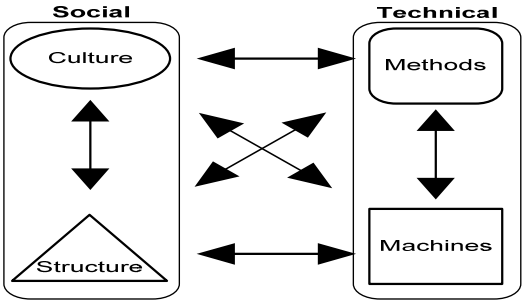

Figure 4: The Socio-Technical System

The Socio-Technical system consists of social and technical parts [1]. The social part consists of culture and structure. Structure refers to the power structure in an organization. People using an information system have culture like ethics, traditions, laws and other social values. The technical part consists of methods and machines. In an IT system the social part can include ethical/cultural, legal/contractual, administrational managerial and operational procedural layers. The Technical part includes the following layers: mechanical/electronic; hardware; operating system; application data, store, process, and collect information. Every system is required to be in balanced state to be able to reach the goals set for the system. When the methods change in a socio-technical system the machines, culture and structure may have to change to sustain the balance [1]. When a new machine is introduced in a company it can lead to changes in procedures, ethical, legal, and administrational issues. In the next section we apply the adaptive information security systems model and the socio-technical systems [1] to analyze the ICT crime cases.

3.2 Analyzing Criminal Cases

We analyzed 41 computer crime cases to see how many systems had deterrence, prevention, detection, response, and recovery measures. In addition, we analyze using the socio-technical system the methods and tools that the hackers applied in attacking the information systems. We present the structure or organization of criminals at the end of the analysis. Out of 41 cases, no system that was attacked had strong deterrence measures to scare away attackers. Seven systems had weak deterrence measures, which could not scare away attackers. 34 systems had no deterrence measures. When it comes to prevention measures, 40 systems had weak prevention measures, which could not prevent attackers. One system had no prevention measures at all. 31 systems had no response measures at all, while 10 systems had weak response measures. As to the recovery, systems 34 systems had no recovery measures while 7 had weak recovery measures. 18 of the cases did weak confidentiality measures. In 31 of the cases authentication, security service was not strong. In ten cases availability security service was weak. In 32 cases, access control was not strong enough. 23 cases had breaches in integrity security service. 9 cases had breaches in privacy security service.

3.2.1Socio-Technical Measures

The Socio-Technical system [1] contains the social and technical parts. Criminals appear to use both social, like social engineering, and technical measures to attack information systems as outlined in table 1. Criminals used social attacking measures in 26.8 % of the crimes. In 31.7% of the crime cases criminals used both social and technical attacking measures. The criminals used technical attacking measures in 41.5 % of the crime cases.

Table 1: The degree of social and technical attacking measures used by criminals

Social attacking measures	Technical attacking measures	Social-technical attacking measures
26.8%	41.5%	31.7%

In Technical part of the Socio-Technical systems, there are methods and machines that the criminal could use to attack ICT systems.

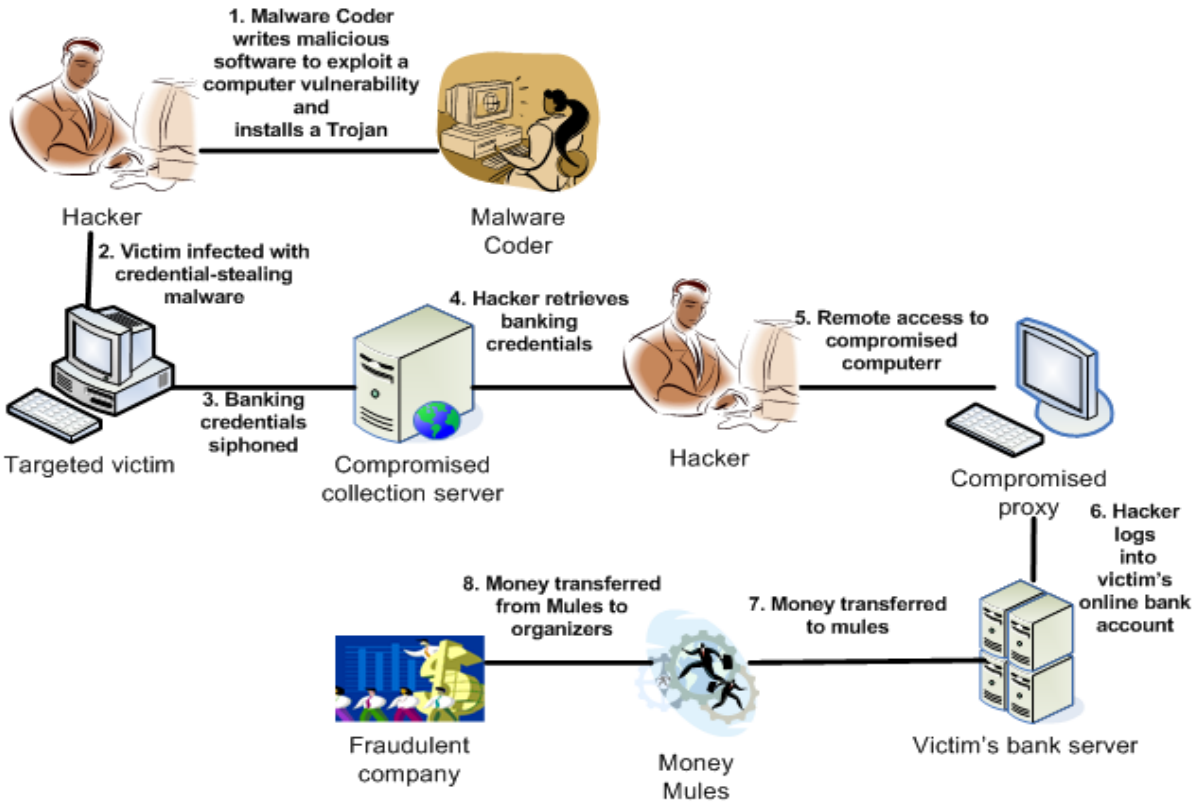

Figure 5: How fraud works [adopted from 6]

The methods that criminals used in the 41 crime cases include stealing credit cards and identities, installing Trojan horses, reconfiguring networks, redirecting traffic, deleting and modifying records. Other methods include impersonation, stealing program codes, diverting salaries, distributed denial of service, SQL injection [21], stealing secrets and formulas from companies and Web defacing. The method of stealing identities and credit card information and selling the information was applied in ten crime cases.

The method of stealing secrets from companies like trade secrets, formulas, and new product designs was used in five crime cases. The method of distributed denial of service was applied in four crimes cases. The SQL injection method used in two of the crime cases. Web defacing method was used by criminals in two crime cases. Another method that used in one of the crime cases was selling the botnet army to other criminals using the state web sites.

As regards machines, it is not easy to understand the exact machines that they used to conduct their criminal activities. However, it appears that they were using powerful computers and fast ubiquitous internet access [19]. The same goes to culture of the criminals they tend to come from different cultural backgrounds. The organizational structure of criminals appears to be as outlined in figure 6.

The first group is of coders who write malicious codes. The second group in the organization consists of keepers of botnet army, which is automated and used to extract information from victims. The next group comprises of researchers who investigate the vulnerabilities in different products and systems [17].

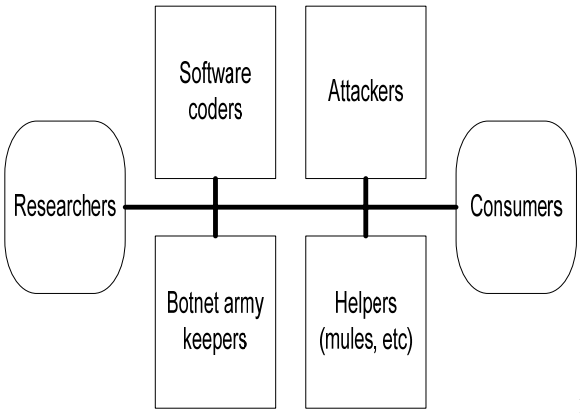

Fig ure 6: Organization of hackers

The next group consists of attackers who hire botnets from the botnet army keepers or use free attacking tools to perform the attacks. The next group is of consumers who

use the stolen information to translate it into money [17]. Then there is a group of helpers, who assist the criminals in performing tasks like transferring money. One example is money mules that created bank accounts using fake documents.

3.2.2 The Cyber Theft Case

In this section, we describe in details the analysis of cyber theft case in which $70 million was stolen [6]. The criminals made surveillance on the different corporations and banks and found out those large corporations and large banks had strong online security. Therefore, the criminals decided to target medium sized companies and even churches. The assistant director of the FBI's cyber division said this kind of crimes was a threat to the financial infrastructures [6]. They caught some of the criminals but it involved much resources and international cooperation. The director said it was not easy because different countries have different culture and cyber laws. It appears that the criminals made surveillance and discovered the weaknesses in the deterrence, prevention, detection, and response security measures in the computer systems involved. If the strong deterrence measures were present, the criminals could not have attempted to steal the money because the risk of being caught would have been too high. We describe the different steps that criminals followed during the crime.

In step 1, figure 5, a malicious coder created a Trojan horse called Zeus [6]. The hackers wrote official looking letters and sent them to small and medium sized companies. One employee of small Michigan company opened the letter and the Trojan captured the banking credentials and within a short time $650 000 had been transferred electronically to bank accounts in Finland, Estonia, Russia, Scotland and USA. In step 2, the hackers installed the Zeus Trojan in victims' computers via e-mail attachments. The method that the hacker used to install the Trojan was social engineering in convincing the victim that the email and the attachment was an official letter from a fellow employee. At this stage, the adaptive model would have prevented the Trojan to run because no program without a special identity, authorization, and registration in the program database would be allowed to run in the computer. There are software agents in the adaptive model that monitor and check the authentication and authorization of every program, which tries to run.

In step 3, the Trojan horse captured bank accounts, passwords, and other credentials for login into financial accounts and stored them in a compromised collection server. The method used here is monitoring and recording the banking credentials. Our adaptive model has agents for monitoring the actions of the programs running on a computer. The adaptive model could have detected the actions of the Trojans. The victim's computer and the collection server lacked deterrence, prevention, detection and response measures both social and technical measures. In step 4, the criminals retrieved banking credentials. In this step, the adaptive model has agents that detect the information that is sent out; the ports used, and check the programs that are sending the information. Here there was no program to detect what was sent out.

In step 5, the criminals remotely accessed the compromised proxy. The compromised proxy lacked deterrence, prevention, and detection, and response measures. The identification, authentication, authorization, confidentiality security services are not working properly in the compromised proxy. Therefore, the hackers were able to compromise and access it, and then used it as a proxy to log to the victim's bank. In step 6, the criminals log into victim's online bank account and transfers money without authorization. The method used is impersonation using the banking credentials that were captured by the Trojan. The bank system lacks strong deterrence, prevention, and detection measures to scare away criminals, or prevent and detect their activities. In addition, the security services authentication, and authorization are not strong to detect the criminals.

In step 7, money was transferred to money mules. The mules create bank accounts using fake documents and phony names. For example, the money from one customer of company called TD Ameritrade landed in a bank account belonging to a fake company called the Venetian Development Construction Service Corp. The mules had registered this fake company an address of an unmarked, building of two stories in Brooklyn [6]. The mules were given about 8 to 10%.

In this step the identification, authentication, authorization, non-repudiation, detection, prevention, and response measures are weak. The systems were supposed to detect fake documents and phony names when creating accounts and they were supposed respond immediately. In addition, when the amounts that were supposed to be withdrawn using ATM cards were raised the banking detection systems were supposed to detect, react, and inform the bank. Money is then wired from mules to criminals or cashed and smuggled out of the country as outlined in figure 5. At the airports, smuggled money prevention and detection services were weak because they did not detect the smugglers.

The criminals in the cyber theft case were also organized as outlined in figure 6. There was a group of coders, who wrote the Trojan called Zeus. Then there was a group of keepers, who maintained the Zeus botnet army. There was a group of researchers [17], which discovered the vulnerabilities in different systems and servers exploited in the cyber theft case.

There was a group consisting of attackers who hired the botnets from the botnet army keepers (or used free). This group had a task to extract bank credentials from victims. In the cyber theft case, the criminals were the consumers who used the stolen information to steal money from victims' bank accounts and transfer the money to accounts that were created by mules. The mules belong to a group of helpers who helped the criminals to transfer stolen money to other countries. The mules created banks accounts using fake documents. The stolen money was transferred from victims' bank accounts to the accounts created by mules. The money was then wired or smuggled to the criminals countries [6].

4. Recommendations to Improve the ICT Security

To be able to prevent crimes we propose to use methods for identifying potential victims. We can identify victims by having a potential detecting model. We have created an adaptive information security systems model, which consists of critical sub systems that should be present in every information system. The critical systems include the deterrence, prevention, detection, response, and recovery sub systems. We made a survey on 60 master students in information security from France, Sweden, Sri Lanka, Libya, USA, Libya, Taiwan, Thailand, Uzbekistan, Spain, Peru, Pakistan, Nepal, Iran, India, Iceland, China, Brazil, Bangladesh, and Serbia Montenegro.

Every master student was to act as a security manager of a company. The security manager was spend 100 000 dollars for information security in the company. Then we made the second survey with international master students in information security from Austria, Bangladesh, China, Greece, Hong Kong, India, Iran, Pakistan, Nigeria, Sweden, Tanzania, and Turkey. The aim of the surveys was to understand whether culture affect the decisions, which users make when deciding, which of the five security value-based chain functions were more important. The results are outlined in figure 7.

The results show that 18.75% of the total security budget would be allocated on deterrence sub system. 24.38% of the total budget would be allocated on the prevention sub system. 23.13% of the total budget would be allocated on the detection sub system. 14% of the total budget was to be allocated on the response sub system. 19.38% of the total budget should be allocated on the recovery sub system. It is interesting to note that all the students from China allocated less than 10% on the prevention, response, and recovery sub systems but allocated around 47 % of the total budget on detection sub system.

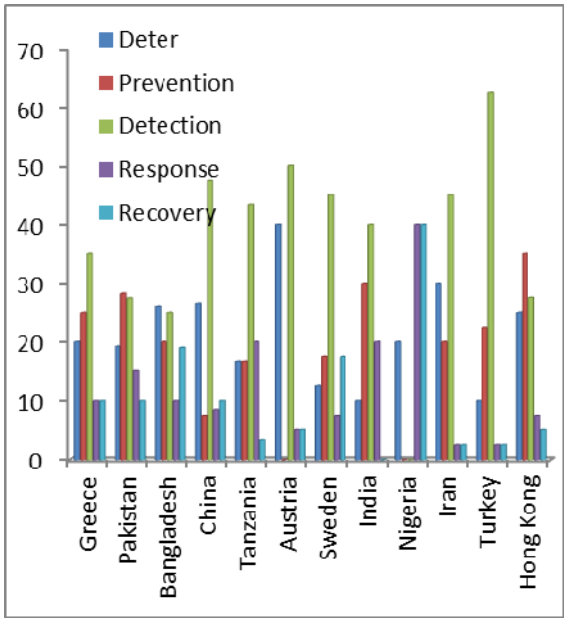

Figure 7: Average allocation of resources on different sub system

Note also that Nigeria allocated nothing on the prevention and detection sub systems. Turkey on other hand spent 62 % of the whole budget on detection sub system. There was an indication that culture of users affects decisions in allocating the security budget.

4.1 Victomological Analysis

Crime prevention theories appear to center on offender-oriented approach [9]. This implies that statics are collected on the categories of offenders, offender's employments, their positions, time taken to do the crime, etc. Steinmetz suggested a victim-oriented approach and proposed a victomological risk-analysis model as outlined in Figure 8 [9]. This model was originally aimed at determining factors related to petty crimes in the Netherlands. Steinmetz suggests that potential victim create opportunities, which the potential offenders seek and can take. There are certain factors that determine a potential victim. One of the factors is the attractiveness like the possession of antiques. In the ICT world, it implies that people who have unsecured computers and IT systems create opportunities for hackers. The other factor is the habits of an individual like certain habits of spending evenings out. The other is the exposure factor. Steinmetz further suggests that there are general influences like economical, social and physical factors influence the opportunities.

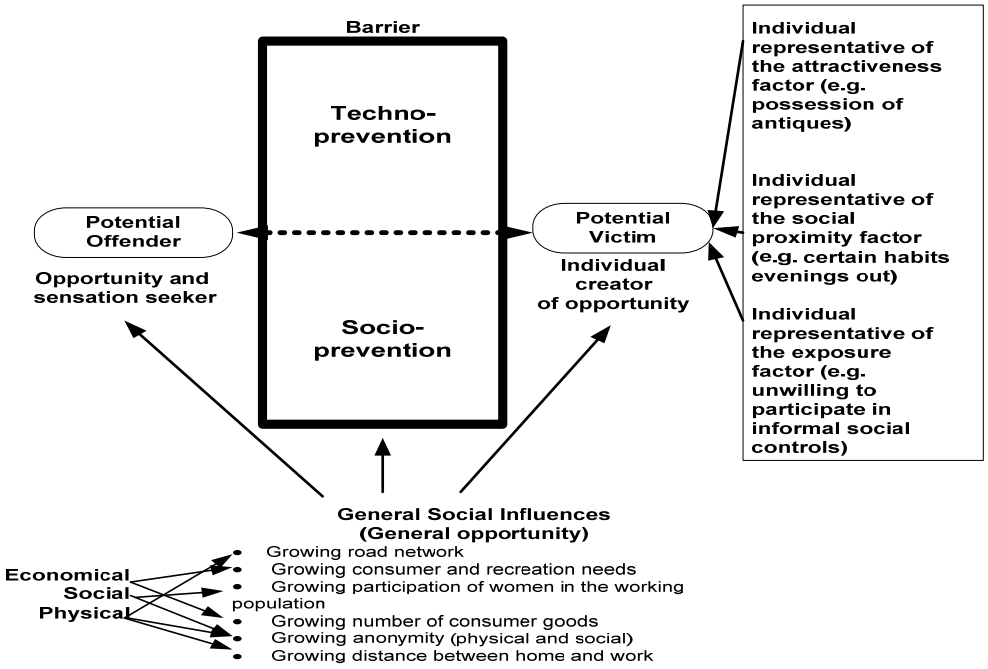

Figure 8: Victomological risk analysis model

Steinmetz proposes three barriers that could be placed between the potential offender and the potential victim. These barriers are the techno-prevention, socio-prevention, and environmental design. Steinmetz proposes techno and socio-prevention between potential victims and potential offenders. In the adaptive information security systems model we apply both socio-technical measures to deter potential hackers. If the deterrence socio-technical measures fail, we apply the socio-technical measures to prevent attacks and intrusions from hackers. If the socio-technical measures for prevention fail, we apply the detection socio-technical measures. When the detection socio-technical measures fail, we apply the response socio-technical measures. If all these socio-technical measures fail then we apply recovery social-technical measures.

In this way, we defend ICT systems using a layered defense in analogy to immune systems. The immune system applies cells to protect bodies in the adaptive information security systems model we apply software agents.

5. Conclusions

We have presented an analysis of 41 ICT crimes. The crimes occurred because of the absence of deterrence socio-technical measures. In addition, the prevention and detection measures were weak which enabled the attacks to take place. In addition, response security measures were lacking or weak, which enabled the ICT criminals to succeed. We recommend that every information system should have the deterrence, prevention, detection, response, and recovery security measures. We also recommend that the security measures should include both social and technical security measures. This is because the hackers use both social and technical measures in attacking or in gathering information before the attacks. The hackers use social engineering to gather information. We also recommend especially to security administrators to detect potential victims by checking whether the deterrence, prevention, detection, response, and recovery security measures are presence and their strength. These functions could act as crime prevention features in ICT products and systems.

References

[1] S. Kowalski, *IT Insecurity: A Multi- disciplinary Inquiry*, Doctoral thesis, Department of Computer Systems Sciences, Stockholm University and Royal Institute of Technology, Stockholm, Sweden, 1994

[2] S. Kowalski & M, Boden, Value Based Risk Analysis: The Key to Successful Commercial Security Target for the Telecom Industry, *2nd Annual International Common Criteria CC Conference* Ottawa 2002

[3] C. Brookson, G. Farrell, J. Mailley, S. Whitehead, and D. Zumerle, "*ICT Product Proofing Against Crime*", ETSI White Paper No. 5, 2007

[4] L. Yngström, *A systemic-Holistic Approach to academic programs in IT Security*, Doctoral thesis, Stockholm

University / Royal Inst. of Technology ISRN SU-KTH/DSV/R--96/21—SE, 1996
[5] United States Department of Justice, Computer Crime & Intellectual Property Section, www.justice.gov/criminal/cybercrime/cccases.html, 2010
[6] Cyber Banking Fraud Global Partnerships Lead to Major Arrests, www.fbi.gov/news/stories/2010/october/cyber-banking-fraud, 2010
[7] J.G. Miller, J. G., *Living Systems*, Great Britain: McGraw Hill, 1978
[8] Porter, M. E. (1985), *Competitive Advantage*, the Free Press, New York, USA
[9] M.P. Stanley, A Methodology for Investigation of Computer Crime, IFIPS/sec, 1992
[10] Bureau of Justice Assistance, 2009 Internet Crime report, Internet Crime complaint center, Bureau of Justice Assistance, US Department of Justice, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf, 2010
[11] S. Leman-Langlois, *Technology, crime and social control*, Willan Publishing, 2008
[12] P. Dalal, Cyber Crime and Cyber terrorism: Preventive defense for cyberspace violations, Cyber crime research center, www.crime-research.org/articles/1873, 2006
[13] S. Forest, S. Hofmeyr & A. Somanaye, Computer Immunology, *Communication of the ACM*, 40 (10), 1997
[14] P. van Soomeren, Crime prevention solutions for Europe: Designing Out Crime, Conference on the relationship between the physical environment and crime reduction and prevention, Szczecin – Poland, 2000
[15] J. Kaneshige, & K. Krishmakumar, Artificial Immune System Approach for air combat Maneuvering. NASA Ames Research Center, Moffett Field, CA, USA 94035, 2007
[16] Kim, J. W. (2002), *Integrating artificial Immune Algorithms for Intrusion Detection*, Doctoral thesis, The Department of Computer Science, University of London
[17] N. Bar-Josef, The Structure of Cybercrime Organization-hackers have Supply Chains Too! Security Week, www.securityweek.com, 2010
[18] Interpol, IT crime – company checklist, http://www.interpol.int/public/technologycrime/crimeprev/companychecklist.asp, 2010
[19] D. J. Paulsen, A Discussion of Technology and those who use it for criminal gain, http://www.criminalbehavior.com/Spring2009/Section%201%20Hackers.pdf, 2009
[20] M. Rogers, *A new hacker Taxonomy*, Department of Psychology University of Manitoba, Winnipeg RSA Security Conference, 2001
[21] Imperva, SQL injection, http://www.imperva.com/resources/glossary/sql_injection.html

Jeffy Mwakalinga received the M. Sc and Licentiate of Technology degrees from the Royal Institute of Technology, Stockholm, Sweden, in 1999 and 2003 respectively. He is currently PhD student at the Department of Computer System Sciences at the Stockholm University and the Royal Institute of Technology. His research interest includes holistic system security, cultural aspects of security, socio-technical security measures, smart card technology, information security architectures, secure mobile agents, and network security. He has published over 17 papers in information security. He has 11 years experience in information security science and technology.

Stewart Kowalski received his Ph D from the Royal Institute of Technology, Stockholm, Sweden in 1994. He has over 25 years of experience with security issues in computer and telecommunication systems. He has both extensive industrial and academic experience. He has worked for a number of major telecommunication players including Ericsson, Huawei, TeliaSonera, HP, and Digital. He has published over 40 papers in the information security area and has taught IT security and information security courses at technical institutions, universities, and business schools. The major focus of his research is applied socio-technical analysis to security in ICT systems. He is currently an associate professor at the Department of Computer and Systems Sciences at Stockholm University.