Austin Journal of Forensic Science and Criminology

Open Access

Austin Publishing Group

Review Article

Cybersecurity: Threats, Challenges and Opportunities

Tanya T[1], Tanuj T[2], Sanjay T[3] and Shikha T[4]*

[1]Samsung India Electronics Pvt.Ltd., Noida

[2]Research Assistant, University of Texas at Dallas, USA

[3]S.O.S. in Electronics & Photonics, Pandit Ravishankar Shukla University, India

[4]State Forensic Science Laboratory Raipur (CG), India

***Corresponding author:** Shikha T, State Forensic Science Laboratory Raipur (CG), India

Received: January 11, 2018; **Accepted:** February 12, 2018; **Published:** March 06, 2018

Abstract

The opportunities and challenges provided by technology continue to evolve with it. Today we are moving from a society already enlaced with the internet to the coming age of the Internet of Things (IoT), automation and Big Data. Cyber Forensics is sizzling topic of the current trends as the Internet has made it easier to perpetrate crimes by providing criminals an avenue for launching attacks with relative anonymity. The increased complexity of the communication and networking infrastructure is making investigation of the cybercrimes difficult. Clues of illegal activities are often buried in large volumes of data that needs to be sifted through in order to detect crimes and collect evidence. Cyber Penetrators have adopted more sophistical tools and tactics that endanger the operations of the global phenomena. These attackers are also using anti-forensic techniques to hide evidence of a cyber crime. Cyber forensics tools must increase its toughness and counteract these advanced persistent threats. The need for computer forensic expertise in law enforcement national security, and information assurance is growing as digital crime increases exponentially. This is a multidisciplinary area that encompasses law, computer science, finance, telecommunications, data analytics, and policing. This paper focuses on foundational concept of cyber forensics, network security issues and current trends in electronic evidence collection.

Keywords: Cyber forensics; Digital evidence; Forensics tools; Cyber crimes

Introduction

According to the FBI's 2015 Internet Crime Report, its Internet Crime Complaint Center (IC3) received 288,012 complaints pertaining to internet-related cybercrimes. The top five complaints concerned business email compromise, confidence fraud, non-payment/non-delivery, and investment fraud and identity theft. These statistics do not include state and local law enforcement agencies, who also receive hundreds of thousands of complaints [1]. Now-a-days as more individuals turn to the interest to help them with tasks that have usually been served by personal service or other traditional means, tasks such as banking, tax filing, shopping and personal communication the Internet as a loci for commerce and communication becomes increasingly critical both to the individual and to the business and industries that serve the individual. As business grows over more dependent on the Internet, the battle to keep corporate networks safe grows more costly. The information ware fare or sneak electric assaults, could easily crash power grids, financial networks, transportation systems and telecommunications among other vital services. A private security company found a malicious program on some 3000 computers that could be remotely activated to launch an attack on a site of choice-a Trojan. Recently, this problem is being exacerbated by the growing emergence of "always-on" connections being made to individual homes and small businesses [2-19]. Deleterious impact on stock market can be created by mapping the IP ranges belonging to the public Internet service providers providing high speed, always-on access and mapping for the NetBIOS ports. As soon as it is mapped, a filtration process starts finding unprotected machines which contain password to personal investment accounts, banking etc., and by the end of mapping period thousands of accounts are discovered which could be exploited. Simultaneously these accounts are used to issue massive sell orders to various brokers and close thousands of bank accounts with money transferred to offshore accounts [20]. According to National Institute of Standards and Technology (NIST), 30-40 new attack tools are posted on the Internet every month.

Cybercrime is the fastest growing area of crime in the world. The demand for cyber security professionals is higher than ever

Cyber Frauds

Cyber- crimes can be categorized as internal or external events. Typically, the largest threat to organizations has been employees and insiders that is why computer crime is often referred to as 'insider' crime. Internal crimes are committed by those with a substantial link to the intended victim. However, with advancement of remote networks, the threat from external source is increasing with a rapid pace. An external event is committed anonymously.

Internal events can generally be contained within the attacked organization as it is easier to determine a motive and, therefore, simpler to identify the offender. However, when the person involved has used intimate knowledge of information technology infrastructure, obtaining digital evidence of the offense is quite difficult.

An external event is hard to predict, yet can often be traced using evidence provided by the organization under attack. Typically, the offender has no motive and is not even connected with the organization, making it fairly straightforward to prove unlawful access to data or systems.

Cyber-crime occurs when information technology is used to commit or conceal an offense. Computer crimes include:

Citation: Tanya T, Tanuj T, Sanjay T and Shikha T. Cybersecurity: Threats, Challenges and Opportunities. Austin J Forensic Sci Criminol. 2018; 5(1): 1076.

Table 1: The most common cyber security technologies and their limitations.

Technology	What is does	Limitation
Firewalls	Control access to and from a network or computer	Some types of firewalls are vulnerable to spoofing. More complex firewalls require more time to pass message traffic through.
Biometrics	Uses human characteristics, such as fingerprints, irises, and voices, to establish the identity to user.	Effectiveness is based on the quality of the devises used. human characteristics change over time and individuals may need to periodically update their I
Smart tokens	Establish identify of users using an integrated circuit chip in a portable device such as a smart card or time synchronized token.	Token can be lost or stolen and hence cannot reliably be bound to specify identify when used in isolation from others methods of authentication.
Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.	Because new types of malicious code are discovered on a regular basis, virus signature updates are required on a regular basis. If not updated, antivirus software will not be able to detect new virus.
Integrity checkers	Monitor alteration to files on a system that are considered critical to the organization.	Does not prevent changes to the files, but can provide a record that changes did occur. Effectiveness depends on the accuracy of the baseline. Cannot always distinguish between authorized and unauthorized changes to the baseline.
Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.	Effectiveness is limited by capture of accurate baseline or normal network or system activity. Technology is prone to false positives and false negatives and is not as effective in protecting against unknown attacks. Cannot prevent attacks from demanding the network or host.
Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.	Effectiveness is limited by accuracy of the intrusion detection component. Technology results in reduced throughput through a network.
Network management	Allow for the control and monitoring of networks, including management of faults, configurations, performance, and security.	Must often work with different vendor specific elements to communicate with its network components.
Scanners	Analyze computers are network for security vulnerabilities.	This technology can identify vulnerabilities but does not have the capability to fix them. Cannot identify unknown vulnerabilities.

- Financial fraud Sabotage of data and/or networks;
- Theft of proprietary information;
- System penetration from the outside and denial of service;
- Unauthorized access by insiders and employee misuse of Internet access privileges;
- Viruses, which are leading cause of unauthorized users gaining access to systems and networks through the Internet [21].

As "first wave" wars were fought for land and "second wave" wars were fought for control over productive capacity, the "third wave" wars are being fought for knowledge. Wars of future would be "net war" and "cyber war". Net war, will be a social- level ideational conflict waged in part through internetted modes of communication. That is net war will be most likely to be a nation- against –nation strategic level conflict.

Network Securities

Companies are spending millions of rupees every year to protect their networks and data from intrusion. This defense- in-depth approach is necessary for companies to prevent unauthorized access to their systems (Table 1).

Cyber Forensic

Cyber forensic is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media and computer peripherals that allow investigators to solve a crime. Cyber forensic adds inspection of transient and other frequently overlooked elements such a contents or state of the memory registers , basic input/output systems , input/output buffers , serial receive buffers, L_2 cache front side and back side system caches, and various system buffers [22]. Cyber forensics focuses on real-time, on-line evidence gathering rather than the traditional off-line computer disc forensic technology.

Two distinct components exist in the emerging field of cyber forensic technology;

First: computer forensics, deals with gathering evidence from computer media seized at the crime scene. It deals mainly with imaging storage media, recovering deleted fields, searching slack and free space and preserving the collected information for court of law. Several computer forensic tools are available to investigators. Computer forensics, therefore, is a leading defense in the corporate world's armory against cyber-crime. Forensic instigations detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanism, and potentially identify the culprit.

The second component, network forensics, is a more technically challenging aspect of cyber forensics. It gathers digital evidence that is distributed across large scale, complex network. Often this evidence is transient in nature and does not preserve within permanent storage media. Network forensic deals primarily with in-depth analysis of computer network intrusion evidence, because current commercial intrusion analysis tools are inadequate to deal with today's networked, distributed environments. Cyber forensic experts should ensure the following steps as:

- No possible evidence is damaged, destroyed, or otherwise compromise by the procedures used to investigate the computer.
- No possible computer virus is introduced to a subject computer during the analysis process.
- Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
- A continuing change of custody is established and maintained.
- Business operations are affected for a limited amount of time, if at all.

- Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and divulged.

Cyber forensic encompasses four key elements

The identification of digital evidence: is the first step in the forensic process. Knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery [23]. Whilst many people think of personal computers as the sole focus of forensic computing, in reality it can extend to any electronic device that is capable of storing information, such as mobile/cellular telephones, electronic organizers (digital diaries) and smart cards. In addition, the computer forensic examiner must be able to identify the type of information stored in a devices and the format in which it is stored so that the appropriate technology can be used to extract it.

The preservation of digital evidence: is a critical element in the forensic process. Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of electronically stored data be carried out in the least intrusive manner. There are circumstances where changes to data are unavoidable, but it is important that the least amount of change occurs. In situation where change is inevitable it is essential that the nature of, and reason for, the change can be explained. Alteration to data that is of evidentiary value must be accounted for a justified. This applies not only to changes made to the data itself, but also includes physical changes that are made to the particular electronic device to facilitate access to the data.

The analysis of digital evidence: the extraction, processing and interpretation of digital data-is generally regarded as the main element of cyber forensics. Once extracted, digital evidence usually requires processing before it can be by people. For example, when the contents of a hard disk drive are imaged, the data contained within the image still requires processing so that it is extracted in a humanly meaningful manner. The processing of the extracted product may occur as a separate step, or it may be integrated with extraction.

The presentation of digital evidence: involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Evidence Collection and Data Seizure

Electronic evidences are very difficult to collect. It has no permanence that conventional evidence has, and it is even more difficult to form into a coherent argument as computer transactions are fast, they can be conducted from any-where, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify criminal. Any paper trail of computer records can be easily modified or destroyed. Still worse, auditing programs may automatically destroy the record when computer transactions are finished with them. Even if details of transactions are restored through analysis; it is very difficult to connect it with a person. Identifying information such as password or PIN does not link the person directly. Therefore with this fast evolving technology following the rules of evidence collection assiduously is very important.

There are five rules of electronic evidence collection [24]. They are:

Admissible: It should be admissible in the court of law;

Authentic: It is must to be able to show that the particular evidence is related with particular incident;

Complete: It's not enough to collect evidence which shows one perspective of the incident. For example it is not only sufficient to show that the attacker was logged in at the time of incident but it is also important to show that who else was logged in at that time, and even if they were logged in at that particular time of incidence, they didn't do it. This is called exculpatory evidence which is quite important in proving a case;

Reliable: Evidence collection and analysis procedures must not cast doubt on the evidences authenticity and veracity;

Believable: The evidence should be clearly understandable and believable by jury. So instead of presenting a binary dump in front of jury it's better to present a formatted and human understandable version that should be able to show the relationship to the original binary.

International Organization on Computer Evidence (IOCE) developed international principles for the standard recovery of computer based evidences. They are:

- Consistency with all legal systems;
- Allowance for the use of common language;
- Durability;
- Ability to cross international boundaries;
- Ability to instill confidence in the integrity of evidence;
- Applicability to all forensic evidence;
- Applicability at every level, including individuals, agency and country;
- Upon seizing digital evidence, action taken should not change that evidence;
- Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles [25].

Conclusion

As information technology and the Internet became more integrated into today's workplaces, organizations must consider the misuse of technology as a real threat and plan for its eventuality. Protecting any organization's information is a big challenge. Organizations are using Intrusion Detection Systems (IDSs) for protection. However, security programs alone will not protect any organization from all incidents, nor will they cover the issues surrounding response to an incident. Fortunately, as computer security field is also progressing at a brisk rate so working with or taking help of cyber forensics will bring new ways of preserving data and insuring protection against the new and unexpected threats. Finally there is need for concentrating on emerging legal, policy and regulatory issues concerning cyberspace and the need for all

stakeholders including lawmakers and judiciary to be more aware about the nuances of emerging cyber technologies.

References

1. Barbara JJ. Digital Forensic Insider: Cybercrime in Perspective. Cybersecurity. 2017.
2. Vacca JR. Elecronic Commerce. Third edition. Charles River Media, 2001.
3. Al-Alawi AI. Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status. Research Journal of Business Management. 2014; 8: 139-156.
4. James JI and Breitinger F. Digital Forensics and Cyber Crime. Springer. 2015.
5. Halboob W, Mahmod R, Udzir N and Abdullah MT. Privacy policies for computer forensics, Computer Fraud & Security. 2015; 8: 9-13.
6. Peterson, Gilbert, Shenoi and Sujeet Eds. Advances in Digital Forensics XIII. Springer. 2017.
7. Fahdi MA, Clarke N, Li F and Furnell S. A suspect-oriented intelligent and automated computer forensic analysis Digital Investing. 2016; 18: 65-76.
8. Baggili I, and Breitinger F. Data sources for advancing cyber forensics: what the social world has to offer. AAAI Spring Symposium. 2015.
9. Beebe N. Digital forensic research: The Good, the Bad and the Unaddressed IFIP International Conference on Digital Forensics. Springer. 2009.
10. Britz MT. Computer Forensics and Cyber Crime: An Introduction Pearson. 3rd.Edition. 2013.
11. Meffert C, Clark D, Baggili I and Breitinger F. Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM. 2017.
12. Zhang X, Baggili I and Breitinger F. Breaking into the vault: privacy, security and forensic analysis of android vault applications. Computers & Security. 2017.
13. Ma G, Wang Z, Zou L and Zhang Q. Computer Forensics Model Based on Evidence Ring and Evidence Chain. Procedia Engineering. 2011. 15: 3663-3667.
14. Scanlon M, Du X and Lillis D. EviPlant: An efficient digital forensic challenge creation, manipulation and distribution solution. Digital Investigation. 2017; 20: S29-S36.
15. Horsman G. Digital forensics: Understanding the development of criminal law in England and Wales on images depicting child sexual abuse. computer law & security review. 2016; 32: 419-432.
16. Sheldon A. Digital Forensics leads the fight against cyber-crime SC Media UK. 2016.
17. Nelson B. Guide to Computer Forensics and Investigations. Boston MA. Thomson Course Technology, 2004.
18. Casey E. Digital Evidence and Computer Crime (Second Edition). Diego S, CA: Academic Press. 2000.
19. Dan F and Venema W. Forensic Discovery. Addison-Wesley Professional, 2005.
20. Vacca JR, Net Privacy: A Guide to Developing and Implementing an Iron-clad ebusiness Privacy Plan. Mcgraw-Hill, 2001.
21. "Computer Forensics: Response vesus Reaction" Ernst and Young Australia, The Ernst and Young Building, 321 Kent Street, Sydney NSW 2000, Australia (Ernst and Ypung LLP, 787 Seventh Avenue, New York, New York, 10019), 2001.
22. WetStone Technologies, Inc, 273 Ringwood Road, Freeville, NY 13068, 2001.
23. Pendyala KS, Cyber frauds, Incident Response and Cyber Forensics, Directorate of Forensic Science, M.H.A.
24. Peter Sommer. Computer Forensics: An Introduction. UK. 2001.
25. US Department of Justice, Federal Bureau of investigations, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington. 2002.

Austin J Forensic Sci Criminol - Volume 5 Issue 1 - 2018
ISSN : 2380-0801 | www.austinpublishinggroup.com

Citation: Tanya T, Tanuj T, Sanjay T and Shikha T. Cybersecurity: Threats, Challenges and Opportunities. Austin J Forensic Sci Criminol. 2018; 5(1): 1076.