On the Novel Network Forensics Perspective of Enhanced E-Business Security

Wei Ren [1,2]

[1] School of Information, Zhongnan University of Economics and Law,
Wuluo Road 114, Wuhan 430064, China
[2] School of Computer, Huazhong University of Science and Technology
renw@public.wh.hb.cn

ABSTRACT

E-business security is crucial to the development of e-business. Due to the complexity and characteristics of e-business security, the current approaches for security focus on preventing the network intrusion or misusing in advanced and seldom concern of the forensics data requiring for the investigation after the network attack or fraud. We discuss the method for resolving the problem of the e-business security from the different side of view - network forensics approaches – from the thinking of the active protection or defense for the e-business security, which can also improve the ability of emergence response and incident investigation for e-business security. It is also for the first time to systematically discuss the network forensics evidence source, network forensics principles, network forensics functions and network forensics techniques.

Keywords: e-business security, network security, digital forensics, network forensics

1. INTRODUCTION

Internet-based business operations offer many benefits, but also bring a broadened range of risks, some of them unprecedented. The actual and perceived lack of system security and reliability are significant deterrents to the rapid growth of the digital economy.

Daily progress is being made in reducing network risks through a variety of software patches, cryptographic algorithms and security tools. These efforts major focus on the prevention of the network intrusion, but always cannot eventually avoid the risk of the network misuse and fraud. We always pay more attention to the passive defensive measures of the e-business system, but ignore the computer evidence acquiring and forensics analysis after the attacks.

Although to some degree the legislation is relative later than the issues of computer and economics crime, once the system is compromised and leads to a large amount of economic lose of the enterprise, to obtain the computer evidence will become more and more important. On the other hand, forensics analysis of the system can also improve the protective and detective ability of network security system. To solve the puzzle of e-business security, we need different approaches to enhance the investigation of the network attack. Network forensics technology can be used for that purpose.

Judd Robbins, a prominent computer forensics investigator, defines computer forensics as “the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.” [1] Other experts, believing computer forensics has evolved into a science, define computer forensic science as “the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.”

The term network forensics is commonly used to describe the task of analyzing information collected on active networks from various intrusion detection, auditing, and monitoring capabilities for the purpose of protection. The monitoring and analysis of data from live systems and networks will become essential to law enforcement as caseloads increase and juridical boundaries blur. [3,4,5,6,7]

In the First Digital Forensic Research Workshop, researches give the definition of Network Forensics, [2] that is: The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.

For the purpose of the network forensics, we always need the toolkits to capture the network traffic fully. There are many toolkits for building network traffic analysis and statistical event records [8,9,10,11,12]. They often use a promiscuous packet interface to pass visible traffic into an internally decision engine which discloses the content of the packets and counting them into statistical data and logging key details into backend disks.

After obtaining the network traffic data, forensics analysis is needed. Data mining techniques can be used for mining stream data or email contents [13,14,15]. Utilizing artificial intelligent approaches to identify

special features [16], IP trace back approaches [17,18] to the attack origin identification and mapping topology approaches for the possible location of the attack origin [19,20,21,22,23,24,25].

Current incident investigation mostly focus on the after attack data analysis. Seldom discuss the active investigative approaches in advance for potential risk and the techniques of the speedup of the emergence response time.

In this paper, we discuss the e-business security from a different point of view. Network forensics system that implement to capture the attacker's behavior and log them for the future analysis and investigation.

The remaining of the paper is organized as follows: First, Section 2 characterizes e-business security issues. Current solutions for implementing e-business security are discussed in Section 3. Section 4 details the discussion of network forensics approaches for e-business security. We give the conclusion and look ahead in Section 5.

2. E-BUSINESS SECURITY ISSUES

2.1 Types of Typical Attacks

There are many types of typical attacks that e-business corporation have to face and consider. The most common types are listed below:

Distributed Denial of Service (DDOS): This type of attack is often used when other protections have provided adequate security to the network. When such protections have denied attackers access, such attackers may resort to denying authorized users access to the network by overloading and hence crippling the network such that its performance significantly degrades or ceases to function altogether.

Viruses: This type of attack is often distributed via email attachment and often infects large numbers of customers and may be created itself replication. Viruses, once activated, may destroy information; provide future improper access to a network.

Data destruction: Improper access is gained and an entity's information is improperly changed or destroyed.

Physical perimeter penetration: It is unauthorized accessing to a user's facility or network.

Password cracking: lists of the most used passwords are tried as a means of unauthorized access to another's network. Numerous cracker, hacker, web sites post lists of the most often used passwords.

Screen emulators: This is where low level access is gained to a network and a screen emulator is placed on the access server that brings up a false screen that emulates the proper login screen. This false screen asks for the users login and password and the brings up a screen that states "login incorrect, please try again." Actually the login was correct and the false screen emulation program has captured another user's correct login and password.

Social engineering: This attack relies on the element of human weakness in protecting access information.

Other attacks that require more sophistication, such as cryptanalysis, man in the middle attacks, Trojan horses, IP hijacking, IP spoofing, sniffing, masquerading, reverse engineering and steganography or covert channels.

2.2 Objectives of e-Business Security

While the list of actual attacking manifestation is long, conceptually, they break down to a few categories. These are spoofing, unauthorized disclosure, unauthorized action, and data alteration. A well-planned information security strategy will address all these areas.

E-business security concerns also fall into four main categories: loss of data integrity; loss of data privacy; loss of service; and loss of control. Responding to these concerns requires an integrated and effective information security policy. In conducting e-business, every organization ought to be able to:

Positively identify or confirm the identity of the party they are dealing with on the other end of the transaction.

Determine that the activities being engaged in by an individual is commensurate with the level of authorization assigned to the individual.

Confirm the action taken by the individual and be able to prove to a third party that the entity did in fact perform the action.

To protect information from being altered either in storage or in transit.

Be certain that only authorized entities have access to information.

Ensure that every component of the e-business infrastructure is available when needed.

Be capable of generating an audit trail for verification of transactions.

Effective information security policy must have the following six objectives: privacy and confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation. If these objectives could be achieved, it would alleviate most of the information security concerns or improve the e-business security circumstance.

3. CURRENT SOLUTIONS FOR E-BUSINESS SECURITY

3.1 Network Level Security

Network level security provides protection against attackers who attempt to deny service to legitimate users by gaining control of machines or resources within a

private network. The most common way to protect private networks that are connected to the Internet from these kinds of attacks is firewall technology. A firewall is located at a network gateway server that protects the resources of a private network from users from other networks. It is a combination of hardware and software used to implement a security policy governing the network traffic between two or more networks. The network firewall is the primary line of defense against external threats to an organization's computer systems, networks, and critical information.

In case an attacker successfully penetrates the firewall, IDS(Intrusion Detection System)can be useful to minimize the risk that any damage can be done to the servers or network. There are two kinds of IDS. One is Host IDS, which deploy on the host or server. The other is Network IDS, which set up in the network and detect the abnormal network traffic.

3.2 System Level Security

System level security is the ability to utilize operating system functions and applications in combination with hardware architecture to help protect against corruption of service and control user access to system resources, such as files, programs, databases and so on. Some technologies to improve system level security: host operating system harden, unsafe processes or services disabled, anti-viruses programs, database system security, data backup and recovery, application security and so on.

3.3 Transaction Level Security

The actual act of completing transactions on the Internet depends on transaction level security. Transaction level security refers to the ability of two entities on the Internet to conduct a transaction privately and with authentication. In assessing e-business security, all the components of a transaction have to be considered: the client, transport channel, servers, operating system, applications and database components. Both the authentication of the component of the transaction is crucial, so it always needs the support of PKI system. This level of security provides a basis to enable the payment for goods and services to occur in privacy. Currently, the leading technologies for implementing transaction security are Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).

3.4 Weakness of Current Solution of e-Business Security

Assuring the availability and security of the network is complex challenge. Historically enterprises employ a patchwork of nonintegrated security products that provide incomplete coverage. There are two weakness of existing solution to the e-business security.

One is individual point of products. Over the past decade, security analysts and network managers have come to rely on a multitude of specialized solutions that address specific points of the network. These include firewall, IDSs, server log files and vulnerability scanners. They are not built into a cooperative or integrated system. Once system is compromised, all products are unfortunately do not present a holistic picture of network activity because their initial purpose is protection but not forensics.

The other weakness is limited sampling. Current products can only capture limited quantity of network traffic. This creates a frustrating guessing puzzle for network managers or incident investigator who must interpret these ambiguous snapshots of the network traffic or attack behavior.

4. NETWORK FORENSICS FOR E-BUSINESS SECURITY

4.1 Network Forensics Evidence Source

Computer evidence must keep the criterion of the traditional evidence, such as confidential, authentication, integration, legitimated. Moreover, it has its own characteristics listed as follows:

Virtual: Computer evidence consists of the computer binary data and files in the computer or devices. They cannot be touched and looked without the processing of computer software.

Multiform: The appearances of the evidence are diversity because they can be stored with different format, such as the words, picture, wave sound and video. Some of them even can be interactive with the computer user. They can be stored in the hard disk, USB disk, compact disk and so on.

Fragile: The computer evidence is easy to destroy by the software or the human interference. It can be deleted, modified and counterfeited by the mistakes of investigators or the premeditation of criminals.

Instant: Some evidence is altered with the time, such as the network traffic packets, process in the host, open ports. They will not replay if investigators do not record them on the disk. The forensics system can record the dynamic data and save them to a safe disk, where other softwares cannot modify the data, so that it will keep the originality and integration of the evidence.

There are four types of data source for the computer evidence.

The data from host or server: It includes the operation system audit trail, system event log, application event log, alert log file, file MAC (Modify/Access/Create) timestamp, recovery data, system time, file slack, erased files, swap files, memory contents, program files. It is the traditional computer forensics data.

The data from network: It is the network traffic data packets. Because the network becomes more and more frequent channel to launch attacks, the data of the traffic

becomes also more and more important to forensics analysis. Especially for the network forensics system, the traffic is a key data source. However, the traffic data always has large volume, therefore the efficiency of dumping data is the major issue of the network forensics system.

The data from other security products: It includes firewall log, IDS log, access control system, router, network interface, PDA and so on. The data on these systems give some digest information of the intrusion and misuse.

The data from Internet: For the Internet forensics, the data from Internet can give some basic information for investigation, such as the personal data from the personal website or search engine, the content of chat room.

4.2 Network Forensics Principles

The evidence obtained after the network forensics process must the keep the legal validity, so some principles must be satisfied in the network forensics procedure.

To keep the originality of the data: The analysis is not directly on the processing of the original data, but on the base of image mirror copy of the original data. The copy is a way of bit-to-bit copy and is the exactly copy of the original data. All the forensics analysis process on the copy version of data will keep the integration of original data and make the replay of analysis procedure possible.

To keep the result believable: It means the forensics software and hardware is safe and believable. The software to capture data, analysis data, process data, and display finial evidence must be the authority software or satisfy the standard of the forensics procedure. Before the forensics standard becomes uniform and certificated software are available, the open source software may be a temporary way with believable.

To keep the procedure believable: Very step of processing action must keep the integration of the analysis data. The data signature or data digest approaches can be utilized for this purpose. Read-only property of files is not always believable because even read-only compact disks may also have data changes on special conditions.

To keep the integration in transportation: If the data need to be transported, the integration and confidentiality of the data must satisfy. Data signature also can be used in this occasion.

Documentation and monitoring: The whole procedure of the forensics must documentation, including the time, location, operator name, approaches, techniques, operations steps, processing results and so on. The procedure must be in the monitor of the third party or authority organization, and they must give the signature on the document of the result.

4.3 Network Forensics Functions

(1) Network investigating

Before the enough evidence is available, some investigation can be provided by the network forensics system. Search engineering tools is the fundamental program in the network forensics system suite or integrated into the system. Browser tools, ftp tools, email tools and other Internet tools are also needed.

(2) Network surveying

Some network survey tools are also included. The first is footprinting tools, such as whois, nslookup, traceroute. The second is scanning tools, such as nmap, Hping2, which can be added into the network forensics package or customized development. The third is enumeration tools used for netbios enumeration, snmp enumeration and active directory enumeration.

(3) Network traffic recording

Network traffic is fully dumped by the network forensics system, which can also filter the traffic according to the rules. Rules can be customized for different purpose.

(4) Data aggregation

Logging data from different location give different feedback of the attacking behavior. The analysis of the aggregation of the data sets, which are from multiple sources, such as firewalls, IDSes and sniffers, can build the chain of the clues and display the full scene of the crime. Network forensics system can aggregation the data and transform the data into a uniform data file or database.

(5) Future attacking pattern predicting

The hacker group always haves some features, such as the types of attacking tools, the frequently utilizing techniques, their often steps and trace routes for intrusion. Therefore the network forensics system can use data mining approaches to discover the potential pattern of attacks and provide the function of predication.

(6) Anomaly pattern discovering

The log data in the forensics system can be mined for the anomaly pattern, which will also give a feedback to influence the setting of firewall rules and intrusion detective signatures.

4.4 Network Forensics Techniques

(1) Mapping topology

Building the topology database and IP location Mapping topology of the network may help to find fraud proxy server, ARP spoofing, or quicken the location of the attack origin.

(2) Honeypot/honeynet learning and collecting

Using the honeypot system and network forensics analysis, we can build a database to profile the blackhat, person or organization, such as the name, nickname, email address, home address, nationality, age and so on. We can store the IP address, blackhat techniques, tactics, motives and psychology in the database. We can use dig

tools to profile the main IP node domain name, topology of network or the location of the hackers. The data in the database can be update automatically and also keep the current data and old data for the future timeline analysis.

(3) TCP session replaying

To analysis the attack behavior by replay the attacking procedure. In the captured network traffic, unrelated packets appear in the order they were transmitted over the wire. Network forensics tools can reorganize the packets into individual transport-layer connections between machines. To reassemble the connections, more forensic details emerge.

(4) Protocol parsing

Protocol parsing and analysis is the major work of network forensics analysis. In the analysis, the POP3, HTTP, FTP and telnet protocols need to be paid more attention.

(5) Covert channel discovering

After the protocol parsing, we need to find the covert channel or data hiding in the traffic. Some attacker use steganography in the communication, it add the burden of the investigation.

(6) Potential pattern recognizing

Some artificial intelligence approaches can be used to forensics analysis. Two types of machine learning approaches can be built into network forensic systems: Artificial Neural Networks and Support Vector Machines. Since the ability to identify the important inputs and redundant inputs of a classifier leads directly to reduced size, faster training and possibly more accurate results, it is critical to be able to identify the important.

(7) Forensics data stream mining

We can also use some data mining approaches to network forensics analysis. Data mining generally refers to the process of extracting models from large stores of data. We choose several types of algorithms in our research: Classification, maps a data item into one of several predefined categories; Link analysis, determines relations between fields in the database. Finding out the correlations in forensics data will provide insight for discovering attack behavior quickly; Sequence analysis, models sequential patterns. These algorithms can help us understand the sequence of forensics events. These frequent event patterns are important elements of the behavior profile of a user or program.

(8) IP trace back to the attack origin

In the investigation we can use some methods to trace a steady stream of anonymous Internet packets back towards their source. These methods do not rely on knowledge or cooperation from intervening ISPs along the path. Sometimes tracing an attacking stream requires only a few minutes once the system is set up for a victim.

(9) Remote OS fingerprinting

Remote OS fingerprinting is always a technique on footprinting. It can obtain the general OS type of the target host. This is useful to estimate the experience level and the possible attack tools of the investigate object. The result also can as a digital evidence for the future forensics.

(10) Remote network forensics

Remote network forensics is a program to capture the network traffic on the remote host. Always it is employed on the local area network forcedly or some key traffic center for capturing fully traffic that is used for the future forensics analysis.

5. CONCLUSION

Network forensics approaches for the e-business security can trace the behavior of the fraud in the e-business, discover the potential risk through the analysis the detail forensics data, quicken the speed of emergence response, enhance the ability of the rapid incident investigation, providing the evidence for the future legal action. The future work is the improvement of the dump performance of the network traffic in the network, development of more mining tools for the analysis of the forensics data.

ACKNOWLEDGEMENT

Thanks go to Dr. Jin Hai for his insightful discussion of the project and paper. We also thank the security team of the Cluster and Grid Computing Lab in School of Computer, Huazhong University of Science and Technology.

REFERENCES

[1] Osles, L. “Computer forensics: The key to solving the crime”, 2001.

[2] Gary, P. (2001) “A Road Map for Digital Forensic Research”, Technical Report DTRT0010-01, DFRWS, November 2001.

[3] Corey, V.; Peterman, C.; Shearin, S.; Greenberg, M.S.; Van Bokkelen, J.; “Network forensics analysis”,Internet Computing, IEEE , Volume: 6 Issue: 6 , Nov.-Dec. 2002 Page(s): 60 –66

[4] Brian Carrier. “Defining Digital Forensics Examination and Analysis Tools”. In Digital Research Workshop II, 2002

[5] Mark Reith, Clint Carr, Gregg Gunsch, “An Examination of Digital Forensic Models”,International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3

[6] J.Tan. “Forensic Readiness”. In The CanSecWest Computer Security Conference,April 2001.

[7] Yanet Manzano and Alec Yasinsac, “Policies to Enhance Computer and Network Forensics”, The 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, at the United States Military Academy, June 2001

[8] Giovanni Vigna Andrew Mitchell , “Mnemosyne: Designing and Implementing Network Short-Term Memory”,

[9] S. Ioannidis, K. G. Anagnostakis, J. Ioannidis, and A. D. Keromytis. “xPF: packet filtering for lowcost

network monitoring". In Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR), pages 121--126, May 2002.

[10] S. McCanne and V. Jacobson. The BSD packet filter: A new architecture for user-level packet capture. In Proc. of the USENIX Technical Conf., Winter 1993

[11] K. G. Anagnostakis, S. Ioannidis, S. Miltchev, and J. M. Smith. Practical network applications on a lightweight active management environment, In Proceedings of the 3rd International Working Conference on Active Networks (IWAN), pages 101-- 115, October 2001.

[12] Fulvio Risso, Loris Degioanni, An Architecture for High Performance Network Analysis, Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC 2001), Hammamet, Tunisia, July 2001.

[13] O. de Vel. "Mining e-mail authorship"In Proc. Workshop on Text Mining, ACM Discovery and Data Mining (KDD'2000).

[14] W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium, 1998.

[15] W. Lee, S. J. Stolfo, and K. W. Mok. Mining in a data-flow environment: Experience in network intrusion detection. In Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD-99), August 1999.

[16] Srinivas Mukkamala1 & Andrew H. Sung, "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques", International Journal of Digital Evidence., Volume 1, Issue 4, Winter 2003.

[17] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. "Practical network support for ip traceback", In Proceedings of the 2000 ACM SIGCOMM Conference, August 2000, An early version of the paper appeared as techreport UW-CSE-00-02-01

[18] Hal Burch and Bill Cheswick. "Tracing anonymous packets to their approximate source". In Proceedings of the USENIX Large Installation Systems Administration Conference, pages 319--327, New Orleans, USA, Decemeber 2000. USENIX.

[19] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger. "Network topology generators: Degree-based vs structural", In ACM SIGCOMM, August 2002.

[20] Bill Cheswick, Hal Burch, Steve Branigan, "Mapping and Visualizing the Internet" ,USENIX Annual Conference, General Session - June 2000,

[21] D. Magoni and J.J. Pansiot. "Analysis of the autonomous system network topology", ACM SIGCOMM Computer Communication Review, pages 26--37, July 2001.

[22] Ramesh Govindan and Hongsuda Tangmunarunkit. "Heuristics for Internet Map Discovery", In Proceedings of the 2000 IEEE INFOCOM Conference, Tel Aviv, Israel, March 2000.

[23] A. Lakhina, J. Byers, M. Crovella, and I. Matta, "On the Geographic Location of Internet Resources", Technical Report BUCS-TR-2002-015, Boston University, 2002.

[24] C. Jin, Q. Chen, and S. Jamin. Inet: Internet Topology Generator. Technical Report Research Report CSE-TR-433-00, University of Michigan at Ann Arbor, 2000.

[25] A. Medina, A. Lakhina, I. Matta, and J. Byers. BRITE: An Approach to Universal Topology Generation. In Proceedings of IEEE MASCOTS'01 August 2001..