On Enhanced e-Government Security - Network Forensics

Ren Wei [1,2]

Contents

Abstract

E-Government security is crucial to the development of e-government. Due to the complexity and characteristics of e-government security, the viable current approaches for security focus on preventing the network intrusion or misusing in advanced and seldom concern of the forensics data attaining for the investigation after the network attack or fraud. We discuss the method for resolving the problem of the e-government security from the different side of view - network forensics approaches ? from the thinking of the active protection or defense for the e-government security, which can also improve the ability of emergence response and incident investigation for e-government security.

1. Cluster and Grid Computing Lab, School of Computer, Huazhong University of Science and Technology, 430074, Wuhan, P.R.China
2. School of Information, ZhongNan University of Economics and Law, 430064, Wuhan, P.R.China, renw@public.wh.hb.cn

I . Introduction

While 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 and totally avoid the risk of the network misuse and fraud. To solve the puzzle, we need different approaches to enhance the investigation of the network attack. Network forensics technology can be used for that purpose.

Network forensics is a new science and technology, which is a special part of computer forensics. 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 has been used frequently for some time. Although no official definition exists, the term 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 [13,14,15,16]. Utilizing artificial intelligent approaches to identify special features [17], IP trace back approaches [18,19] to the attack origin identification and mapping topology approaches for the possible location of the attack origin [20,21,22,23,24,25,26].

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-government 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-government security issues. Current solutions for implementing e-government security are discussed in Section 3. Section 4 details the discussion of network forensics approaches for e-government security. We give the conclusion and look ahead in Section 5.

Ⅱ. E-Government Security Issues

2.1 Types of Typical Attacks

There are many types of typical attacks that e-government corporation have to face and consider. The most common 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 are: 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-Government Security

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

What are the goals of information security and what is the nature of the e-government security problem? E-government security concerns 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-government, 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-government 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-government security circumstance.

Ⅲ. Current Solutions for e-Government 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 with 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, application security and so on.

3.3 Weakness of Current Solution of e-Government Security

Assuring the availability and security of the network is complex challenge, historically requiring enterprises to employ a patchwork of nonintegrated security products that provide incomplete coverage. The weakness of existing solution to the e-government security include:

Many individual point 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 where security can be compromised. These include IDSs and firewalls at the perimeter, server log files and vulnerability scanners, but all useful products t unfortunately do not present a holistic picture of network activity.

Sampling limitations: Products that do

sample packets traveling over the network can only capture and extremely limited quantity. This creates a frustrating guessing game for network managers who must interpret these ambiguous snapshots of the network traffic or attack behavior, leading to false positives and false negative that can jeopardize mission-critical network operations.

IV. Network Forensics System for e-Government Security

4.1 Network Forensics Analysis Tools

To achieve the enhancement of the e-government security and computer business crime investigation, NFAT(Network Forensics Analysis Tools) can be employed in network. NFATs are products that always combine the ability to passively monitor and capture all network traffic, use forensics tools to analyze traffic, track down security violations and protect against future attacks. Network forensics analysis tools can give functions as follows: Detection of employee misuse/abuse of company networks and/or computing resources; Risk assessments; Network forensics and security investigations; Exploit (break-in) attempt detection; Data aggregation from multiple sources, including firewalls, IDSes and sniffers; Incident recovery; Prediction of future attack targets; Anomaly detection; Network traffic recording and analysis. (King, N. 2002)

As an essential complement to existing security systems, an NFAT must perform three tasks well: capture network traffic; analyze the traffic according to the user' s needs; let system users discover useful and interesting things about the analyzed traffic.

4.2 Network Forensics Analysis

Forensics data analysis can be employ after attacking or on attacking. 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.

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.

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

Some artificial intelligence approaches can be used to forensics analysis. We use two types of learning machines to build network forensic systems: Artificial Neural Networks or ANNs and Support Vector Machines or SVMs. 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

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.

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.

Using the honeypot system and network forensics analysis, we can build a database to profile the blackhat, person or organization. We 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.

Email is an important evidence for the computer crime, so email content mining can find the trace of the fraud. Other techniques can also used to discover the forensics, which always need the experts to involve, such as chat room wandering, instant message logging, newsgroup checking and so on.

4.3 Function of Network Forensics System

(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 need to 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 attack mode predicting

The hacker group always haves some features, such as the types of attacking tools, the frequently utilizing techniques, the often stepping traces for intrusion.Therefore the network forensics system can provide the function of analysis and predication.

(6) Anomaly pattern discovering

The log data in the forensics system can be mined for the anomaly pattern, which will also influence the firewall rule set and intrusion detection matching pattern.

4.4 Techniques Perspective of Network Forensics

(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 hinding 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. We use two types of learning machines to build network forensic systems: Artificial Neural Networks or ANNs and Support Vector Machines or SVMs. 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.

V. Conclusion

Network forensics approaches for the e-government security can trace the behavior of the fraud in the e-government, 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 backbone network, development of more mining tools for the analysis of the forensics data.

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. Mining E-mail Authorship Olivier de Vel,http://www.cs.cmu.edu/~dunja/KDDpapers/DeVel_TM.pdf

14. Kulesh Shanmugasundaram, November,10,2001,"Data Mining for Security Applications", http://isis.poly.edu/kulesh/ forensics/docs/ miningsec.pdf

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

16. 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.

17. Srinivas Mukkamalal & 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.

18. 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 tech report UW-CSE-00-02-01

19. 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.

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

21. Bill Cheswick, Hal Burch, Steve Branigan, "Mapping and Visualizing

the Internet" ,USENIX Annual Conference, General Session - June 2000,

22. D. Magoni and J.J. Pansiot. "Analysis of the autonomous system network topology", ACM SIGCOMM Computer Communication Review, pages 26-37, July 2001.
23. Ramesh Govindan and Hongsuda Tangmunarunkit. "Heuristics for Internet Map Discovery" , In Proceedings of the 2000 IEEE INFOCOM Conference, Tel Aviv, Israel, March 2000.
24. 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.
25. 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.
26. A. Medina, A. Lakhina, I. Matta, and J. Byers. BRITE: An Approach to Universal Topology Generation. In Proceedings of IEEE MASCOTS '01, August 2001.