On A Network Forensics Model For Information Security

Ren Wei
School of Information,
Zhongnan University of Economics and Law, Wuhan, 430064
renw@public.wh.hb.cn

Abstract: The employment of a patchwork of nonintegrated security products can only provide incomplete coverage, which cannot give the total panorama of the network misuse behavior. Network forensics is a new approach for the incident investigation and emergence response, which also enhance the network security from a different point of view. However, the current network forensics system is confused with the network monitor system or sniffer system. It always is misconstrued to an only network traffic capture system. In this paper, we for the first time discuss the concept model of network forensics system, which can give guidance for the implementation of network forensics system and the formalization of the network forensics procedure, which is a principle element of the recognition between the law enforcement participation. Particularly, some novel approaches for network forensics system are discussed for the first time, such as network forensics server, network forensics protocol and standardization, and so on.

Keywords: network, computer forensics, network forensics, network security, incident investigation, information security

1 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 dilemma, 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. Some researchers define computer forensics as the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. 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. [Ga01, Co02, Br02]

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. [Io02, FL01, MJ93] After obtaining the network traffic data, forensics analysis is needed. Data mining techniques can be used for mining stream data or email contents [LS98, LSM99]. Utilizing artificial intelligent approaches to identify special features [SA03], IP trace back approaches [St00, HB00] to the attack origin identification and mapping topology approaches for the possible location of the attack origin [Ta02, MP01].

In this paper, we at first time discuss the concept model of network forensics system, which can guide the implementation of the network forensics system and form a standard procedure to speedup the investigation of the incident and improve the ability of emergence response. The goal of the concept model is the formalization of the network forensics procedure, which can lead to the recognition of the effectiveness and integration of the forensics data. Particularly, some novel approaches for network forensics system are discussed for the first time, such as network forensics server, network forensics protocol and standardization, and so on.

The remaining of the paper is organized as follows: First, overview of network forensics system is discussed in Section 2. Section 3 details the concept model of network forensics system. We give the conclusion and look ahead in Section 4.

2 Network Forensics System for Information Security

2.1 Weakness of Current Solution

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 is firewall technology and Intrusion Detection System. Assuring the availability and security of the network is complex challenge. Historically enterprises employ a patchwork of nonintegrated security products that provide incomplete coverage. The weakness of existing solution includes individual points of protection and sampling limitations.

2.2 Overview of Network Forensics System

To achieve the enhancement of the network security and computer crime investigation, network forensics system can be employed in network. They 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: Network forensics and security investigations; Data aggregation from multiple sources; Prediction of future attack targets; Anomaly detection; Network traffic recording and analysis. Essentially an network forensics system 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.

3 The Conceptual Model of Network Forensics System

3.1 Principle Perspective

(1) Standardization
Because of the specialty of digital forensics, the effectiveness of the evidence must be satisfied. Therefore the major computer software arithmetic, such as the encryption, signature, need keep the same.
(2) Uniformity
The major forensics tools and the basic operation procedure should be kept the same, which includes the forensics program, basic data store media and operation flow.
(3) Protocol
Different parts of the law enforcement should negotiate about the protocol and finally can accept the result of the every step during the procedure of the forensics.

3.2 Function Perspective

(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.
(4) Future attack mode predicting
The hacker group always haves some features, such as the types of attacking tools, the frequently utilizing techniques and the frequently stepping traces for intrusion. Therefore the network forensics system can provide the function of analysis and predication.
(5) 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 pattern.

3.3 Architecture Perspective

(1) Network forensics server
Forensics data can be stored in the server, which deployed in the distributed network forensics or remote network forensics. The most important function of network forensics server is for the trace back to the malicious origin.
(2) Network forensics client agent
Agents are deployed on the key point of the network and capture network traffic and convert into local database or upload the index of data to the network forensics server.

3.4 Data Objective Perspective

(1) Digest Data
One type of network forensics system processes digest data. Logging system is digest data, it is consists of host system logging, firewall logging, IDS logging and alert. This type of data often is used to discover the malicious behavior.
(2) Full Data
Network traffic packets capture data by network forensics system. The network traffic data is fully captured, so the whole procedures of the attack are recorded. These data often are used to reconstruct the attacking behavior.

3.5 Time Perspective

(1) Potential Time
The attack may start up a new sequence of abuse behavior in the future; some clues can be obtained by the forensics system through the network and keep the preparation.
(2) Behavior Time
Misuse behavior is on hand, then network forensics system can peer the procedure and record the full behavior.
(3) Bequeathal Time
A part of network forensics system is used for the forensics data analysis when they work on the bequeathal time. The attack is end and the trace data is left on the log system.

3.6 Techniques Perspective

(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 and network survey

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.

4 Conclusion

Network forensics system can trace the behavior of the network abuse, discover the potential risk through the analysis the detail forensics data, quicken the speed of emergence response, enhance the ability of the incident investigation, providing the evidence for the future legal action. The concept model of network forensics system will give the guide to implementation of a network forensics system, which is also pursue the formalization of the network forensics procedure, which can lead to the recognition of the effectiveness and integration of the forensics data between the law enforcement participation. The future work is the improvement of the distinguishing features of the model and its guidance function for the system implementation.

References

[Br02] Brian C.: Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II, 2002

[Co02] Corey, V. et. al.: Network forensics analysis ,Internet Computing, IEEE , Volume: 6 Issue: 6 , 2002 pp: 60 –66

[FL01] Fulvio R, Loris D, An Architecture for High Performance Network Analysis, Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC 2001), Hammamet, Tunisia, 2001.

[Ga01] Gary, P.: A Road Map for Digital Forensic Research, Technical Report DTRT0010-01, DFRWS, 2001.

[HB00] Hal, B.; Bill, C.: Tracing anonymous packets to their approximate source, In Proceedings of the USENIX Large Installation Systems Administration Conference, New Orleans, USA, 2000. pp 319--327.

[Io02] Ioannidis, S. et. al.: xPF: packet filtering for lowcost network monitoring. In Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR), 2002.pp121--126

[LS98] Lee W., Stolfo S. J.: Data mining approaches for intrusion detection, In Proceedings of the 7th USENIX Security Symposium, 1998.

[LSM99] Lee W., Stolfo S. J., Mok K. W.: Mining in a data-flow environment: Experience in network intrusion detection, In Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 1999.

[MJ93] McCanne S., Jacobson V.: The BSD packet filter: A new architecture for user-level packet capture. In Proc. of the USENIX Technical Conf., 1993

[MP01] Magoni D., Pansiot J.J.: Analysis of the autonomous system network topology, ACM SIGCOMM Computer Communication Review, 2001, pp26--37.

[SA03] Srinivas M. & Andrew H. S.: Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques, International Journal of Digital Evidence, Volume 1, Issue 4, 2003.

[St00] Stefan S. et. al.: Practical network support for ip traceback, In Proceedings of the 2000 ACM SIGCOMM Conference, 2000.

[Ta02] Tangmunarunkit, H. et. al. : Network topology generators: Degree-based vs structural, In ACM SIGCOMM, 2002.