Design and implementation of an event correlation model in a network security linkage system

Sizu Hou[1*], Xiaorong Cheng[2]

[1]*Department of Electronic & Communication Engineering, North China Electric Power University, Baoding 071000, China*

[2]*Department of Computer Science, North China Electric Power University, Baoding 071000, China*

Received 1 October 2014, www.cmnt.lv

Abstract

Based on the shortcomings of poor compatibility, weak practicality, and low accuracy in current linkage systems, this paper designed a gradation of event correlation model with real-time response mechanism. It will be analyzing technology in data mining association rules is introduced to analyse the processing of security incidents. Then the system through the analysis of a large number of real-time data collecting all kinds of security devices found hidden in the data and related information to improve detection precision and safety accident treatment work. At last, apply this model into the system, to demonstrate the effectiveness of the model and priority.

Keywords: linkage system, event correlation model, correlation rule, security event

1 Introduction

With the rapid development of the Internet and the widespread use of e-commerce, the importance of computer communication networks in all aspects of society is increasing; computer and Internet technologies are changing the face of society. Security and reliability issues [1, 2] have become the main problems facing network security operations. To ensure that critical network information is always complete and confidential, to protect against attacks from external and internal networks, security products, such as firewalls [3], intrusion prevention systems [4], antivirus systems for all aspects of internal and external networking were developed. On the one hand, they guarantee the safety of system, on the other hand they generate many security events. These events are multifaceted in nature, vary considerably, take different formats, are sometimes false alarms, or are not be able to be used fully.

How to effectively manage all kinds of heterogeneous security devices, extract important information from massive information sets (and do so timeously), forecast system attacks that may occur accurately and efficiently, has become the urgent problem facing network security linkage systems.

By associating various security events, an event correlation [5] model matches security events with other of the same type, large quantities, different formats, and false alarms mixed with genuine cases, can not only be greatly reduced in number, and unified in format, improved in readability, and ultimately produce more real event reports, but also allow a system administrator to discover intrusive behaviours timeously and take effective measures to reduce loss.

2 Design of the event correlation model

2.1 OVERALL DESIGN OF THE MODEL

The overall structure of the event correlation model is shown in Figure 1.

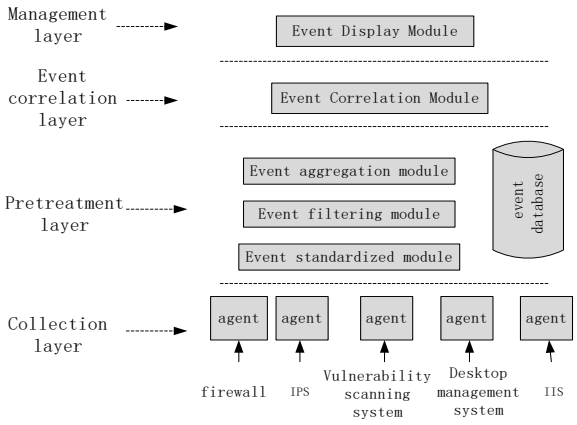


FIGURE 1 Structure of the event correlation model

The basic composition of the event correlation model included: a security event information collection module, an event standardised module, an event filtering module, an event aggregation module, an event correlation module, an event display module, and a security event database. The entire model was divided into four levels: the event collection layer, the pre-treatment layer, the event correlation layer, and the event management layer.

The lowermost layer was the collection layer, which comprised various types of information collection agent. These agents can run on a variety of operating systems and

[*]***Corresponding author*** e-mail: 867038858@qq.com

are responsible for collecting all kinds of security event information, such as IDS alarm logs, firewall logs, host logs, vulnerability information, *etc*., from different security devices.

The event pre-treatment layer included the event standardised module, event filtering module, event aggregation module, and the event database. The event standardised module unified the format of the information collected for subsequent processing. The event filtering and event aggregation modules were used to remove useless information for data mining, reducing the number of original data items. The security event database was mainly used to store all kinds of security event information produced by pre-treatment.

The event correlation layer was to uncover specific, potentially threatening, security event information through associating/matching events: this was a core part of the network security event correlation system and a critical section of the system.

The uppermost layer was the management layer, which was responsible for displaying security events, so that administrators can query, delete, or browse current network conditions.

2.2 DESIGN OF EACH MODULE IN THE MODEL

In this section, the design of the function of each module is considered at four levels, and the corresponding implementation method is introduced.

2.2.1 Event collection layer

This layer was mainly used to collect event information generated by various types of safety equipment. Here Agent is used to collect information. Agent can be installed on all kinds of safety equipment or on the router in the network where the devices sit. Agent can fully capture event information generated by the security equipment which it has been monitoring. The flowchart through the event collection layer is shown in Figure 2.

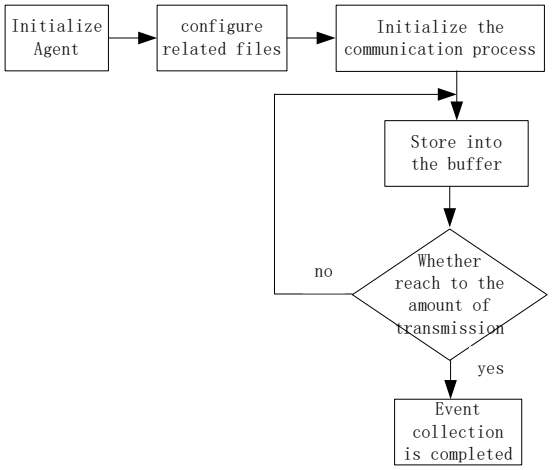


FIGURE 2 Flowchart for security event information collection

As seen in Figure 2, before collecting a certain type of security event, the information collection agent had to be initialised; secondly, we configured related files, specifying the server's IP address, port number, file location including security event/information, and the quantity of data sent each time. Then the communication process was initiated and a communication connection with the server-side established; thirdly, the specified information was collected, and finally sent from agent to server.

The event collection process mainly depended on each information collection agent which was developed independently in this research and cross-platformed, including host log collection agents, IIS service log collection agents, intrusion detection alarm collection agents, firewall log collection agents, vulnerability scan results collection agents, *etc*.

2.2.2 Pre-treatment layer

The flowchart through the event pre-treatment process is shown in Figure 3. In the pre-treatment process, firstly, we normalised and unified the formatting of various events. A security event correlation process may receive security events of different types or of one type but from different devices: there are certain differences between the formats of these events, such as security events from different types of firewall which can be compiled into different formats. A standardised module aimed to put all security events into a unified format, filter the events, removing those with nothing to do with system security, to get events that are real threats to system security. Finally, aggregation and incorporation of repeat events to reduce the number of data were undertaken and the output stored in the event database.

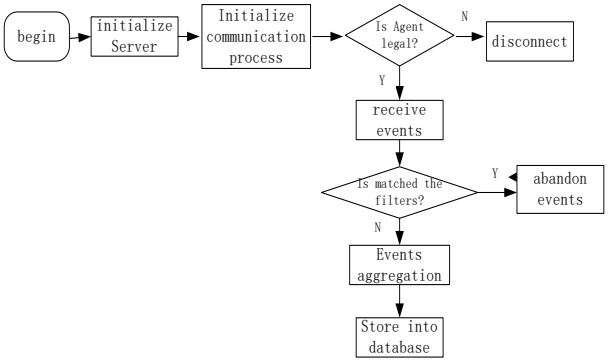


FIGURE 3 Flowchart through the pre-treatment process

2.2.2.1 Event standardised module

Security events refer to the original security event information produced by all kinds of security equipment, including log events produced by the firewall, intrusion alarm events generated by intrusion detection systems, system vulnerability events produced by vulnerability scanners, host system log events, router log information,

IIS Service log events, etc. These network security events are the main analysis objects in this research, they not only have different characteristics, but contain different content and record formats. The following is a simple introduction to some type of events:

1) Properties included in firewall logs.

int log_id
time createtime
string type
string src
string dst
string protocol
string service
string operation
int severity
int probability
int priority

2) Properties included in intrusion alarm events.

int analyzeid
time createtime
string classification
string src
string dst
string protocol
string suggestion
int probability
int priority

3) Properties included in vulnerability scanning events.

string name
string owner
time release_time
int cve_id
string request
string consequence
int severity
string solution

From the above, it can be seen that the formats of security events differed: therefore to facilitate the unified analysis of all kinds of security incidents, it was necessary to carry out the standardisation, to derive a unified format capable of expressing diversified event information from all relevant security devices.

To facilitate event correlation, events will be expressed in the following octuple form: (ID, Time, Host name, Type, Src, Dest, PRI, MSG). Among them, ID is a unique identifier of the information; Time is the production time; Host name is the device name of the recorded information; Type describes the information type; Src is the description of the source of invasion; Dest describes the purpose of the invasion; PRI refers to the priority of the event; and MSG is a description of the log.

2.2.2.2 Event filtering module

Network security events which occur in large numbers and are of low quality, contain both real events corresponding to attacker intrusion behaviour and false events with little or nothing to do with system security. The purpose of filtering for all kinds of network security events is to filter out false information as well as event information that had no relationship with the system security, at the same time, obtain only those events which posed a real threat to system security. The work included: excluding false information from detection and revealing event information corresponding to attacker intrusion behaviour from a large event log dataset.

Filtering rules mainly includes two aspects:

1) Filtering based on priority: we read PRI values of the event, and compared them with the pre-set threshold *k*. If PRI > *k*, this data had to be dealt with instantly, then sent to the next process. Otherwise it was abandoned with further processing.

2) Filtering based on key field: we included two methods:

a) Ignorance. Treat security events lacking key parameters as illegal event information, and delete it directly. For example, event information with empty log types had no analytical value and was filtered out. In addition, we deleted events with obvious error messages. For example, each part number of an IP address is an integer between 0 and 255, if the attribute value of a certain security event lay outwith that range it was clearly erroneous and was filtered out.

b) Filling. When missing only a few attributes of a record event, linear prediction, a global constant, or the average of the local properties were used to provide the missing attributes. A flowchart through the filtering process is shown in Figure 4.

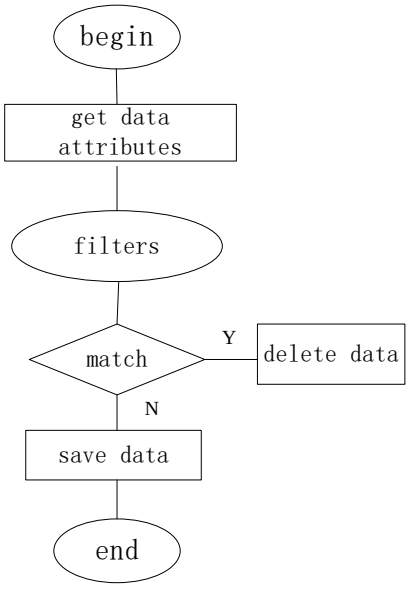


FIGURE 4 Filtering flowchart

2.2.2.3 Event aggregation module

Event aggregation aimed to merge a large number of duplicate events and reduce data redundancy. The main causes of a large number of repeats in security events were

that: the same attack, which is from the same place at the same time, often triggered different security equipment items to generate security incident records respectively; attackers often test different attack methods against specific targets or run the same attack multiple times to evaluate some parameters (such as, the offset and memory address of cache attack). Generally, all attributes or key attributes of these events are the same, and if we stored all of them in the database, they would not only occupy a large amount of storage space, but also the database grew too large, which was not conducive to the follow-up work and affected system efficiency: merging was therefore necessary.

2.2.3 Event correlation layer

After pre-treatment, the number of security events was reduced significantly. Analysing the processed results with the event correlation analysis algorithm and finding the association rules that may exist behind these data, while predicting potential dangerous events in the network, provided decision-making information for system managers.

2.2.4 Event management layer

The event management layer was responsible for displaying the data in the event database to the administrator in a pre-set way: at this time, the alarm information presented to the administrator was concise and clear, which made it convenient for the system administrator to respond to the current display and take appropriate precautionary measures. The main function of this layer included: security event querying: according to specific requirements, administrators can search associated event information by typing the appropriate query condition in the query box; and statistical analysis, for example the statistical analysis tables of various security events over a certain period (flow statistics or attack type statistics) making it easier for administrators to have an overall grasp of the current security situation.

3 Implementation of the event correlation model

To evaluate this correlation model, a strategy-based network security equipment linkage platform was used as the experimental platform and logs generated by the Venus firewall and user were taken as the data source for this experimental trial.

3.1 EXPERIMENTAL PROCEDURE

Specific steps were as follows:

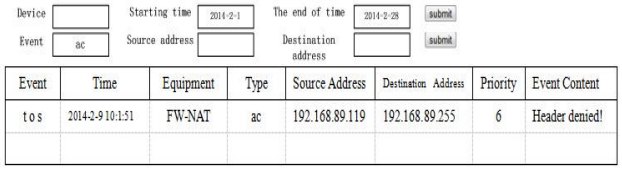
1) Pre-process the data collected by Agent to unify formats and streamline the data, store the results were then stored in the event database;

2) Discretise the data (correlation rules only deal with logical data, while these data had both numeric and class properties), thus necessitating their translation into logical data;

3) Analyse the data in the event database with an improved FUP [6] algorithm and automatically mine the dangerous events that may exist behind these data. Mining results were as follows:

TCP SYN scan => SYN flood attacks 0.8
Ftp, Telnet password detection => Trojan 0.6

Network administrators searched correlated event information through the management interface, part of which looked as follows:



Event	Time	Equipment	Type	Source Address	Destination Address	Priority	Event Content
tos	2014-2-9 10:1:51	FW-NAT	ac	192.168.89.119	192.168.89.255	6	Header denied!

FIGURE 5 Information query interface

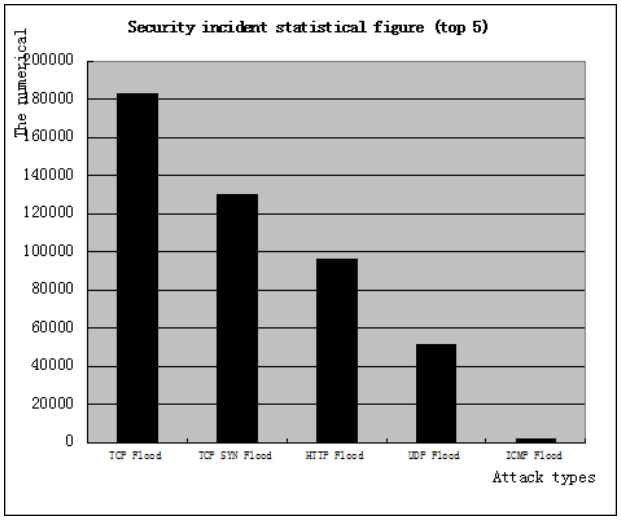


FIGURE 6 Security event statistics chart

3.2 EXPERIMENTAL RESULTS ANALYSIS

As the policy-based network security equipment linkage platform was still in its research stage, we just tested it simplistically: from the test results, this event correlation model was seen to effectively analyse alarm events, reducing the number of alarms significantly. Compared with traditional correlated systems, this event correlation model had the following advantages:

1) As it was the core module of a real-time network security equipment management system, it could process security events immediately for a timeous response.

2) The associated security events came from various heterogeneous security devices; therefore it could also improve the accuracy of correlation operations.

3) It undertook a series of processes to deal with the original security event(s) before executing correlation operations, including event normalisation, event filtering

and event consolidation, which improved the quality of the security event management and reduced the number thereof significantly. It was therefore deemed to have improved the efficiency of correlated events.

4 Conclusions

This research first introduced the overall design of the model, and then elaborated each module hierarchically. This model collected event information from agents, formatted the data into a unified event form; then eliminated redundant duplicate data with filtering and aggregation rules, stored the processed security event into an event database, and uncovered association rules hidden behind data by mining security events with an improved FUP algorithm. It then notified the system administrator thus allowing timeous preventative measures to be taken to prevent possible dangerous events. The system administrator can query the specific security event, current network status, *etc*. Finally, this model was applied to a network security equipment linkage system, using a firewall log and a user log as its data sources, and, according to the data processing flow of the model, realised the prediction of abnormal behaviour and attack behaviour, verified the effectiveness of the model, and so further improved overall system performance.

References

[1] Xin L 2009 Security Event Extraction Methods Based on Multiple Log Sources *Harbin Engineering University*
[2] Li H 2008 Research of Network Security Events Correlation and Design of System *PLA Information Engineering University*
[3] Wu Q 2006 Research on Integration of Intrusion Detection System and Firewall *Chongqing University*
[4] Luo Z 2012 Analysis network intrusion detection system *Network Security Technology and Application* **18** 54-5
[5] Agrawal R, Imielinski T, Swami A 1993 Mining association rules between sets of items in large database *Proceedings of the ACM SIGMOD Conference on Management of Data* 207-16
[6] Zhang S, Liang Z, Hu L 2012 Research and Application of Improved Multidimensional Association Rule Mining Algorithm *Engineering and Computer Science* **34** 174-9

Authors

Sizu Hou, born on May 23, 1962, Yuncheng, Shanxi province, China

Current position, grades: North China Electric Power University, professor.
University study: Master of Engineering of North Jiaotong University, specializing in communication and electronic systems, 1988.
Research activities: power systems communication technology, information and communication engineering.
Professional Activities and Memberships: Broadband Power Line Communication Technology Research, Communications network monitoring and management system, Integrated Network Management System.

Xiaorong Cheng, born on April 25, 1963, Handan, Hebei province, China

Current position, grades: North China Electric Power University, professor.
University study: Master of Engineering of North China Electric Power University, Power Systems and Automation, 1994.
Research activities: computer network technology, network information security.
Professional Activities and Memberships: Network Security Research, GIS-based Ethernet management software, Panjin Power Administration Cable Management Software, Concentrate on the practice teaching reform and research.