STUDIA INFORMATICA 2003
Volumen 24 Number 2B (54)

Gunasekaran NARENDRAN, G. Nelson VIMAL JEBARAJ, Rajendran SUGESH KUMAR
Sri Sivasubramaniya Nadar College of Engineering, Department of Computer Science
Raju ILAYARAJA
Sri Siva Subramaniyanadar College of Engineering
Panner NARAYANASAMY
Easwari Engineering College, Department of Computer Science & Engineering

PROACTIVE NETWORK SECURITY EVENT MANAGEMENT USING MOBILE AGENTS

Summary. This paper introduces a novel implementation of an upcoming paradigm in network security. The Network Security Event Management paradigm aims at detecting events in the network and correlating them with attacks, so that the attacks can be prevented even from being successfully attempted. The use of mobile agent technology provides distinctive advantages over client-server architecture and the use of an expert system adds to the intelligent analysis and correlating capabilities of the system. The event management paradigm has been successfully implemented by integrating the modules of Network Monitor, Network Traffic Analyzer and an Expert System for intelligent decision making. This system provides with various advantages over traditional network security tools in manners that, this system detects and acts on pre-attack postures itself, reduces the network traffic by transporting the know-how to the client itself. Other advantages include intelligent analysis and correlation of events, flexible reporting, automated alerting and preventive action enabling.

Keywords: Mobile Agent, Network Security Event Management, Proactive Network Security.

ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI PRZEZ ANALIZĘ ZDARZEŃ ZA POMOCĄ RUCHOMYCH AGENTÓW

Streszczenie. Artykuł przedstawia implementację nowej polityki bezpieczeństwa w sieci, polegającej na wykrywaniu zdarzeń w sieci i ustalaniu ich korelacji z występującymi atakami, co pomaga zapobieżeniu tych ataków. Wykorzystanie technologii ruchomych agentów przynosi znaczne korzyści w stosunku do architektury klient-serwer, a zastosowanie systemu eksperckiego wspiera inteligentną analizę zdarzeń i ustalanie korelacji. System zarządzania zdarzeniami jest zrealizowany poprzez

integracje modułów Monitora Sieci, Analizatora Ruchu i Systemu Eksperckiego. Niektóre zalety opisywanego systemu w stosunku do tradycyjnych narzędzi zabezpieczających sieć to możliwość uprzedzania ataków, zmniejszenie natężenia ruchu w sieci poprzez przeniesienie niezbędnej wiedzy na poziom użytkownika, inteligentna analiza i korelacja zdarzeń, raportowanie dostosowane do indywidualnych potrzeb, automatyczne alarmowanie i podejmowanie akcji zapobiegawczych.

Słowa kluczowe: ruchomi agenci, zarządzanie zdarzeniami dotyczącymi bezpieczeństwa w sieci, aktywna polityka bezpieczeństwa sieci.

1. Introduction

Network Security has evolved over the years and today it follows the paradigm of "Network Security Event Management" and dynamic decision making, instead of the traditional "Network Monitoring" and enforcement of a standard set of policies and rules. Network Event Management involves intelligent decision making on part of the management system. Mobile Agent (MA) Technology provides the necessary paradigm and methods to implement an Intelligent Monitoring and Event Management system. Mobile Agent technology is considered as an enhancement of distributed computing as it provides powerful and efficient mechanisms to develop applications for heterogeneous networks. Traditional Client Server architecture treats local and remote resources in the same way, as illustrated in Fig. 1. The Mobile Agent technology treats the local interaction as much more interactive than the remote one. Figure 2 illustrates the Mobile Agent paradigm.

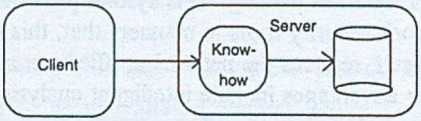

Fig. 1. Client Server Paradigm
Rys. 1. Model klient-serwer

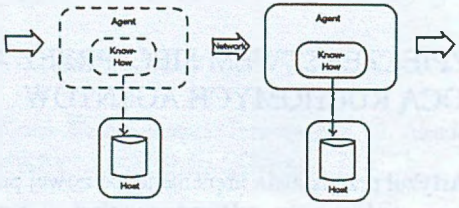

Fig. 2. Mobil Agent Paradigm
Rys. 2. Model ruchomego agenta

A new model for Intelligent Network Security Event Management is implemented using IBM's Aglet Software Development Kit (ASDK). The modules in this model include Mobile Agents, Network Traffic Analysis Engine and an Expert System based on Java Expert Shell System (JESS).

2. Traditional Network Security Paradigm

Conventional Network security tools depend on the occurrence of the event to determine that a security breach has occurred. The traditional network security paradigm distributes the onus of ensuring security equally between the system administrator and the computer. The majority of tools are involved with the collection of relevant data from the network traffic, whereas the onus of the interpretation of the data and gleaning of attacks is left to be handled by the Network administrator. Hence these traditional tools, such as Anti-virus engines, Firewalls and Intrusion Detection Systems are said to be "Passive" in their mode of providing security. These traditional tools will not be able to adapt themselves to the changing modes of attacks since they lack the intelligence to do so. Our model aims at identifying the threat even as the pre-attack measures such as ping sweeps, port scans, network-browsing and website crawling are attempted. Hence this model aims at "Proactive" network security, thereby preventing security breaches even before they occur.

3. Network Security Event Management Paradigm

The sheer number of threats and intrusions to corporate IT systems has grown phenomenally in the past few years - along with the sophistication of attacks. As a result, companies across the globe are experiencing security events such as attacks, intrusions, and policy violations on a scale never seen before. Security events and other information from numerous point products such as network-based intrusion detection systems, firewalls and anti-virus products are overwhelming security managers and intrusion analysts. In struggling to properly monitor their security environments, companies realise that there must be a better way and this belief has evolved into the concept of " Security Event Management".

Security event detection technologies must start to identify more than just attacks and intrusions - the traditional domain of intrusion detection systems that often rely on specific signatures for detection. Security event detection technologies must also identify precursors of attacks such as port scans, network browsing and website crawling. They need to identify

policy violations such as configuration changes that deviate from security standards and user breaches of user policies.

Successful security event management must rely on the detection of more than just attacks and intrusions. While these are very important events, intrusion management technologies and processes have to begin making sense of large volumes of information and using this information to highlight only those events or combination of events that are relevant to the organisation's security posture.

The various vital processes that must be put into place for successful security event management include:

1. *Enterprise security event collection*: The event management system must be able to collect events from numerous disparate technologies including security and network devices.
2. *Data Normalisation*: The event management system must also parse and normalise event data i.e glean relevant information from the database.
3. *Event correlation*: Security event correlation is the process of relating several distinct security events that emanate from the same attack.
4. *Alerting and automation*: The event management system must be able to be automated and must provide flexible alerting services.

This work follows the newer paradigm of "Network security event management" instead of the traditional "Network Monitoring" paradigm at providing Proactive Network Security. The implementation of this work takes advantage of the features offered by the mobile agent technology, the expert system features offered by JESS for making intelligent decisions and packet capture libraries for network traffic analysis.

4. Advantages of Security Event Management Paradigm

The major advantages that can be attained by embracing the concept of "Network Security Event Management" instead of the traditional concept of " Network Monitoring" as evidenced in this work are:

1. Pre-attack measures are detected and prevented from becoming full fledged attacks.
2. Automated analysis of security event data and flexible reporting.
3. Intelligent automated preventive measures are deployed by the system itself and hence does not require the presence of the network administrator always at the terminal.
4. Reduces network traffic as Mobile Agent Technology is used.

5. Mobile Agents in Network Security Event Management

In this new Mobile Agent based Network Security Event Management system, various strategic nodes in the network maintain a database of the network traffic in that segment, collected and maintained by the Network Traffic analyzer module. These nodes have the network traffic analyzer module installed in them apart from the Java Development Kit (JDK 1.4) and ASDK2 installed for the support of Mobile Agents. The three main modules of Network Event Monitor, Network Traffic Analyser and Expert system are involved to facilitate the Network Security Event Management operations.

6. System Architecture

Fig. 3 depicts the complete picture about the system. The network traffic analyzer in this system collects the information of the network traffic from the various nodes placed strategically on the network. These nodes will act as databases for the Event monitor to query and analyse the data collected. The network traffic is captured and analysed in real-time so that the data remains current and the security events get detected as and when they occur. This provides the necessary leverage for the event correlation to be performed by the Expert system module. The various network security events are compared with attack patterns as specified in the rules base of the Expert system, and if any correlation is found then the Mobile agents are triggered into action. The mobile agent triggered into action may perform various preventive measures such as clamping down certain ports from access or triggering a firewall to prevent packets from a source machine from reaching the network. These preventive measures effectively counter the various attack postures taken. If the intruder tries to use another open port for the purpose of attack, the same will be detected and the open port will be automatically closed.

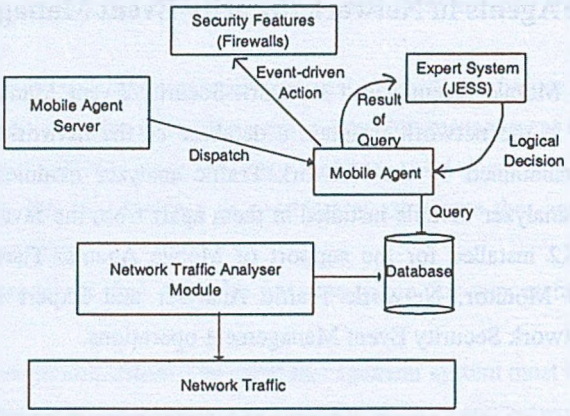

Fig. 3. Mobil Agent based model for Network Security Event Management
Rys. 3. Model ruchomego agenta wykorzystujący zarządzanie zdarzeniami w sieci

7. Network Event Monitor

A Mobile Agent is created in the managing node, cloned and dispatched to all the strategic nodes in the network where the network traffic databases are maintained. The agent migrates to each node and collects the information on network traffic and processes the information present in the database by normalising the data collected by the network traffic analyser module as the network traffic collected will be huge and not all of the raw information has to be processed. Once the normalised data is available it passes on the information processed from the database to the expert system to check if any security event correlating with attacks has occurred. The mobile agent is implemented using the ASDK2 provided by IBM. Fig. 4 shows the working algorithm for the mobile agent network event monitor.

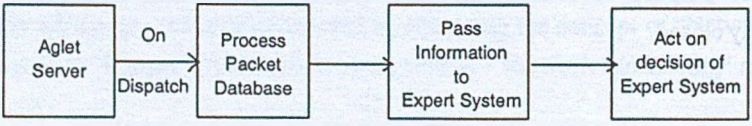

Fig. 4. Algorithm for Network Monitor module
Rys. 4. Algorytm pracy modułu Monitorowania Sieci

8. Network Traffic Analyzer

The network traffic analyzer serves to collect information on the sort of traffic that the network is carrying at any given point of time. The network traffic analyser module is based

on a packet capture library to collect the various packets that constitute the network traffic. The packet capturing is implemented using PCAP libraries which is an open source project and is provided with most major distributions of Linux. The PCAP libraries have been written using the C programming language. To interface PCAP library with Java, since the aglets are written using java, another excellent library using Java Native Interface (JNI) to interface the C language libraries with the aglets, JPCAP, has been used. The architecture of the network traffic analyzer is explained in Fig. 5. Once the network traffic packet capturing process has begun, the relevant information regarding the various packets such as the source address, the destination address, the nature of the packet and other information as can be obtained from the header of the packet are collected and stored in the database. This information is stored so that the mobile agents may be able to analyse the information with the help of the expert system module to glean traces of pre-attack measures. Fig. 6 illustrates the algorithm behind the traffic analyzer module. This module is implemented using a packet capture library and works as a network sniffer.

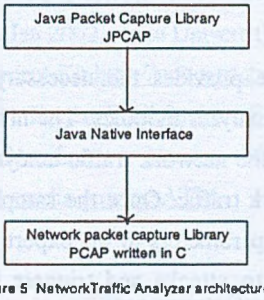

Fig. 5. Network Traffic Analyzer architecture
Rys. 5. Architektura Analizatora Ruchu Sieci

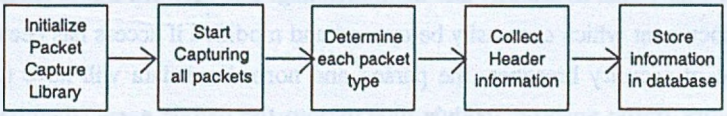

Fig. 6. Algorithm for Network Traffic Analyzer module
Rys. 6. Algorytm pracy modułu Analizatora Ruchu Sieci

9. Expert System Module

The Expert system is a rule based engine that is built using the Java Expert Shell System (JESS). This module is based on a set of rules that define the various types of attacks and their

pre-attack measures. This module analyses the information provided to it by the Mobile Agent and instructs the Mobile agent to take preventive measures based on the Security event detected. A port scan event can trigger the Firewall to close vulnerable ports, or a ping sweep can be traced to a source machine and the Mobile agent can block the source machine. Fig. 7 illustrates the algorithm for the Expert system module.

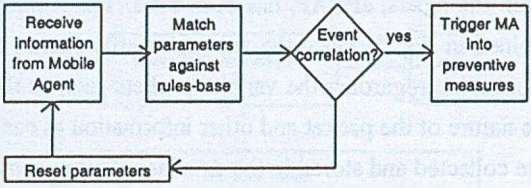

Fig. 7. Algorithm for Expert system module
Rys. 7. Algorytm pracy modułu Systemu Eksperckiego

10. Discussion

The network monitor module provides the necessary interface for the Expert system module and the Network Traffic analyzer modules. The information so queried and processed from the database maintained by the network traffic analyzer module is normalised so that it represents a sample of the network traffic. Once the sample data parameters are fed into the mobile agent, it then passes these parameters to the expert system. The expert system decides if there is any event correlation to attacks and triggers the mobile agents into preventive action. The entire system is based on the java language implementation. Hence the performance of the system is relatively slow. The use of Java language provides certain advantages on issues such as security and multithreading. The network traffic database is just a plain ASCII document which can easily be opened and modified if access has been gained. To avert this type of security breaches, the parsed and normalised data will have to be passed from the network traffic analyzer module directly into the mobile agent, thereby eliminating static storage of information collected from the network traffic. This work clearly shows how mobile agent technology can be effectively used to leverage the implementation of the Network Security Event Management paradigm.

11. Conclusion

This paper has clearly outlined the advantages of the Network Security Event Management paradigm over the traditional network monitoring paradigm. This paper has also

outlined the advantages of the mobile agents over the client - server technology. The use of mobile agents lends itself to a reduction in the network traffic. Moreover, this work shows that a rule based engine may be used to relieve the network administrator of some of his work.

REFERENCES

1. Ilayaraja R., Narayanasamy P., Sugumar M.: Proceedings of International Conference on Artificial Intelligence in Engineering and Technology. July 2002, Sabah, Malaysia.
2. Lipperts S.: Enabling Alarm Correlation for a Mobile Agent Based System and Network Management – A Wrapper Concept. IEEE conference on Networks, October 1999, Australia.
3. Lange D. B., Oshima M.: Programming and Deploying Java Mobile Agents with Aglets. Addison Wesley, Tokyo 1998.
4. Ilayaraja R.: Mobile Agent based Network Management System. Thesis submission to Master of Engineering Degree. Jan 2002, Anna University, India.
5. IBM Aglets Software Development Kit http://www.trl.ibm.co.ip/aglets .
6. Friedman-Hill E.: JESS the Java Expert Shell System. Forum Technical Committee: Private Network-Network Interface Specification Version 1.0. ATM Forum af-pnni-0055.000, March 1996, http://herzberg.ca.sandia.gov/jessATM .

Recenzent: Prof. dr hab. inż. Tadeusz Czachórski

Wpłynęło do Redakcji 5 kwietnia 2003 r.

Streszczenie

Artykuł przedstawia implementację nowej polityki bezpieczeństwa w sieci, polegającej na wykrywaniu zdarzeń w sieci i ustalaniu ich korelacji z występującymi atakami, co pomaga zapobieżeniu tych ataków. Wykorzystanie technologii ruchomych agentów przynosi znaczne korzyści w stosunku do architektury klient-serwer, a zastosowanie systemu eksperckiego wspiera inteligentną analizę zdarzeń i ustalanie korelacji. System zarządzania zdarzeniami jest zrealizowany poprzez integracje modułów Monitora Sieci, Analizatora Ruchu i Systemu Eksperckiego. Niektóre zalety opisywanego systemu w stosunku do tradycyjnych narzędzi zabezpieczających sieć to możliwość uprzedzania ataków, zmniejszenie natężenia ruchu w

sieci poprzez przeniesienie niezbędnej wiedzy na poziom użytkownika, inteligentna analiza i korelacja zdarzeń, raportowanie dostosowane do indywidualnych potrzeb, automatyczne alarmowanie i podejmowanie akcji zapobiegawczych.

Adresy

Gunasekaran NARENDRAN: Sri Sivasubramaniya Nadar College of Engineering, Department of Computer Science, Old Mahabalipuram Road, Kalavakkam, Kanchipuram District, Tamil Nadu – 603 110, India, naren_30in@yahoo.com .

G. Nelson VIMAL JEBARAJ: Sri Sivasubramaniya Nadar College of Engineering, Department of Computer Science, Old Mahabalipuram Road, Kalavakkam, Kanchipuram District, Tamil Nadu – 603 110, India, vimaljebaraj@yahoo.co.in .

Rajendran SUGESH KUMAR: Sri Sivasubramaniya Nadar College of Engineering, Department of Computer Science, Old Mahabalipuram Road, Kalavakkam, Kanchipuram District, Tamil Nadu – 603 110, India, sugesh_kumarr@yahoo.com

Raju ILAYARAJA: Sri Siva Subramaniyanadar College of Engineering, Kalavakkam – 603 110, Tamilnadu, Chennai, India, ilayaraja_r@yahoo.com .

Panner NARAYANASAMY: Easwari Engineering College, Department of Computer Science & Engineering, Bharathi Salai, Chennai, Tamilnadu, India, anarayan65@yahoo.co.in .