하드웨어 기반의 침입탐지 시스템의 설계에 대한 분석

김정태
목원대학교

Analyses of Design for Intrusion Detection System based on Hardware Architecture

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

A number of intrusion detection systems have been developed to detect intrusive activity on individual hosts and networks. The systems developed rely almost exclusively on a software approach to intrusion detection analysis and response. In addition, the network systems developed apply a centralized approach to the detection of intrusive activity. The problems introduced by this approach are twofold. First the centralization of these functions becomes untenable as the size of the network increases.

I. Introduction

A Wireless Sensor Network (WSN) usually consists of a number of sensors of different modalities which, when combined with a microprocessor and a low-power radio transceiver, form a smart network-enabled node. The sensed data can be related to different applications but in terms of capabilities all the nodes that cooperate in the WSN can be assumed as homogeneous. Because of the critical environments where such kind of networks may be used. The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. The problem of detecting anomalies, intrusions, and other forms of computer abuses can be viewed as finding non-permitted deviations (or security violations) of the characteristic properties in the monitored (network) systems. Facing with progressive ubiquitous environment, we have felt altemative impressions, diversity or security. While the ubiquitous network is really functional and useful when the diversity is in normal states, it is hard to control if abnormal states once happen among widely spread devices. Ad hoc networks arouse imminently an important interest within industrial and research communities. Actually, their salient features, essentially the absence of infrastructure and auto-management, promise huge applications and possibilities for wireless communication. However, the tremendous boom ofthese networks depends incontestably on their reliability in terms of security and quality of services (QoS). In this paper, we study the ad hoc security vulnerabilities for which cryptographic-based solutions are ineffective and which require IDS. Appropriate designed IDS services appear essential as countermeasures to those

threats.

II. Structure of IDS agents

The obvious advantage of using mobile agents is when they present a single general framework in which many distributed applications can be implemented easily, efficiently and robustly. Intrusion detection system is a guard system that automatically detects malicious activities within a host or a network, and then reports that for subsequent response. IDSs may work on a host level and become host-based, or on a network level and become network based. Depending on the detection techniques used, IDS can be classified into three main categories: signature-based, anomaly-based and the hybrid of both. IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the mobile wireless network. The proposed IDS is built on a mobile agent framework. It is an agent system and employs several sensor types that perform specific certain functions. Network monitoring: Only certain nodes will have : ; sensor agents for network packet monitoring, since we are interested in preserving total computational power and battery power of mobile hosts.

Host monitoring: Every node on the WAN will be monitored internally by a host-monitoring agent. This includes monitoring system-level and application-level activities.

Decision-making: Every node will decide on the intrusion threat level on a host-level basis. Certain nodes will collect intrusion information and make collective decisions about network level intrusions.

Action: Every node will have an action module that is responsible for resolving intrusion situation on a host.

Communication: Every node can exchange information about malicious behaviors on some network segments or at certain host and response intrusions against them. Fig.1 shows a conceptual model for IDS agents.

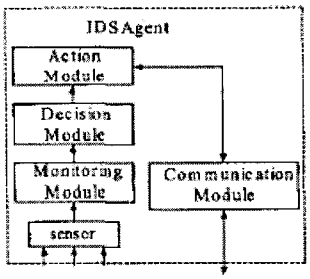

Fig. I. A conceptual model for IDS agents

Each module represents a lightweight mobile agent with certain functionality, making a total network load smaller by separating the functional tasks into categories and dedicating an agent to a specific purpose.

In addition to authentication, Integrity, confidentiality, availability, access control and non-repudiation, which have to be address differently in a mobile, wireless, battery-powered and distributed environment, mobile as hoc networks raise the following security issues;

1) Cooperation and fairness
2) Confidentiality of Location
3) No traffic diversion
4) Routing
5) Forwarding

III. Hardware cryptography embedded architecture

A hardware cryptography embedded multimedia mobile processor we have developed for ubiquitous computing. This is completely different from trusted platform module and is able to implement

an extremely huge length common key scheme. In view of efficiency, usability, and cryptographic strength. According to the discussion described above, a reasonable choice for such applications will be multimedia cryptography in bidirectional communication. This is impossible for TDM, a cutting edge technique commonly known as security chip. TPM implements RSA, and its major role is implicitly digital signing. TPM works for a short, password size text data, but the encryption of long length multimedia data like an image is definitely outside of the security chip in view of running time. In view of efficiency, usability,, and cryptographic strength, Embedded processor is suitable for the cryptography of multimedia data.

IV. Security Processing Architectures

Security processing refers to computation that need to be performed specially for the purpose of security. For example, in a secure wireless data transaction, security processing includes the execution of any security protocols transactions, security processing includes the execution of any security protocols that are utilized at all layers of the protocol stack.

A. Embedded processor enhancement for securing processing

There have been several attempts to improvement the security processing capabilities of general purpose processors. Since most microprocessors today are word oriented, researchers have targeted accelerating bit level arithmetic operations such as the permutations performed in DES/3DES. Multimedia in struction set architecture

B. Cryptographic hardware accelerators

Highest levels of efficiency in processing are often obtained through custom hardware implementations. Since cryptographic algorithm form a significant portion of security processing workloads, various companies offer custom hardware implementations of these cryptographic algorithms suitable for mobile appliances including smart cards and wireless handsets.

C. Programmable security protocol engines

While cryptographic accelerators alleviate the performance and energy bottlenecks of security processing to some extent, achieving very high data rates or extreme energy efficiency requires a view of the entire security processings workload. In additional to cryptographic algorithms, security protocols often contains a significant protocol processing components, including packet header/trailer allocation parsing

Wireless intrusion detection systems are an important addition to the security of wireless local area networks. While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides.

V. Distributed Intrusion Detection Using Mobile Agents

This system employs several sensor types performing different functions. Each module represents a lightweight mobile agnt with certain functionality. This makes the total network load smaller by separating the functional tasks into categories and dedicating each aegnt to a specific purpose. Moreover, the use of mobile agents to this architecture facilitates sensor's mobility and the intelligent routing of intrusion data through the network. There are three major agents catagories, namely: action, decision-making,

and monitoring agents. Monitoring agents monitor packets as they arrive to host or network. While host monitoring sensors are present on all mobile hosts, networks monitoring sensors are distributed to a selected group of nodes. Moreover, monitoring agents are classified into packet, user and system monitoring agents. Decision-making agents, on the other hand, are present on each node and will decide on the threat level on a host-level basis. Finally, action agents are present on every host and are responsible for resolving intrusion situations on a host they occur

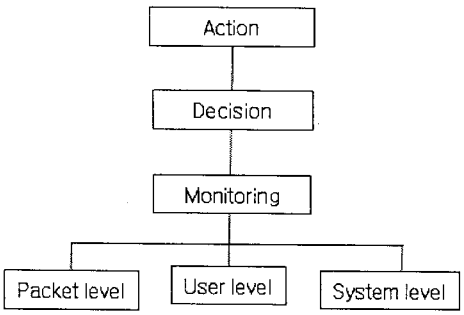

Figure 1. Configuration of mobile agents architecture

The IETF policy framework working group has developed a policy management architecture that is considered the best approach for policy management over the Internet.

- Policy Decision Point(PDP) : A logical entity, or a policy server, that interprets policies stored in a repository, makes policy decisions, and communicate them to a PEP.
- Policy Enforcement Point(PEP) : A logical entity that can apply and execute the different policies. A PEP usually exists in network nodes such as routers, firewalls, and hosts.
- Local Policy Decision Point(LPDP) : A local representative of a P에. It exists within a network nodes or a device to make local policy decision. Basic policy decisions can be programmed into this component. Any local decision or policy changes will be relayed to the PDP.

VI. Conclusion

We have analysed design of agent for intrusion detection in wireless Ad Hoc Networks. The disadvantages of mobile agents are their architecture inherited security vulnerabilities and the extra weight they may add. Many researches have been conducted to secure mobile agents functionality. Moreover, new researches are being made that concern with light weight designs for mobile agents.

References

[1] P. H. W, Leong, etc, "A microcoded elliptic curver processor using FPGA technology," IEEE TRANS. on VLSI Syst., v.10, n.5, pp.550-559, Oct, 2002

[2] M, Fukase, etc, "An experiment in the design and development of a multimedia processor for mobile computing," Technical report of IEICE, v.102, n.400, pp.13-18, Oct. 2002

[3] C. Perkins and E. Royer, "Ad Hoc and Distance Vector Routing, "Proc, Second IEEE Workshop on Mobile Computing Systems and Application, IEEE Computer Society Press, Feb, 1999

[4] Hongmei Deng, "Routing Security in Wireless AD Hoc Networks", IEEE Communication Magazine, Oct. 2002, pp.70-75