國立交通大學

電機資訊學院 資訊學程

碩 士 論 文

一個以警報為基礎的聯合防禦系統

A Study of Alert-Based Collaborative Defense

研 究 生：辛文義

指導教授：曾憲雄　教授

中 華 民 國 九 十 四 年 六 月

一個以警報為基礎的聯合防禦系統

A Study of Alert-Based Collaborative Defense

研 究 生：辛文義　　Student：Wen-Yi Hsin

指導教授：曾憲雄　　Advisor：Shian-Shyong Tseng

國 立 交 通 大 學

電機資訊學院 資訊學程

碩 士 論 文

A Thesis

Submitted to Degree Program of Electrical Engineering and Computer Science
College of Electrical Engineering and Computer Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science
in
Computer Science
June 2005
Hsinchu, Taiwan, Republic of China

中華民國九十四年六月

一個以警報為基礎的聯合防禦系統

學生：辛文義　　指導教授:曾憲雄 教授

國立交通大學電機資訊學院 資訊學程（研究所）碩士班

摘　　要

本篇論文提出一個以警報資料為基礎的聯合防禦解決方案。

我們注意到在企業內部很難防止惡意的攻擊，因為每天所產生的大量日誌記錄與警報資料很難分析，造成系統管理員無法掌控狀況且無法針對事件的處理做出立即的決策。病毒、病蟲和特洛伊木馬程式迅速地傳播並擴及全球。論文中，我們探討分析了入侵偵測系統、分散式入侵偵測系統、聯合防禦、警報資料分析與資訊分享機制，發現目前的網路安全系統有許多困境與挑戰點。

我們延伸分散式入侵偵測的模式，提出一個聯合防禦的架構。包含警報收集、萃取、分析、回報、資料倉儲和分析。此外我們發展一個混合式的安全資訊分享的方法，就像升起狼煙警告其他夥伴一般，藉由資訊分享，參與電腦安全事件回報團隊的成員能獲得安全防禦相關的解決資訊，例如黑名單、入侵偵查的規則和安全防禦知識。這個架構提供學術界和企業界一個建立有效合作的安全聯防團隊方案。

我們進行了評估可行性的實驗，並追查出 SQL Slammer 蠕蟲的傳播情形。結果發現，透過聯合防禦的機制，廣泛部署系統，能更加準確地追查出攻擊的行為，並且可以協助成員評估威脅的衝擊和採取適當的行動來降低風險。

關鍵字：聯合防禦、合作式安全系統、分散式入侵偵測系統、入侵偵測系統、網路安全、警報、電腦病蟲

A Study of Alert-Based Collaborative Defense

Student: Wen-Yi Hsin Advisors: Prof.Shian-Shyong Tseng

Degree Program of Electrical Engineering Computer Science

National Chiao Tung University

ABSTRACT

This thesis proposes a lightweight alert-based collaborative defense solution.

We notice that malicious attack is difficult to prevent in the enterprise interior. Because it is hard to analyze a large number of logs and alerts, the administrator can not control the situation and make decision immediately. The Worms, Virus and Trojan spread rapidly, the scale of the problem is large and growing rapidly. Modern Security Systems have many predicaments. We had discussed the intrusion detection, distributed intrusion system, collaborative defense system, security information sharing mechanism and alert analysis in this thesis.

We propose a framework for collaborative defense by extending the original distributed intrusion detection model. It contains alert's collector, extractor, analyzer, report's generator, alert warehouse and alert's analysis. Besides, we develop a hybrid approach to share security information like raising the wolf smoke to warn partners. By the security information sharing, the members of CSIRT can obtain the solutions of defense, such as blacklists, detection rules, and security knowledge about alerts. The framework provides a solution to build effective cooperative security teams for academia and industry.

We evaluate the feasibility of our framework and track the spreading behaviors of the

SQL Slammer Worm. As a result, we can deploy security system more widely and detect the aggressor's behavior more accurately. The alert-based collaborative defense mechanism can help members to evaluate the impact of the threats and take proper actions to mitigate the risk.

Keywords: Collaborative Defense, Collaborative security, Cooperative Intrusion Detection, Distributed Intrusion detection, Incident Response, Alert, Worm

誌　　謝

感謝恩師曾憲雄教授的教導，在知識見聞上，在研究學問中，甚至課堂教學與學生輔導的方法與用心都讓為人師表的我獲益良多。而實驗室的林順傑、王慶堯兩位學長平日的協助、解惑與惕勵，不藏私地引導老學弟，讓我的學習研究路上不孤單。

感謝任教的學校-新竹縣立湖口高中，允許我在課餘的時間前往交大進修，在教學工作與在職進修，都給予最大的便利與支持。在系統驗證上，感謝新竹縣的教育網路中心、關西國中曾清曄老師、富光國中王迺仁老師、湖口國小簡錦焜老師、二重國小周世玉老師提供了學校實際的網路環境，讓我可以更真實地評估系統可行性，並建構了一個聯合防禦團隊的雛形。在論文寫作上，感謝三姐辛麗玲老師，仔細不厭煩地校正我的英文文稿。

特別感謝我的妻子林秀娟小姐。能體諒我，一肩扛起兩個小寶貝的教養和瑣碎家事的重擔。能陪著我，同甘共苦一起度過，讓我可以沒有後顧之憂的衝刺努力，我們是最佳拍檔，您們是我活力的泉源，我愛您們。

以在職生的身分可以如期完成研究所學業，著實不容易。慶幸自己能獲得父母、家人、朋友、同事、學長、老師的支持與勉勵，才有源源不斷的動力克服萬難，順利更上一層樓。感謝您們，您們都是我生命中的貴人，文義銘感腑內。僅將這個研究的成果獻給您們!

文義

于 交通大學知識工程實驗室 2005.6.14

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

With the evolution of computer systems into both local and wide area networks, the scope of computer security has increased dramatically over the past two decades.

There have been several large-scale worm attacks on the Internet since 1988 and highly visible and coordinated denial-of-service attacks in the last few years causing billions of dollars in damage. These attacks indicate that responding, if anything, to such incidents is increasingly more complex, and requires technical knowledge, communication, and coordination among the staff responding to an incident, along with an adherence to applicable standards [Masurkar03-2].

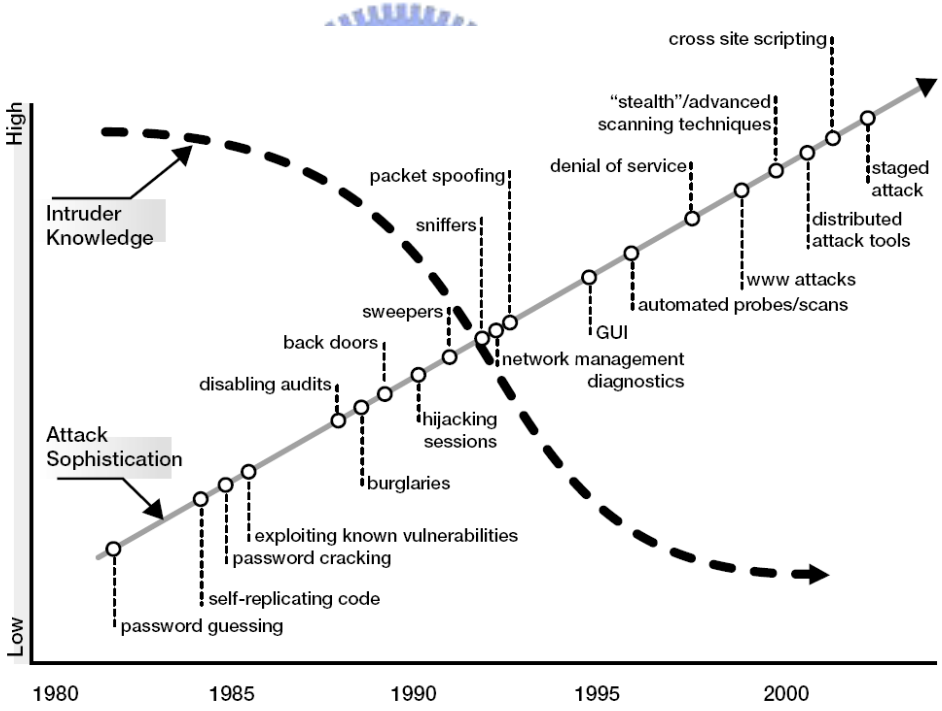


Figure 1-1: Attack sophistication versus intruder technical knowledge [HOW00]

Intrusion-detection products have become widely available in recent years, and are beginning to gain acceptance in enterprises as a worthwhile improvement on security. The fast spreading worms have presented a major threat to the security of the Internet. Worm detection and response received renewed focus in both academia and industry. The threat posed has

changed from what once appeared as an unstructured threat from adventurous hackers, to a structured, hostile attack on elements of the critical infrastructures of different countries. In some cases, governments and organizations with substantial resources are increasingly backing such attacks.

The survey [CU+04] of last year shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions. Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization. Respondents say that e-crime cost their organizations approximately $666 million in 2003.

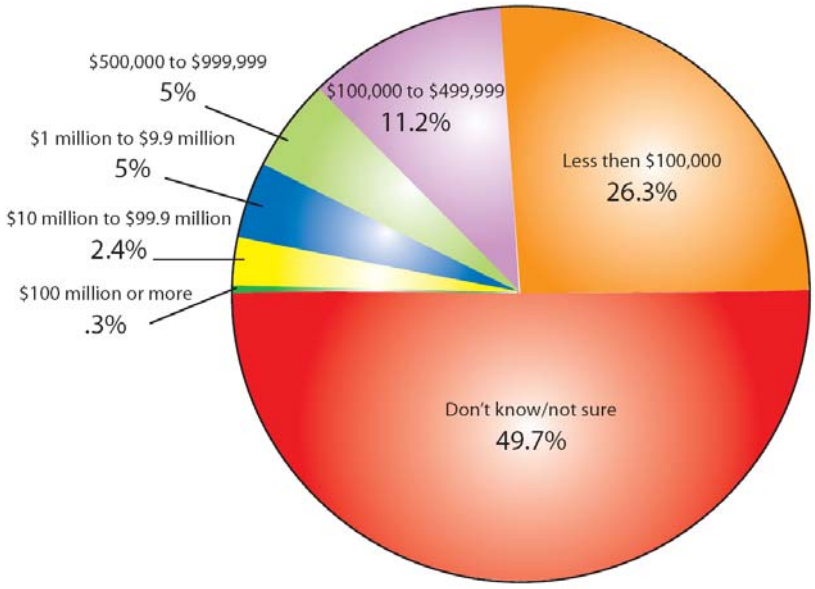


Figure 1-2: 2003 Dollar Losses Due to Electronic Crimes or System Intrusion [CU+04]

As knowledge about computers and networking has spread, and as standardized open systems replace proprietary architectures, attacking such networks has become easy work, even for amateurs. Where attacks are organized and professional, no network is safe.

1.1 Scenario

Currently many defenders (Network administrators) do not share detailed security information automatically with others outside their organization. But attackers and their machines share vulnerability information rapidly, efficiently and openly. Network defense viewed as local responsibility and individual sites defend themselves only. It works OK against low or moderate levels of attack, but Internet-scale threats are not well addressed in this self-defense mode.

We should notice that malicious attack is difficult to prevent in the enterprise interior. Secondly, it is hard to analyze a large number of Logs and Alerts. So the administrator can not control the situation and make decision immediately. Thirdly, with Worm, Virus, Trojan spreading rapidly, the scale of the problem is large and growing rapidly. The individual attacks take over one million machines, more and more successful attacks.

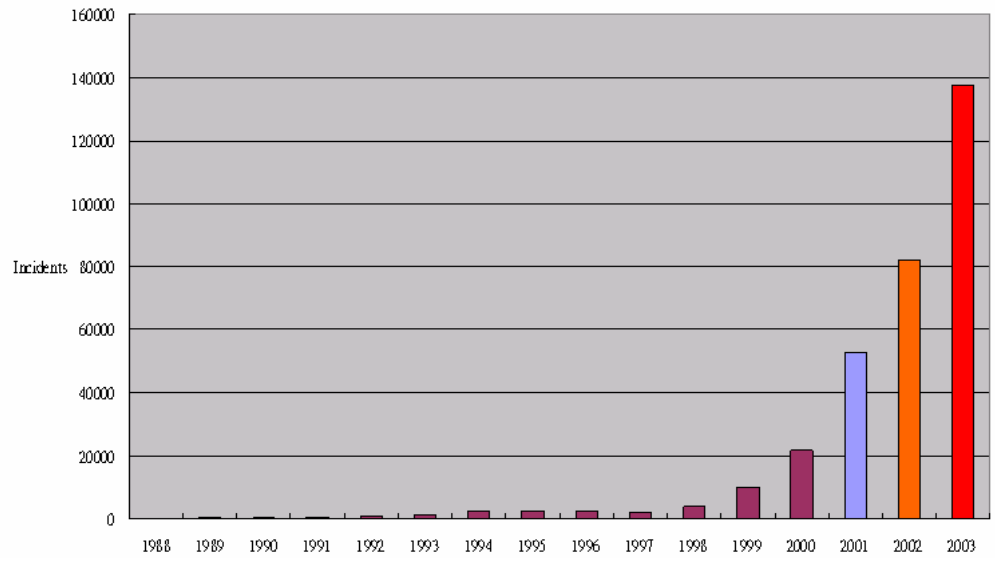


Figure 1-3: Growth in number of incidents handled by the CERT/CC®

We may, therefore, reasonably conclude that how to share security information and how to do collaborative defense with partners are important.

1.2 Motivation

Modern Security Systems encounter many predicaments.

1.2.1 The predicament of Intrusion Detection System

First, a single security system such as a network based IDS may flag thousands of alerts per day, and multiple security systems make the situation even worse. Large numbers of alerts may overwhelm the analysts.

Second, among a large volume of alerts, a high proportion of them are false positives , some of them are low-severity alerts (e.g., an attack to an inactive port), and some others correspond to severe attacks. It is challenging to differentiate these alerts and take appropriate actions. The low level and high volume of the alerts also make extracting the global view of the adversary's attack strategy challenging.

Third, different security systems usually run independently and may flag different alerts for a single attack. Discovering that these alerts are actually triggered by the same attack can be time-consuming, though it is critical in assessing the severity of the alerts and the adversary's attack strategy [XN04].

Finally, Intrusion-detection systems are prone to alert flooding; i.e., they provide a large number of alerts to the operator, who then has difficulties coping with the load. This problem has been recently highlighted by the release of *stick* [Stick00] and *IDSwakeup* [IDSwakeup00], two tools that flood an intrusion-detection system with unrelated alerts, carrying an effective denial-of-service attack against the operator if the intrusion detection system manages to cope with the flux of anomalous events [DW01].

1.2.2 The predicament of Collaborative Defense System

It can be best summarized in the following sentences:

(1) The size and complexity of the Internet, including end host operating systems, make it likely that there will continue to be vulnerabilities in the future.

(2) Privacy issues complicate sharing of information on intrusion activity between networks, and while there are certainly anecdotal reports of specific port scanning methods and attacks, there is very little broad understanding of intrusion activity on a global basis.

(3) Because of these challenges, current best practices for Internet security rely heavily on word-of-mouth reports of new intrusions and security holes through entities such as CERT [CERT04] and DShield [DShield05].

1.2.3 Summary

From these remarks two general points become very clear: Firstly, we think that combining information from multiple detectors might help detection accuracy. Secondly, the automatic collaborative work will heavily rely on the quality of the responses mechanism.

The motivations behind the development of the Alert- Based Collaborative Defense system are intended to the following

(1) Provide an expansible structure which could efficiently be used both within a small local network and a combination of complicated networks within different enterprises.

(2) Build a system for detecting intrusions which span organizational boundaries.

(3) Permit organizations to work together to warn (or defend) each others without requiring them to give up local control over security policies or providing external organizations

with information which might itself present a vulnerability [FW01].

(4) Allow heterogeneous systems (both operating systems and detection systems) and heterogeneous networks to share information.

1.3 Goal

Our main goal is to build alert-based collaborative defense system. We propose a mechanism for network defense: a hierarchical network of lightweight combined with a distributed, collaborative intrusion detection environment. By security information sharing, the mechanism provides academia and industry with a wider array of information. The information helps them take the correct incident response activities. For that reason, we need mechanisms to share findings across end systems, and alert management and analysis facilities to add a network-wide perspective to the analysis. The Collaborative Defense Mechanism includes:

(1) Enhancing ID Sensor and Console: Amount and Capability

(2) Combining different organizations based on distributed intrusion detection (DID) framework

(3) Alert's analysis: Classify, Reduce, Warehouse, and Data Mining.

(4) Information sharing

1.4 The Overview of our study

The contribution of this thesis is two-fold. First, we propose a framework for collaborative defense by extending the original distributed intrusion detection model. This framework contains alert's collector, extractor, analyzer, report's generator, alert warehouse, alert's analysis and information sharing. The framework provides a solution to build effective cooperative security teams for academia and industry.

Secondly, we focus on Alert-based data source and enhance the analysis of alerts. As a result, we can deploy security system more widely and detect aggressor's behavior more accurately. Besides we develop a hybrid approach to share security information like raising the wolf smoke warning partners.

This thesis is organized as follows. We describe studies related to this work in Chapter 2. Chapter 3 proposes our collaborative defense framework and components and Chapter 4 describes the details of data schema, our methods for alert’s analysis and the use of shared information. In Chapter 5, we evaluate the feasibility of our framework and demonstrate the real worm defense example. We conclude the thesis and point out some future work in Chapter 6.

Chapter 2. Related Work

Our work falls into the research domain of collaborative security. The related researches include intrusion detection, distributed intrusion system, collaborative defense system, alert analysis, security information sharing mechanism and related techniques.

2.1 IDS

What is an Intrusion Detection System (IDS)? Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. Webster's dictionary defines an intrusion as "*the act of thrusting in, or of entering into a place or state without invitation, right, or welcome*." When we speak of intrusion detection, we are referring to the act of detecting an unauthorized intrusion by a *computer* on a *network*. This unauthorized access, or intrusion, is an attempt to compromise, or do harm, to other network devices.

Intrusion detection has been an active field of research for about two decades, starting in 1980 with the publication of John Anderson's *Computer Security Threat Monitoring and Surveillance* [Anderson80], which was one of the earliest papers in the field. Dorothy Dennings seminal paper, An Intrusion Detection Model [Denning87] published in 1987 provided a methodological framework that inspired many researchers and laid the groundwork for commercial products. Since then, several techniques for detecting intrusions have been studied.

2.1.1 The Type of IDS

An Intrusion Detection System (IDS) is used to detect abuses, misuses and unauthorized

uses in a network; more generally, they detect violations against the security policy of a network. They identify intrusions by spotting known patterns called signatures or by revealing anomalous behaviors of protected resources. So the intrusion detection techniques can be classified into two categories: *misuse detection* and *anomaly detection*. Misuse detection looks for signatures (i.e., the explicit patterns) of known attacks, and each matched activity are considered as an attack. Misuse detection can detect known attacks effectively, though it usually cannot accommodate unknown attacks. Anomaly detection models the subject (e.g., a user or a program) behaviors and each significant deviation from the normal behaviors is considered as the result of an attack. Anomaly detection has the potential to detect unknown attacks; however, it is not as effective as misuse detection for known attacks. In practice, both misuse detection and anomaly detection are often used as complementary components in IDSs [NJ+01].

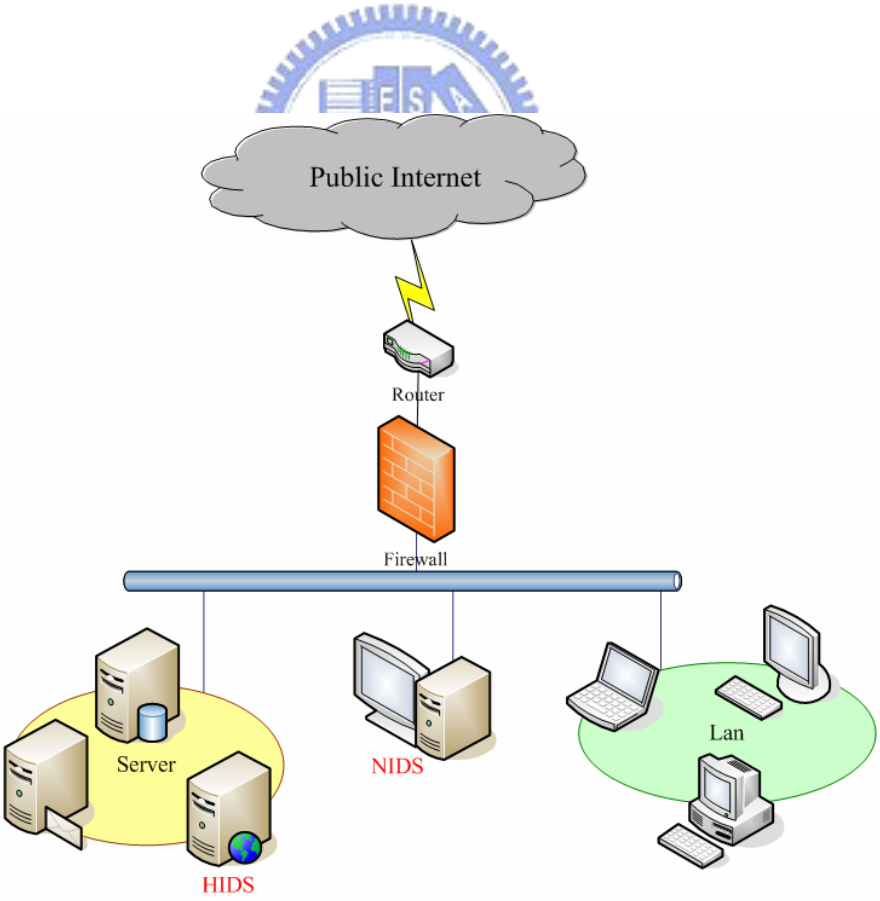


Figure 2-1: HIDS and NIDS

Intrusion Detection Systems (IDS) are classified by their functionality and are loosely grouped into the following three main categories: Network-Based Intrusion Detection System (NIDS), Host-Based Intrusion Detection System (HIDS) and Distributed Intrusion Detection System (DIDS). NIDS resides on a separate system that watches network traffic, looking for indications of attacks that traverse that portion of the network. A HIDS resides on a particular host and looks for indications of attacks on that host. The DIDS always deploys detection sensors widely located, remote control and report to a centralized management station.

2.1.2 Challenge of current IDS

One of the main weaknesses of intrusion detection is that the detection system can be overwhelmed by false alarms. Professional hackers can blast a network or system and desensitize the human monitors. It isn't uncommon for IDS to shut off alarms because they become a nuisance.

The challenges of current IDS include:

(1) The coverage and accuracy of your detection depends solely on the ingenious pattern description or signature definition corresponding to that specific point.

(2) Traditional IDS only probes at a point of a system. It has limited view of the whole system.

(3) Providing visibility into large networks requires a well-implemented system (with lots of expensive hardware).

(4) Large networks require many more sensors; it costs money to protect money. A poorly implemented solution adds little to the overall security. Current intrusion-detection system architectures make it difficult to achieve large-scale deployment.

(5) Attacks are likely to generate multiple related alerts. Current intrusion-detection

systems do not make it easy for operators to logically group related alerts [DW01].

(6) Single IDS (detector) can have false positives (false alarms) or false negatives (missed alarms). It only tells you YES or NO and usually can't tell you how much the alarm can be trusted.

(7) Single IDS (detector) is specialized for certain kinds of attacks. It only has limited view of the whole attack and less accuracy. An single attack could have multiple symptoms (cascaded attack)

2.1.3 Summary

About the above several points, we may use the network society group the strength, fast provides accurate patterns definition or rules description for the challenge (1). Many studies about alert's correlation [XN04] [MM+03] [DW01] [AL+04][NC+04][HS+04][Mi è ge02][CN+04][QL03][MD03] have proposed solutions for the challenge (5). As we shall see later in the next section, the distributed intrusion detection system gives a good choice to the challenge (2) (3) (4) (6) (7).

2.2 Distributed intrusion detection system

During the last decade, research in intrusion detection has developed different approaches to doing intrusion detection. There has been a shift from a centralized and monolithic framework to a distributed one. Spafford and Zamboni [SZ00] define such systems as distributed intrusion detection systems based on the location and number of the data analysis components.

2.2.1 Evolution of Framework

Centralized framework: Early distributed intrusion detection systems collect audit data

from distributed component systems but analyze them in a central place (e.g., DIDS [SB+91], Cisco NetRanger [Cisco01], and NetSTAT [VK98]). Although audit data are usually reduced before being sent to the central analysis unit, the scalability of such systems is limited due to the centralized analysis [NJ+01].

However, such a method does not scale well to large distributed systems, because information collected from a large distributed system may exceed the capacity of any single system and the intrusion detection related messages will take the network bandwidth.

Hierarchical framework: A few of the intrusion detection systems that adopt the distributed methodology are GrIDS [SC+96], EMERALD [PN97] and AAFID [22, 23]. All these systems are hierarchical in nature. The local intrusion detection components look for local intrusions and pass their analysis results to the upper levels of the hierarchy. The components at the upper levels analyze the refined data from multiple lower level components and seek to establish a global view of the system state [Gopalakrishna01].

For example, EMERALD [PN97] organizes IDSs for individual hosts under the IDSs for departments, which are under the IDS for the entire enterprise. The hierarchical approach scales better than the aforementioned centralized approach. However, it is not always the most efficient way to detect distributed attacks. For example, if two IDSs that are far from each other in terms of the hierarchy are designated to detect a known distributed attack, the data sent by them may have to be forwarded several times (to higher-level IDSs) before they can be finally correlated. Indeed, the two IDSs can communicate more efficiently if they directly talk to each other. Thus, it is worth further research to seek more efficient alternatives to the hierarchical approach [NJ+01].

In our study, we design a hybrid approach that includes hierarchical and peer-to-peer architecture. It will be suitable for our hierarchical organizations and decentralized network.

2.2.2 Benefits

The benefits of DIDS have

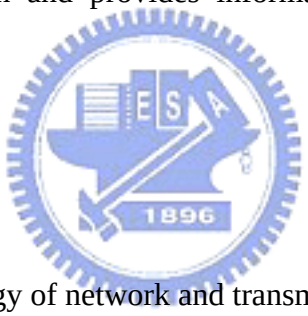
(1) It is good to carry out efficient wholly defense.

(2) It is suitable for heterogeneous network.

(3) It uses distributed and parallel processing concepts to reduce the system loading.

(4) It protects enterprise's internal and external online security, prevents the inner intrusion (Backdoor, Worm and Trojan), and avoids the internal staff deliberately destroying the network with abuses.

(5) It does local detection and provides information to perform global detection of intrusions.



2.2.3 Challenges of DIDS

The DIDS focuses on topology of network and transmission of data. It is faced with many challenges.

(1) The DIDSs mentioned above have not considered the cooperation mechanism between the enterprise departments. They are suitable for local network or single organization.

(2) DIDS often generates a very large number of alerts for practical attack scenarios. This large volume of alerts makes it difficult for a system administrator or even an automated intrusion response system to take appropriate actions.

(3) To counteract the problem about alert flooding, several researchers have developed alert correlation methods to construct attack scenarios and reduce alerts.

2.2.4 Summary

In this section, we discussed what framework is suitable for collaborative defense. The DIDS offers a very good infrastructure. But we need to overcome the challenges mentioned above.

2.3 Collaborative Defense

Having observed IDS and noticed DIDS, one can then go on to consider Collaborative Defense. We have concentrated on study about Architecture, Scale (Internet or local network), Data Source, Information's Sharing and Defense Mechanism. Besides, we pay more attention to Automated Trend or Threat Analysis.

2.3.1 FIRST

In 1990, U.S.'s National Institute of Standards and Technology (NIST), in conjunction with CERT/CC, CIAC, NASA, and other agency response teams, organized a cooperative activity known as the Forum of Incident Response and Security Teams (FIRST) at *http://www.first.org*. This coalition brings together a variety of computer incident response teams from governments, commercial organizations, and academic organizations. FIRST fosters cooperation and coordination in incident prevention, prompts rapid reaction to incidents, and promotes information sharing and learning among the members of its community [Masurkar03-2].

FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

2.3.2 DShield System

DShield.org – a research effort funded by SANS [SANS04] Institute as part of its Internet Storm Center [DShield05]. DShield's objectives include detection and analysis of new worms and vulnerabilities, notification to ISPs of exploited systems, publishing blacklists of worst offenders and feedback to submitters to improve firewall configuration [YB+03].

DShield is a distributed intrusion detection system. It provids a platform for users of firewalls to share intrusion information and collect crackers' activities from all over the Internet. It can be used to discover trends in activity and prepare better firewall rules.

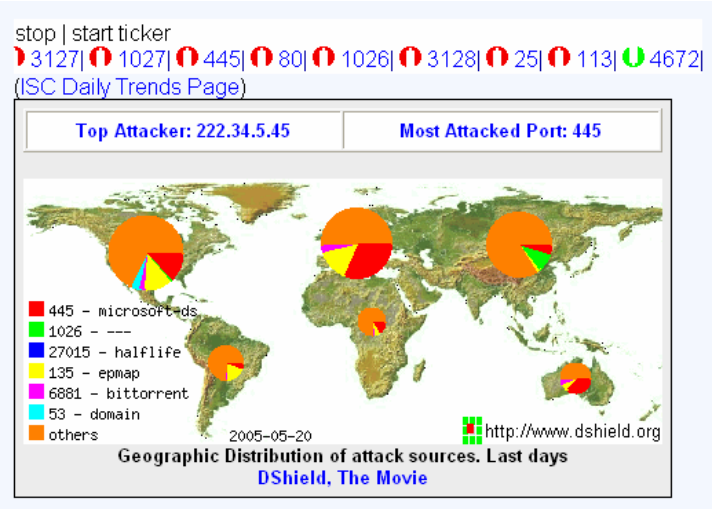


Figure 2-2: Internet Storm Center Status (DShield)

The analysis methods of DShield mainly have two: first is the statistics Top N which focus on the value of port and IP address, and the trend analysis which includes increasing (positive) or decreasing (negative) in activity, if the last two days are compared to the total dataset (about 33 days).

DShield has provided the "Block" list of networks, a ticker which reflects trends, and help users to fight back against attackers.

2.3.3 Computer Security Incident Response Teams

The definition of Computer Security Incident Response Teams (CSIRT) is that an entity with a security role or responsibility in a given organization has a communication and collaborative component. The tasks of CSIRT include Announcements, Vulnerability announcements and responses, Artifact analysis and response, Incident tracing, Intrusion detection, Security consulting, Risk analysis, Technology watch, Security process development, Collaboration and Cooperation with other internal or external related entities [WS+98] [Masurkar03-1].

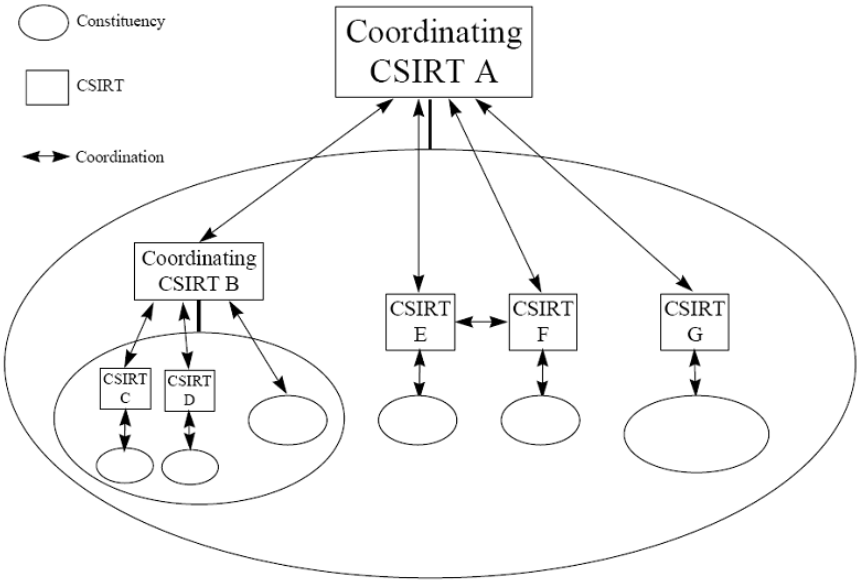


Figure 2-3: The Framework of CSIRT [WS+98]

The key points of CSIRT include:

(1) The source(s) and target(s) of system misuse, as well as the analysis of their behaviors.

(2) The evidence of supporting any analysis results.

(3) The scheme to document the incident investigation and analysis process.

(4) Facilitating the exchange of security information across administrative domains.

Table 2-1: Examples of CSIRT Types with Associated Missions and Constituencies [WS+98]

CSIRT Type	Nature of Mission	Type of Constituency Served
International Coordination Center	Obtain a knowledge base with a global perspective of computer security threats through coordination with other CSIRTs. Building a "web-of-trust" among CSIRTs.	Other CSIRTs around the world
Corporation	Improve the security of the corporation's information infrastructure and minimize threat of damage resulting from intrusions.	System and network administrators and system users within the corporation
Technical	Improve the security of a given IT product.	Users of the product

2.3.4 The European CSIRT Network

The European CSIRT Network (eCSIRT.net) is a Distributed IDS Sensor Network [European04]. Partners of the eCSIRT.net project provide the resources for a distributed IDS sensor network monitoring specific honeypot systems. As the sensors are distributed across Europe, the centralized analysis provides interesting trend information.

The tasks of eCSIRT.net are firstly to provide a forum for exchanging experiences and knowledge. Secondly, it establishes pilot services for the European CSIRTs community. Thirdly, it promotes common standards and procedures for responding to security incidents. They aim to

- Improve: Exchange of incident related data
- Add: Collection and Analysis of shared data
- Enable: Efficient cooperation

Information Exchange includes two categories, incidents and statistics.

(1) Incidents

Report the average number of incidents handled by a team in the respective time period. The value for "Incidents" is the sum of all registered incidents of the different categories.

(2)Statistics

a. Complete Statistics.

b. Daily stats of attacks seen by the sensors.

c. Monthly stats of attacks seen by the sensors.

d. Different kinds of attacks per attacker.

e. Hosts that attacked more than one sensor.

The following graph shows all alerts since the deployment of the IDS sensor network across Europe.

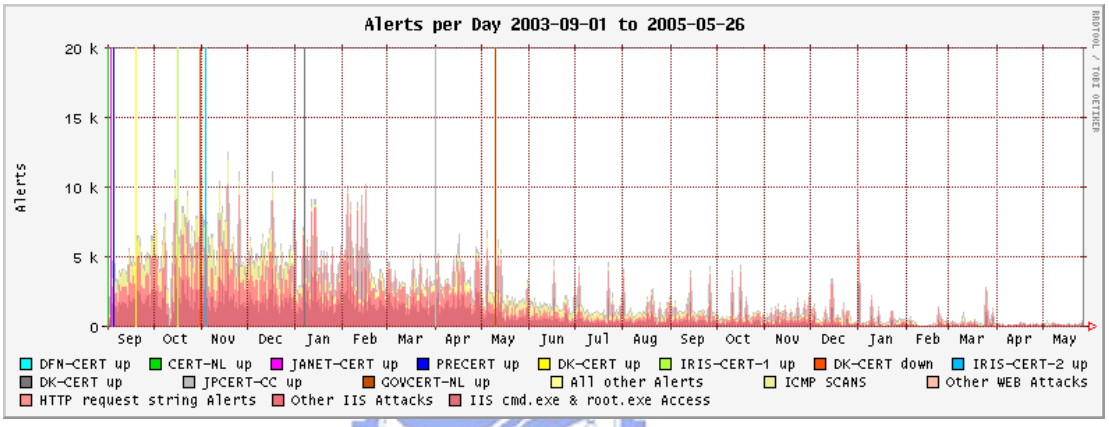


Figure 2-4: The Alert Statistics of eCSIRT

2.3.5 JPCERT/CC ISDAS

JPCERT/CC watches network traffic and reports trend information on their web site. The ISDAS is Internet Scan Data Acquisition System. JPCERT/CC has started deploying the ISDAS since the fiscal year 2003. ISDAS [JPCERT04] has a wide distributed arrangement of sensors, and observes various scan activities: worm infections, probing vulnerable systems, etc.

It provides the summarized scan trends observed on the web page. Moreover, the observed data are used as a basis of JPCERT/CC activities on publishing alerts and advisories, security awareness programs, etc.

2.3.6 Symantec DeepSight™

Symantec DeepSight™ threat management system [DeepSight05] is an example of a centralized scheme, where sites can opt-in and share their IDS alerts. The characteristics of DeepSight™ include

(1) Monitors vulnerabilities in more than 18,000 technologies, operating systems, and application product versions from 2,200 vendors.

(2) Vulnerabilities monitored 24x7.

(3) Enabling secure Web-based queries to an industry-leading vulnerability database.

(4) Prioritized alerts.

(5) Current and historical alerting and response reports.

(6) Administrative user status giving control over subordinate users in order to share information, collaborate for early mitigation, and increase accountability.

(7) Alert status tracking streamlines task assignment and reporting by providing status and documenting resolutions.

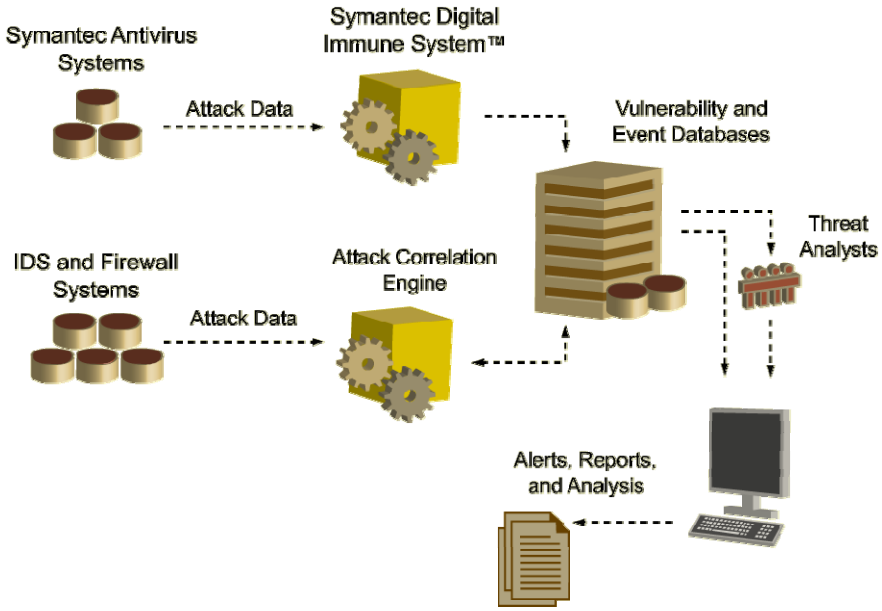


Figure 2-5: Architecture of Symantec DeepSight™

2.3.7 Information Sharing

It is important for collaborative defense to share information in order to discover attacks involving multiple organizations. Sharing information among intrusion detection systems (IDSs) is important, especially for the purpose of detecting coordinated intrusions and intrusions distributed across a set of hosts and network elements.

At present the Information Sharing solution mainly has two kinds; the first kind is Web-based information like FIRST, DShield and JPCERT/CC ISDAS, and the second kind is XML messages like CSIRT and eCSIRT.

In order to exchange incident handling information unambiguously between CSIRTs a common language is required. It is the responsibility of each team to translate the message to a local database format that is suitable for the incident tracking system used by each team. Furthermore, the messages are machine readable, and thereby departing from the current best practice of exchanging advisories in ASCII between the teams by the means of electronic mail. Due to the nature of the problem being investigated, XML is viewed as fundamental building

stone both to provide the document structure and multi-lingual capabilities.

Although there has been some ongoing research on infrastructure and language support that allows IDSs to share event data and analysis results with each other (e.g., Common Intrusion Detection Framework (CIDF) [ST+98] and IETF's Intrusion Detection Exchange Format (IDEF) [CD01]), there is no framework for an IDS to either request from or send to another IDS data that are relevant to specific events.

IETF's Intrusion Detection Working Group (IDWG) has been working on data formats and exchange procedures for sharing information among IDSs, response systems, and management systems. XML has been chosen to provide the common format and an Intrusion Detection Message Exchange Format (IDMEF) has been defined in an Internet draft [CD01].

The Incident Object Description and Exchange Format (IODEF) [HS03] is compatible with IDMEF and is capable of including IDMEF message into Incident Object. Current IODEF implementation provides two options: to use IncidentAlert class container to wrap up Alert/IDMEF and to decompose Alert/IDMEF message into Incident/IODEF classes.

The IODEF is more human (interface/interaction) oriented, human readable, but machine parsable. Incident Object has longer lifetime compared to one time use of IDMEF message. IODEF is helpful to the incident handling (reporting, investigation, etc.), incident storage, statistics and trend analysis.

2.3.8 Summary

These systems focus on Automated Trend or Threat Analysis, such as DShield, FIRST systems, and other Threat Management System, such as SANS [SANS04], DOMINO [YB+04]. There are benefits as the following:

(1) Global View:

Providing Global statistical information, these systems focus on the development of

a quantitative characterization of intrusion activity in the global Internet.

(2) Teamwork

They provide a simple collaborative mechanism over Internet scale.

(3) Security knowledge sharing

With information exchange, they take Web based Information (DShiled, FIRST) or XML Message (CSIRT, eCSIRT).

These systems have some drawbacks:

(1) The data source is low-level Network packets (OSI Layer 1 to 3).

(2) They do not suit the small and medium-sized enterprise or the school organization.

(3) Trust between members is not easy to establish.

(4) Some are expensive.

2.4 Alert Correlation

Timing and correlation information might be useful for estimating speed of propagation of attack. There is no consensus on the definition of correlation for intrusion detection. There are at least five different definitions:

(1) Correlation of events within one log.

(2) Correlation of events between homogeneous logs on the same network.

(3) Correlation of events between heterogeneous logs on the same network.

(4) Correlation of events between homogeneous logs on different networks.

(5) Correlation of events between heterogeneous logs on different networks.

In this thesis we focus on definition (4).

Managed security service providers sell protection based on definitions (2) and (3). With there being so many attacks on the Internet, there are several organizational/commercial websites where you can submit log files for correlation in the meanings of (4) and (5), and they report what they find back to the source as well as overall trends to the larger Internet community [AL+04].

Now several researches have developed alert correlation methods to construct attack scenarios and reduce alerts, such as EMERALD [PN97] and TIAA [NC+04].

2.5 Summary

We have constructed the feasible plan step by step and gradually studied intrusion detection, distributed intrusion system, collaborative defense system, security information sharing mechanism and alert analysis. We clearly see the following several problems and try our best to propose some solutions.

(1) What kind of collaborative defense mechanism is suitable to academic network?

(2) How to decide work division between the cooperative organizations? How to make proper response policies?

(3) How to avoid alert flooding under our framework?

(4) How to take advantage of Alerts? What is its value?

(5) How to share security information? What is information to share?

Chapter 3. Framework

As mentioned above, the collaborative defense system that is operating at present can't meet the demand of medium and small-scale organizations. Therefore we propose a system framework for the network administrators. We have referred to related studies about distributed intrusion detection and CSIRT to outline our approach to the problem.

We may consider the subject under three headings: (1) Definition (2) Operational Requirements (3) Architecture Design and (4) Data Schema.

3.1 Definition

3.1.1 Event and Alert

In the intrusion detection field, event and alert are generally two distinct concepts. An event is a low level entity (TCP packet, system call, syslog entry, for example) from which an analysis is performed by a security tool. An alert is a message from an analyzer signaling that one or more events of interest have been detected. We say that an alert is a kind of event, since it reflects the state of IDS [MM+03].

3.1.2 Incident

An incident is an unauthorized use or abuse of the protected system. We have followed CLCSI [BJ+04] that defines an incident taxonomy based on three key concepts: *events*, *attacks* and *incidents*.

(1) An event is an *action* directed at a *target* that is intended to result in a change of state of the *target*.

(2) An attack is defined as a sequence of actions directed at a target taken by an *attacker* making use of some tool exploiting a computer or network vulnerability.

(3) Finally, an incident is defined as a set of attacks carried out by one or more attackers with one or more goals.

In brief, an alert is a message passed from a detection mechanism when it matches an event to a known pattern. In most incidents, the first piece of information that an analyst reviews is an alert.

3.1.3 Vulnerability

Vulnerability is a flaw in a target that could allow an unauthorized result. Knowing the vulnerabilities in our network is the main source of knowledge to automatically decide whether a given alert corresponds to an innocuous attack or not. We have incorporated common vulnerabilities and exposures (CVE) dictionary provided by the MITRE Corporation into our framework [MP03].

3.1.4 CSIRC

We will use the term "CSIRC" to refer to "Computer Security Incident Response Center". We design a component called CSIRC in every collaborative organization. The CSIRC is responsible for coordinating sensors, collecting alerts, analyzing alerts, data warehousing and reporting.

3.1.5 ABCD System

The abbreviation is called ABCD for our Alert-Based Collaborative Defense System.

3.2 System Requirements

These requirements focus on the interaction of the entire collaborative defense system with the viewpoint of management. Such management environments are often capable of handling hundreds of alerts per second. Basically, the intrusion detection system must *integrate* with the management platform, and ensure an easy *configuration* and a certain level of *performance*. But the requirements of collaborative defense system are more and complicated. It must contain *collaborative, modularity, scalability, heterogeneity, availability, and decentralization.*

(1) Collaboration

It permits organizations to work together to warn (or defend) each other's security system.

(2) Modularity

It provides an expansible structure, which could efficiently be used both within a small local network and a combination of complicated networks within different enterprises.

(3) Scalability

The system architecture makes it easy to achieve large-scale deployment. The communication mechanism is one of the bottlenecks to the scalability of IDS.

(4) Heterogeneity

It must allow heterogeneous systems (both operating systems and detection systems) and heterogeneous networks to share information

(5) Availability

It is cheap and easy to set up and use, so we take the free and ready-made open source tools to design the system.

(6) Decentralization

In order to reduce the waste of processing time, storage and network bandwidth, we propose hybrid approach that includes hierarchical and P2P architecture. It can improve the centralized intrusion detection mechanism and be adapted to the different scale network environments. No node is more important than any other.

3.3 Architecture Design

In this section, we present an approach to organizing autonomous but cooperative component systems to detect distributed attacks and exchange information. Our approach is based on the dependency among the distributed alerts in a signature. Unlike the hierarchical architecture, we organizes the cooperative IDSs according to the intrinsic relationships between the distributed alerts involved in attacks, and, as a result, a Local CSIRC needs to send a piece of information to Global CSIRC only when the information is essential for detecting the outer attackers.

The target of our design aims mainly at the academic use as well as at industrial purpose. It can cooperate with the hierarchical structure of enterprises and take the limitation of network's bandwidth into consideration.

3.3.1 Collaborative Defense Model

Firstly, we propose a basic and hierarchical model for constructing Collaborative Defense System. We can represent the model in a simple diagram as follows:

Inside the Collaborative Defense Model, Several companies or schools organize Computer Security Incident Team (CSIRT). The CSIRT cooperates by using a hierarchical

communication framework. This cooperation is driven by interests expressed by the CSIRTs.

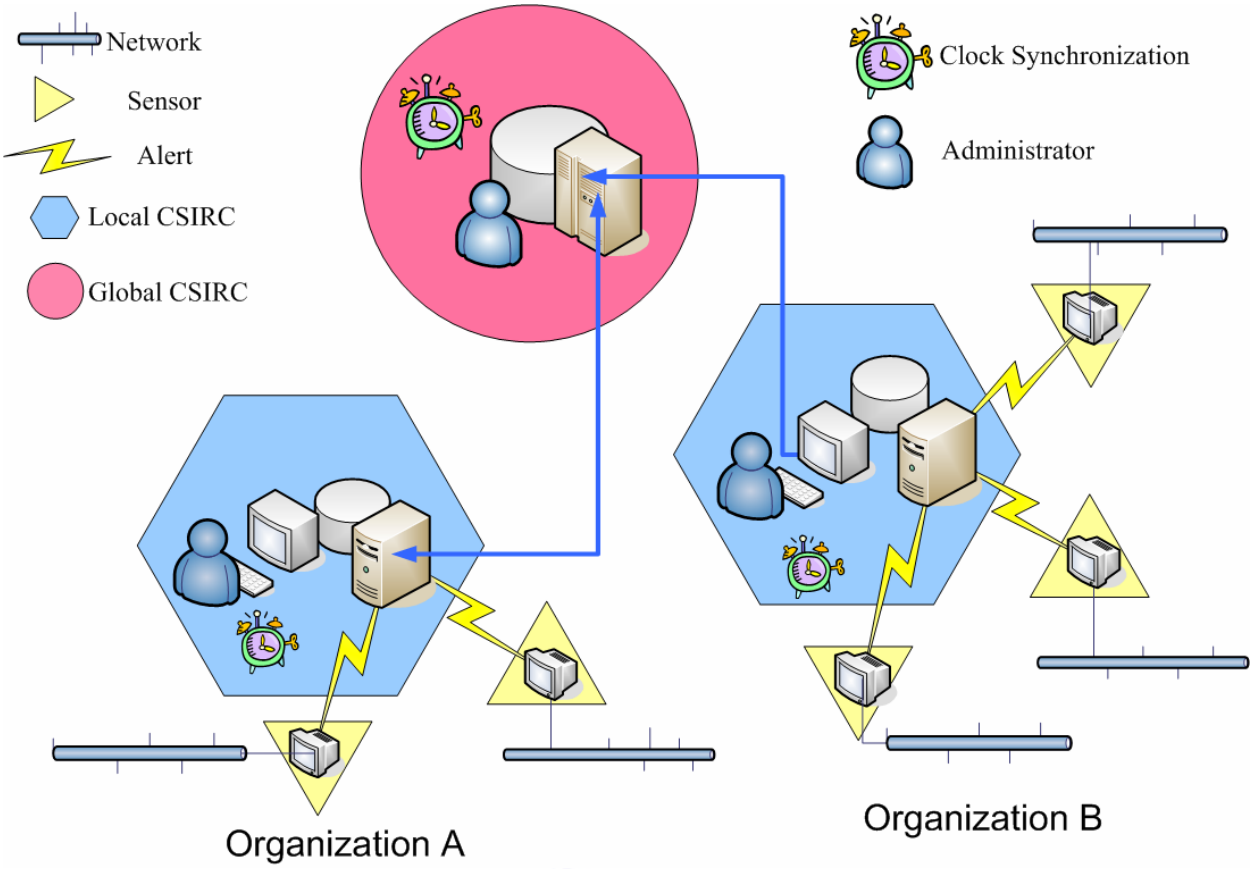


Figure 3-1: Collaborative Defense Model

This model can divide two levels: *Local View* and *Global View.*

Level 1: Local View

Here we present a framework for doing distributed intrusion detection with centralized analysis components. We design a local CSIRC to collect alerts data from sensors which are deployed in different sub network of organization. Then the local CSIRC extract, store and analyze these alerts, and send the alert selected to global CSIRC.

- As Figure 3-1 shows, the red circle represents global CSIRC, the blue hexagons are local CSIRC, and the yellow triangles indicate IDS sensors.
- Establish a Global CSIRC to coordinate the sub-organizations.

- Install the CSIRC component in every organization.
- Set up the IDS's sensors in different sub networks.

Level 2: Global View

CSIRTs cooperate by using a hierarchical communication framework. The local CSIRCs report information to the global CSIRC. It is a very important task for the global CSIRC to coordinate the members of CSIRT. The purpose of the global CSIRC would be to offer a means to coordinate intelligence related to possible cyber attacks and provide a conduit to warn collaborative organizations that such attacks may take place. The Global CSIRC plays a security consulting role serving as a clearinghouse for security information.

Because our collaborative defense system seeks to determine the time sequence of alerts resulting from the threat across multiple organizations, synchronization of clocks among the involved hosts is necessary. The degree of synchronization needed depends on the time granularity expected. The use of NTP [Mills92] should be sufficient to meet such requirements [GS01].

3.3.2 Computer Security Incident Response Center

Let us introduce the components of Computer Security Incident Response Center as following. And please refer to the Figure 3-2.

(1) Collector

The component of Collector is responsible for collecting the alerts from sensors. Then the collector puts alerts to a temporary storage called "Alert Pool," due to the consideration of decreasing processing time and increasing storage capacity before the system collect huge alerts.

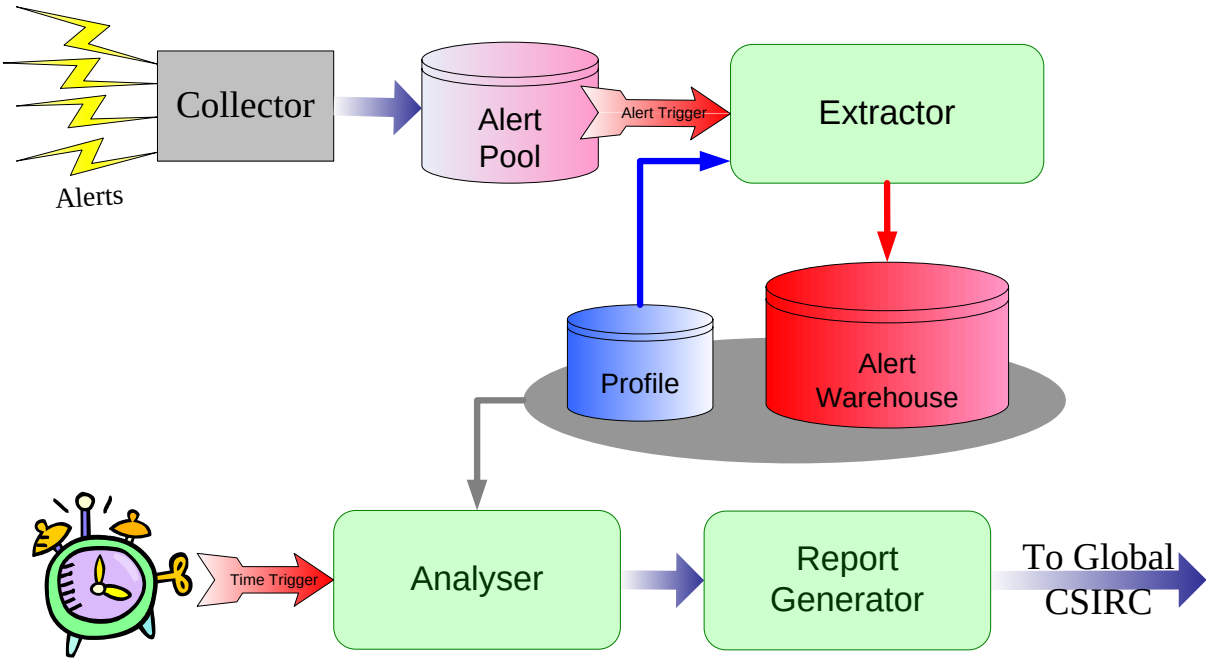


Figure 3-2: Computer Security Incident Response Center

(2) Extractor

When Alert Pool receives alerts, it will trigger the extractor. The main task of Extractor is to extract alerts according to the definition of local profile. By the way, we can reduce, filter and classify alerts in order to prepare for long-term analysis.

(3) Analyzer

The second stage focuses on the data analysis of long-term alerts. The Analyzer component makes periodic analysis of alert, such as per hour or per day. The analysis method may be divided into two categories: statistics method and data mining. The purpose of the analysis is to summarize the alerts and look for the abnormal threat.

(4) Reporter

The Reporter reports to Global CSIRC the abnormal alerts as well as the result of analysis. At the same time, it shares information with other Local CSIRC on suspicious alerts and determines when to be more vigilant or more relaxed.

3.4 Data Schema

In data treating processes, the jobs of data transformation and storage play a very important role.

3.4.1 Alert Pool

The Alert Pool provides a temporary storage for IDS's Alerts. The design purpose is to avoid too many alerts simultaneously resulting in processing time not enough. Therefore, we have designed one more collection tier. The alert data are saved in the original IDS's alert format.

For the detailed Alert Pool Schema [Snort05], please see Appendix A.

3.4.2 Profile

In the profile, we can find specification about sub-network, including basic information of network administrator, sensors, hosts, and network. The profile describes the environment of the network, just like to build a model. Properly modeling the network allows the importance of each alert to be correctly assessed. Furthermore, the profile offers data for extraction and analysis, for instance, to classify the alerts or determine whether they are false alarms. Therefore, the data in the profile are like a "White list" which tells us what's normal.

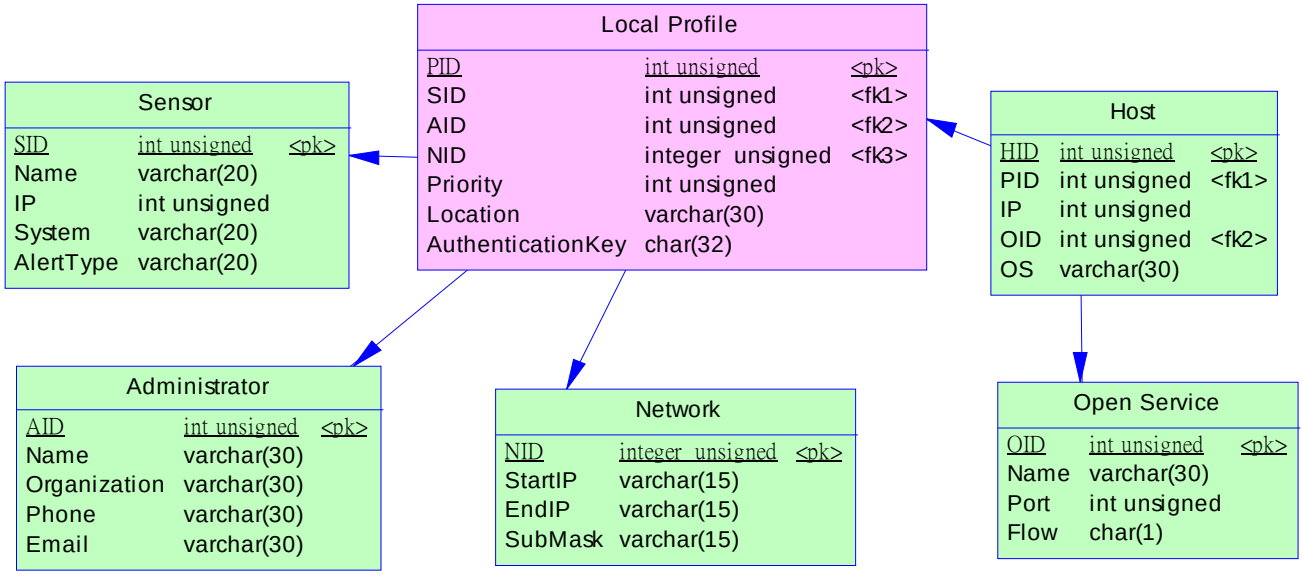


Figure 3-3: The Schema of Profile

3.4.3 Alert Warehouse

The objectives of the long-term data warehouse resemble those of the original data management. The alert warehouse can provide evidence for *computer forensics* and serve as data source for future *data mining*.

For the detailed Alert Warehouse Schema, please see Appendix B.

3.5 Summary

We propose a system framework for the collaborative defense (CD). It can be described by the CD model which is divided into two viewpoints, local view and global view. The main component in the kernel is *CSIRC* which includes *Collector*, *Extractor*, *Analyzer*, and *Reporter*. They have completed two work stages: short-term processing by alert trigger and long-term analyzing by time trigger. Furthermore, we carefully design the data schema of database, such as alert pool, profile, alert warehouse, and report.

Chapter 4. Alert Data Processing

The following sections elaborate on alert extraction, alert analysis, and information sharing of our architecture and discuss in detail the implementation of our ABCD system.

4.1 Alert Extraction

As mentioned in related works, on any given network, on any given day, any IDS's sensor can fire thousands of alerts. How can we deal with so many alerts? How can we find the real threats and vulnerabilities?

We have designed a component of *Extractor* to do extraction of alerts. The Alert Extraction functions act as the module of classifying, filtering, labeling, and aggregating. It will solve the following problems:

(1) Work division between the cooperative organizations.

(2) How to make proper response policies.

(3) How to avoid alert flooding.

At the same time, alert extraction might be useful for estimating speed of propagation of alert.

4.1.1 Alert Classification

From the administrator's viewpoint, it is very important to deny attacks from outside and try to find victims inside. Based on the principle of responsibility division, we classify alert in a simple way and make different policies reacting to different categories of alerts. We divide alerts into three categories according to the sources and the targets in Table 4-1.

Table 4-1: Alert Response Classification

Source / Target	LAN	WAN
LAN	A1 Inner Alerts	A3 Outer Alerts
WAN	A2 Inner Alerts	Exceptions

Description of these four categories of alerts is as follows:

(1) *The first category of alerts (A1)*

Both of the sources and the targets are the computers inside the organization. They are classified as inner attack events. For this kind of alerts, our response policy is to notify the users to carry on safety inspection and patch mending.

(2) *Second category of alert (A2)*

The inside computer attacks the computer outside. The reason for the attack is the computer may be infected by Worms or Trojans; perhaps it is the misuse of the users.

The response policy of A2 alert: Notify users to carry on safety inspection and patch mending. A1 and A2 are the inner events which the administrator must eliminate the vulnerabilities immediately. They are the responsibility for the local administrator.

(3) *Third category of alert (A3)*

A3 alerts are the outer event which should be blocked from WAN and reported to the global CSIRC.

The response policies of A3 alert: First, undergo the safety and vulnerabilities inspection for the victims. Secondly, we will act as a defense against the threats; for example, establish the rule of firewall to keep out the attackers. Thirdly, notify this kind of incidents to other cooperative organizations.

Others: Exceptions

Besides the three kinds mentioned above, there are some exceptions. For instance, the sources of the attack may not be in the range defined by the profile.

The response policy of exceptions: Notify the administrator to check the detail of alerts. They are the responsibility for the local administrator

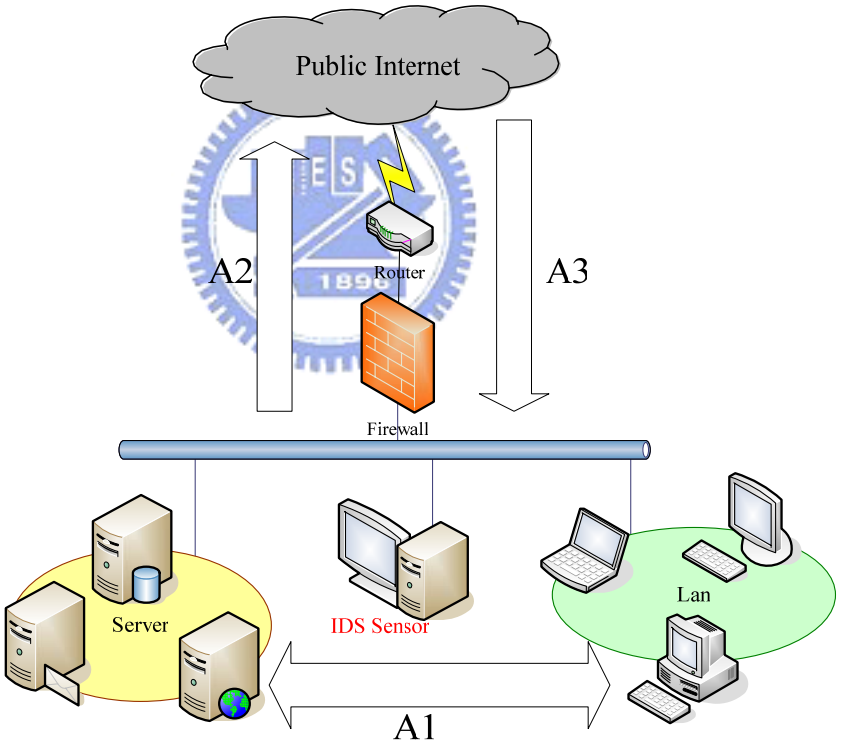


Figure 4-1: The Flow of Alerts

4.1.2 Rules of Extraction

To extract alerts according to the definition of the profile might be useful for estimating the speed of propagation of attack information.

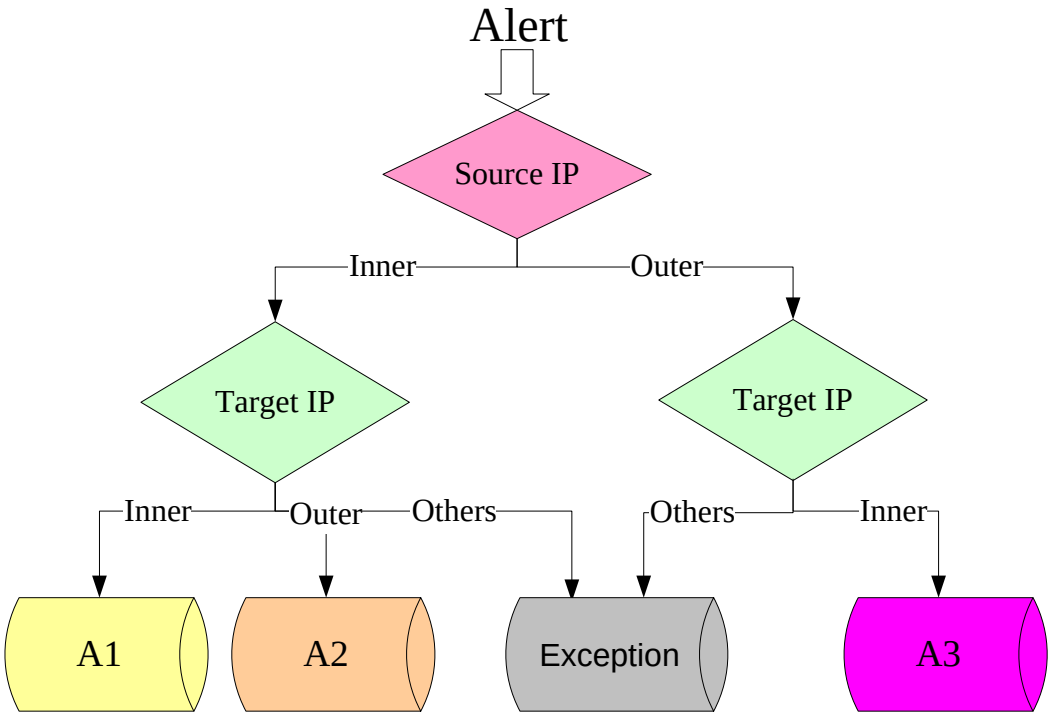


Figure 4-2: Each alert is assigned exactly to one alert type

The rules listed below can be combined as the Expert System to make the task of extraction more flexible.

Rule 1: Classification

Each alert is assigned exactly to one alert type, as shown in Figure 4-2.

Rule 2: Priority

If Local.Priority or Alert.Priority=high then send alert to Administrator and Warehouse and Labeling “urgent”.

Rule 3: Source IP

If SourceIP included in LocalIP then send to Exception and Labeling “Inner event”.

Rule 4: Target IP

If Target IP included in LocalIP then send alert to Warehouse and Labeling “defend”

Else send to Exception.

Rule 5: Target Port

If TargetPort included in Port.WhiteList send to Warehouse and Labeling “service attack”

Else send to Exception and Labeling “try attack”

4.2 Alert Analysis

The alert analysis is a very extensive research issue. As mentioned earlier, there are a lot of ways in the analysis of alert.

Alert analysis is an investigation into a network incident. In order to assess the risk to your organization as well as to evaluate the impact of the incident and take actions to mitigate the threats, we make use of two simple methods to analyze alert data, trend analysis and association rule analysis.

4.2.1 Trend Analysis

In typical collaborative defense system, such as DShield, it provides the statistics of Top N and the trend analysis which includes increasing or decreasing in activity, and fetches the threshold from the dataset in the past thirty-three days.

In this thesis, we pay attention to the quantitative changes of threats and vulnerabilities. The special propose for the analysis of the trend is the selection of threshold. The using of network in school usually has periodicity; for example, we have less flow during weekends, winter and summer vacations but higher flow when in class and working hours.

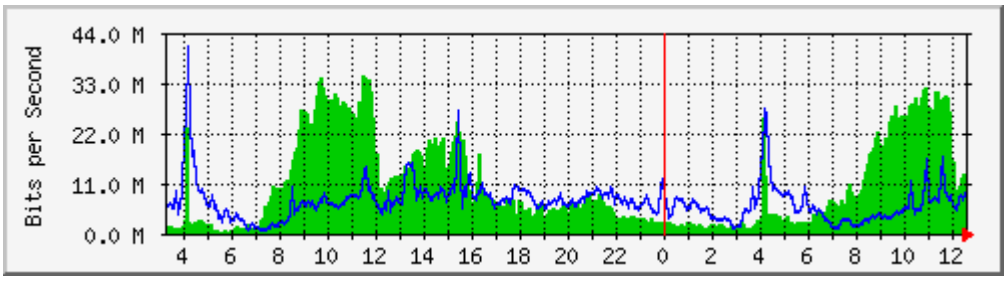


Figure 4-3: The daily flow of Educational Network

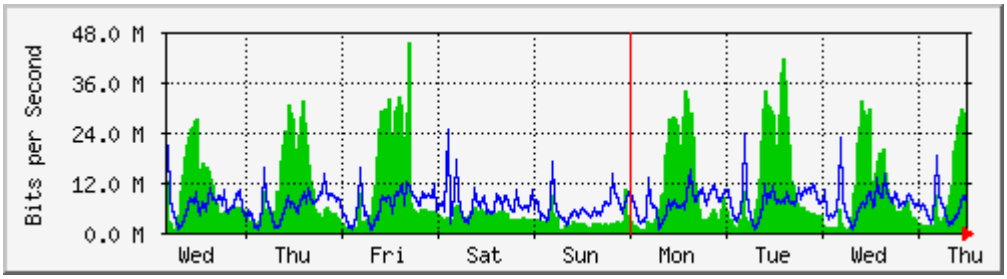


Figure 4-4: The weekly flow of Educational Network

Therefore, in making the choice of threshold value, we can't only take the statistics calculated in the past few days into account. We must consider the pattern of the cycle. For example, to determine the threshold value for Monday, we fetch the statistics value of the past eight weeks.

(1) Day Trend: Calculate median from the previous eight weeks.

(2) Week Trend: Calculate median from the past six months.

Our trend analysis focuses on the amount and categories of alerts, the variation of the amount, and the first offense of alerts.

4.2.2 Association Rule Analysis

Association analysis is the discovery of association rules showing attribute-value conditions that occur frequently together in a given set of data. It can help us find the frequent co-occurrences of attribute values belonging to different attributes that represent various alerts. For example, through association analysis, we may find many MS-SQL Worm attacks are from the source IP address 61.159.15.X to the target IP address 140.126.167.Y at the

destination port 1434.

When performing association analysis, there are two input parameters. The first is the set of alerts (represented by the Alert collection ID, AID), and the second is the support threshold. Given a set S of alerts and a support threshold t%, a frequent attribute set A1=a1 ^ A2=a2 ^ ... ^ An=an (A1, A2, ...,An are attribute names, and a1, a2, ..., an are attribute values) denotes that there are at least t% of the alerts, where their attribute values satisfy A1=a1 ^ A2=a2 ^ ... ^ An=an [NC+04].

After association rule analysis, we can get the results of frequency, support and confidence for alert type and the sources. A sample result of association analysis is as follows.

	Body	Implies	Head	Support(%)	Confidence(%)
1	Alert = [4]	==>	Dest = [2357110763] AND DPort = [0] AND Source = [2357110750]	85.639	99.924
2	Dest = [2357110763]	==>	Alert = [4] AND DPort = [0] AND Source = [2357110750]	85.639	99.981
3	DPort = [0]	==>	Alert = [4] AND Dest = [2357110763] AND Source = [2357110750]	85.639	96.738
4	Source = [2357110750]	==>	Alert = [4] AND Dest = [2357110763] AND DPort = [0]	85.639	99.942

Figure 4-5: A sample result of association analysis

4.2.3 Advance Analysis

Two alert analysis mentioned above are just two most well-known techniques. We can get more detailed anomaly information from alerts with the choice of features. For examples:

(1) An outside host/subnet contacting many inside hosts, may be a sign of an anomaly (e.g. DDoS attack)

(2) An inside host contacting many outside hosts, and should be further analyzed as it

may be a sign of an anomaly (e.g. compromised host trying to compromise outside hosts by exploiting vulnerability).

(3) Increased bandwidth consumption may be a sign of a misuse (e.g. the use of company resources to download excessive media content).

(4) Asymmetry a node with in/out unbalanced network connections may be a sign of a DoS attack [AL+04].

4.3 Information Sharing

It is important for collaborative defense mechanism to share information in order to discover attacks involving multiple organizations.

4.3.1 Information sharing flow

Please refer to Figure 4-6. The Local Layer consists of many Local CSIRCs and the Global Layer consists of many Global CSIRCs. At the same layer, these CSIRCs can share information with each other. The Local CSIRCs publish the A3 alerts to the Global CSIRC in the same collaborative defense team. Furthermore, the Local CSIRCs can subscribe the results of analysis from other CSIRCs and observe certain system behaviors. With the cooperation between the Local CSIRC and the Global CSIRC, the information sharing flow is established by the Alert-based content publishing and subscribing.

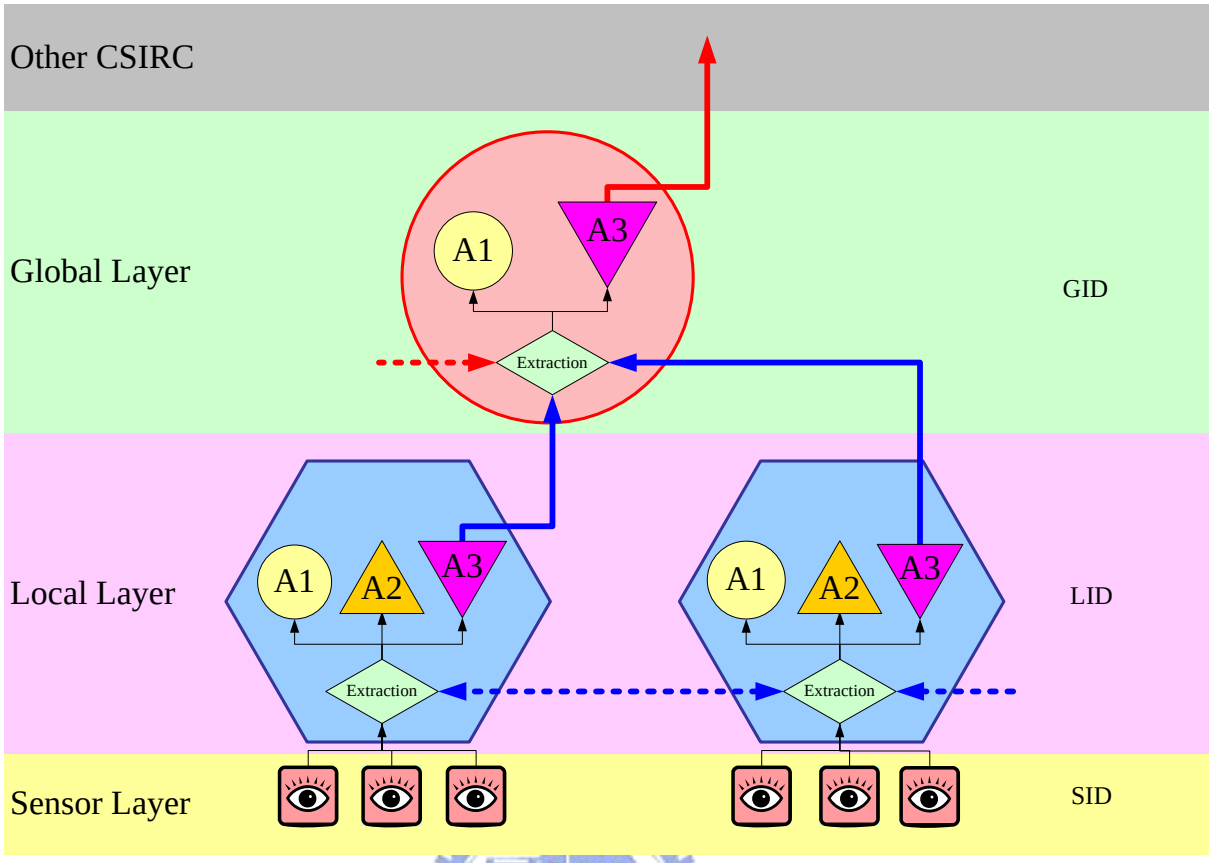


Figure 4-6: Information sharing flow

4.3.2 What to share

From the Local CSIRC to the Global CSIRC, the sharing information mainly are A3 alert, including the alerts of vulnerabilities and the summaries of security. The summaries of security are represented by the regular report which consists of attack source, alert signature, high support value alert and high confidence alert.

From the Global CSIRC to the Local CSIRC, the information of feedback mainly are the outer threats represented by the Top N statistics of alerts and attackers. The Global CSIRC plays a security consulting role serving as a clearinghouse for security information. It can provide solutions and security knowledge of alerts for the CSIRT's members. Furthermore, it can provide more suitable policies for Firewall, such as submit blacklists (a list of suspicious addresses), and more efficacious detection rules for IDS.

4.3.3 Report Format

Our ABCD system is based on the alert data. The signature of alert has been embedded with the service, port, protocol and payload. So a signature ID number can represent these detail data and simplify the report format.

When we make reference to the formats of IDMEF and IODEF, we find both their advantages and disadvantages. The formats are complicated and some fields are optional. However, it's worthwhile to use the XML format. So we simplify the format and design the structure of reports as follows:

WHAT: Nature of alerts. (*Signature ID*)

WHERE: Attacker information on the sources of alerts. (*Source IP*)

WHO: Victim information on destination of alerts. (*Target IP*)

HOW: Method of attack, analysis of the incidents. (*Signature Name*)

WHEN: Start Time, End Time. (*Duration*)

PROOF: Evidence, support for incident analysis. (*Support, Confidence Value*)

OWNER: Authority, incident creator. (*Administrator*)

Extension mechanism: Additional Data.

4.4 Summary

Let me summarize the main points that have been made in this section. By the simple classification, filtering, labeling and aggregation, the alert extraction has defined methods to make work division and make response policies between the cooperative organizations. At the

same time, it is useful to avoid alert flooding.

If we plot an Alert Map (Source IP vs. Target IP) with the alert classification of the two organizations (IP Address: 163.19/16 and 140.113/16), we shall get the figure as followed. It can be clear to find out how the different types of Alert distribute.

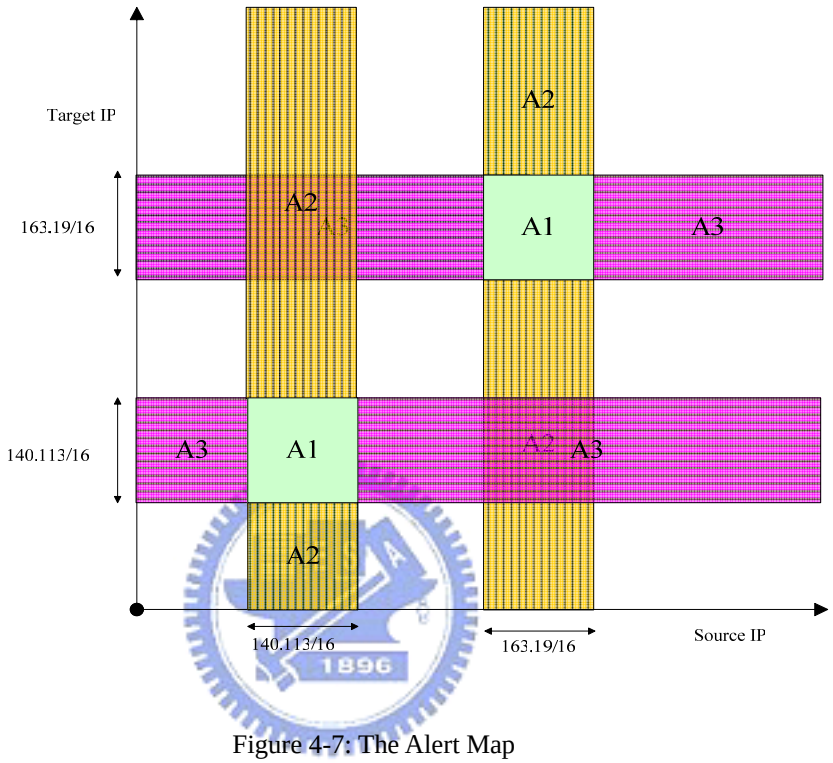


Figure 4-7: The Alert Map

The trend analysis of alert in Global CSIRC can provide the local members information about the overview of Internet and prediction of threats. The association rule analysis of alert in Local CSIRC can provide the evidence with support value and confidence value. Moreover, it helps us find the relationship between alerts.

By the security information sharing, the members of CSIRT can obtain the solutions of defense, such as blacklists, detection rules, and security knowledge about alerts. By the way, it can help members evaluate the impact of the threats and take proper actions to mitigate the risk.

Chapter 5. System Evaluations

5.1 Environment

Our experiment environment is set up in the academic network. We organize an experimental CSIRT for the evaluation of the Alert-Based Collaborative Defense (ABCD). The members of CSIRT include KDE Lab in NCTU, Hukou High School, HsinChu County Network Center, two primary schools and two junior high schools in HsinChu County.

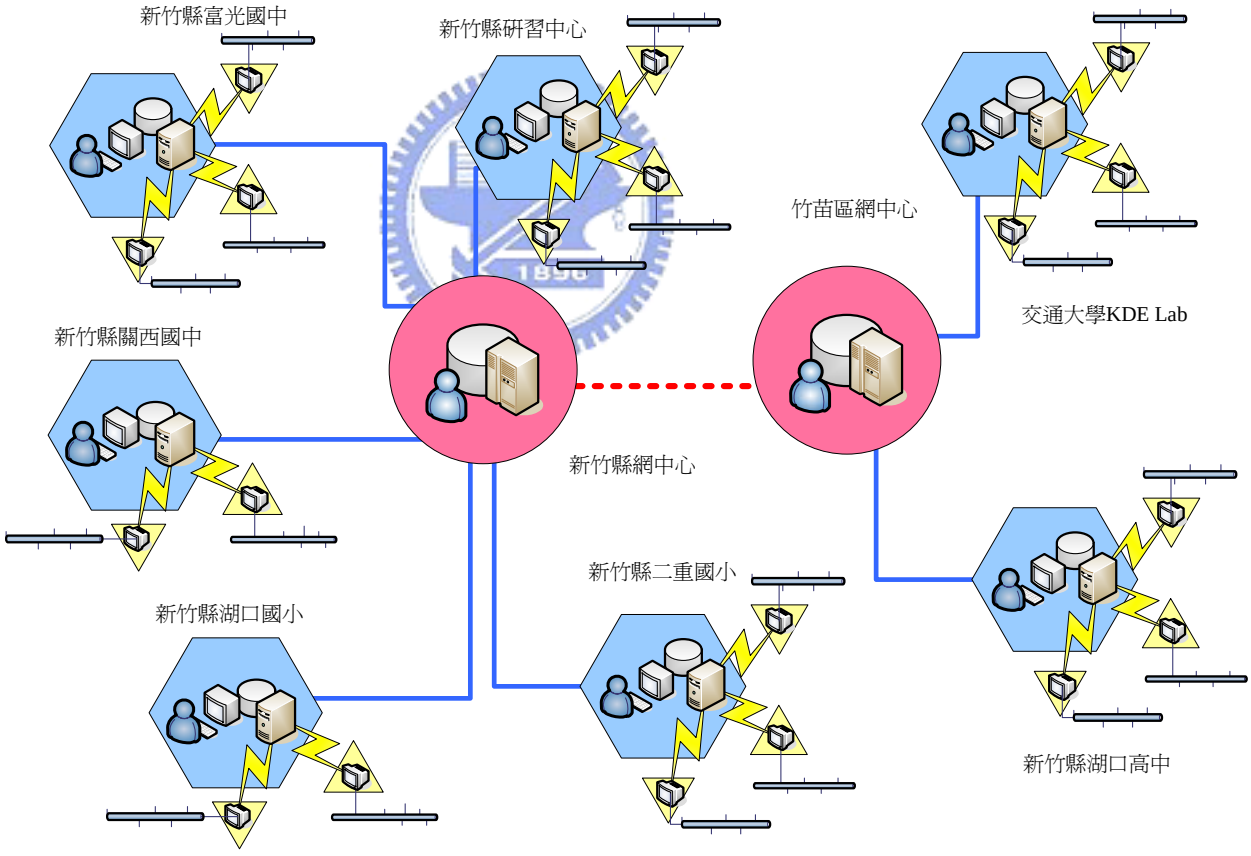


Figure 5-1: Our Experimental CSIRT

The design of messages flow is done according to the physical topology of the network and the intrinsic relationships between these organizations.

On the other hand, we also deploy the ABCD into the campus, as shown in Figure 5-2. In the environment of high school, firstly we deploy the IDSs in the different buildings, such as the library, offices, computer classrooms, and the network center. The center CSRC collects and extracts alerts.

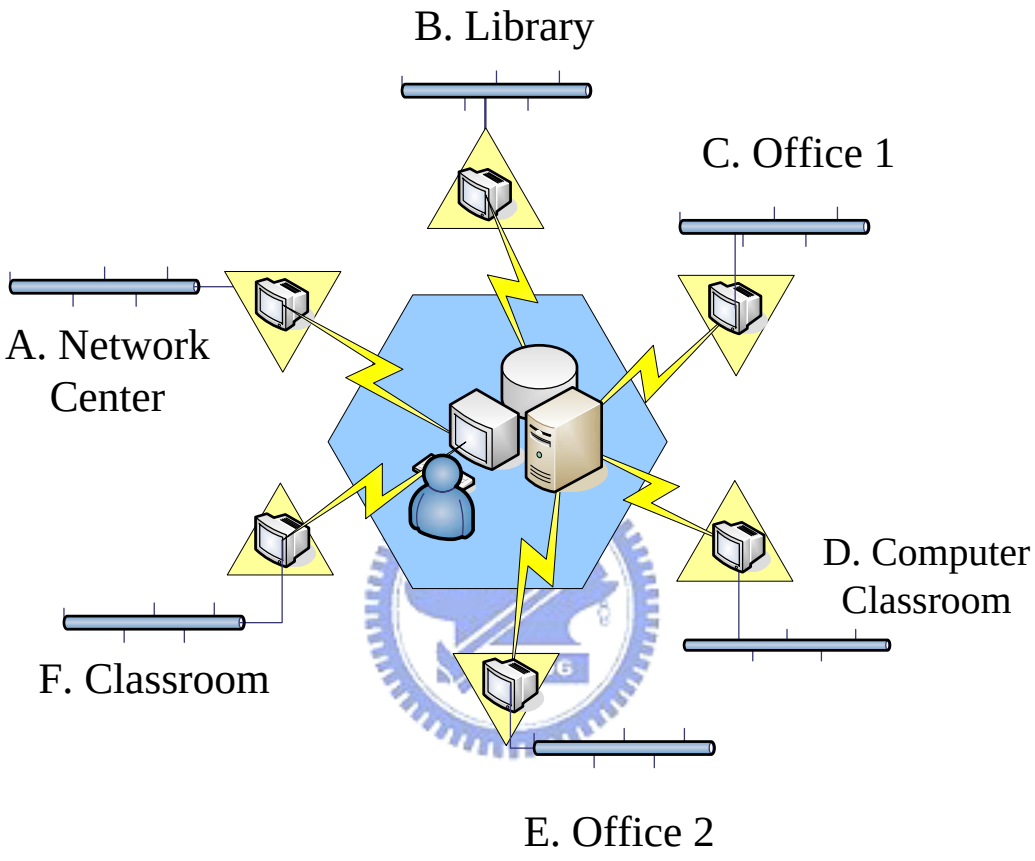


Figure 5-2: Collaborative Defense inside the campus

5.1.1 Profile

Table 5-1: The Profile of CSIRC

CSIRC	IP Range	Sensors	Service	Priority	Bandwidth	Hosts	Firewall
HKHS	140.126.167/24 163.19.12/24	7	Open	2	1.54M 3M/640K	<300	Yes
HCC	163.19.0/24 ~ 163.19.103/24	3	Half	1	>100M	>1000	Yes
HCC1	163.19.30/24	1	Open	3	3M/640K	<100	NO

CSIRC	IP Range	Sensors	Service	Priority	Bandwidth	Hosts	Firewall
HCC2	163.19.41/24	1	Open	3	3M/640K	<100	NO
HCC3	163.19.64/24	1	Open	3	3M/640K	<100	NO
HCC4	163.19.82/24	1	Open	3	3M/640K	<100	NO
NCTU	140.113/16	2	Open	3	>100M	>1000	NO

5.2 Requirement

The requirements of the experimental system include:

(1) *Sensor*: OS (FreeBSD, Linux, Windows), IDS (Snort), Database (MySQL).

(2) *CSIRC*: OS (Windows), Database (MS-SQL 2000 Server).

(3) *Web-based Analysis Console*: Web Server (Apache), PHP, BASE [EJ05], Database (MySQL).

(4) *Alert Analysis Console*: Database Client (for MS-SQL 2000 Server), Analysis Services of MS-SQL 2000 Server, MS-Excel, DBMiner.

5.2.1 The overview of the related tools

The Snort is a signature-based intrusion detection system and open source software. It represents a cost-effective and robust NIDS solution that fits the needs of many organizations. The Snort is very flexible in the ways it can be deployed. Many security industry watchdogs include Snort signatures in their security announcements (CERT and SANS). When worms are ravaging the Interet and there are constantly new variants, even there are multiple updates weekly. The Snort mailing lists are fantastic resource for people who are trying to run Snort or write their own signatures. There are a number of appalications that can act as central monitoring and alerting consoles, such as BASE [EJ05].

The BASE is the Basic Analysis and Security Engine. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web front-end to query and analyze the alerts coming from a Snort IDS system. The BASE is a web interface to perform analysis of intrusions that the Snort has detected on your network.

To post processing of alert data and data mining techniques requires commercial databases. We choose the MS-SQL and DBMiner. The MS-SQL 2000 Server helps us to do DTS (Data Transformation Services). It can automate processes to extract, transform and load data from heterogeneous sources. The MS-SQL 2000 Server Analysis Services includes OLAP, data mining, and data warehousing tools. It makes better decisions, performs rapid, and sophisticates analysis on large and complex data sets using multi-dimensional storage.

DBMiner is a cutting edge, on-line analytical data mining system running on the Microsoft SQL Server Plato system. This professional release allows industry users to mine data warehouses fast, and also provides many other mining functions. We use the DBMiner to visualize the threats.

5.2.2 Data Source

We have conceptualized alerts according to the Snort [Snort05] rule set. The Snort is a network IDS where alerts are triggered by a collection of rules. Each Snort rule is composed of a Snort identification number (SID), a message that is included in the alert when the rule is triggered, an attack signature, and references to sources of information about the attack. Each alert is provided with an identifier, time and date, sensor identifier, triggered signature, IP and TCP headers and payload. These alerts will be stored in the relational database as our data source.

5.3 Experiment

We have carried on the following several experiments mainly.

(1) Alert's Extraction and Information publish.

(2) Alert's Analysis in the CSIRC.

(3) Case study: To study the fast spreading worms: MS SQL Slammer Worm.

In Global CSIRC, we used MS-SQL Server 2000 software to construct the distributed database environment and manage the huge dataset over 6,000,000 records. We used the SQL DML statements to publish and subscribe alerts between the Local CSIRC and Global CSIRC. Combining the Data Transformation Services of MS-SQL, we can automate processes to extract, transform and load alert data from other CSIRCs. The examples of DML statements are:

Statement 1: Subscribe A2 Alert

```
SELECT     *
FROM    All_Alerts
WHERE (ip_src BETWEEN Profile.StartIP AND Profile.EndIP)
            AND (ip_dst BETWEEN Profile.StartIP AND Profile.EndIP)
ORDER BY    [timestamp]
```

Statement 2: Subscribe A3 Alert of T-day

```
SELECT     *
FROM    All_Alerts
WHERE ((ip_src NOT BETWEEN Profile.StartIP AND Profile.EndIP)
            AND (ip_dst BETWEEN Profile.StartIP AND Profile.EndIP))
            AND ([timestamp] BETWEEN ' T-day 00:00:00' AND ' T-day 23:59:59')
ORDER BY    [timestamp]
```

Statement 3: Top N List of Attackers

```
SELECT    ip_src AS Attacker, COUNT(ip_src) AS Counts
FROM      A3_Alerts
GROUP BY  ip_src
ORDER BY  Counts DESC
```

Statement 4: Top N of the alert's signatures in Global CSIRC

```
SELECT    sig_name AS Signature, sig_priority AS Priority,
          LID AS CSIRC, COUNT(*) AS Counts
FROM      All_A3
GROUP BY  LID, sig_name, sig_priority
ORDER BY  sig_name, CSIRC
```

5.4 Result

We had collected over 6,000,000 alerts about 3GB in the three main CSIRCs: HKHS, HCC and NCTU from March 25 to May 25. Let us analyze the results from two viewpoints: Local View and Global View.

5.4.1 In Local CSIRC

The results in the CSIRC of HKHS are:

(1) A large number of alerts: There are 180,000 alerts every day at most.

(2) The amounts of alerts in the campus have periodicity, as shown in Figure 5-3; the days in the red circle are Saturday and Sunday. The day of April 5 is a holiday.

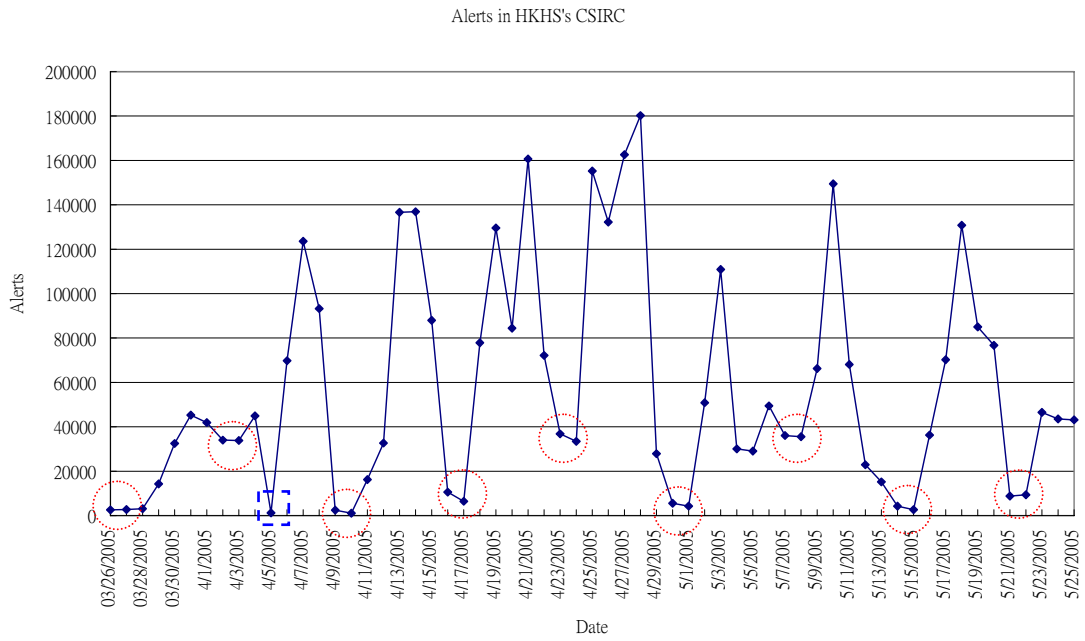


Figure 5-3: Periodic change of alerts

(3) After extraction of alert, the pie chart (Figure 5-4) shows that there are 23% A1, 40% A2, 11% A3 and 26% Exception. The alerts of A1 and A2 occupy the higher proportion.

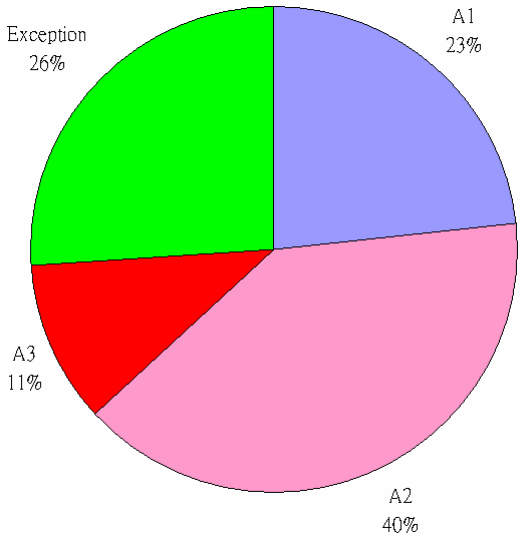


Figure 5-4: The classification of alert in Local CSIRC

(4) In the A1, there are many SNMP alerts and ICMP redirect alerts because of the faults of network management.

(5) In the Exception, we forgot considering these IP addresses: 255.255.255.255 (broadcast address) and 224.0.0.0~ 239.255.255.255 (the IP address of Class D

for Multicast). These addresses are inner IP added into Local Profile.

(6) The Table 5-2 shows the Top N of A2 alerts. We can find immediately who the killer of bandwidth is. There are many connections of P2P and many behaviors of portscan inside.

Table 5-2: The Top N of A2 alerts

NO	Signature Name	Counts
1	(portscan) TCP Portsweep	21083
2	P2P GNUTella client request	13606
3	P2P Outbound GNUTella client request	11757
4	P2P BitTorrent transfer	11664
5	(http_inspect) IIS UNICODE CODEPOINT ENCODING	2408
6	(http_inspect) BARE BYTE UNICODE ENCODING	2093
7	WEB-PHP myPHPNuke partner.php access	1294
8	ICMP IRDP router selection	881
9	ICMP Router Selection	881
10	(portscan) TCP Portscan	818
11	(portscan) UDP Portsweep	456
12	P2P BitTorrent announce request	395
13	MS-SQL ping attempt	317
14	SHELLCODE x86 NOOP	241
15	SNMP request udp	191

(7) The A3 alerts in the campus have *no* periodicity, as shown in Figure 5-5.

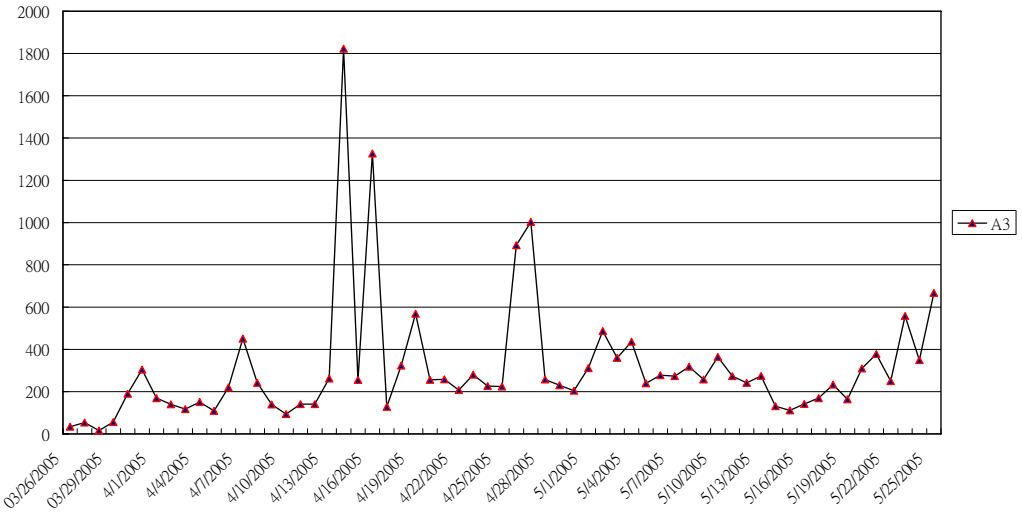


Figure 5-5 : The A3 Alerts in Local CSIRC

Table 5-3: The Top N of Attackers

Top N	Attacker IP (Integer)	Counts
1	1111034339	1600
2	3395324244	1104
3	3726848708	642
4	2356791882	410
5	1033834242	369
6	3232235962	337
7	2357086845	267
8	2736165889	211
9	3699898130	206
10	3422311304	203
11	1078601036	179
12	2356505897	159
13	3232235919	151
14	1031873043	144
15	3232235991	123

5.4.2 Global CSIRC

The Global CSIRC provides the statistics of alerts and attackers. This information can help the administrator understanding the trend of threats and make proper decision. The next table shows the Top N of alert's signatures. We can find many alerts coincided in two places or more.

Table 5-4: Top N of alert's signatures

NO	Alert Signature	CSIRC			Totals
		HCC	HKHS	NCTU	
1	ICMP PING speedera		612	16554	17166
2	SNMP request udp	14690	6	560	15256
3	SNMP public access udp	14690	4	294	14988
4	MS-SQL version overflow attempt	2514	1958	5921	10393
5	MS-SQL Worm propagation attempt	2514	1950	5915	10379
6	MS-SQL Worm propagation attempt OUTBOUND	2514	1950	5915	10379

NO	Alert Signature	CSIRC			Totals
		HCC	HKHS	NCTU	
7	SHELLCODE x86 NOOP	75	2714	1	2790
8	(http_inspect) BARE BYTE UNICODE ENCODING	27	1898	54	1979
10	ICMP PING CyberKit 2.2 Windows		50	1922	1972
11	(http_inspect) IIS UNICODE CODEPOINT ENCODING	11	1145		1156
12	ICMP PING NMAP	3	307	373	683
13	WEB-IIS cmd.exe access		673		673
14	(http_inspect) OVERSIZE CHUNK ENCODING	1	666		667
15	(http_inspect) DOUBLE DECODING ATTACK		627		627
16	WEB-CGI calendar access		586		586
17	(portscan) TCP Portscan	2	174	264	440
18	(http_inspect) OVERSIZE REQUEST-URI DIRECTORY		240	6	246
19	WEB-FRONTPAGE /_vti_bin/ access		97	5	102
20	ICMP Large ICMP Packet		73	3	76
21	SHELLCODE x86 0x90 unicode NOOP	53	9	2	64
22	MISC MS Terminal server request		52		52
23	DDOS mstream handler to client		35		35
24	WEB-CGI campus access		35		35
25	WEB-FRONTPAGE rad fp30reg.dll access		22	5	27
26	WEB-ATTACKS id command attempt		20		20
27	ICMP L3retriever Ping	1	18		19
28	SNMP missing community string attempt	11			11
29	SHELLCODE x86 setgid 0	6	2		8
30	WEB-IIS _mem_bin access		8		8
31	SHELLCODE x86 stealth NOOP	4			4
32	P2P eDonkey transfer		3		3
33	TFTP Get		1	2	3
34	WEB-IIS CodeRed v2 root.exe access		3		3
35	DDOS mstream client to handler			1	1
36	MULTIMEDIA Windows Media download		1		1
37	RPC portmap listing TCP 111			1	1
38	SCAN SSH Version map attempt			1	1
	Totals	37116	15939	37799	90854

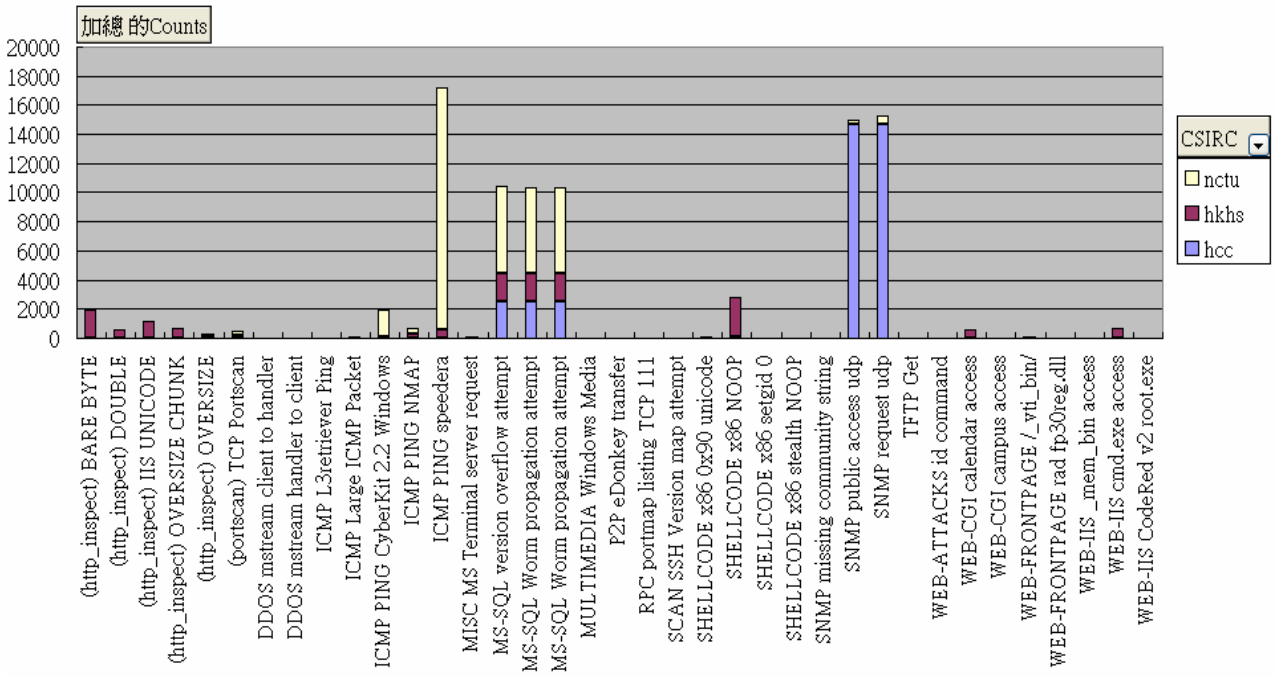


Figure 5-6: The bar chart of global Alerts

5.5 Case Study

We tracked the behaviors of the Worm propagation from the A3 alerts in the Global CSIRC. We found the “SQL Slammer Worm” which called “MS-SQL Worm propagation attempt” by the Snort. Its target port is 1434 and the protocol is UDP.

In Figure 5-7 an alert corresponding to an attempt of propagation of the MS-SQL worm is shown. We can understand the situations of the attacks of MS-SQL Worms.

(1) The MS-SQL Worm spread over our experimental network.

(2) In the duration of A, there were two immediate sharp increase and decrease.

(3) At the time of B, the CSIRC of HCC added a rule to firewall to block the connections by port 1434. Therefore, sensors did not detect the worm again after April 9.

(4) In the duration of C, the CSIRC of NCTU joined in the team. The amount of MS-SQL Worm alerts was a steep rise.

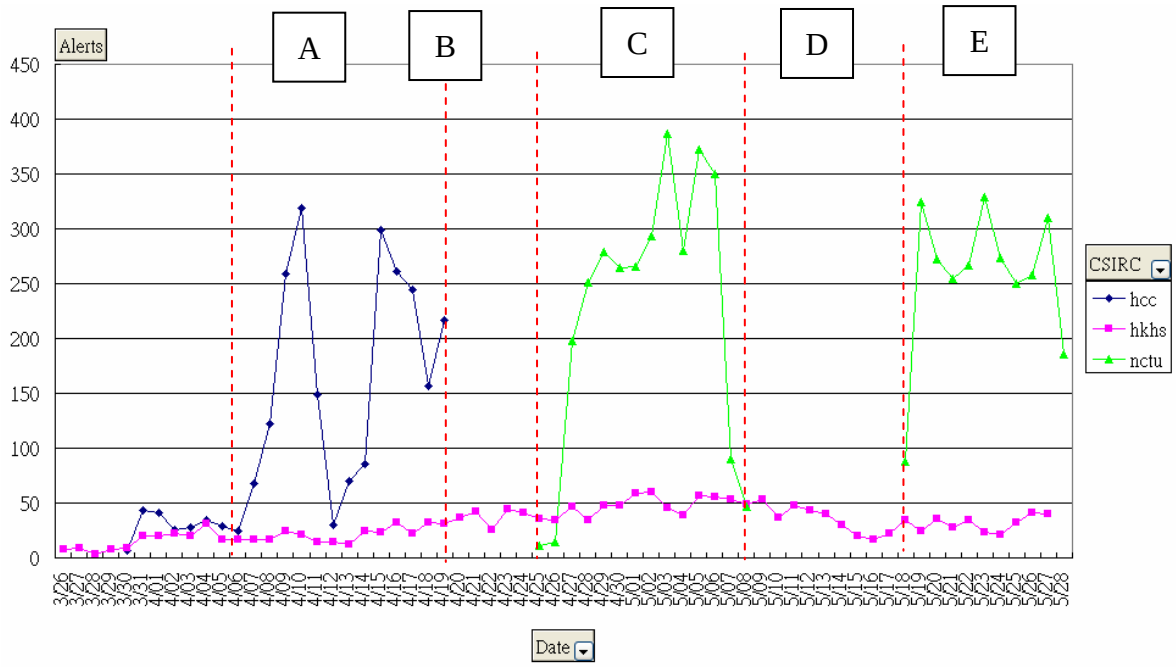


Figure 5-7: The spreading MS-SQL worm

(5) In the duration of D, The amount of alerts fell right down to the lowest point in NCTU because its CSIRC had crashed down.

(6) Finally, it shows the MS-SQL worms spreading again.

From the Global CSIRC, we can gain the information of defense, such as Top N of attacker. It can be used to discover trends in activity and prepare better firewall rules.

Table 5-5: The Attack Source of MS-SQL Worm

NO	Attack Source (Integer)	CSIRC			Totals of Alerts
		HCC	HKHS	NCTU	
1	1033834242	479	123	388	990
2	3670575618	4	41	207	252
3	1033473956	19	37	173	229
4	1031873043		48	178	226
5	3396177109	3	39	176	218
6	3395531217		24	174	198
7	3726771501		16	169	185
8	3702525640	60	27	89	176
9	1440579587		15	150	165

10	1019183190	2	37	125	164
11	3546441735		18	145	163
12	3395399394	40	14	93	147
13	3548912154		17	124	141
14	1035389507	113	11	12	136
15	1019150756		12	110	122

We also can find the range of the unfriendly IP from the statistics of connections in the Global CSIRC as shown in Figure 5-8.

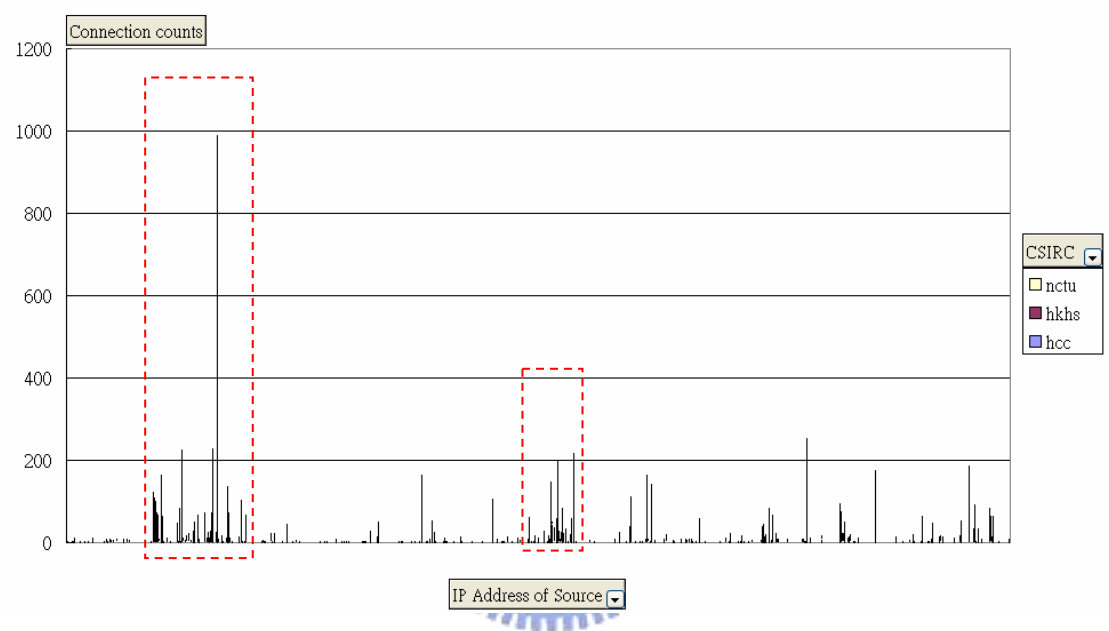


Figure 5-8: The distribution map of attackers' IP

According to our experimental results, many attacks are over the Internet. The results are presented in Figure 5-9. Therefore, the collaborative defense can help us kick the abominable attacker out as soon as possible.

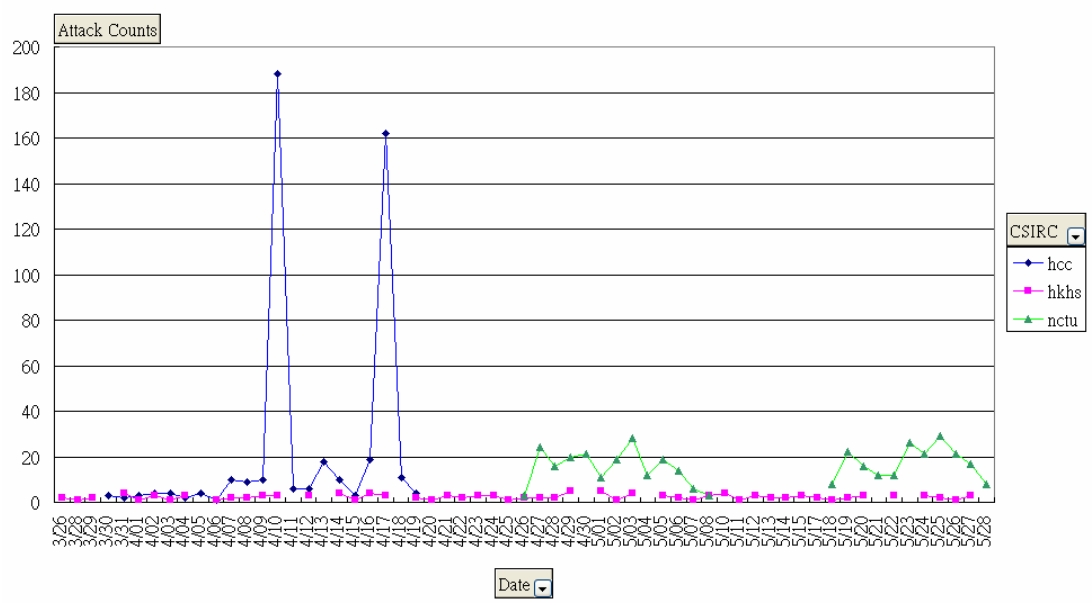


Figure 5-9: The attack counts of single attacker

5.6 Visualization of Threat

After creating data cube with MS Analysis services, then we used IBM DB Miner to do data mining and the visualization of threats.

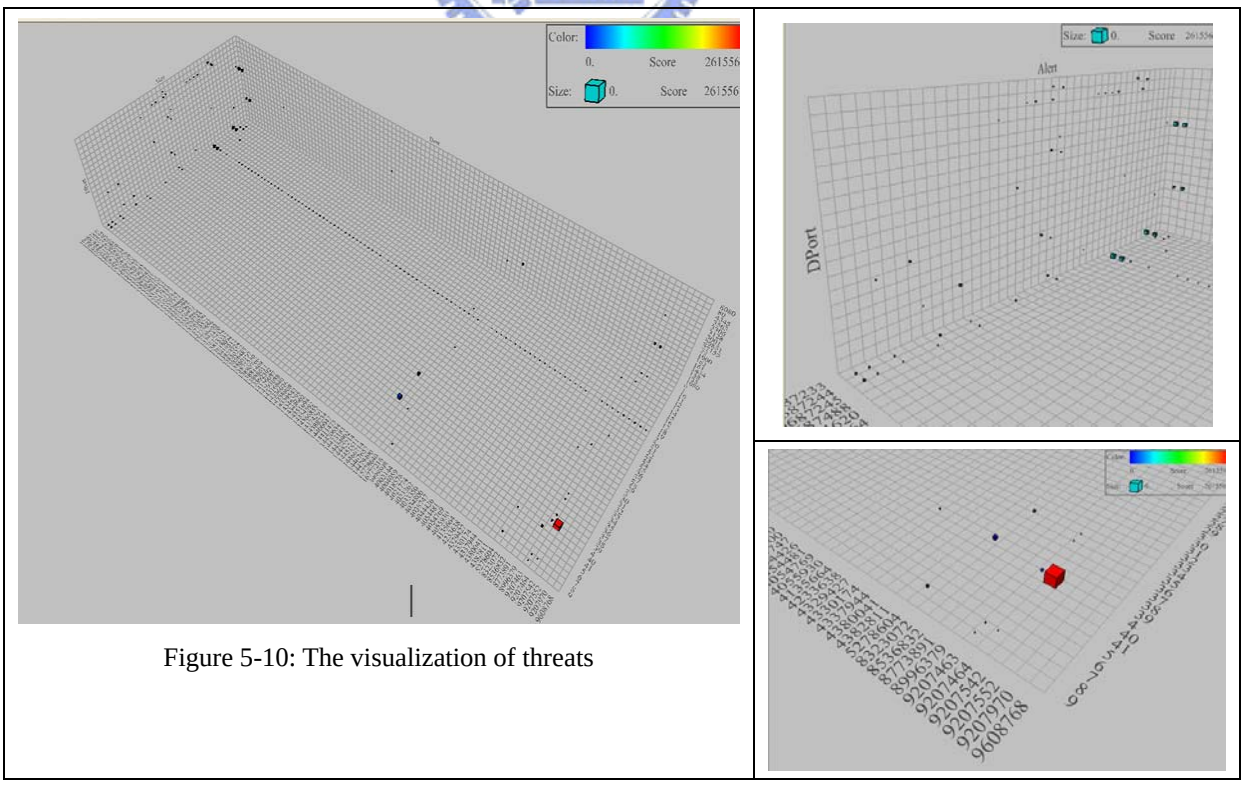


Figure 5-10: The visualization of threats

Chapter 6. Conclusion and Future Work

6.1 Conclusion

Collaborative and cooperative activities are significant. We present an approach to organizing autonomous but cooperative component systems to detect distributed attacks and exchange information. We provide a collaborative defense mechanism to share findings across end systems, to undergo alert management and facilities analysis, and to add a network-wide perspective to the analysis.

The lightweight Collaborative Defense Solution includes*:*

(1) Integrate the resources of security defense and reduce cost of alert analysis.

(2) Distinguish everybody's responsibility in the Collaborative Defense Team clearly. The work division is especially suitable for hierarchical administrative organizations.

(3) The Alert-based system provides high level information up to ISO's OSI layer 7 and easily combines the experts' knowledge.

(4) Report these alerts of threats and share security knowledge to build a security knowledge warehousing framework.

(5) Improve the alert analysis, including frequency and trend.

(6) Assist administrators to make quick response for each anomaly situation.

The contribution of this thesis is: First, we have proposed a framework for collaborative defense by extending the original distributed intrusion detection model. This framework contains alert's collector, extractor, analyzer, report's generator, alert warehouse, alert's analysis and information sharing. The framework provides a

solution to build effective cooperative security teams for academia and industry.

Secondly, we have focused on Alert-based data source and enhanced the analysis of alerts. As a result, we can deploy security system more widely and detect the aggressor's behavior more accurately. Besides, we developed a hybrid approach to share security information like raising the wolf smoke to warn our partners.

The deployment of our framework allows the organization to take mitigation and preemptive threat responses without having been directly attacked. Our framework will benefit from having a wide variety of organizations integrated with it.

6.2 Future Work

Our future work focusing on collaborative security will include combining system with expert system and provide a Solution-based Collaborative Defense System, developing the collaborative distributed incremental association rule mining to enhance the potency of alert analysis.

At present we have not yet considered the questions about the privacy protection. This is an important issue which includes message encryption, hiding of private data and trust management.

References

[AL+04] Cristina Abad,Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, William Yurcik, “Correlation between NetFlow System and Network Views for Intrusion Detection”, 2004.

[Anderson80] James P. Anderson Co., “Computer security threat monitoring and surveillance”, Technical report, 1980.

[BJ+04] Barford, Paul; Jha, Somesh; Yegneswaran, Vinod. ”Fusion and Filtering in Distributed Intrusion Detection Systems”, In Proceedings of the 42nd Annual Allerton Conference on Communication, Control and Computing, September, 2004.

[CD01] David A. Curry and Herve Debar, “Intrusion detection message exchange format data model and extensible markup language (xml) document type definition”, Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, February 2001.

[CERT04] CERT Coordination Center, URL: http://www.cert.org/, 2004.

[Cisco01] Cisco, “NetRanger Docmentation”, URL: http://ww.cisco.com/univercd/cc/td/doc/product/iaabu/netranger/, 2001.

[CN+04] Tobias Chyssler, Simin Nadjm-Tehrani, Stefan Burschka, Kalle Burbeck, “Alarm Reduction and Correlation in Defence of IP Networks”, 2004.

[CU+04] CSO Magazine,US Secret Service,CERT Coordination Center, “2004 E-CRIME WATCHTM SURVEY SHOWS SIGNIFICANT INCREASE IN ELECTRONIC CRIMES”, May 25 2004.

[DeepSight05] DeepSight™ Threat Management System, Symantec Co., URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=158&EID=0, 2005.

[Denning87] Dorothy E. Denning, “An Intrusion Detection Model” , IEEE Trans. Software Eng., Vol. SE-13, No. 2, Feb. 1987, pp. 222–232.

[DShield05] DShield.org, URL: http://www.dshield.org/, 2005.

[DW01] Herv´e Debar, and Andreas Wespi, “Aggregation and Correlation of Intrusion Detection Alerts”, 2001.

[EJ05] Joel Esler, Kevin Johnson, Basic Analysis and Security Engine (BASE), URL: http://secureideas.sourceforge.net/, 2005.

[European04] The European CSIRT Networkt, URL: http://www.ecsirt.net/, 2004.

[FW01] D. Frincke, E. Wilhite, “Distributed Network Defense” Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, West Point, NY, June 2001, pp 236-238.

[Gopalakrishna01] Rajeev Gopalakrishna, “A Framework for Distributed Intrusion Detection using Interest-Driven Cooperative Agents”, CERIAS Tech Report, 2001.

[GS01] Rajeev Gopalakrishna, Eugene H. Spafford, “A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents”, 2001.

[HS+04] Antti Hätälä, Camillo Särs, Ronja Addams-Moring and Teemupekka Virtanen”, Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks”, 2004.

[HS03] Arne Helme, Stelvio, “eCSIRT.net Deliverable1 Common Language Specication & Guideline to Application of the Common Language part (i)”, December 2003.

[IDSwakeup00] IDSwakeup, URL: http://www.hsc.fr/ressources/outils/idswakeup/, 2000.

[JPCERT04] JPCERT/CC ISDAS, URL: http://www.jpcert.or.jp/isdas/, 2004.

[Lipson00] Howard F. Lipson, Ph.D., “A New Security Paradigm for Protecting

Highly Distributed Mission-Critical Systems", CERT Coordination Center, 2000.

[Masurkar03-1] Vijay Masurkar, "Responding to a Customer's Security Incidents—Part 1: Establishing Teams and a Policy", 2003.

[Masurkar03-2] Vijay Masurkar, "Responding to a Customer's Security Incidents—Part 2: Executing a Policy", 2003.

[MD03] Benjamin Morin and Herve Debar, "Correlation of Intrusion Symptoms: an Application of Chronicles", France Telecom R&D, France, 2003.

[Miège02] Frédéric Cuppens Alexandre Miège, "Alert Correlation in a Cooperative Intrusion Detection Framework", 2002.

[Mills92] D. Mills, Network time protocol (version 3). RFC 1305, March 1992.

[MM+03] Benjamin Morin, Ludovic M´e, Herv´e Debar1, and Mireille Ducass´e, "M2D2: A Formal Data Model for IDS Alert Correlation", 2003.

[MP03] Francisco J. Martín and Enric Plaza, "Alba: A cognitive assistant for network administration", In I. Aguiló et al. (Eds.), Artificial Intelligence Research and Development, Frontiers in Artificial Intelligence and Applications, Vol. 100, p. 341-352. IOS Press, 2003.

[NC+04] Peng Ning, Yun Cui, Douglas Reeves, and Dingbang Xu, "Tools and Techniques for Analyzing Intrusion Alerts," in ACM Transactions on Information and System Security, Vol. 7, No. 2, pages 273--318, May 2004.

[NJ+01] Peng Ning, Sushil Jajodia, Xiaoyang Sean Wang, "Abstraction-based Intrusion Detection in Distributed Environments", 2001.

[PN97] Phillip A. Porras and Peter G. Neumann, "EMERALD: event monitoring enabling responses to anomalous live disturbances", In 1997 National Information Systems Security Conference, Oct 1997.

[QL03] Xinzhou Qin and Wenke Lee, "Satistical Causality Analysis of INFOSEC

Alert Data", Georgia Institute of Technology, USA, 2003.

[SANS04] SANS Institute, Computer Security Education and Information Security Training, URL: http://www.sans.org/, 2004.

[SB+91] S. Snapp, J. Brentano, and G. Dias et al., "DIDS (Distributed Intrusion Detection System) – motivation, architecture, and an early prototype", In Proceedings of the 14th National Computer Security Conference, October 1991.

[SC+96] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, "GrIDS-a graph based intrusion detection system for large networks", In Proceedings of the 19th National Information Systems Security Conference, September 1996.

[Snort05] Snort® Intrusion Detection/Prevention System, URL: http://www.snort.org/, 2005"

[ST+98] Staniford-Chen, S., Tung, B., and Schnackenberg, D., "The Common Intrusion Detection Framework (CIDF)", Position paper accepted to the Information Survivability Workshop, Orlando FL, October 1998.

[Stick00] Stick, URL: http://www.eurocompton.net/stick/projects8.html, 2000.

[SZ00] Eugene H. Spafford and Diego Zamboni, "Intrusion detection using autonomous agents", October 2000.

[VK98] G. Vigna and R. A. Kemmereer, "NetSTAT: A Network-based Intrusion Detection Approach", 1998.

[WS+98] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, "Handbook for Computer Security Incident Response Teams (CSIRTs)", December 1998.

[XN04] Dingbang Xu, Peng Ning, "Alert Correlation through Triggering Events and Common Resources", in Proceedings of 20th Annual Computer Security

Applications Conference, December 2004.

[YB+03] Vinod Yegneswaran, Paul Barford and Johannes Ullrich, “Internet Intrusions: Global Characteristics and Prevalence”, 2003.

[YB+04] Yegneswaran, Vinod; Barford, Paul; Jha, Somesh, “Global Intrusion Detection in the DOMINO Overlay System”, In Proceedings of Network and Distributed Security Symposium (NDSS), 2004.

Appendixes

Appendix A. The Schema of Alert Pool

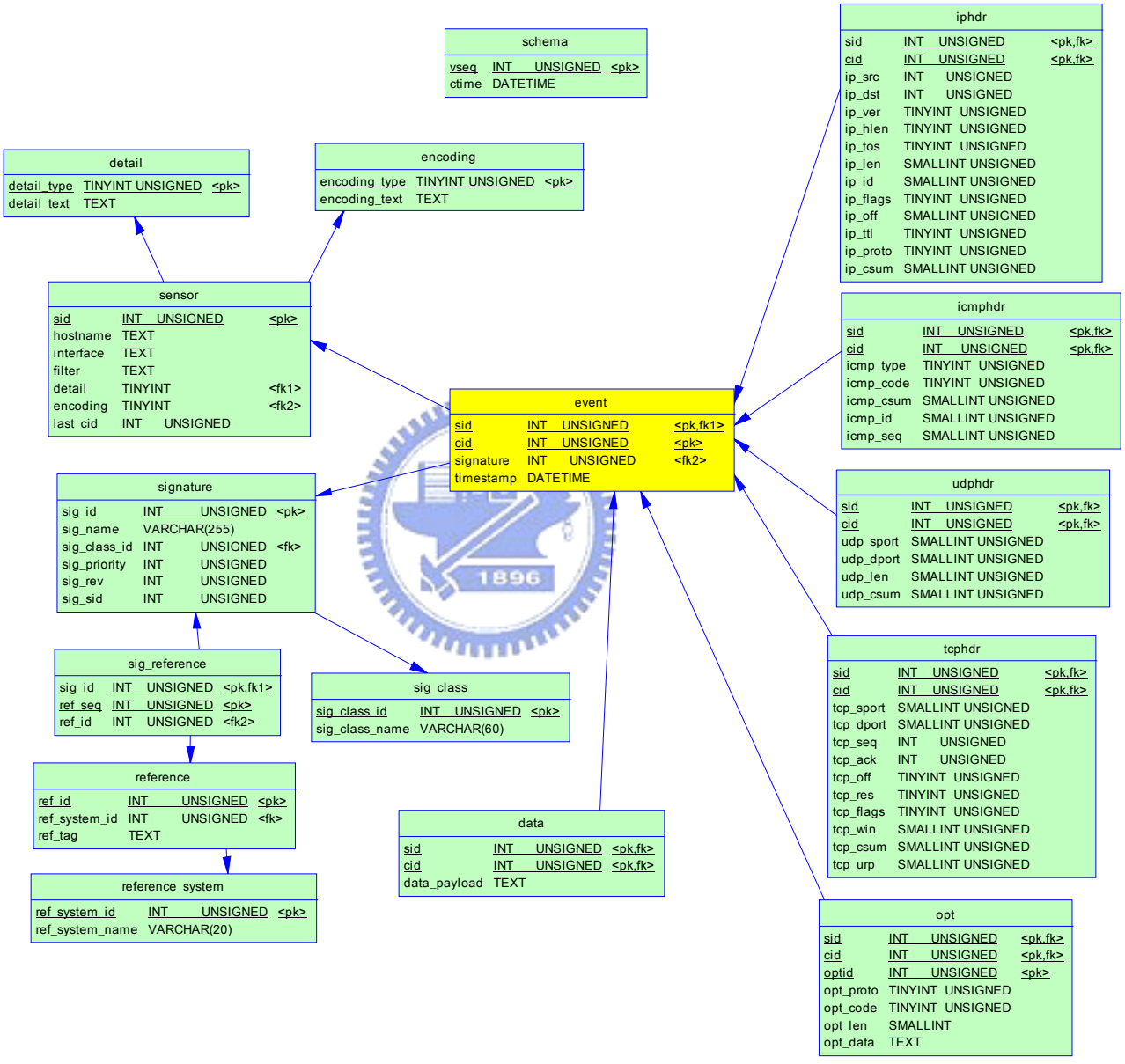


Figure A- 1: The Schema of Alert Pool

Appendix B. The Schema of Alert Warehouse

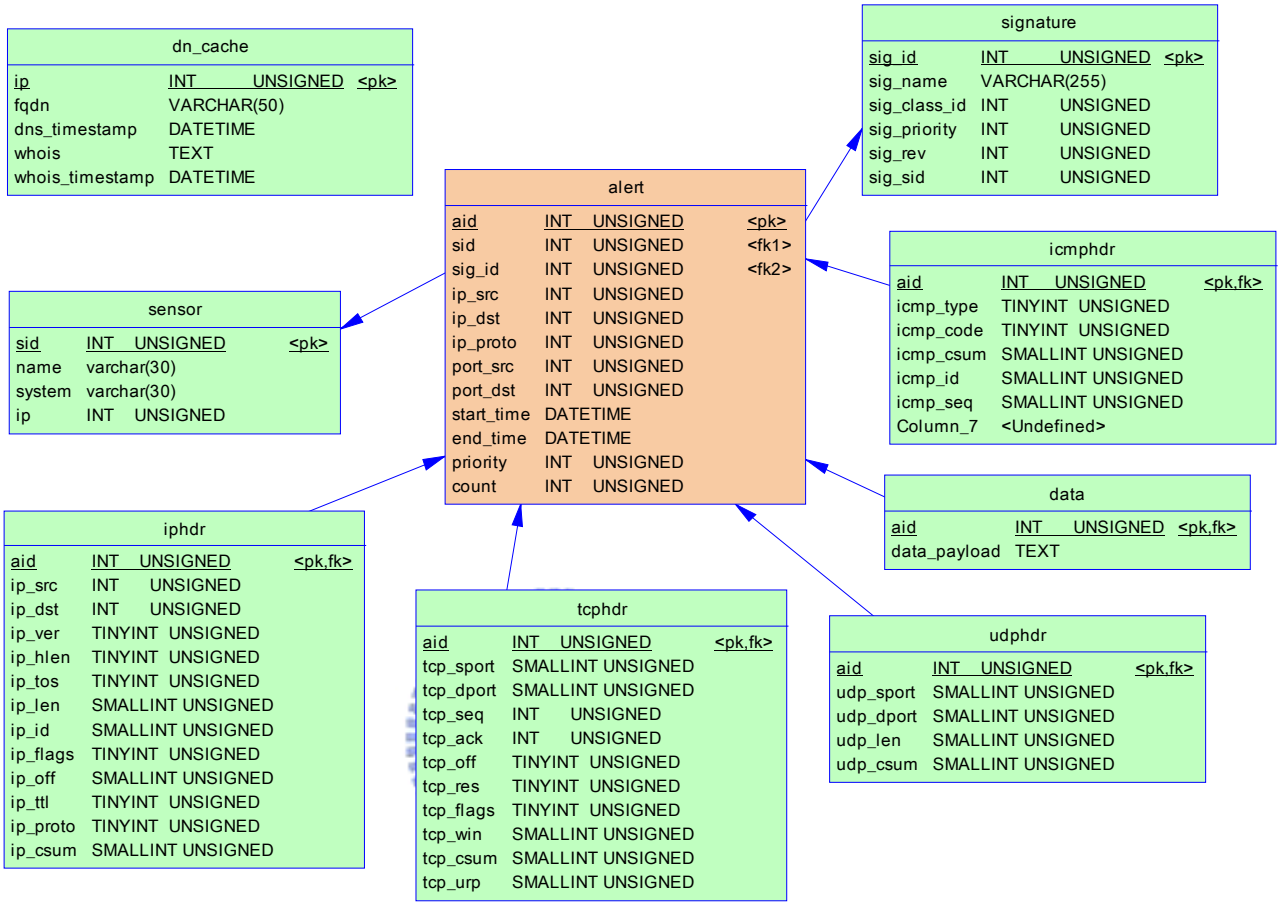


Figure B-1: The Schema of Alert Warehouse