Collection, analysis and response stages
Consisting 6 core module

www.ecsc.go.kr
Overview

- Technical Introduction to Korea’s ECSC security monitoring method
  - How to collect security information from different institutional heterogeneous security systems
  - How to implement correlation analysis on the mass data collected
  - How to effectively respond to intrusion incidents

[Security Information]
- Information detected by pattern-based security system such as IPS or IDS
Classify the patterns of attacks and apply different correlation analysis to them.

Collect logs in real time from pattern-based detection systems of individual institutions.

Share intrusion information in real time through and information sharing system and respond quickly.

Stages of security monitoring:

1. Collection
2. Analysis
3. Response
6 Core Modules

ECSC’s 6 Core modules

Collection Module

Integration module

Correlation analysis module

Information Sharing Module

Threat Management Module

Monitoring Support module
Collection Stage

- **Issues related to the collection stage**
  - **What information** to collect
  - **How to collect** the logs detected from individual systems?
  - **How to regularize** different logs of heterogeneous security systems?
  - **How to collect massive amounts** of data?
Issues of the analysis stage

- Is all the collected information related to hacking incidents?
- How to implement correlation analysis on collected information?
- How to classify hacking attack patterns?
- What analysis strategy should be applied to the mass data?
Response Stage

Issues of the response stage

- What are efficient response strategies and methods for different attack patterns?

- What is the most efficient response system to intrusion incidents?
Process of collecting security information

- Pattern-based real-time detection logs
- Network traffic information

Collection module

Transmission:
- Regularization
- Filtering
- Reduction
- Encryption
Collecting Security Information

❖ **Pattern-based security information**

- Real-time logs from **pattern-based detection system** such as IPS or IDS
- **The key to precise detection is** patterns: to combine patterns of individual security systems and ECSC’s own pattern
- Operate a consultative organization to apply a **precise detection pattern**

[ECSC detection pattern]
- Develop its own patterns by investigating and analyzing actual cases and use open source of IDS snort
- Share patterns in cooperation with related institutions

❖ **Network Traffic Information**

- Real-time traffic information form the backbone switch in related institutions and information on CPU usage
ECSC Detection Pattern

❖ Develop own pattern

- Develop highly accurate patterns by investigating actual cases
- Apply them to individual institutions through consultative organization for detection pattern sharing

[An example of ECSC detection pattern]

- POST method run through command 
  "netstat ", ".exe", "dir", "ls",
  alert tcp any any <> any $HTTP_PORT (content:"POST";depth:4;pcre:"/\x0d\x0a.*
  (netstat(%20|\+)+\x2Da|\x2Eexe(%20|\+)+\x2Fc|cmd(%20|\+)+\x2Fc|dir(%20|\+)+
  c\x3A\x5C|ls(%20|\+)+152\x2E99\x2E)/i";)


Regularization of Security Information

- Regularize real-time logs from individual systems

- Regularize real-time logs from heterogeneous systems through an xml-based policy

XML regularization policy

```xml
<Analy>
  <Policy src="original" type="1" separator=",">
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="7" />
    <Field regular_pos="8" />
    <Field regular_pos="12" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
    <Field regular_pos="NO" />
  </Policy>
</Analy>
```

- DST_IP: '203.226.253.91'
- SRC_IP: '203.228.53.222'
- COMP_YN: 'Y'
- ATTACK_NM: 'IM: NateOn Traffic Detected'
- CNT: '1'
- EQP_IP: '210.125.200.80'
- EQP_TYPE: '05'
- DST_PORT: '5004'
- COMP_CNT: '1'
- PAYLOAD: ''
- BODY_TYPE: 'LOG_IA'
- INST_CD: '73034000'
- SRC_PORT: '1593'
- PROTOCOL: '6'
- OPTION2: ''
- OPTION1: ''
- EQP_TIME: '20110329171929'
- SIMS_TIME: '20110329171929'
- OPTION3: ''
Filtering, Reduction, Encryption

- Filtering, reduction, and encryption of security information
  - Filter detection errors (false positive)
  - Reduce recurring information: reduce logs with the same starting IP, arriving IP, and attacking name
  - Transmit encryption to the central center (SSL)
Contents

1. Overview
2. Collection
3. Analysis
4. Response
Analysis Method on Security Information

Integrated and Correlated Real-time Pattern-Based Analysis

Profiling Analysis

Data Mining Analysis

Collected information from institution

Detection and Response to intrusion.
Analysis Method on Security Information

**Pattern**
- real-time correlation analysis on information detected by patterns with high accuracy

**Profiling**
- analyze critical values by profiling information detected by patterns with low accuracy

**Mining**
- create statistics for 5 minute increments to utilize for security monitoring
Real-time Pattern-Based Analysis

❖ Real-time pattern-based analysis

- **Grade risk level by real-time correlation analysis** on information detected by accurate detection pattern (ECSC pattern)

- Correlation analysis:
  - Correlation analysis on logs with the **same attack pattern based on attack IP**
  - Correlation analysis on **black list IP** based on attack IP
  - Correlation analysis on **vulnerabilities** based on target IP

[Classification of attack patterns and correlation analysis methods]

- Cooperation between ECSC monitoring researchers and related institutions
Real-time Pattern-Based Analysis

- **Real-time correlation analysis**
  - **Calculate risk level** through correlation analysis based on attack patterns, attack information, vulnerabilities, and critical values

\[ \text{Risk level} = \text{initial risk level} \times \text{significance of risk level} + (\sum \text{risk level through correlation analysis}) \]

- **Black List IP, Port**
- **Vulnerabilities**
- **Risk level of attack patterns**
- **Critical values**
Profiling-based Analysis

Profiling pattern-based analysis

- Analyze information detected through patterns with **low accuracy** by comparing it with profiled critical values

- Profile critical values in advance: **profiling critical values by different institutions and patterns**

[Standard of profiling]
Profiling pattern by different institutions: Analyze weekly averages or the average of the previous day
Through profiling-based analysis, we register patterns with high accuracy as a real-time monitoring pattern that is analyzed automatically.

- Collecting information
- Profiling pattern-based analysis
- Real-time pattern-based analysis
- Analysis on IPS/IDS pattern
- Register & respond to intrusion
Data mining analysis

- Create a statistic **every 5 minutes** from the original data and **utilize it for monitoring**
- Data mining **based on the top attack name, top place, top target, and top traffic increase**
Data mining Analysis

Primitive security information

Data mining

Detect security information in hourly units

Apply **new monitoring pattern** based on mining results
Analysis on mass data

**Architecture for analysis on mass data in real time**
- Utilize **memory DB** for real-time correlation analysis
- Maximize capacity of resources by establishing integration structure
Response to Intrusion Incidents

**Monitoring support module**
- provide efficient analysis environment to monitoring researchers through 3D visualization

**Threat management module**
- supports future statistical management by registering and controlling analyzed data

**Information sharing module**
- provide intrusion incident and threat information to related institutions in real time
Provide an efficient monitoring environment

- Enable immediate monitoring through 3D visualization
- Enable an individual monitoring environment for each researcher
- Establish real-time monitoring based on Web2.0
Situation Board of ECSC
Threat Management Module

❖ Systematic threat management
  - Efficient threat management with the 6 sigma process
  - Systematization of registration-processing-completion of intrusion incident
  - Efficient management of statistics
Sharing updated information on intrusion and new technology

- Share updated security trends
- Share statistics of intrusions and detailed information
- Share vulnerabilities
- Share new hacking technologies
정보공유 모듈

단위기간 전체 침해공격 현황
- 전화기関
  - 발생 종류별
    - 악성코드 감염 [68%]
    - 블랙호 [15%]
    - 서비스가격 출력 [9%]
    - 단순접속시도 [4%]

단위기간 기반유형 침해공격 현황
- 단위기간
  - 인물
    - 악성코드 감염 [45%]
    - 서비스가격 출력 [15%]
    - 단순접속시도 [10%]

단위기간 침해공격 현황
- 교육사이버안전센터
  - 악성코드 감염 [100%]

리소스 현황

트래픽 현황

존결 995

1. 침해율 [62%]
2. 악성코드 감염 [26%]
3. 경유지 악용 [5%]
4. 서비스가격 출력 [4%]
5. 단순접속시도 [0%]
Countermeasure against Intrusion Incident

Information Sharing

Threat Management

Monitoring

Countermeasure against intrusion incident
What do we need for a powerful countermeasure system?
Thank You!

www.ecsc.go.kr