International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.261-268
http://dx.doi.org/10.14257/ijsia.2016.10.6.25

# A Study on Vulnerability Assessment Technique of People-Oriented Security through Pattern Analysis

Choon Park and Dae-Sik Ko*

*Dept. of Electronic Engineering, Mokwon University, Doctor's Course,*
*Dept. of Electronic Engineering, Mokwon University, Professor*
*cpark@nicecom.com, kds@mokwon.ac.kr*
**Corresponding author*

***Abstract***

*This paper introduces people-oriented security vulnerability assessment techniques through pattern analysis in order to overcome the limits of the prevalent system-centered and data-centered security vulnerability assessments. This paper suggests algorithms to detect abnormal patterns due to security breach by analyzing physical and logical patterns of people who approach to IT information system. As a result of the*

*analysis, we found that the information system users' access patterns and behaviors belong to certain categories, and by combining these patterns, it is possible to identify abnormal patterns ($\phi$= 1) which lead to security breach accidents. This research will enable a new way of user-oriented security vulnerability assessment.*

***Keywords****: Access types, abnormal pattern, history bit, command's impact*

## 1. Introduction

IT environment as a significant for companies to thrive, and among the factors that threaten the IT environment, IT security field is risky in many aspects. Thus, the demand for risk management of the IT security field is also increasing.

Risk management techniques in the IT security field include system-oriented risk management, which emphasizes the system that stores the main personal information to access the system; data-oriented risk management, which manages direct risk to the data that include the personal information; and people-oriented risk management, which focuses on people who create, store, inquire and use the data [1].

Today's existing security management techniques are based on the system and data. However, even though security is enhanced in the current security management techniques, there is fundamental limitation in handling and managing IT security threats because handling and managing important data are still done by people. Unless people who handle and manage the data are strictly controlled, it would be difficult to cope with security threats.

Researches on people-oriented security control are ongoing using Common Vulnerability Scoring System (CVSS) developed under the support of National Infrastructure Advisory Council. The CVSS assesses the security control using two sets of metrics: one that evaluates based on AV, AC, PR, and UI; and the other that evaluates based on C, I and A [2].

CVSS provides standards in assessment of security threat, but it is limited when directly measuring and assessing security threat posed by people. In other words, under the assumption that human behavior has certain patterns and there will be a sign of deviation in any form from a normal pattern that indicates human behavior that causes security incident, the existing researches on people-oriented security vulnerability

* Corresponding Author

ISSN: 1738-9976 IJSIA

assessment were conducted to discover what types of patterns of human behavior exist in reality and how this can be used in detecting users that threaten the security [3-5].

## 2. Types of Security Control

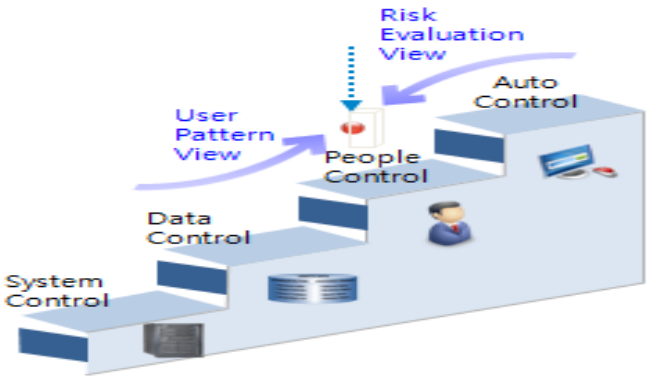


**Figure 1. Types of the Security Management**

Security Management can be categorized into four types: system, data, people, and automation which integrate all three. First, the system management consists of intrusion prevention system (IDS), intrusion prevention from the system (IPS), antivirus systems, vulnerability diagnosis system, security event monitoring, security policy enforcement and management system health check, and cyber infringement analysis and response, since about 25 years ago, and it is still under use [6].

Data management is initially managed as a form of asset management, and since 2011, it has been developed and managed in the form of Privacy Act, consisting of source code diagnosis, mock hacking, and data classification and security diagnostics and others [7].

People management consists of user-specific pattern analysis, risk analysis for each pattern, and risk assessment, based on the RBAC (Role Based Access Control) approach, and many researches about the people management are currently in process [8, 9].

Automation management means the automation of security management interconnecting system, data, and people management, and requires various techniques such as monitoring, log analysis, setup and application of concrete scenario-specific response policies, and verification of results. The automation management is in a stage where further researches are necessary [10, 11].

## 3. People-Oriented Security Vulnerability Assessment Techniques

### 3.1. Access Type p Pattern Analysis

In order to analyze the risk for each person accessing the information assets, it is important to determine whether it is possible to formalize the access types for each person. Thus, in this study, the access type pattern is divided into the following three layers.

On the first layer, the information system is divided into PL (Physical Layer), SL (System Layer), DL (Data Layer) and AL (Action Layer). For PL, it is divided into FL (Floor Layer) and TL (Time Later), and each is further divided into NE (Normal Entrance) and AE (Abnormal Entrance). For SL, it is divided into AA (Authorized Access) and UA (Unauthorized Access), and UA is further divided into SA (Simple Access) and IA (Intentional Access). For DL, it is divided into ND (Normal Data), SD (Sensitive Data), and CD (Critical Data), and each is further divided into RA (Read Access) and WA (Write Access). Here, Critical Data means data which can be influenced

 

by system commands execution. Lastly, for AL, it is divided into SP (Simple Process) and MP (Mass Process), and each is further divided into NR (Normal Result) and AR (Abnormal Result). Various access types are summarized in the Table 1 below.

**Table 1. Access Types for Each Layer**

| 1st Layer | 2nd Layer | 3rd Layer |
|---|---|---|
| PL | FL | NE |
| | | AE |
| | TL | NE |
| | | AE |
| SL | AA | NA |
| | UA | SA |
| | | IA |
| DL | ND | RA |
| | | WA |
| | SD | RA |
| | | WA |
| | CD | RA |
| | | WA |
| AL | SP | NR |
| | | AR |
| | MP | NR |
| | | AR |

People's access patterns can be formalized and categorized into different types using the classification system as shown in Table 1. For example, it becomes possible to define a type of pattern such as "on a specific date and time, accessed to a specific system, attempted to process certain data and eventually processed the data in a certain way." However, in order to determine whether such access pattern is a normal access pattern, a separate algorithm is needed.

### 3.2. Algorithms to Determine Abnormality of a Pattern

The simplest way to determine whether it is a person that is eventually responsible for a security incident to an IT information system is by using the abnormal result (AR) value of action layer (AL). However, this method is not preferable as security incident can still occur even in the case of a normal SL, DL and AL.in order to complement such cases, a more sophisticated algorithm incorporating PL and SL would be required to determine that intentional attack propensity is latent when PL_FL_AE and SL_UA_IA occur repeatedly or PL_TL_AE occurs. In this case, "abnormal bit" becomes 1 as shown in Table 2.

Table 2 below describes the abnormality determination standards for each classification sign.

**Table 2. Criteria for Abnormal Pattern**

| 1st Layer | 2nd Layer | 3rd Layer | Criteria for abnormal Pattern |
|---|---|---|---|
| PL | FL | AE | Abnormal Bit '1' (happened more that 3) |
| | TL | AE | Abnormal Bit '1' (happened more that 1) |
| SL | UA | SA | Abnormal Bit '1' (happened more that 3) |
| | | IA | |
| DL | SD | RA | Abnormal Bit '0, Linked to AL |
| | | WA | Abnormal Bit '0, Linked to AL |
| | CD | RA | Abnormal Bit '0, Linked to AL |
| | | WA | Abnormal Bit '1' (happened more that 1) |
| AL | SP | AR | Abnormal Bit '1' |
| | MP | NR | Abnormal Bit '0' or '1' |
| | | AR | Abnormal Bit '1' |

Firstly, for the cases to handle SD (Sensitive Data, Data including personnel information) or CD (Critical Data, Data containing system parameters or modules) of DL, abnormality determination depends on the result of AL (Action Layer). For the cases where AR (Abnormal Result) happens in SP (Simple Process) or MP (Mass Process), abnormal pattern ($\oint$=1) exists clearly. For other cases, it is possible to express as follows.

Abnormal Pattern $\oint$= XOR((DL_SD) ∩ (AL_SP_AR)) or
Abnormal Pattern $\oint$= XOR((DL_SD) ∩ (AL_MP_AR))or
Abnormal Pattern $\oint$= XOR((DL_CD) ∩ (AL_SP_AR)) or
Abnormal Pattern $\oint$= XOR((DL_CD) ∩ (AL_MP_AR))

Secondly, for the cases that result of AR (Action Layer) is NR (Normal Result) in SD or CD, abnormal pattern ($\oint$=1) exists potentially where abnormal bit '1' exists in PL or SL. For such cases, abnormalities can be determined through managers' further inspection and the patterns of the abnormalities can be expressed as follows.

Abnormal Pattern $\oint$=XOR((PL) ∩ (DL_SD) ∩ (AL_NR)) or
Abnormal Pattern $\oint$=XOR((SL) ∩ (DL_SD) ∩ (AL_NR))

### 3.3. Additional Algorithms to Determine Abnormality of a Pattern

In order for a security incident to forge or leak a massive amount of sensitive data such as personal information, corresponding commands must be used. The use of risk commands was added to the abnormality determination algorithm since corresponding commands must be used when directly affecting the availability, integrity and confidentiality of the system [12] [13].

**Table 3. Table for Command's Impacts**

| Command | Types | Impact | | | |
|---|---|---|---|---|---|
| | | Very Low | Low | High | Very High |
| READ | ND | √ | | | |
| | SD | | | √ | |
| | CD | √ | | | |
| WRITE | ND | | √ | | |

 

| | | | | | |
|---|---|---|---|---|---|
| | SD | | | | √ |
| | CD | | | | √ |
| MASS READ | ND | | √ | | |
| | SD | | | | √ |
| | CD | | √ | | |
| MASS WRITE | ND | | | √ | |
| | SD | | | | √ |
| | CD | | | | √ |
| Privileged Command | SD | | | | √ |
| | CD | | | | √ |

The impact of the data types for each type of command can be categorized as shown in Table 3 above. Some of these commands are menacing since execution of such commands has significant impact. Therefore, when executing such risky commands, the past execution history must be referred. If such history exists at least once a month, the history bit is set to 0; otherwise, the history bit is set to 1. The correlation of the history bit with abnormality pattern can be expressed as follows.

Abnormal pattern ∮=XOR((DL_SD) ∩ (AL_SP_AR) ∩ history Bit '1') or
Abnormal pattern ∮=XOR((DL_SD) ∩ (AL_MP_AR) ∩ history Bit '1') or
Abnormal pattern ∮=XOR((DL_CD) ∩ (AL_SP_AR) ∩ history Bit '1') or
Abnormal pattern ∮=XOR((DL_CD) ∩ (AL_MP_AR) ∩ history Bit '1') or
Abnormal pattern ∮=XOR((PL) ∩ (DL_SD) ∩ (AL_NR) ∩ history Bit '1') or
Abnormal pattern ∮=XOR((PL) ∩ (DL_CD) ∩ (AL_NR) ∩ history Bit '1')

## 4. Simulation

Abnormality determination algorithm (∮=1) was applied around the recent incidents. The cases of massive personal information leak incidents occurred in 3 major Korean financial companies in 2014. The algorithm was applied as shown below.

System Layer: SL_AA = “0”, ∮=“0”
Data Layer: DL_SD_RA = “0”, linked to AL
Action Layer: AL_MP_NR, ∮=“0” or “1”
Command History(History Bit): ∮=“1”

Thus the value of abnormal pattern(∮) = XOR((SL_AA) ∩ (DL_SD_RA) ∩ (AL_MP_NR) ∩History Bit) = XOR(0 ∩ 0 ∩ 0 ∩ 1) = 1, is calculated. This case is an incident occurred where the users who have aright access to the sensitive data repetitively mass read the data and the history bit value influenced judgment on the existence of abnormality.

Next, the application of total service suspension incident of banking services by Korean company N in 2011 is as follows:

System Layer: SL_AA =“0”, ∮=“0”
Data Layer: DL_CD_WA =“1”, ∮=“1”

Thus the value of abnormal pattern (∮) = XOR((SL_AA) ∩ (DL_CD_WA)) = XOR(0 ∩ 1) = 1, is calculated. This case is an incident occurred where the users who have access rights to execute system privileged commands and influenced judgment on the existence of abnormality.

The algorithm presented above for determining the abnormality pattern was confirmed applicable through the simulation thus far. However additional case studies would be necessary on the association with physical layer and detailed statistical verification.

## 5. Conclusion

This paper studies and analyzes people-oriented security vulnerability assessment techniques in order to overcome the limitations of the prevailing system-oriented and data-oriented security vulnerability assessment techniques. This paper focuses on the method to analyze the patterns of the security breach incidents caused by IT users, and confirms that such patterns of human-caused security breach can be categorized into certain cases. It is also confirmed that the cases of abnormal patterns where $\oint$=1 can be extracted from such categorization and that the execution history of critical commands can be added as an additional requirement for determining security abnormal pattern, which enables the people-oriented assessment and analysis of security vulnerability. However, further research would be necessary on how to minimize the variances in the determining factors for abnormal patterns, the effectiveness of such factors, and correlation with the real cases.

## Acknowledgements

This study was financially supported by the research year fund of Mokwon University in 2015

## References

[1] C. Park and D.-S. Ko, “Mesh Type Security Model Based on Key Data Flow”, The Journal of Korean Institute of Information, vol. 12, no. 3, **(2014)** Mar., pp. 77-78.
[2] Common Vulnerability Scoring System (CVSS - SIG), https://www.first.org/cvss, **(2015)** June 10.
[3] D. M. Keinzle, M. C. Elder and D. S. Tyree, “Security patterns template and tutorial”, **(2002)** June.
[4] R. Wassermann and B. H. Cheng, “Security Patterns”, Technical Report MSU-CSE-03-23, Computer Science and Engineering, Michigan State University, **(2003)** Aug.
[5] J. Yoder and J. Barcalow, "Architectural Patterns for Enabling Application Security", **1997**.
[6] STIG (Security Technical Implementation Guide) V6.26, **(2016)** Jan.
[7] Ministry of Public Administration and Security Announcement #2011-45, **(2011)** Sep. 30 legislate, **(2011)**, Sep. 30, enforcement.
[8] A. Collins, “Building a people-oriented security community the ASEAN way”, Routledge, **(2013)**.
[9] L. I. U. Zi-Lin, “Discussion on People-Oriented Management of the University Laboratory”, Research and Exploration in Laboratory, **(2010)**.
[10] K.-i. Kim and H.-s. Park, “An Auto-Verification Method of Security Events Based on Empirical Analysis for Advanced Security Monitoring and Response”, Journal of The Korea Institute of Information Security & Cryptology, vol. 24, no. 3, **(2014)** Jun.
[11] P. Ning, D. Xu, C. G. Healey and R. S. Amant, “Building Attack Scenarios through Integration of Complementary Alert Correlation Methods”, Proc. on the 11th Annual Network and Distributed System Security (NDSS '04), **(2004)** Feb, pp. 97-111.
[12] IBM z/OS UNIX Commands Reference, SA22-7802-14, **(2016)**.
[13] IBM z/OS Commands Reference, SA22-7627-25, **(2016)**.

## Authors

**Choon Park,**

Aug 1986: SNU, Department ofMathematics Education
Feb 2014: Mokwon University, Master of Engineering
1986 ~ 1993: IBM Korea
Oct 2008 ~ Sep 2009: Korea Communications Commission, Security Expert

 

1998 ~ Now: CEO of NICECOM Consulting Co. LTD
Area of Interest: Security, Converged IT, Cloud

**Dae-Sik Ko,**

Feb 1982: Kyunghee Univ. Department of Electronic Engineering (Master Degree)
Feb 1991: Kyunghee Univ. Department of Electronic Engineering (Doctor Degree)
1994~1995: UCSB Post-Doc
1998 ~ Now: Mokwon University, Professor of Electronic Engineering Department
Area of Interest: Multimedia, Converged IT, Cloud