International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.187-194
http://dx.doi.org/10.14257/ijsia.2015.9.8.15

A Study on the Development of the Emergent System Recovery in an Effective Way from Hacking Attacks or Security Incidents

Jeongbeom Kim

Professor, Industry-Academic Cooperation Foundation, Namseoul University, 91 DaeHakRo, SeongHwanEup, SeoBukKu, CheonAnSi, ChungNam, KOREA
jbkim@nsu.ac.kr

Abstract

The purpose of this paper is to study on the development of efficient system recovery from various hacking attacks or computer virus incidents. When computer system was damaged by hacking attacks or cyber incidents, and needed to be recovered efficiently, the best way is to roll back to the original system status. If the situation were unable to return to its original status, one of the best ways in system recovery would be going back to prior day status using security technology effectively. By applying filter driver, one of the key points of this development, which resides between MBR (Master Boot Records) driver and BIOS (Basic Input Output System), can enable to go back to the prior day system status for the efficient recovery. The main objective of this paper is to study about the development of emergent system recovery solution concerned with security incidents to react rapidly and correctly from the viewpoints of system reliability and stability.

Keywords: *System Recovery, Roll Back, Security Incident, System Down, Emergent System Recovery, Hacking, filter driver, MBR, BIOS*

1. Introduction

When the system was damaged by hacking attacks or security incidents, it should be recovered emergently and effectively using the proper system recovery. This study of development can be more complete and concrete solution compared to the existing methods or technologies solution in terms of reliability and stability. Some existing solutions can only react partially or be defenseless by new hacking attack or computer virus. This development suggests new concept about emergent system recovery efficiently and effectively in operating IT systems securely. In this paper, some new technologies are introduced from the perspective view point of system reliability concerned with security related incidents. There are many solutions and studies about recovery solution already. The main difference between this development and existing solution is that this mechanism is real time system recovery from security incidents using filter drive which is transparent layer technology. Building the exact infrastructure for system recovery from cyber incidents in effective way is very important in business operation for the company or every organization. This study details how the technical infrastructure of effective system recovery enables important shifts in a company's leadership and organizational models–shifts that improve the company's interface to customers and enable increased revenue. The effective management of the total security information management is a fundamental concern for the long-term growth of each organization or company in competitive markets. There is no organization which is not keen to security issue and efficient growth. The most pressing issues about security management in these days are quick response to various kinds of hacking attacks. Hence, many organizations are concerned with business enablement architecture to avoid impact and damage from outside security

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

attacks. Information security is practiced in daily operation as people respect the policies and principles related with it A company that becomes security-driven can change shape reliable and radically as its structure conforms to its new business logic.

2. Concept of Technology Development about Emergent System Recovery from Security Incidents in an effective Way

2.1 Architecture of Development System

The key point of this development is system architecture using filter driver, one of the key points of this development, which resides between MBR (Master Boot Records) driver and BIOS (Basic Input Output System), can enable to roll back to the prior day system with emergent recovery. This filter driver can be transparent layer as security kernel. When the system is initialized, BIOS (Basic Input and Output System) give order MBR (Maser Boot Records) to read HDD (Hard Disk Drive) data. Usually MBR is the program list to be triggered firstly for system booting. MBR is system related data positioning at top of memory with priority. As soon as HDD starts to operate CPU reads MBR firstly for the initialization of system. MBR can be the direction order as a map. It is a collection of system required data just before OS (Operating System) is loaded. Filer Drive, which is the new concept of this technology, is positioned between BIOS and MBR as security kernel. This can be another BIOS and control MBR as security kernel mode. Below diagram describes the architecture about a new concept of this technology. As shown below picture, this architecture is using filter drive which is transparent layer located between BIOS and MBR driver to control system completely during recovery action securely.

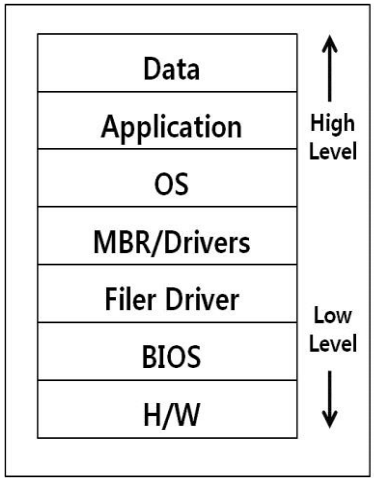

Figure 1. Architecture of Development System

The main purpose of filer drive is to control system BIOS data to do the system recovery when the system has a problem with security incidents.

2.2 Related Study about System Roll Back

There is some research about the algorithm of system roll back from system down to do the instant recovery. Related studies are virtual storage structure, transparent layer mechanism, and peel-off recovery algorism. Keeping Security for system is priority in terms of reliability for competitive edge in business operation. Effective recovery management lies at the core of system security. Below table describes the comparison among the related studies.

 Copyright ⓒ 2015 SERSC

Table 1. Comparison Among the Related Studies

	Real Time System Recovery Solution	Vaccine S/W	Image Recovery Solution
Concept	**Total recovery and deletion of computer virus, hacking codes, system error on spot timing**	Detect computer virus which have uniform form and Delete	Reinstallation of system with system copy on designated spot
Objective	**Keeping clean system status by immediate deletion of all security incidents and prompt system recovery in emergency situation**	Protection of known pattern computer virus and Deletion	Reinstall when system error during operation and operate normally
Installation Process	**Installation of S/W**	Installation of S/W and constant pattern update	Installation of S/W, and production of existing system image copy
Recovery Algorithm	**Every Booting time, real time system recovery if needed, in 3 seconds**	Consistent update and system inspection , deletion of damaged file and clean for several minutes	Reinstallation and image copy for several miniatures
Action for cyber incidents	**When security incidents are happened, system recovery promptly**	Collection of unknown patterned virus, and Analysis, and application of vaccine program	Reinstallation of all damaged system
Key Difference	**Keeping the optimum security status by regular deletion of unknown computer virus, hacking codes, harmful codes**	When the system is damaged by harmful virus or worm virus, complicated cleaning process is needed..	Not effective way by reinstallation of damaged system from the incidents

2.3 Algorithm of System Roll Back for the Effective Recovery

This algorithm is applying the concept of transparent layer which is filter drive between BIOS and MBR/Drivers, using system drive and data drive. Data drive is kind a of virtual storage to store updated data which is change from system data. At the initial status, A B C D and E data are stored in transparent layer (filter driver) of system drive. When there are some change for A, C data, and new input F, G data, then F, G and A1 and C1 are stored in another address in system drive during operation. If emergency situ-

Copyright ⓒ 2015 SERSC

ation happen, and there is a need to roll back original status, then by switching off the channel of only changed data which are A1, C1, F, and G make to system time back or roll back to prior status in real time. The best benefit of this algorithm is real time base in rolling back the system to its original status. This method can be a new way of system recovery in short time in terms of security-driven strategy. Following diagrams show about the technical architecture of system recovery mechanism during system operation. Using this simple algorithm, system roll back for the complete recovery can be executed with time back base in a short time securely. This mechanism is using system drive, data drive, and mapping table for the change of data. The function of mapping table is the key points of this technology in system area for the efficient recovery activity in terms of system maintenance and reliability.

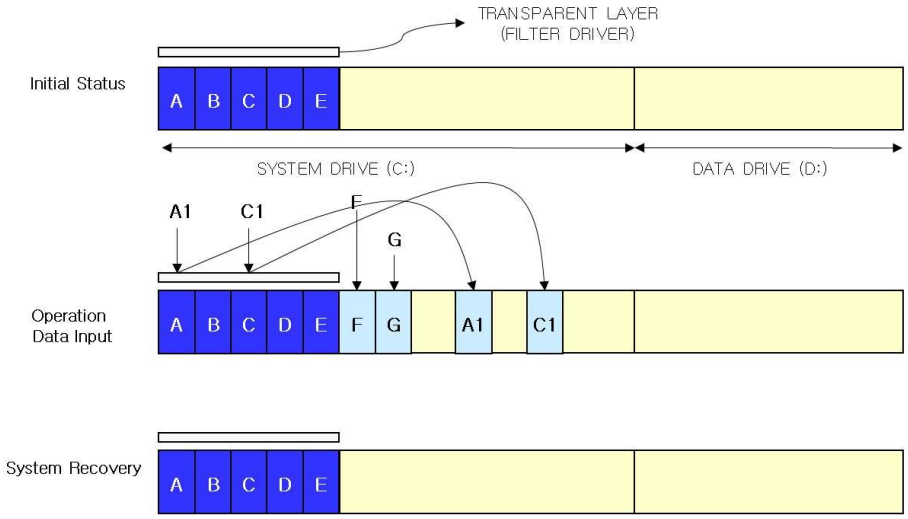

Figure 1. Algorithm of System Roll Back

2.4 Configuration of Development System

The following is a system configuration of emergency recovery solution with roll back algorithm in an effective way. When normal condition system has been impacted by a system error, system hacking, batch error or virus codes, that system condition changed to abnormal condition and needs prompt action to recovery. The time back so called roll back algorithm can recover the damaged system to normal condition with prior day status in real time. This solution uses information table and mapping table in system area so that protection is being done only for the security needed portion, not all system area, reducing the necessary buffer size which is protecting the system area. This data protection mechanism divides system area and buffer area, which use meta information table, system area information table, and mapping table. Mapping table enables the data sync between normal status and abnormal status in a system area on the occasion of time back action activity. This time back is conducted rapidly and completely the form of roll back action. Below picture shows the total configuration about this solution.

Copyright ⓒ 2015 SERSC

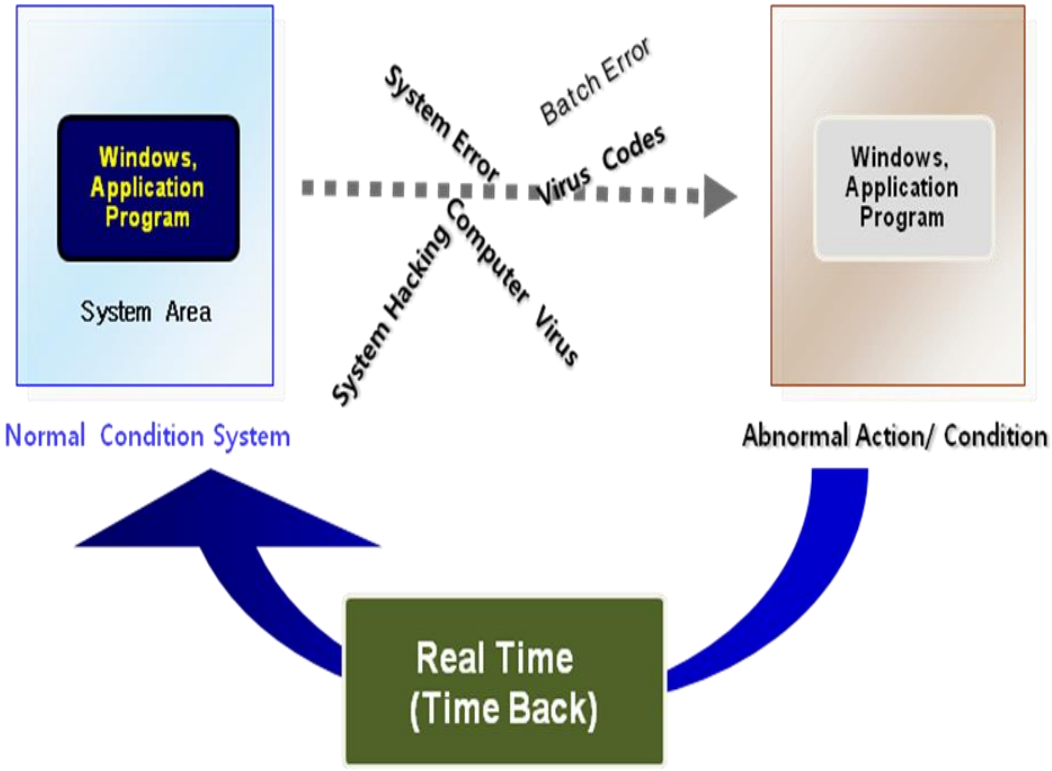

Figure 2. Configuration of Development System

3. System Flow about the Effective Way of Emergency System Recovery from Security incidents

The effect of system emergency recovery solution can be described as the following. Firstly, through the rapid and perfect system recovery all kinds of software problem caused by security incidents can be solved to do an operation of IT system continuously. Secondly, this solution can save the cost of system maintenance resources and recovery time dramatically. Thirdly, by using new concepts of back up algorism this solution can compensate existing security plan from hacking attacks, incidents, and firewall and intrusion system.

Copyright ⓒ 2015 SERSC

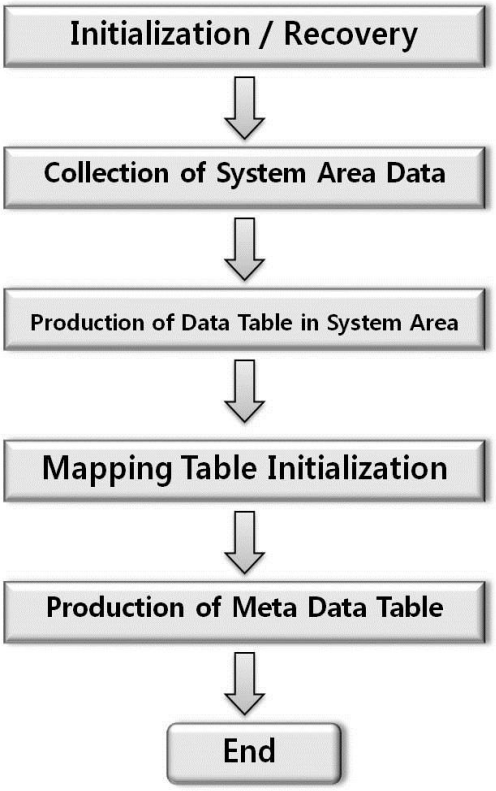

Figure 3. System Flow of New Recovery Solution

4. The Benefits of Time Back Recovery Solution

Through this thesis, the development about system recovery from security incidents and hacking virus attacks in emergency situation has been studied technically. To protect from cyber incidents which can be APT (Advanced Persistent Threat) or Computer Virus or hacking attacks, this algorithm can secure the system area using filter drive as transparent layer and mapping table mechanism. The system recovery can be done almost in real time through experiment of this development in many ways with PC platform and NT platform base. Using this algorism many developments will be executed to be implemented for business purpose. The following are the benefits of time back recovery solution. Firstly, this solution can do system recovery rapidly and completely through accomplishing secure system recovery from S/W related error during system operation and worm virus or cyber attacks from external networks. Secondly, this solution can secure continuity of system operation concerned with system recovery or various system errors with real time roll back mechanism. Thirdly, this solution can save resources and costs about system maintenance extensively and in a simple way. Usually 70% of system errors are S/W related problem and this can be solved by system roll back recovery solution. This solution can save cost of purchasing S/W about computer virus search/cure, or back up related solution. Thirdly, this solution is a new concept of security effect in protection of system and networks. This solution can be a new security scheme in protecting virus and hacking attacks, and intrusion which is compared with existing incomplete security solution. So far, the existing solutions can react only to current viruses partially and are not protective in limited ways. This solution can also maintain complete security clean condition during normal operation and doing system recovery in every time of booting. One of the advantages of this solution is conducting rapid and total system control in emergent situation with the functions of a system control and recovery in real time base.

Copyright ⓒ 2015 SERSC

5. Conclusions

Organizational resistance to change is, of course, not unique to companies becoming security-driven, although initial discomfort may be stronger than usual for the simple reason that becoming security-driven means an extensive revamping of processes and the way of doing business. Until a company or organization becomes security-driven, its process and as its system, are unreliable to cyber incidents. Initial resistance and confusion are not surprising. Operating in the security-driven environment is not necessarily more complex, although it is natural for something new to feel complex. Some decision makers, put off by the more challenging new environment, are tempted to point out what's wrong with becoming security-driven rather than anticipating the benefits once new complexity is mastered. Leadership must play a role in inspiring people to change, explaining the superior value of change-to customers and to company or organization-and patiently educating employees or members how to thrive in the new environment to have a competitive edge. Most of existing solutions are not able to recover system with real time, using time back scheme of going back to prior day status. When the system was attacked and damaged by cyber incidents i.e. APT(Advanced Persistent Threat) or Computer Virus or hacking, one of the best way is to time back the system to prior day status in terms of reliability, availability, and stability. In this thesis, the development of system emergency recovery from various kinds of security incidents is verified. This solution can be executed in system area, temporary area, and data base area in the form of partition drive units to increase the stability of system and instant recovery from system disaster caused by security incidents mainly. For the emergency system recovery this solution applied peel-off recovery algorism which extends transparent layer data input and output. By applying this PRA algorism, we can construct more solid disaster recovery system than existing system back up method. From the secure system operation view points, this development can influence to emergency recovery of IT system from security incidents or hacking attacking attacks in many ways. Some similar studies are being done to provide IT systems with the best possible services with these circumstances. There are some limitations of this research that should be considered. Firstly, the verification of this total architecture through questionnaire and survey has not been proposed. Further study can do this research using real reference cases. Secondly, the value of this solution can be compared with real cases if there is statistical result analysis. Thirdly, application of this research can be extended in many security management areas through the implementation of this solution for validity. Thirdly, all of the diverse factors about intelligent security model have not been discussed in this paper. These limitations can be studied for future research, which can be contributed to the development in security management areas.

In the future, real implementation of this development will be studied empirically with many real cases.

References

[1] Ye Zhang and Kaigui Wu, Software Cost Model Considering Reliability and Time of Software in Use, Journal of Convergence Information Technology, Volume7, Number13 (2012), pp. 135-142
[2] H. S. Nalwa, Editor, Magnetic Nanostructures, American Scientific Publishers, Los Angeles (2003)
[3] Method of Data Resource Secure and Quality Management in Big Data Era, NIA, (2012)
[4] Denning P, Computer Under Attack Intruders, Worms and Virus, Addision Wesley, (1990).
[5] C.P. Pfleeger and S.L. Pfleeger, Security in Computing, Prentice Hall , (2003)
[6] Hojin Lim and Shinhye Park, Security 3.0, IDam Publisher, (2011), pp. 305-307
[7] Jongsun Hwang and Jingon Son, Data Structure in JAVA langage, published by Junggik, (2000) pp.168--171.
[8] Wan Soo Cho, "Information System Security", HongRyung Science Publishers, Seoul, vol. 1, (2003), pp. 399.
[9] J. Davis, G. J. Miller and A. Russel, "Information Revolution", Published by John Wiley &Sons, Inc,. New Jersey, (2006), pp. 133-139.

Copyright ⓒ 2015 SERSC

[10] Vivek. Ranadive, "The power of now", published by Mcgraw-Hill, (1999), pp.1722-175.
[11] W. S. Cho, "Information System Security", HongRyung Science Publishers, Seoul, vol. 1, (2003), pp. 19-25.
[12] A. Hoog, translated by K. Yoon, "Android Forensic", Acorn Publishers, Seoul, vol. 1, (2013), pp. 209-213.
[13] C. M. Christensen, S. D. Anthony and E. A. Roth, "Seeing What's Next", published by Harvard Business School Press, (2004), pp.55-59.
[14] JeongBeom. Kim, "A study on the development of Integrated Security Technology based on Big Data", Advanced Science and Technology Letters, (Security, Reliability and Safety 2015), http://dx.doi.org/10.14257/astl.2015.93.09, vol. 93, pp. 40-43.
[15] K. Son, "Information Security Industry Trend and Forecast", Proceeding of Korea Information Processing Society Review, vol. 17. 6th, (2011) November, pp. 99-101.

 Copyright ⓒ 2015 SERSC