제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

저장장치시스템의 취약성 분석 및 연구

김훈*, 윤희용*, 최성춘*, 이보경**, 최중섭**, 김홍근**
*성균관대학교 정보통신 공학부
**한국 정보 보호 진흥원 정보 보호 기술팀
*{hunkim, youn, choisc}@ece.skku.ac.kr , **{bklee, jschoi, hgkim}@kisa.or.kr

Vulnerability Analysis and Research on Storage System

Hun Kim*, Hee Yong Youn*, Sungchune Choi*
Bo Kyoung Lee**, Joong Sup Choi**, Hong Geun Kim**
*School of Information and Communication, Sungkyunkwan University.
**Information Security Technology Division, Korea Information Security Agency.

요 약

컴퓨터 네트워크 기술의 급속한 발전은 네트워크를 이용한 전자상거래와 전자금융 같은 서비스를 다양하게 발전시켰고, 이로 인하여 발생되는 데이터의 양은 기하급수적으로 증가하고 있다. 이에 따라 폭발적으로 증가하는 데이터를 효율적으로 저장하고 관리할 수 있는 저장장치시스템의 중요성이 극대화되고 있으며, 다양한 취약성을 극복할 수 있는 보다 안전한 저장장치시스템이 요구되고 있다. 따라서 본 논문에서는 데이터가 오용, 남용, 변형, 유출, 그리고 손상될 수 있는 저장장치시스템의 다양한 취약성에 대하여 분석하고, 발생 가능한 취약성들을 해결할 수 있는 침입감내 및 복구 시스템에 대하여 연구한다.

1. 서론

오늘날 컴퓨터 네트워크 기술의 급속한 발전은 네트워크를 이용한 서비스를 다양하게 발전시켰고, 그 결과 많은 정보를 생산하게 되었다. 멀티미디어 정보의 폭발적인 증가, 기업 데이터베이스의 규모 증대, 각종 업무 자료의 디지털화, 전자상거래, 그리고 전자금융으로 인하여 대용량 정보의 발생은 필수 불가결하게 되었고, 이러한 정보의 효율적인 관리 및 저장을 위해 스토리지의 중요성 또한 중요하게 부각 되었다.

저장장치시스템은 물리적인 결함이나 오류, 침입 또는 내부의 공격, 그리고 환경적 요인으로 인하여 데이터의 손실이나 변형 및 유출이 발생 할 수 있다 [1]. 이를 해결하기 위해 국가연구 기관이나 연구소들이 저장장치의 결함에 대해 효과적으로 대처하기 위한 연구들을 다방면에서 수행하고 있다. 그럼에도 불구하고 현재까지 저장장치시스템의 종합적인 취약성 분석에 대한 연구는 미비한 상태이다. 따라서 본 논문에서는 저장장치의 데이터가 손실, 변형, 그리고 유출될 수 있는 저장장치의 다양한 취약성에 대하여 연구하고, 발생 가능한 취약성들을 해결할 수 있는 기법들에 대해 소개하며 보다 안전한 저정장치시스템을 구성할 수 있는 침입감내 및 복구 시스템에 대하여 논의 한다. 이에 근거하여 스토리지의 취약성 방어 및 복구를 허락하는 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 현존하는 저장장치 시스템에 대한 취약성을 분석하고 그에 따른 대책방안에 대하여 논의하고, 3 장에서는 저장장치시스템의 취약성을 해결하기 위한 안전한 침입감내 및 복구시스템에 대하여 논의하고, 마지막으로 4 장에서는 결론을 맺는다.

2. 저장장치 시스템의 취약성 분류 및 대책방안

이번 장에서는 저장장치시스템에 저장된 데이터가 손실, 변형, 그리고 유출될수 있는 취약성의 원인에 대하여 세부적으로 분류하고 분석하려 한다.

2.1 저장장치 시스템을 위한 보안 작업 분류

우선 저장장치 시스템의 취약성을 세부적으로 분류하기 이전에 취약성을 최소화 하기 위한 보안작업의 분류가 우선 필요하다. 저장장치 시스템에 대한 보안작업의 분류는 정책적 보안, 네트워크 보안, 호스트 보안, 그리고 애플리케이션/데이터 보안의 4 가지로 나뉜다.

정책적 보안은 저장장치시스템에 접근하는 사용자의 접근 절차 및 범위를 관리하고 통제하기 위한 부분으로 내부 사용자의 공격으로 인한 저장장치시스

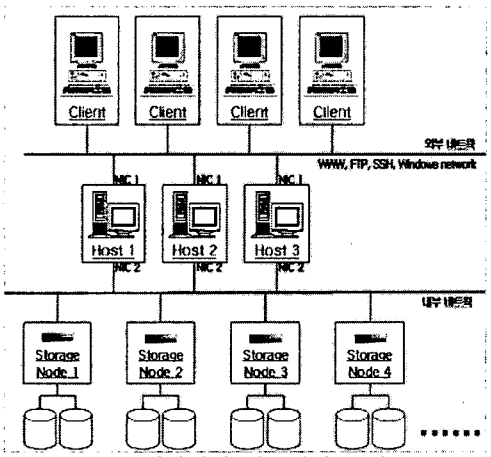
템의 취약성을 최소화할 수 있다. 네트워크 보안은 현대의 저장장치시스템이 네트워크 기반 시스템이기 때문에 네트워크를 구성자체에서 발생할 수 있는 취약성을 낮추기 위한 부분이며, 네트워크을 구성하는 장비 자체의 잘못된 설정으로 인한 위험을 최소화할 수 있는 부분이다. 호스트 보안은 정책적 보안 및 네트워크 보안이 침입자에 의해 무력화되어 자료가 손상되거나 유출되지 않도록호스트 자체의 보안성을 강화시킬 수 있는 보안 방법이다. 마지막으로 애플리케이션/데이터 보안은 애플리케이션 자체에 있을 수 있는 취약성과 데이터 베이스 등의 취약성을 강화할 수 있는 부분이다. 이러한 분류된 보안 작업을 통해 저장장치시스템의 취약성을 최소화 할 수 있다.

2.2 저장장치 시스템의 취약성 분석

이번 장에서는 저장장치시스템에서 발생할 수 있는 다양한 취약성에 대하여 세부적으로 분류하고 각 취약성에 맞는 대응방안에 대하여 논의하려 한다.

저장장치시스템은 (그림 1)에서 보는것과 같이 서비스를 요청하는 클라이언트, 저장장치 시스템을 관리하면서 사용자의 요청을 처리하는 호스트, 그리고 실제 데이터를 저장하는 대용량 저장장치로 분류된다. 따라서 저장장치시스템의 취약성 또한 다음과 같이 나뉘게 된다.

- 네트워크 기반 공격에 대한 취약성
- 소프트웨어적인 공격에 대한 취약성
- 저장장치의 물리적인 취약성
- 사용자(내부/외부)에 의한 공격에 대한 취약성



(그림 1) 저장장치 시스템의 구성도.

2.2.1 네트워크 기반 공격에 대한 취약성

현재의 컴퓨팅 환경은 네트워크를 기반으로 구성되고 있으며, 대용량의 데이터 관리 및 저장을 위한 저장장치시스템 또한 Fibre Channel [2]을 이용한 고성능의 네트워크를 기반으로 동작한다.

최근 네트워크를 이용한 네트워크 절단과 시스템 자원 고갈 등과 같은 서비스 거부 공격이 급증하고 있다. 서비스 거부 공격은 고의적으로 대량의 네트워크 트래픽을 유발하여, 정상적인 네트워크 서비스를 불가능하게 만드는 공격을 의미한다. 대표적인 서비스 거부 공격에는 SYN Floodin 공격 [3]과 Smurf 공격 [4]이 있다. 이러한 네트워크를 통한 공격으로부터 저장장치 시스템을 보호하기 위해 현재 가상사설네트웍(VPN) [5]과 방화벽(Firewall) [6]등의 기술이 널리 사용되고 있다.

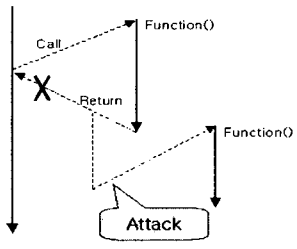
VPN 은 종단간에 적절한 암호기술을 이용하여 한 조직의 내부 사용자들이 사내나 사외에서 서로 안전하게 통신할 수 있는 채널을 형성해 주며 또한 필요에 따라 접근제어 기능을 제공해 준다. 반면 방화벽은 기본적으로 인터넷과 자신의 네트워크를 보호하고자 하는 일차적인 방어 역할을 한다. 그러나 방화벽에 의한 접근통제는 주로 TCP/IP 프로토콜 헤더의 정보나 약간의 응용 데이터 해석 정도를 이용하므로 복잡한 네트워크 공격이나 호스트에 대한 공격 등을 차단하는데 한계가 있다. 또한 내부의 합법적인 사용자에 의한 불법적인 자원 남용에 대해서는 그 역할을 전혀하지 못한다. 이러한 방화벽의 부족한 부분을 보강해줄 수 있는 것이 3 장에서 설명하게 될 침입탐지시스템으로 로컬 네트워크나 호스트에 위치하여 정밀한 분석을 통해 보다 다양한 공격이나 불법행위 등을 탐지하여 대응방안을 세울 수 있게 해준다.

2.2.2 소프트웨어적인 공격에 대한 취약성

소프트웨어적인 취약성은 일반적으로 실제 사용자의 요청을 처리하는 호스트 운영체제에 파일 시스템의 구조적인 문제점이나 프로그램상의 오류를 이용한 인증받지 않은 사용자 즉 공격자에 의한 공격이다. 최근에도 파일 시스템의 취약성을 이용한 공격이 다양하게 발생하고 있으며, 그 중에 대표적인 공격으로 버퍼 오버플로워 공격 [7]이 있다.

버퍼 오버플로워 공격은 (그림 2)와 같이 서버가 프로그램을 실행할 때, 메모리 구조를 이용하여 프로그램의 흐름을 조정하는 공격으로, 루트(최고사용자)의 권한을 얻기 용이한 공격이다. 이러한 공격에 취약한 프로그램은 (표 1)에 나타낸것과 같다.

이러한 파일 시스템의 취약성으로 인한 공격을 예방하고 방지하기 위해서는 파일 시스템의 동작에 대한 코드를 수정하고, 취약성을 보완하기 위한 코드를 추가해야 한다.



(그림 2) 버퍼 오버플로워 공격의 기본 개념.

(표 1) 버퍼 오버플로워 공격에 취약한 프로그램 예

운영체제	프로그램
Solaris	Ffbconfig, gethostbyname(), fdformat, eject, getopt(), at, ps, chkey
Linux	cron, NLSPATH, inn, lpr, cfingerd 1.2.3, elm
IRIX	df, pset, eject, login/sheme, ordist, xlock
AIX	libDtSvc.a

2.2.3 저장장치의 물리적인 취약성

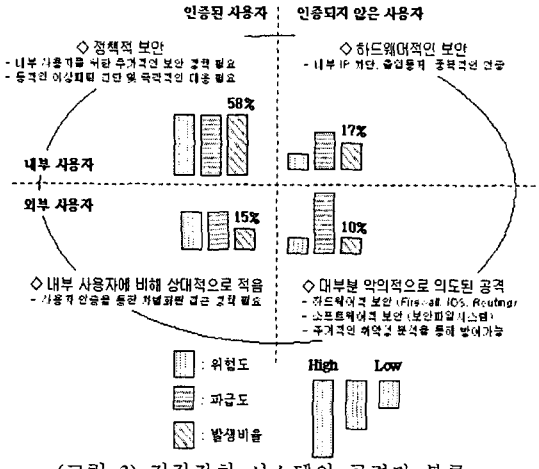
정보저장시스템은 물리적인 장치로써 기계적인 오류, 침입, 그리고 천재지변으로 인하여 전체 저장장치 시스템을 이루는 저장장치 중 일부가 손상받을 수 있다. 이러한 저장장치의 물리적인 취약성은 전체 저장장치 시스템의 가용성을 낮게 하는 원인이 된다. 또한 데이터의 보안성을 높이기 위해 데이터를 분할하여 다수의 저장장치에 분산 저장할 경우, 하나의 저장장치가 복구 불가능 하게 되면 완전한 데이터를 복구하기가 어렵게 된다. 이러한 저장장치의 하드웨어적인 결함을 극복하기 위한 방법은 동일한 데이터를 여러 개 복사하여 유지하는 것이다.

여러 개 존재하는 데이터의 복사본을 사용할 때, 데이터의 중복적인 읽기/쓰기로 인하여 시스템의 성능이 저하될 수 있으며, 데이터의 일관성문제가 발생하기 쉽다. 그렇기 때문에 현재 사용되는 복제 데이터의 관리는 논리 구조를 이용하여 보다 효율적으로 중복된 데이터를 관리할 수 있는 Tree Quorum 프로토콜 [8] 이나 Grid 프로토콜 [9]을 사용하고 있다. 이들 프로토콜의 사용으로 시스템에 발생할 수 있는 성능 및 가용성문제를 해결하고 저장장치 시스템의 생존성을 높일 수 있다.

2.2.4 악의적인 공격자에 대한 취약성

실제 저장장치 시스템의 취약성의 대부분을 차지하고 있는 부분이 악의적인 침입자나 내부 관리자의 공격에 인한 것이다. 이전 장에 설명한 네트워크를 통한 공격이나 파일 시스템 공격 또한 외부의 침입자에 의한 공격의 일종이다. 실제 물리적인 하드웨어의 결함을 제외하면 공격자에 대한 취약성 문제가 저장장치시스템에서 가장 심각한 문제이다.

(그림 3)은 공격자의 유형에 따라 저장장치 시스템을 공격하는 공격자를 4 가지로 분류한 그림이다. 저장장치 시스템을 공격하는 공격자의 인증 여부에 따라 인증된 사용자와 인증되지 않은 사용자로 나뉠 수 있고, 공격자의 위치에 따라 내부 사용자와 외부 사용자로 나뉠 수 있다. (그림 3)에서 주목할 만한 점은 각 공격의 발생 비율로 보아, 인증 받지 않은 외부의 공격자 즉 해커의 공격 비율이 가장 적게 나타난다는 것이다. 반면에 정상적인 인증을 거친 내부자에 의한 공격이 4 가지 경우 중 가장 많은 비율을 가지며, 위험도나 파급도면에서도 가장 위험하다는 것을 볼 수 있다. 이러한 이유는 실제 저장장치시스템의 보안체계가 외부의 악의적인 침입자를 막기위해서 각각의 특성에 맞는 동작을 수행하지만, 실제적으로 내부의 인증된 관리자에 의한 공격에는 저장장치 전체가 거의 무방비 상태로 놓여 있기 때문이다.



(그림 3) 저장장치 시스템의 공격자 분류.
(출처: Gartner Consulting)

(그림 3)의 내부 사용자에 대한 공격 중 인증된 내부 사용자에 의한 저장장치 시스템의 공격은 외부로부터 침입에 대응하기 위해 사용하는 침입감내시스템과 같은 보안 시스템으로는 공격을 막을 수 없다. 따라서 이러한 공격에 대해서는 공격의 범위를 최소화하기 위해 내부 사용자를 위한 저장장치 시스템의 접근에 제한을 두고 접근 불가능한 프로그램이나 데이터에 접근했을 때 즉시 접근을 판별하여 이에 대한 대책을 수립하는 것이 최선의 방어이다. 인증되지 않은 사용자의 경우는 실제 시스템에 접근이 불가능 하므로 내부 네트워크에 대한 보안을 강화하고 중복적인 인증 절차를 사용해야 한다.

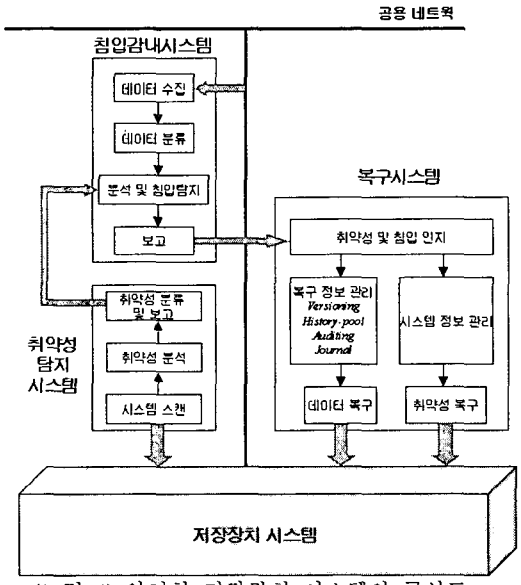
(그림 3)의 외부로부터의 공격은 다음 장에 설명하게될 자기보안 스토리지 시스템과 서버와 사용자간에 상호 인증을 다루는 보안 파일 시스템의 사용으로 피해를 최소화 할 수 있다. 보안 파일 시스템은 네트워크 보안이나 침입감내 시스템과 같은 보안 정책이 무력화 되었을 경우에도, 서버와 사용자간에 종단간 암호화 및 인증를 제공해 주기 때문에 중복적인 보안정책의 수립이 가능하다. 또한 보안 파일 시스템은 일반 유닉스와 같은 파일 시스템에서 제공해줄 수 없는 파일 저장에 대한 암호화를 제공해 줄 수 있으므로 파일 시스템으로부터 인증을 받지 않은 사용자는 저장장치시스템에 물리적으로 접근하더라도 파일의 존재 여부조차 알 수 없게 된다. 이러한 기능을 제공해주는 대표적인 보안 파일시스템으로는 Self-Certifying 파일 시스템 [10], Cryptographic 파일 시스템 [11], 그리고 Steganographic 파일 시스템 [12] 등이 있다.

3. 제안된 스토리지 취약성 방어 및 복구 방법

저장장치 입장에서는 서비스를 요청하는 사용자가 인증된 사용자인지 악의적인 침입자인지 분간할

방법이 없다. 그렇기 때문에 스토리지 노드는 자료의 생존성을 보장하고 자료에 대한 모든 접근을 확인 할 수 있는 구조로 설계되어야 한다. 또한 만약 침입자를 발견하였을 경우 피해 범위를 파악하고 이를 복구할 수 있는 능력을 갖추고 있어야 한다. 이를 위해 (그림 4)와 같이 침입감내시스템, 취약성탐지시스템, 그리고 복구시스템 모두를 갖춘 안전한 저장장치시스템이 요구된다.

(그림 4)의 침입감내시스템은 사용자의 접근을 분석하여 악의적인 침입자를 발견하고, 발견된 침입자가 저장장치 시스템의 어떤 취약점을 이용했는지 분석하고 복구시스템에게 보고하는 작업을 담당한다. 복구시스템은 침입감내시스템으로 받은 정보에 근거하여 침입자가 저장장치 시스템에 침입하여 어떤 작업을 했는지 알아내고, 백업된 정보를 이용하여 저장장치 시스템의 손상된 정보를 복구하는 기능을 담당한다. 마지막으로 취약성탐지시스템은 계속 증가하는 저장장치의 취약성 항목에 기준하여 저장장치시스템을 주기적으로 스캔하여 현재 저장장치가 가지고 있는 취약성에 대하여 분석하고, 분석된 정보를 침입감내 시스템에게 보고하여 차후 침입에 대해 미리 대응한다. 또한 복구시스템을 통하여 저장장치 시스템이 가진 취약성을 제거하게 된다.



(그림 4) 안전한 저장장치 시스템의 구성도.

네트워크화된 저장장치시스템에서는 미처 대처하지 못하는 공격이나 침입이 존재 할 수 있다. 이와 같은 침입에 대비하여 발생된 피해를 신속히 복구하고 가용성 높은 시스템을 제공해 주기 위해서는 서비스를 제공하는 시스템을 중복하여 준비하거나 정보를 여러 디스크나 시스템에 분산하여 저장하는 방법을 사용하고, 침입에 의하여 시스템이 다운되거나 서비스가 마비되는 경우에 다른 복제 시스템을 사용하여 서비스를 지속적으로 제공하도록 하는 방법이 요구된다. 이와 같은 방법의 사용을 위해서는 적절한 복제 전략과 피해 발생이 탐지 되었을 때 복제시스템으로부터 자원를 효과적으로 재 할당하고 서비스의 연속성을 제공하기 위한 기술의 추가적인 연구가 필요하다.

4. 결론 및 향후과제

현재 정보의 폭발적인 증가로 인해 발생하는 정보를 저장하고 관리하는 저장장치시스템의 중요성이 극대화되고 있다. 이에 따라 저장장치시스템에 대한 공격으로 인해 데이터의 손실 및 유출 문제가 매우 심각한 상태에 있다. 따라서 본 논문에서는 네트워크화된 저장장치시스템에서 발생할 수 있는 취약성을 세부적으로 분류하고 효율적인 대처 방법에 대하여 논의하였다.

향후 목표는 침입을 포함한 다양한 유형의 결함에도 불구하고, 저장장치시스템의 가용성, 기밀성, 그리고 무결성을 보장하는 침입감내 및 복구 시스템을 보다 구체적으로 설계하는것이다.

참고문헌

[1] E. Miller, D. Long, W. Freeman, and B. Reed, "Strong security for distributed file systems", *Proceedings of the IEEE International Conference on Performance, Computing, and Communications*, 2001, 34-40.

[2] C. Jurgens, "Fibre Channel : A Connection to the Future", *Proceedings of the IEEE Computer*, 28(8), August, 1995, 82-90

[3] H. Wang, D. Zhang, and K. G. Shin, "SYN-dog : sniffing SYN flooding sources", *Proceedings of the 22nd International Conference on Distributed Computing Systems*, 2002, 382 -389

[4] S. Capshow, "Minimizing the Effects of DoS Attack", *Application Note*, 2000. http://www.juniper.net

[5] Venkateswaran, R., "Virtual private networks", *IEEE Potentials*, 20(1), Feb-March, 2001, 11 -15

[6] Zalenski, R., "Firewall technologies", *IEEE Potentials*, 21(1), Feb.-March, 2002, 24 -29

[7] 류혁곤, "Buffer Overflow 개념 및 대응방법", WIO 97. http://www.postech.ac.kr.

[8] D. Agrawal and A. El Abbadi, "The tree Quorum protocol: An Efficient Approach for Managing Replicated Data", *In Proceeding of the 16th Very Large Databases (VLDB) Conference*, 1990, 243-254.

[9] S. Cheung., M. Ammar, , and M. Ahamad, "The Grid Protocol: A High Performance Scheme for Maintaining Replicated Data", *In Proceedings of the 6th International Conference on Data Engineering*, 1990, 438-445.

[10] D. Mazières, "Self-certifying file system", *PhD thesis*, MIT, May, 2000.

[11] Matt Blaze, "A cryptographic file system for unix.", *In Proceedings of the 1st ACM Conference on Communications and Computing Security*, November, 1993, 9-16.

[12] R. Anderson, R. Needham, A. Shamir, "The Steganographic File System", *International Workshop on Information Hiding*, 1998.