SAN의 취약성 분석 및 대응방안

김광혁*, 이상도*, 정태명**
*성균관대학교 전기·전자 및 컴퓨터공학과 실시간시스템연구실
**성균관대학교 전기·전자 및 컴퓨터공학부
{byraven*, sdlee*, tmchung**}@rtlab.skku.ac.kr

Vulnerabilities Analysis and Security Measures of Storage Area Network

Kwang-hyuk Kim*, Sang-do Lee*, Tai-myung Jung**
*Real-Time Systems Laboratory, Dept of Electrical and Computer Engineering, SungKyunKwan University
**School of Electrical and Computer Engineering, SungKyunKwan University

요 약

인터넷의 보급으로 데이터의 생산, 수요, 유통이 급격히 증가하였으며, 조직내의 정보의 공유 및 활용의 요구가 점차 증대되었다. 이에 대한 해결책으로 스토리지 네트워크의 사용이 확산되어 중요정보의 백업, 긴급복구등의 기능을 쉽게 사용할 수 있게 되었다. 그러나 조직내의 중요한 데이터에 대한 백업 및 공유를 수행하면서도 데이터에 대한 보안은 상대적으로 매우 취약한 실정이어서 향후 보안문제가 대두 될 것으로 보인다.

본 논문에서는 SAN의 구성과 동향을 살펴보고 현재 보편화된 SAN 보안 기법인 LUN Masking과 Zoning의 구조와 기능, 이들의 한계점등을 알아보도록 한다. 또 향후 SAN 동향과 그중 IP 네트워크와 스토리지 네트워크의 결합으로 발생되어지는 보안 문제점과 해결책을 제시하도록 한다.

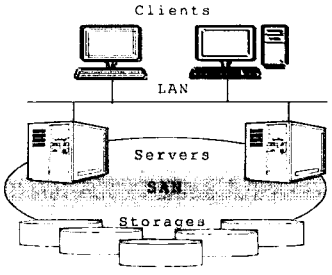
1. 서 론

인터넷을 이용한 비즈니스의 활성화로 여러 인터넷 기반 주요 기술들이 발전해 가고 있다. 인터넷 기반 주요 기술들이 사용하는 데이터는 기본 데이터뿐만 아니라 연산의 결과로 산출해내는 데이터들 모두 많은 양에 달하고 있다. 한편 최근 여러 천재지변, 사고 등으로 인한 기업 데이터 손실로 인하여 기업의 파산을 초래하는 경우가 빈번해지고 있다. 이것은 유형의 인프라를 중요시하던 과거의 관행과는 달리 기업의 데이터가 기업의 존립에 영향을 끼칠 정도로 매우 중요시되고 있음을 말해주고 있다. 따라서 재해, 사고로부터 데이터의 유실을 막고 피해를 최소화 하고자 데이터 백업, 긴급복구에 노력을 기울여 왔다. 과거의 백업은 필요성 및 비즈니스상의 요구부족, 고가의 관련장비, 백업기술의 부재 등으로 인하여 소수의 기관에 그 사용이 그쳤다. 현재는 장애 및 사고로 인한 데이터의 유실이 사업의 연속성을 유지하는데 심각한 영향을 미치므로 비지니스 요구로 인한 백업의 필요성 및 요구가 점점 증가하고 있는 실정이다. 특히, 멀티미디어 데이터의 증가, 전사적 자원관리, CRM (Customer Relationship Management), 데이터웨어하우스, 그룹웨어등의 사용으로 백업의 필요성이 크게 대두된다. 백업의 적절한 솔루션으로 부각되고 있는 것이 SAN(Storage Area Network)이다. SAN은 이런 요구사항을 수렴하여 백업·복구기술을 포함한 스토리지 관리의 비용 감소, 신속한 재난복구, 장기적인 확장성 및 내장애성 등의 강점을 지니고 점차 그 사용이 확대되고 있는 실정이다[10,11]. 국내에서도 10여개 업체 이상이 SAN 솔루션을 공급하고 있으며 매년 큰 성장률을 보이고 있다. 그러나 현재의 SAN 솔루션 공급은 스토리지 기능에만 치우쳐 있으며 데이터 보호에는 많은 관심을 기울이지 않고 있다. 이것은 향후 보안 문제를 야기할 가능성이 있으며 SAN의 Security에 많은 투자가 이뤄져야 할 것이다.

본 논문에서는 현재 SAN Solution의 보안 기능을 살펴보고, 향후 SAN의 발전에 따른 보안 문제를 고려해본다. 본 논문의 구성은 다음과 같다. 2장에서는 현재 SAN의 보안, 3장에서는 SAN의 발전 방향을 제시하고 그에 따른 보안문제를 고려해보고 4장에서는 SAN 보안에 대한 결론을 제시한다.

2. 현재 SAN 기술 및 보안

SAN은 스토리지 네트워크를 구축하는 것으로 스토리지에 대한 고속 액세스 및 공유를 목적으로 하는 네트워크이다. [그림 1]처럼 대규모 네트웍 사용자들을 위하여 서로 다른 종류의 데이터 저장장치를 관련 데이터 서버와 함께 연결되어있다. 대체로, SAN은 한 기업의 전체 컴퓨팅 자원을 연결해 놓은 네트웍의 일부가 된다. SAN은 대개 메인프레임과 같은 다른 컴퓨팅 자원에 아주 근접하여 밀집해 있게 되는 것이 보통이지만, 그러나 백업이나 기록의 영구보관 저장을 위해 광역통신망 기술을 이용하여 원거리에 있는 장소로 확장될 수도 있다.



[그림 1] SAN 구조

복잡한 네트워크 환경과 유기적으로 연결되는 서버-클라이언트들로 인해 데이터 전송량이 증가하여 기존 네트워크로는 더 이상 데이터의 이동 경로가 포화상태에 이르게 되어 기존의 SCSI방식의 한계를 드러냈다[5].

1994년 기본규약이 미국 표준협회(ANSI)에서 인증된 Fibre Channel(ANSI-X3T.11, 이하 FC)은 현재 실용화된 기술로 전송거리 10Km, 전송속도는 200MB/s에 이르는 고속 I/O 채널이다[5]. FC의 채용으로 SAN은 거리와 속도면에서 많은 개선점을 보였다.

이런 SAN을 이용할 때에 얻을 수 있는 이점들은 다음과 같다.

- 빠른 데이터 액세스
- 좋은 확장성
- 높은 이용율과 신뢰성
- 스토리지 자원의 공유 개선
- 기존망으로의 통합의 용이성
- TCO(Total Cost of Ownership)의 감소

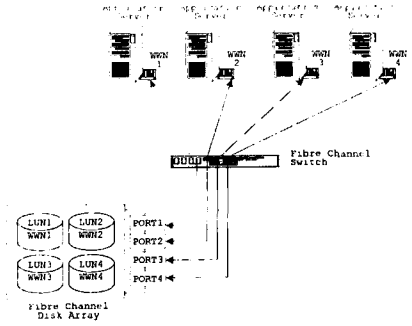
FC는 많은 이점을 제공하고 있지만 FC 프로토콜은 안전한 보안 프로토콜이 아니다. 그러므로 FC를 이용한 SAN에서는 사용자의 동시 접근으로 인한 유효성 유지등을 지원하기 위해서는 보안 기술을 반드시 같이 사용하여야 한다[1].

SAN 보안관리는 데이터 센터 자체에 대한 보안을 먼저 고려하여야 한다. SAN은 주로 인터넷과 단절되거나 멀리 떨어져 있고 몇몇 방화벽들로 싸여 있기 때문에, 대부분의 위협은 내부에서 발생되어진다. 따라서 인력 고용, 보안 정책의 수립에 있어서 신중을 기해야 하며, SAN안에 배치되어지는 서버와 기기들에 대한 접근도 인가되고, 신뢰성 있는 인원을 배치하여야 한다.

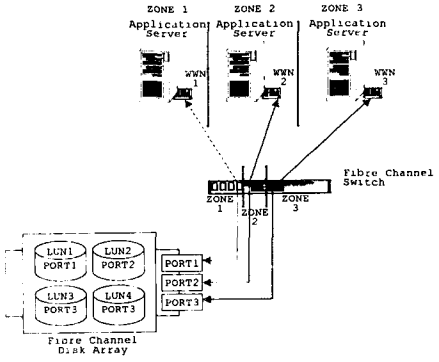
SAN으로부터 데이터를 가져가는 요구나, SAN에 데이터를 저장하는 서버에 대한 보안도 고려하지 않을 수 없다. 만일 공격자가 이들 서버들 중 하나라도 공격하여 권한 획득 시에는 SAN에 있는 데이터를 제한 없이 취득할 수 있다. 따라서 서버 관리자는 정례적인 감시와 더불어 보안 기능의 완전한 구현 등 서버보안에 각별한 주의를 기울여야 한다. 현재 FC와 함께 보안기능을 수행하도록 구현되어 있는 방법은 LUN(Logical Unit Number) masking과 Zoning(Partitioning) 방법이다. LUN masking은 [그림 2]처럼 SAN을 논리적으로 재구성하여 SAN 가상풀(SAN virtual pool)을 구성하는 것으로 SAN의 일부분만을 접근할 수 있도록 동작하게 만든 것이다[4].

Zoning(Partitioning)은 [그림 3]처럼 스위치에서 주어진 Port로부터 특정 데이터로의 접근만을 허용함으로써 유사한 효과를 낼 수 있다. 이런 LUN masking이나 Zoning은 사용자로 하여금 다른 데이터로의 접근을 막을 뿐 아니라, 침해 발생시 침입자로부터 데이터의 유실 및 노출을 최소화 할 수 있다. 이 이외에도 Volume 관리 소프트웨어를 이용한 보안관리 등이 있을 수 있다.

그러나, LUN Masking이나 Zoning을 사용하는 SAN이 외부의 보안위협이나, 취약성이 없다고 말할 수 없다[2].



[그림 2] LUN Masking 예



[그림 3] Hard Zoning 예

SAN에 대한 공격은 웹 해킹과는 다르게 매우 복잡한 드라이버 수준의 코드를 작성해야 한다. 드라이버 수준의 공격은 일반적인 해커의 기술로는 작성되기 어렵지만, 백오리피스(BackOriffice)와 같이 고수준의 자동화된 도구의 제작 유포시 일반인들도 치명적인 해를 입힐 수 있다[8,9].

기본적으로 SAN은 네트워크의 형태를 가지므로 SAN Security에 많은 관심과 투자가 이뤄져야 할 것이다.

SAN 보안 관리 범주를 다음과 같이 나열 할 수 있다.

- Physical security
- Authorization
- Authentication
- Access control
- Virus detection
- User/group management
- SAN Security Policy Management

[표 1]에는 SAN이 받을수도 있는 위협 및 그에 대한 해결책들을 기술하였다.

WWN(World Wide Names, 이하 WWN)은 FC에 붙이는 전세계적으로 고유한 구분자로 제조업체가 지정하여 IEEE에 등록하게 된다. FC는 포트 및 노드로 나누어 지는데 모든 포트와 노드에는 AL_PA의 유효성 검사에 사용되는 고유한 WWN이 부여된다[7].

[표 1] SAN 보안 위험성 및 솔루션

SAN 보안 위험성	해결책
무단 및 인증되지 않은 SAN 액세스	무단 및 인증되지 않은 SAN 액세스를 방지하기 위한 멀티레벨 암호 제어
보안되지 않은 관리 액세스	ACL(Access Control List) 관리 및 특정 인터페이스로 암호화
WWN 스푸핑	포트레벨 ACL
다른 액세스 지점에서 허용되는 제어관리	신뢰할수 있는 스위치나 보안관리 뿐만 아니라 PKI(Public key infrastructure) 기반 인증 및 보안(디지털 인증서)으로 향상된 구성 아키텍처

이렇게 SAN의 보안은 SAN 설계시 보안에 대한 요소들을 충분히 고려한 후에 구성이 이뤄져야 한다. 분석한 취약점을 식별하고 신뢰할 수 있는 보안 솔루션을 구축하는 것이 SAN 보안의 기본이라고 할 수 있겠다.
3장에서는 현재 연구개발에 주력하고 있는 SAN 연구방향에 대해 기술하고 향후의 SAN 보안에 대해 살펴보도록 하겠다.

3. 미래의 SAN

현재의 FC(Fibre Channel)을 이용한 SAN 접속은 10Km라는 거리 제한과 점대점연결, 채널확장기를 통한 거리의 연장이라는 제약을 가지고 있다. 기존의 SCSI 방식의 25m의 접속거리에 비하면 비약적인 발달이지만, 근래 네트워크의 요구에는 미치지 못하고 있다. 따라서 앞으로의 스토리지 네트워크의 요구에 부응하기 위하여 IP 네트워크를 이용한 몇몇 기술들이 제안되고 있다[12,15]. 이것은 FCIP(Fibre Channel over Internet Protocol)로 불려지고 있다. 또한 IP 네트워크를 통한 SCSI 명령어를 전송할 수도 있을 것으로 보인다. 이것은 iSCSI(IP SCSI)로 IP 네트워크를 통한 SCSI전송은 FCIP보다 비용을 더 절감시킬 수 있을 것으로 예상하고 있다[3]. 이외에도 SANoIP(SAN over IP), DAFS(Direct Access File System)등이 있으며 이들 모두 IP를 기본으로 하는 스토리지 시스템이다. 최근 이러한 기술이 IETF 표준화 그룹에 제출되었으며 이들을 하나의 워킹그룹 IPS(IP Storage)로 통합하였다[6].
기존의 화이버채널을 이용한 스토리지 시스템에서 발생하지 않았던 보안 취약점 및 공격의 가능성들이 발생할 수 있는데, 이것은 IP를 사용하기 때문이다. IP의 사용으로 지역적 제한없이 스토리지 시스템에 접근 가능하지만 인터넷으로부터의 위협에 노출되게 된다.
따라서 이에 IP의 사용으로 인한 보안 취약성 및 위협을 적절히 해결할 수 있도록, IPSec(IP Security), VPN(Virtual Private Network), 방화벽, 암호화 기법, 기타 보안 솔루션등을 활용하여 충분히 고려하여야 할 것이다[8].

4. 결론

우리가 가지고 있는 정보 배포의 다양한 채널로 인해 이제는 출입문을 잠그는 것만으로는 정보보호에 대한 내실을 기대할 수 없게 되었다.
인터넷의 사용으로 도달 가능한 사업 영역이 넓어졌다 할지라도 그것은 데이터를 보호할 수 있는 범위내로 제한이 되어야 할 것이다.
현재 SNIA(Storage Networking Industry Association), FCIA(Fibre Channel Industry Association)등에서는 SAN 보안에 초점을 맞추고 FC에서의 인증 방법, 이기종 스위치에서의 인증 방법, 디스크 혹은 테이프 장치에서의 암호화 저장 방법 등의 SAN Security에 대한 표준안 마련, SAN 관련 제품들에 대한 호환성 검증 및 표준화를 수행하고 있다[13,14].
SAN 보안에 대한 표준이 부재하고, 보안위원회에서는 여전히 모든 논점들을 고려하려는 노력이 진행되어지고 있다. 따라서 현재 SAN 보안은 명백한 해결방안이 없지만 기존의 제시된 솔루션과 기법들을 이용하여 보안 위협을 최소화하려는 노력이 계속되어야 할 것이다.

<참고 문헌>

[1] Hu Yoshida, 'LUN Security Considerations for Storage Area Networks', 1999, HITACHI Data Systems Corporation.
[2] Greg P. Schulz, 'MTI's DataShield : Data Security and Flexibility for SAN Environments', 2000. 1. 14, MTI Corporate Headquarters
[3] Nick Allen, 'SAN Fabric Scenario: Strap In and Hold On Tight', Gartner Storage 2001 Presentation, 2001. 6.
[4] 'Fibre Channel Security Whitepaper', FalconStor Software
[5] Dave Tang, 'Storage Area Networking-The Networking Behind the Server', 1997, Gadzoox Microsystems. Inc
[6] IPS(IP Storage), IETF Working Group, http://www.ietf.org/html.charters/ips-charter.html
[7] 'Data Security - Further Realization of the Benefits of SANs', INLINE Corporation, http://www.inlinecorp.com/datasecurity.pdf
[8] Tom Clark, 'Storage Area Network Security', 2001. 10. 8, Windows & .NET Magazine
[9] 'Advancing Security In Storage Area Networks', 2001, Brocade Communications Systems
[10] '전세계 FC(Fibre Channel) SAN 시장 동향 및 전망', 2002.01.23
[11] 김정환, 강희일, 이동일, 'SAN 기술 및 시장동향', 전자통신동향분석, 2000. 2, 제15권 제1호, pp24-37
[12] 'Storage over Internet Protocol-SoIP : The Next Generation SAN', Nishan Systems, 2000
[13] SNIA, http://www.snia.org/
[14] FCIA, http://www.fibrechannel.com/
[15] 'Interconnecting Fibre Channel SANs Over Optical and IP Infrastructures', SAN Valley, http://www.sanvally.com