무선 Storage Area Network의 차세대 보안 인프라 연구

함동읍*, 김동수*, 김지호*, 송오영*, 박세현*

*중앙대학교, 전자전기공학부

A Study of Next Generation Security Infrastruction for Wireless Storage Area Network

Dong Eup Ham*, Dong Su Kim*, Ji Ho Kim*, Se Hyun Park*, Oh Young Song*,

School of Electrical & Electronics Engineering Chung Ang Univ.

요 약

무선 단말기를 통한 멀티미디어 데이터의 이용증가로 인해 무선 단말기의 저장 용량 한계에 대한 문제가 제기되었다. 지속적으로 성장하고 있는 무선 인프라 상에서 사용자의 중요한 데이터를 완벽하게 보호하고 시스템 장애 시간을 최소화하여 사용자가 언제든 원하는 데이터를 저장하고, 제공받기 위해 SAN 보안 인프라 연구는 필수적이다.

I. 서론

SAN는 Fibre Channel을 이용하여 LAN으로 구성된 기종 망과는 별도로 스토리지 전용 네트워크를 구성하여 사용해 왔다. 이를 통해 LAN를 통한 일반적인 업무에 영향을 주지 않으면서 고속으로 네트워크를 사용할 수 있게 되었다. 그러나 Fibre Channel는 10km라는 거리의 제한을 가지고 있어서 그 이상의 거리에서 저장장치에 접근하여 사용이 불가능하다. 또한 별도 저장장치 네트워크를 구축하기 위한 비용 문제가 발생하였고 Fibre Channel을 공급하는 업체별로 특화된 기술을 사용함으로써 상호 호환성이 떨어지는 문제가 발생하였다. 이러한 문제들과 기가비트 이더넷 기술의 발달로 인해 IPSAN이라고 불리는 IP network를 이용한 저장장치 네트워크 기술이 제기 되었다. 이러한 기술로 iFCP, FCIP, iSCSI가 있다. iFCP나 FCIP는 기존의 Fibre Channel를 이용하여 구축된 SAN을 IP network를 통해 상호 연결하거나 확장하는 기술이다. iSCSI는 기존에 광범위하게 사용된 SCSI를 tcp/ip를 이용하여 확장하는 기술이다.

최근 무선 단말기를 통한 멀티미디어 데이터의 이용 증가로 무선단말기의 저장용량 부족문제가 제기되고 있다. 무선 단말기의 저장 용량을 늘리기 위해서는 고가의 메모리를 늘려야 함으로 비용 문제가 발생한다. 그러나 IPSAN 기술 중 iSCSI를 이용하여 무선 SAN을 구축하고 이를 이용하면 원격지에 있는 저장장치를 무선 단말기의 저장장치로 사용할 수 있게 된다. 또한 이를 통해 저장장치에 기록되어 있는 많은 양의 데이터를 자신의 데이터처럼 사용할 수 있게 된다. 또한 안전한 곳에 데이터를 저장함으로써 데이터의 내장애성을 높일 수 있다. 따라서 본 논문에서는 iSCSI로 구성된 무선 SAN 대한 보안 인프라를 제안하고자 한다.

무선 SAN을 위한 차세대 보안 인프라로 본 논문에서는 PMI를 이용한 Role Based Access Control를 제안한다. 이를 위해 무선 환경에서 PKI 및 PMI를 사용하는데 발생하는 검증부하를 감소시키기 위한 SCVP사용을 제시하고 SAN에서 예상되는 DDOS 공격 모델에 대한 대응 알고리즘을 제안한다. 2장에서는 SAN의 구조를 설명한다. 3장에서는 SAN 보안 고려사항과 기존의 보안 기법에 대해 설명한다. 4장에서는 제안한 차세대 무선 SAN 보안 인프라에 대해서 설명하고 5장에서 결론에 대해 설명한다.

II. SAN 구조 및 보안 고려사항

2.1 SAN 구조

SAN이 등장한 배경에는 기업 내의 IT 시스템, 데이터베이스, ERP, 전자우편 등에 따라 데이터가

폭발적으로 증가하고 있다는 점을 들 수 있다. 이러한 시스템을 운용하고 있는 관리자는 특정 서버가 다운되는 영향을 최소한으로 줄이기 위해, 복수의 처리를 묶어 1대의 머신으로 운용하는 것을 피하려고 하는데, 그러기 위해서는 데이터는 복수의 서버로 분산시킬 수밖에 없다. 그런데, 여기에서 문제가 발생하다. 데이터가 서버마다 분단된 채 증가되면, 그것에 대응해 유지/보수에 시간과 일손이 많이 들기 때문이다. 그리고, 서버마다 다른 제조업체의 하드웨어를 구입한다면, 스토리지의 증설계획이 상당히 복잡하고 성가시게 된다. 또한, 백업 문제의 심각성도 늘어날 것이다. 각각의 스토리지 내에 저장된 데이터를 각각 백업하는 일과 백업할 때에 발생하는 트래픽이 망에 미치는 영향은 무시할 수 없게 된다.

위와 같은 문제점들을 해결하기 위해 스토리지를 각 서버로부터 분리해 일원적으로 관리하는 것이 필요하다. 그리고 스토리지를 추가하면서 이중화 및 RAID(Redundant Array of Inexpensive Disks) 구성을 실현할 수 있다면, 높은 확장성과 신뢰성도 얻을 수 있다. 게다가 기존 LAN으로부터는 독립된 망을 구성하는 것으로 스토리지 간의 복사와 백업 장치와의 교환이 발생해도 그 트래픽이 LAN에 영향을 미치는 것은 아니다. 이것을 실현한 것이 바로 SAN인데, 스토리지는 집중시키면서도 서버와 어플리케이션은 분산시킬 수 있다. 그림 1에서와 같이, 서버 성능과 대규모 스토리지 용량의 핵심 빌딩블록을 가진 LAN 네트워킹 모델을 결합함으로써, SAN은 기존 SCSI 버스-기반의 아키텍처에 의해 제기된 대역폭 병목현상과 확장된 한계를 극복하고 있다.

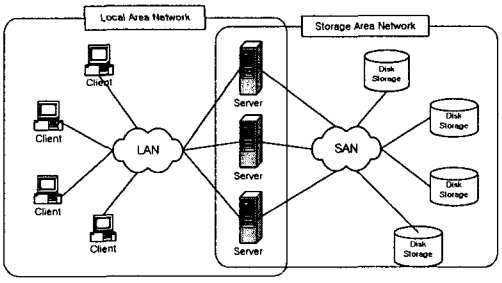

그림 1 SAN 환경

SAN은 망에서 데이터를 이동시키는 거의 모든 어플리케이션들의 성능을 향상시킬 것이다. 기존의 서브넷과 같이, SAN은 기본 망에 대한 부하를 주지않고 특별한 기능을 위한 대역폭을 부가하는 방법으로 LAN과 WAN을 보조한다. 또한 SAN은 데이터 웨어하우싱과 같은 고성능 솔루션을 가능하게 하며, 많은 네트워킹 환경에 포괄적으로 이용 수 있다.

2.2. iSCSI를 이용한 무선SAN

iSCSI protocol를 이용하여 IP network를 통해 SAN에 직접 접속하여 스토리지를 사용하는 것이 가능해짐으로써 무선 네트워크를 통한 무선 단말기에서도 직접 스토리지에 접근하는 것이 가능해졌다. 무선 단말기에서 iSCSI 프로토콜을 통해 스카시 명령어를 이용하여 원격지에 있는 스토리지에 데이터를 블록 단위로 읽거나 쓰기가 가능해짐으로서 단말기의 제한 된 저장 용량 문제를 해결하고 언제 어디서나 원격지 스토리지에 저장된 무한한 크기의 데이터를 사용할 수 있게 되었다.

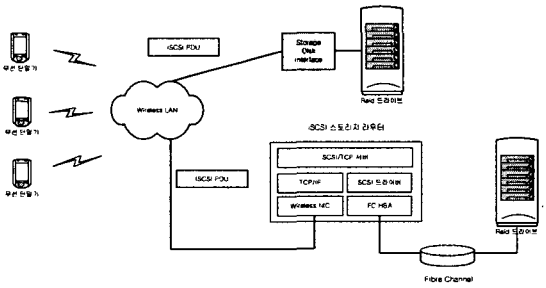

그림 2 전체 무선 SAN 구성도

III. 무선 SAN에서의 보안 요구사항

3.1. SAN 보안 이슈

스토리지에 저장된 중요 데이터가 Wireless IP network를 통해 전송되면서 기존의 IP network에서 발생된 보안 문제들이 SAN에서도 문제점으로 부각되기 시작했다.

■ 인증 및 권한문제

iSCSI 프로토콜은 상대방과 세션을 형성 할 때 Challenge Handshake Authentication Protocol(CHAP) 및 Secure Remote Password Protocol(SRP)를 이용하여 상대방을 인증한다. 그러나 상대방에 대한 권한 및 그룹에 대한 고려는 되어있지 않다. 권한은 사용자를 관리자와 일반 사용자 등으로 세분화하여 나누고 일반 사용자는 그룹별로 나누어 스토리지에 대한 사용자 관리 효율을 높여준다.

■ iSCSI 도청 및 위·변조

iSCSI 프로토콜은 패킷에 대한 인증, 기밀성, 무결성, replay protection을 제공하지 않는다.

■ 분산 서비스 거부 공격(Distributed Denial of Service Attack)

현재 iSCSI 뿐만 아니라 인터넷 상의 거의 모든 서버들에게 분산 서비스 공격은 주요한 보안 고려 사항이다. iSCSI에서는 발생 할 수 있는 분산 서비스 거부 공격에 대한 예로는 공격자가 분산된 에이전트를 사용하여 인증 요청을 반복함으로서 서버의 자원을 고갈 시키고 서버를 서비스 불능 상태로 만드는 것을 들 수 있다. 따라서 분산 서비스 거부 공격을 막기 위해서는 공격자가 각 에이전트에서 연속적으로 인증 요청을 보내는 것을 제한해야 한다.

본 논문에서는 위와 같은 문제점들을 해결하기 위해 PKI 및 PMI를 이용한 인증 및 권한 관리 방법을 제안한다. 그리고 무선 환경에서 PKI 및 PMI를 적용시 예상되는 검증 문제를 해결하기 위한 방안을 제시한다. 또한 사용자 인증 과정에서 발생 가능한 DDOS 공격 모델에 대한 대응 방안을 제안한다.

IV.제안하는 iSCSI를 이용한 무선 SAN의 보안 인프라

4.1. 본 논문에서 제안하는 SSL

현재 SSL은 End to End 통신의 지원하는 TCP을 기반으로 하여 상호인증과 통신 데이터의 기밀성 및 무결성을 제공하는 보안 프로토콜이다. SSL에서 제공하는 상호인증은 PKI의 인증서를 이용한 방법으로 상대방이 인증서에 담긴 공개키와 맞는 적절한 개인키를 가지고 서명을 생성해 내는지 확인함으로써 이루어진다.

본 논문에서는 Attribute Certificate를 이용하여 SSL에서 RBAC이 이루어지도록 SSL의 변형을 제안한다. 변형된 SSL에서는 클라이언트가 클라이언트의 인증용 인증서를 전송하고 이어서 속성 인증서를 전송한다. 서버쪽에서는 클라이언트의 인증용 인증서를 검증하고 검증이 성공하면 속성 인증서를 인증한다. 속성인증서가 정상적으로 인증되면 속성인증서가 적절한 Role을 가지고 있는지 체크하고 SSL 세션을 맺는다.

위에서 제안한 방식은 AC를 사용하지 않은 방식에 비해 AC를 검증하는 오버헤드가 증가하지만 사용자가 증가할수록 증가하는 접속가능한 사용자의 ACL보다 항상 일정한 크기로 유지되는 Role based ACL을 사용함으로써 서버측 오버헤드를 줄일 수 있고 관리측면에서도 사용자의 접근권한이 변경될 때마다 서버의 ACL을 수정하기보다 사용자의 AC을 폐기 또는 수정함으로써 간단히 사용자의 접근권한을 변경할 수 있는 장점이 있다.

또한 위에서 제안한 방식은 SSL을 맺고 AC를 보내는 경우와 비교하면 정상적인 사용자의 경우 차이가 없지만 비정상적인 사용자의 경우 서버측에서 master Secret와 Cryptographic Parameter를 만드는 과정 전에 SSL 세션이 종료함으로 그만큼 부하를 제거할 수 있다.

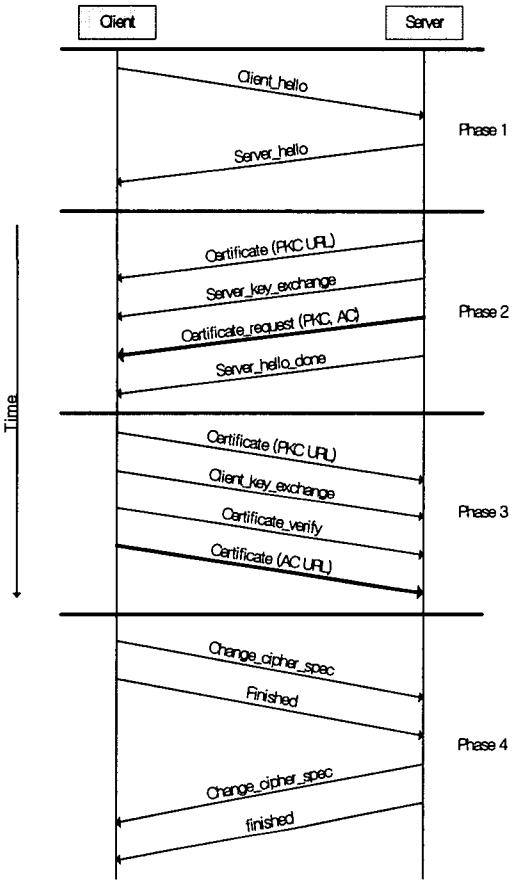

그림 3 제안하는 SSL 메시지 흐름도

Phase 1 : 클라이언트와 서버 상호간에 Secure Association을 맺기 위한 SSL version, random number, session ID, 상호간에 사용할 수 있는 CipherSuite을 교환한다.

Phase 2 : 서버인증과 키 교환이 이루어진다.

서버는 클라이언트가 자신을 인증할 수 있도록 PKC URL과 자신의 서명용 개인키로 server_key_exchange을 서명해서 보낸다. 또한 클라이언트를 인증하기 위해 클라이언트의 인증용

및 속성용 인증서를 요청한다. 클라이언트는 서버 인증서를 SCVP 서버를 통행 인증하고 Server_key_exchange을 서명을 검증한다.

클라이언트는 서버의 인증서 URL을 무선용 SCVP 서버를 통해 검증 요청을 하고 SCVP 응답 메시지에 담긴 서버 인증서를 이용하여 서버가 보낸 서명값을 검증한다.

Phase 3 : 클라이언트 인증과 Role 및 Group을 확인한다.

클라이언트는 서버의 요청에 따라 PKC 및 AC의 URL를 보낸다.

서버는 클라이언트의 인증용과 속성용 인증서를 무선용 SCVP 서버를 통해 검증하고 SCVP 응답 메시지에 담긴 클라이언트의 PKC를 이용하여 Certificate_verify의 서명을 검증한다. PKC 및 AC가 정상일 경우 서버는 클라이언트의 Role과 클라이언트가 속한 Group에 따라서 클라이언트의 접근을 제어한다.

Phase 4 : 클라이언트와 서버 사이에 상호 인증이 끝나면 Phase 2에서 교환한 pre_master_secret로부터 master_secret을 계산하고 master_secret로부터 client write MAC secret, server write MAC secret, client write key, server write key, client write IV, server write IV을 만들기 위한 key_block을 계산한다.

4.2. 제안하는 SSL에서의 PKC와 AC의 검증

제안하는 SSL에서는 PKC을 이용한 상호인증 및 클라이언트의 AC를 검증하도록 하고 있다. 기존의 SSL은 인증서의 경로 검증 및 CRL 검증을 하지 않은 것이 일반적이다. 그러나 본 논문에서 제안하는 SSL은 중요한 저장 장치의 데이터를 보호하고 불법적인 사용자의 접근을 제한하기 위해 인증서 상태검증을 할 것을 권장한다. 그러나 제한된 단말기 및 저장장치의 iSCSI interface의 계산 능력을 고려하고 일관된 보안 정책의 적용을 위하여 단말기 및 저장장치의 iSCSI interface에서 직접 상태검증을 하기 보다 Simple Certificate Validation Protocol[9]을 이용한 PKC 검증 및 AC를 검증한다.

PKI 서비스에는 이러한 인증서의 검증을 대행해 주는 서비스가 있는데 대표적인 것이 OCSP와 SCVP가 있다. SCVP는 OCSP보다 유연한 포맷을 제공한다. 특히 해당 인증서를 나타내는 방법은 'CHOICE' 형태로 되어 있어서 인증서 자체나 인증서에 대한 약간의 정보만을 제공하여 해당 인증서를 나타낼 수 있다. 이를 무선 PKI 환경에 알맞게 수정할 수 있다.

따라서, 무선 환경에서는 OCSP보다는 SCVP를 사용하는 것이 성능의 제약이 많은 무선 단말에는 좋은 선택이다. 또한, SCVP는 AC에 대한 검증도 실시할 수 있으므로 PMI 환경에서도 사용될 수 있는 프로토콜이다.

4.3 본 논문에서 제안하는 iSCSI protocol을 이용한 SAN

4.3.1 시스템 구성요소

본 논문에서 제안하는 무선 SAN의 차세대 보안 인프라의 구성 요소는 다음과 같다.

- SAN Controller : Initiator에 대한 AC를 발행, 폐기 등의 관리을 한다.
- Policy Builder : SAN의 보안 정책에 따라 Role을 정의한다.
- LDAP Server : Target의 PKC 및 Initiator의 PKC와 AC를 저장한다.
- SCVP Server : Target 및 Initiator의 PKC와 AC를 검증한다.
- iSCSI interface : Storage에 접속하려는 Initiator을 검증하고 그 role 및 group에 따라 SCSI 명령의 실행을 제어하고 설정을 변경할 수 있게 한다.
- Mobile terminal : 저장 장치를 사용하려는 Target으로 노트북, 휴대폰, PDA등이 될 수 있다.

4.3.2 사용자 등록 및 AC의 발급 절차

사용자는 저장장치를 사용하기 위해 SAN controller에 접속하여 인증 받고 AC를 발급 받는다. SAN는 사용자의 PKC를 통해 인증하고 Policy builder를 통해 AC를 발급하고 LDAP에 AC를 저장한다. 그림 4은 사용자가 SAN controller에서 관리하는 저장장치에 접속하기 위한 AC를 발급 받는 과정이다.

Step 1 : 사용자는 저장장치에 접속하기 위한 권한을 얻기 위해 SAN에 적절한 AC 요청을 한다.

Step 2 : SAN controller는 SCVP server를 통해 사용자를 인증한다.

Step 3 : SAN controller는 인증된 사용자에게 Policy builder를 통해 사용자의 AC를 발급 받는다.

Step 4 : SAN controller는 받급 받은 AC를 LDAP에 저장한다.

Step 5 : SAN controller는 발급 받은 AC 또는 AC URL를 사용자에게 전송한다.

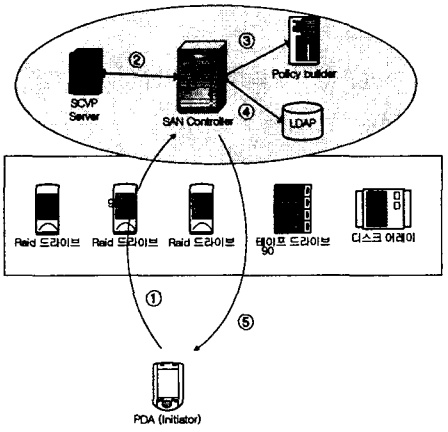

그림 4 사용자의 AC 발급 절차

4.3.3 SAN 로그인 및 사용 절차

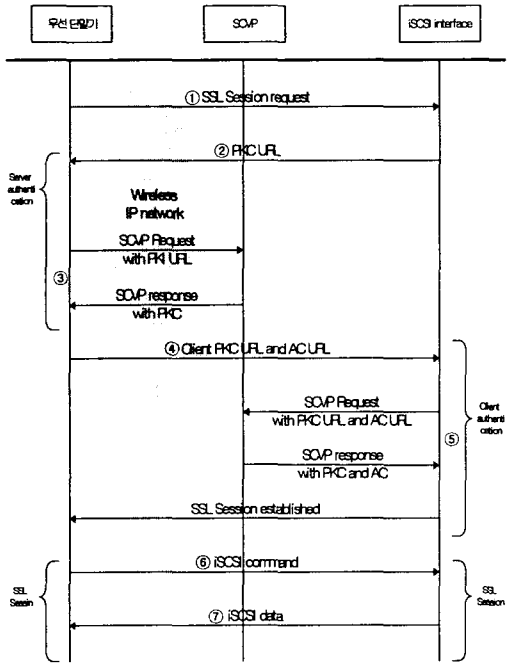

그림 5 사용자의 SAN 로그인 및 사용절차

무선 SAN에 있는 저장장치를 사용하려는 무선 단말기 사용자는 다음과 같은 과정을 통해 사용권한을 획득하여 사용한다.

① 사용자는 접속하려는 저장장치의 IP address와 port번호로 SSL connection을 시도한다.

② 저장 장치는 자신의 인증서 URL과 서명값, Nonce를 보낸다.

③ 사용자는 저장 장치의 인증서URL로 SCVP 요청 메시지를 생성하여 SCVP 서버에게 보내고 SCVP 응답 메시지에 담긴 저장 장치의 인증서를 이용하여 저장 장치의 서명값을 검증한다.

④ 저장장치가 사용자에 의해 인증되면 사용자는 자신의 ID, Nonce에 대한 개인키 서명값, PKC URL과 AC URL를 저장장치에게 보낸다.

⑤ 저장장치는 사용자의 PKC URL과 AC URL로 SCVP 요청메시지를 만들어 SCVP 서버에게 보내고 SCVP 응답 메시지에 담긴 사용자의 PKC와 AC를 이용하여 사용자의 서명값과 사용자의 Role 및 Group을 확인한다.

⑥ 사용자는 SSL connection을 통해 iSCSI command를 보낸다. 저장 장치는 사용자의 Role 및 Group에 따라 command를 실행한다.

⑦ iSCSI command에 따른 데이터를 SSL connection을 통해 사용자에게 보낸다.

표 1은 사용자의 AC의 Role과 Group에 따른 Privilege를 보여준다.

Role	Group	Privilege
manager	A	• change configuration • read data • write data • delete data
user level 1	A	• read data • write data
user level 2	A	• read data
manager	B	• change configuration • read data
user level 1	B	• read data • write data • delete data
user level 2	B	• read data • write data

표 1 Role 및 Group에 따른 Privilege

4.3.4 DDOS 공격 모델과 대응방안: exponential waiting time mechanism for DDOS attacker

공격자가 다수의 에이전트를 사용하여 연속적인 인증 요청을 하게되면 그림 5에서의 인증과정 중 ①~⑤과정을 반복 하게 되는데 이중 ⑤과정이 SCVP와 iSCSI 인테페이스에 부담을 많이 주게되어 DDOS가 가능 해진다.

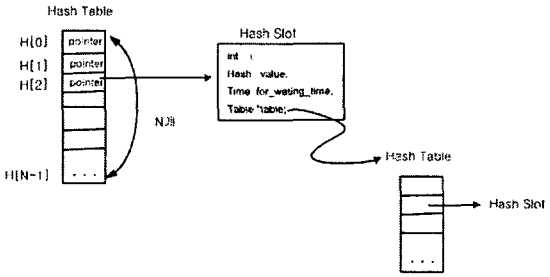

그림 6 해쉬 테이블 구조

본 논문에서는 이와 같은 DDOS에 대한 대응방안을 제안 한다. 인증 처리 과정에서 알고리즘을 적용하여 공격자의 지속적인 인증 요청을 막을 수 있다. 인증에 실패한 사용자의 인증서URL의 해쉬값, 현재시간에 $a \cdot N^2$을 더한 시간과 인증 실패 횟수을 메모리 해쉬테이블에 등록을 한다. 그림 5의 인증과정 ④에서 인증서URL의 해쉬값이 등록되어 있을 경우 현재시간이 해쉬테이블에 기록된 시간 보다 작으면 요청을 거부한다. 즉 사용자 인증이 실패 할수록 인증 대기시간이 지수적(exponential)으로 증가하므로 공격자는 연속적인 인증 요구로 서버에 많은 부하를 주기가 어려워진다. 또한 정상적인 공격의도가 없는 사용자들은 일반적으로 매우적은 수의 인증 실패만 하기 때문에 이 경우 에는 인증 대기시간 짧으므로 불편을 느끼지 못할 것이다. 그리고 이 방법은 각 인증 요청에 대해서 1번의 해쉬 함수와 메모리 읽기, 쓰기 작업을 수행하므로 서버 측 부하를 최소화 한다.

V. 결론

아직 무선 SAN는 실제로 사용되지 않고 있고 어떤 모델도 제시되어 있지 않다. 그러나 현재 카메라폰과 같이 핸드폰에서 멀티미디어 데이터의 사용은 핸드폰의 저장 용량을 압도하고 있다. 또한 무선 노트북에서의 데이터를 안전하게 저장하거나 사용하기 위해서는 무선 SAN이 필요로 하게 된다. 따라서 본 논문에서는 iSCSI protocol을 이용한 무선SAN 모델을 제시하였다.

또 무선 SAN 사용시 발생이 예상되는 보안 문제를 고려하여 필요한 보안 인프라를 제시하였다. 본 논문에서는 PKI를 이용하여 상호인증을 제안하고 PMI를 이용하여 SAN 사용자의 권한에 따라 SAN의 사용을 제한하도록 하고 있다. 이를 구현하기 위해 본 논문에서는 국내 무선PKI 환경을 고려한 상호 인증이 가능하고 Role Base Access Control이 가능한 SSL의 모델과 무선 환경에서 인증서 URL을 통해 인증서 검증이 가능한 SCVP 프로토콜을 제시했다.

이를 이용하면 보안성이 뛰어나고 효율적인 무선 SAN 구현이 가능하다고 예상된다.

참고 문헌

[1] Hui, J.Y. 'Wireless optical ad-hoc networks for embedded systems', Performance, Computing, and Communications, 2001. IEEE International Conference on. , Apr 2001, Page(s): 140 -144

[2] Jo Maitland, 'Credit Union Erects Wireless SAN', HTTP://www.byteandswitch.com/document.asp?doc_id=28997, Byte and Switch

[3] Internet Draft, "Fibre Channel over TCP/IP(FCIP)", Rajagopal, M., et al., draft-ietf-ips-fcovertcpip-12.txt Auguest 2002

[4] Internet Draft, "iFCP - A Protocol for Internet Fibre Channel Storage Networking", Monia, C., et al., draft-ietf-ips-ifcp-13.txt, Auguest 2002

[5] Internet Draft, "iSCSI" Julian Satran, etc., http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt, January 2003.

[6] H.X Mel, Doris Baker, "보안과 암호의 모든것", The Wesley Press, 2001

[7] 이용, '무선PKI규격', TTA 저널 81호

[8] S. Farell and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[9] Internet Draft, "Simple Certificate Validation Protocol", A. Malpani, R. Housley, T. Freeman, http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-11.txt, 2003