韓國國防經營分析學會誌
第37卷 第1號, 2011. 3. 31.

전장관리체계 전자결재시스템을 위한 역할기반 스토리지 암호화 기법

(A Role-based Storage Encryption for the Electronic Approval System of Battle Management Systems)

허 경 순(Kyoung-Soon, Her)*, 이 수 진(SooJin, Lee)**

초 록

전장관리체계의 전자결재시스템은 가용성과 신뢰성이 최우선이기 때문에 서버와 스토리지를 가장 신뢰성 있게 구축하기 위해 SAN(Storage Area Network)을 이용하고 있다. 본 논문에서는 전장관리체계 내 전자결재 시스템에서 중요한 군사자료가 저장되는 SAN을 대상으로 보안취약점을 분석하고, 분석된 결과를 바탕으로 가상 공격 시나리오를 작성하여 내부자에 의한 자료 유출이 가능할 수 있음을 실험을 통해 검증한 후, 내부자에 의한 자료 유출 위협을 방지할 수 있는 새로운 개념의 사용자 역할 기반 스토리지 암호화 기법을 제안한다.

ABSTRACT

The most important factors of Electronic approval system of battle management system are availability and reliability. Therefore, the electronic approval system uses a SAN(storage area network) to construct the reliable server and storage. In this paper, we analyze the security vulnerabilities of the SAN storage that stores the critical military information in the electronic approval system of battle management system. Based on the analysis, we verify the possibility of information leakage by the inside attackers through the scenario-based experiment. And we finally propose a new storage encryption algorithm on the basis of user's role that can prevent the leakage of information by the inside attackers.

Keywords : Electronic Approval System, Battle Management System, SAN, Security, Encryption

논문접수일 : 2010년 12월 1일 심사(수정)일 : 2011년 3월 2일 논문게재확정일 : 2011년 3월 8일

* 국군통신사령부

** 국방대학교 국방정보체계전공 교수

1. 서 론

2008년 2월 국내 최대 인터넷 오픈 마켓인 모 업체는 중국 해커로부터 공격을 받아 1천만 명이 넘는 고객정보가 유출되는 사고가 발생하였으며, 이어 7월에는 인터넷 포털업체에서 55만 명의 이메일 정보가 유출되는 사고가 발생했다. 또한, 9월에는 1천 1백만 건에 달하는 정유회사 고객 정보가 내부직원에 의해 유출되는 등 크고 작은 정보유출 사고가 잇따르고 있다[1].

국방 분야에서도 이메일을 통해 국방과학연구소 내부 연구원에 의해 프랑스 군수업체로 차기호위함의 레이더 관련 군사기밀이 유출되었고, 차기 보병전투장갑차의 개발 내용이 담긴 국방중기계획('03-'07)이 국내 국방관련 소프트웨어 개발업체로 유출되는 사고가 발생하여 큰 충격을 준 바 있다.

이러한 내부자에 의한 중요정보 및 핵심기술 유출 사고는 향후에도 지속적으로 발생할 것이며, 국가 경제뿐만 아니라 국가 안보에 상당한 위험을 초래할 수 있을 것으로 예상된다. 따라서 우리는 급변하는 해킹 기술에 대한 대응기술도 지속적으로 연구하고 개발해야겠지만, 중요정보 및 핵심기술, 군사자료를 전자적으로 안전하게 보호하고 내부자에 의한 유출을 방지하기 위한 스토리지 보안 기술에 대한 연구가 필요하다.

따라서 본 논문에서는 중요한 군사자료들이 생성·저장·유통되고 있는 전장관리체계 전자결재 시스템에서 중요한 군사자료가 저장되는 스토리지 시스템을 대상으로 내부자의 공격에 대한 보안 취약점을 분석하고 대응방안을 제시한다.

전장관리체계의 전자결재시스템은 가용성과 신뢰성이 최우선이기 때문에 서버와 스토리지 시스템을 가장 신뢰성 있게 구축하기 위해 SAN (Storage Area Network)을 주로 이용하고 있다. 따라서 본 논문에서는 전장관리체계에서 사용하고 있는 SAN 환경의 취약점을 분석하고, 분석된 결과를 바탕으로 가상 공격 시나리오를 작성하여 내부자에 의한 자료 유출이 가능할 수 있음을 실험을 통해 검증한 후, 내부자에 의한 자료 유출 위협을 방지할 수 있는 새로운 개념의 스토리지 암호화 기법을 제안한다.

제안된 기법은 기존의 스토리지 암호화 기술에 역할기반 개념을 적용하여 전장관리체계의 응용 레벨에서 동작하도록 설계되었으며, 공공기관의 기록물 관리법에 준하여 동일 부서 내에서만 자료를 공유할 수 있도록 전자문서 자료를 대상으로 전장관리체계 부서별로 사용자의 역할을 구분하여 자료를 암호화한다. 또한, 운영체제 수준에서 제안된 기법의 원활한 수행을 보장하기 위한 API를 포함한다.

본 논문의 구성은 다음과 같다. 2장에서는 스토리지와 암호화 파일시스템 및 전장관리체계 전자결재시스템을 분석한다. 3장에서는 스토리지 시스템의 일반적인 보안취약점을 이용한 스토리지 공격 시나리오를 작성하고, 전장관리체계에 적용된 SAN을 대상으로 실시한 스토리지 취약점 공격 실험 결과를 기술한다. 4장에서는 내부자에 의한 자료유출을 방지하기 위한 대책으로 본 논문에서 제안된 역할 기반 스토리지 암호화 기법의 운영개념과 개략설계 및 구현 모델링 결과를 기술한다. 5장에서는 제안된 스토리지 암호화 기법의 전자결재시스템에 대한 적용방안을 기술하고 기존 암호화 기법들과의 비교 및 안전성 평가결과를 기술한다. 마지막으로 6장에서 향후 연구방향을 제시하고 결론을 맺는다.

2. 관련 연구

2.1 스토리지 네트워크

스토리지 네트워크는 정보시스템의 대용량 데이터를 관리하고, 운영하기 위한 필수적인 요소로서 서버, 스토리지 그리고 통신장치로 구성되어 있다. 이러한 스토리지 네트워크는 DAS (Direct

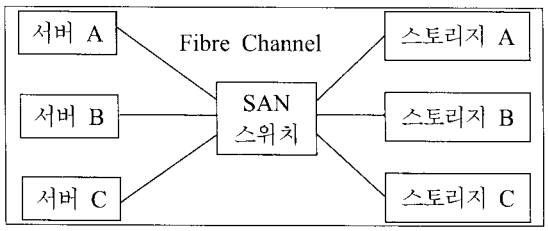
Attached Storage)와 SAN(Storage Area Network) 및 NAS(Network Attached Storage)로 구분할 수 있다.

가. DAS(Direct Attached Storage)

DAS는 서버와 외장형 스토리지 사이를 중간 매개체 없이 전용 케이블로 직접 접속하는 가장 단순하고 일반적인 스토리지 네트워크 연결법으로서, 서버와 스토리지 간 주로 사용하는 네트워크 통신 프로토콜로 SCSI나 Fibre Channel 등이 주로 사용된다. 서버와 스토리지 간에 전용선을 사용하기 때문에 주어진 성능이 보장되며 안정성도 뛰어나다. 그러나 파일 시스템의 공유가 힘들고, 확장성 및 유연성이 상대적으로 떨어지는 단점이 있다[2].

나. SAN(Storage Area Network)

SAN은 <그림 1>과 같이 스위치를 통해 서버와 스토리지를 연결하는 방법으로, 효율적인 데이터 관리와 확장의 용이성 때문에 전장관리체계는 대부분 이 방식을 적용하고 있다.



〈그림 1〉 SAN 구조

그러나 SAN은 벤더 간 호환성을 유지하기 어려우며, 데이터를 공유하는 경우에는 네트워크 통신 및 디스크 처리속도에서 병목현상이 발생한다. 또한, 통신 시 패킷 회송주소가 확인되지 않기 때문에 외부 침입자에 대한 보안이 취약하여 SAN의 보안시스템이 쉽게 침해됨으로써 치명적 결과를 초래할 수 있다[2][3].

다. NAS(Network Attached Storage)

NAS는 전용 파일서버를 통해 서버와 스토리지를 연결하는 방법이다. 서버와 스토리지 사이에 전용 파일서버가 있어 서버와 스토리지 사이의 프로토콜 변환과 파일 공유 기능을 제공한다. NAS의 장점은 파일공유, 확장성, 네트워크 트래픽 관리 및 관리 비용의 절감 등을 들 수 있으며, 현재 파일공유 솔루션 중 가장 안정적이다[2].

2.2 스토리지 암호화 기법

스토리지 암호화 파일시스템은 사용자 개개인 혹은 조직 등에서 기밀을 유지하여야 하는 중요한 데이터에 대한 안전한 저장을 목적으로 개발되었다. 현재까지 개발된 대표적인 암호화 파일시스템으로는 Cryptographic File System (CFS), Transparent Cryptographic File System (TCFS), Cryptfs 등이 있다[4].

가. CFS

CFS는 NFS(Network File System) 내에 암호화 기능을 추가한 것으로 데이터 암호화를 위해 DES를 사용하며, 암호화된 파일에 대해 표준 유닉스 파일시스템 인터페이스를 적용함으로써 시스템 수준에서의 보안 저장장치를 제공한다.

기본개념은 시스템 내에서 신뢰되는 부분(Trusted Components)은 신뢰되지 않은 부분(Untrusted Components)으로 데이터를 전송하기 전에 무조건 암호화해야 한다는 것이다[5]. 그리고 사용자는 보호하고자 하는 디렉토리(directory)를 하나의 암호화키와 연관시켜 각 디렉토리마다 암호화에 사용할 키를 명시한다. 이후 디렉토리 내의 파일들은 더 이상의 사용자 개입 없이 명시된 키를

이용하여 암호화와 복호화를 수행한다.

나. TCFS

TCFS는 CFS를 개선한 것으로서 암호화 서비스와 파일시스템 사이에 더 깊은 통합을 제공하며 [6][7], NFS를 기반으로 암호화 기능을 결합하여 구현되었다.

TCFS는 동적 암호화 모듈 특성을 가지고, 사용자가 TCFS에 의해 사용될 암호화 엔진을 명시할 수 있도록 해준다. 암호화 엔진은 리눅스 모듈 형태로 주어지며, 현재 사용가능한 암호화 모듈로는 Triple DES, RC5, Blowfish 알고리즘 등이 있다.

TCFS에서 모든 파일들은 같은 암호화 알고리즘으로 암호화되고, 사용자 키는 로그인 암호를 기본으로 하며, 키는'/etc/tcfspasswd'라는 특정한 파일에 저장되므로 보안성이 취약하다고 할 수 있다[8]. TCFS의 또 다른 특징은 TCFS를 효율적으로 사용할 수 있도록 BKMS(Basic Key Management System)라는 표준 키관리 시스템을 제공하고, 사용자에게 사용자 로그인 암호 이외의 어떠한 암호도 기억할 필요가 없도록 해준다는 점이다.

CFS와 TCFS의 차이점은 다음과 같다. 우선 CFS와 TCFS는 투명성 제공 측면에서 많은 차이를 가진다. CFS는 보안 디렉토리를 사용하기 때문에 암호화된 파일을 액세스하기 전에 사용자는 보안 디렉토리를 특별한 마운트 디렉토리에 부착하고, 각각의 부착된 디렉토리에 키를 공급할 필요가 있다. 반면, TCFS는 사용자에게 완전히 투명성을 제공하고, 마치 NFS처럼 사용되어질 수 있다. 즉, 암호화 파일과 복호화된 파일 모두가 같은 방법으로 엑세스되고, 사용자는 자신의 파일이 암호화되어 있는지 알 필요가 없다.

둘째, CFS는 암호화 디렉토리에 대해서 암호화가 가능하지만, TCFS는 각각의 파일과 디렉토리에 대해서 암호화가 가능하고, 특별한 플래그인 'X'를 적용함으로써 암호화 및 복호화를 할 수 있다. 셋째, CFS는 사용자 영역에서 동작하는 반면, TCFS는 커널 영역에서 동작하므로 개선된 성능과 보안성을 제공한다.

다. Cryptfs

Cryptfs는 Stackable Vnode Layer loadable kernel module로 설계 및 구현된 파일시스템으로서[9][10], 사용자에게 클라이언트 파일시스템을 캡슐화함으로써 투명한 암호화를 수행하며 커널 수준에서 동작한다. 커널 수준에서 동작한다는 것은 암호화 기능이 파일시스템 일부가 되어 파일을 액세스 하는 모든 응용에 대해 일관된 암호화를 자동적으로 제공하고, 문맥 교환의 횟수를 줄일 수 있으며, 사용자 수준이나 NFS에 기반한 파일시스템보다 효과적인 보안성 및 성능을 제공할 수 있음을 의미한다.

그리고 Cryptfs의 키는 사용자 ID와 프로세스 세션 ID에 기반하고, 커널 메모리의 액세스가 사용자 메모리보다 더 어렵다는 사실 때문에 좀 더 강한 보안성을 제공한다.

파일을 암호화함에 있어서는 충분히 강한 암호화를 제공하기 위해 CBC(Cipher Block Chaining) 모드로 암호화한다. 그러나 어느 한 부분을 액세스하기 위해 전체 부분을 복호화하는 것은 시스템의 성능 저하를 가져오므로, 운영체제가 사용하는 블록 크기와 같은 CBC 모드를 적용한다. 암호화 알고리즘으로는 빠르고 간단한 64bit 블록 암호인 Blowfish를 사용한다.

2.3 전장관리체계 전자결재시스템

직접 전투에 참가하는 병력과 무기가 군대의 손과 발이라면 두뇌와 신경에 해당하는 것은 전장관리체계로 불리는 지휘통제체계이다.

전장관리체계는 지휘와 통제를 위한 통신과 컴퓨터로 구성되어 정보를 제공하며, 각종 감시 장

비와 수집 수단을 통해 수집한 정보를 합쳐 종합 상황을 만들고 이를 지휘관과 전투부대에 신속히 전파하여 동일한 전장 상황을 공유하며, 작전 명령을 신속·정확하게 작전부대에 알리고 정밀 유도무기를 이용해 목표물을 공격할 수 있게 해 준다[11].

본 논문에서는 전장관리체계 내 합참 및 육·해·공군 전술C4I체계에서 평문이나 비밀문서를 송·수신하여 지휘관의 의사결정 및 상하 제대 간 지휘에 활용하고 있는 전자결재시스템을 중점적으로 분석한다.

전자결재시스템이란 사무관리규정과 동 시행규칙의 관련 규정을 준수한 소프트웨어로서 기관 내에서 운영되는 업무연락, 기안, 보고문서, 메모, 파일 등의 정보를 컴퓨터를 통하여 처리함으로써 사용자의 정보활동을 보다 신속하게 하며, 사무의 생산성과 효율성 향상을 극대화하기 위한 시스템으로, 그룹웨어 기술을 이용하여 기존의 종이문서에 결재하는 것이 아니고 컴퓨터의 근거리 통신망(LAN)을 통해 결재를 상신하면 결재권자가 컴퓨터상의 전자문서에 결재하는 사무자동화 시스템이다[12].

전장관리체계의 전자결재시스템은 부대 간 또는 부대 내의 평문 및 비밀문서 유통을 자동화한 기능으로, 결재를 필요로 하는 각종 보고 및 지시 등의 전문 송수신 처리를 위한 전문유통처리 기능과 사용자 간의 의사소통을 위한 전자우편 기능, 전자문서를 관리할 수 있는 전자문서관리 기능, 비밀문서의 유통내역을 관리할 수 있는 비문관리 기능, 그리고 관리자를 위한 기능을 제공한다.

가. 전자문서 처리

전자결재시스템은 기안 문서를 전자적으로 작성하고, 작성된 문서를 전자적으로 결재권자에게 전달하면 최종적으로 결재권자가 전송된 문서를 열람, 결재하는 과정을 마친 후 수신부서로 전달한다. 이 과정에서 전장관리체계 전자결재시스템의 비밀문서는 수신측 공개키를 이용하여 암호화되며, 문서 수신자는 자신의 개인키를 이용하여 암호화된 문서를 복호화한다[13].

이런 암호화 과정은 단말기에서 수행되며 LAN, WAN 구간 이동은 물론 스토리지 저장시도 암호화된 상태로 저장된다. 그러나 일반문서의 경우는 예외적으로 스토리지에 암호화하지 않은 평문으로 저장되어 내부자에 의한 유출이 가능할 수도 있다.

나. 전자문서의 보안위협요소

비밀문서가 전자적으로 생성된 후 그 문서에 대한 적절한 관리체계 및 접근체계가 없을 때에는 불특정 다수에 의한 무작위적인 접근이 용이하여 그 정보의 가치가 희석되고 외부로 유출될 가능성이 높아진다.

일단 문서 전달의 수신자에게 문서가 전달된 이후 그 문서를 통제할 수단이 없으면 향후 계속되는 중요정보의 무분별한 전송 및 내부자에 의한 정보유출의 가능성이 커지게 되며 문서 내용의 일부가 무단으로 도용되거나 악용될 가능성이 있다[14].

3. 스토리지 보안취약점 분석 및 실험

본 장에서는 전장관리체계에 주로 적용하고 있는 스토리지 네트워크인 SAN을 중심으로 공격 시나리오를 작성하고, 이에 대한 실험을 통해 스토리지 보안취약점을 분석한다. 스토리지 공격기법은 일반 해킹기법과 동일하게 다양한 방법이 있을 수 있으나 본 논문에서는 주요 공격기법인 Session Hijacking, Man-In-The-Middle(MITM) Attack, WWN (World Wide Name) Spoofing 등 세 가지 공격에 대해서만 취약점 분석 및 실험을 실시한다.

3.1 Session Hijacking[15]

Session Hijacking은 신뢰할 수 없는 제 삼자가 두 명의 신뢰할 수 있는 엔티티 간의 유효한 세션을 가로채 이를 조정하는 행위이다.

Session Hijacking은 IP 기반의 네트워크를 대상으로 IP 패킷의 TCP 헤더에서 ISN(Initial Sequence Number)을 예상할 수 있는 취약점을 이용해 공격하는 기법으로 알려져 있으며, HUNT [16]와 Ettercap[17]과 같은 간단한 IP 툴을 이용해 쉽게 수행할 수 있다. 또한 최근에는 웹 환경에서도 HTTP의 쿠키를 사용하는 응용프로그램에서 세션 ID를 유추하여 공격 가능하다.

본 논문에서는 이러한 취약점이 SAN의 Fibre Channel 프레임에서도 동일하게 적용할 수 있다는 점에 착안하여 SAN 환경에서 스토리지를 공격하는 시나리오를 작성하였으며, 작성된 시나리오는 <그림 2>와 같다.

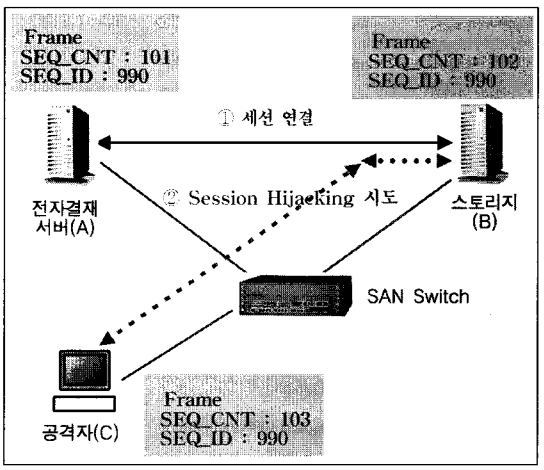
1. 공격자 C에 Hunt 프로그램을 다운로드
   (http://lin.fsid.cvut.cz/~kra/#HUNT)
2. 프로그램의 압축 해제
   a. cd /usr/local/bin
   b. gunzip --c hunt.tar.gz | tar xvf--
3. 프로그램 컴파일
   c. cd /usr/local/bin/hunt-1.5
   d. make
   e. make install
4. 프로그램 실행
   f. ./hunt
5. 전자결재서버(A)에서 전자결재서버(B)로 텔넷 접속
   g. telnet 전자결재서버(B)
6. 공격자(C)는 HUNT의 a)옵션(arp/simple hijack) 선택
7. 공격할 텔넷 세션 선택

〈그림 2〉 Session Hijacking 공격 시나리오

SAN은 Fibre Channel을 이용하며, SAN 스위치를 통해 네트워크를 구성한다. 이때 Fibre Channel 통신은 두 개의 Fibre Channel 노드 간 세션이 맺어져야 한다. 세션 정보는 Sequence Count Number (SEQ_CNT)와 Sequence Identification Number (SEQ_ID)로 관리된다.

SEQ_CNT는 각 프레임이 순차적으로 전송될 때 이를 식별하기 위한 숫자로 1씩 증가한다. SEQ_ID는 고정된 숫자로 각 프레임이 순차적으로 전송될 때 세션의 한 부분임을 식별하기 위해 함께 전송하며, 동일 세션의 각 프레임은 동일한 SEQ_ID를 가진다. 따라서 서로 다른 FC 노드 간 세션을 유지하고 있을 때 만약 100개의 프레임을 전송한다면 SEQ_ID는 모두 동일한 값을 가지고, SEQ_CNT는 순차적으로 1씩 증가한다[15].

본 실험의 주 아이디어는 Fibre Channel의 노드 간 프레임을 송·수신하는 과정에서 인증 과정이 없다는 점을 이용하였으며, 공격 수행 모델은 <그림 3>과 같이 나타낼 수 있다.



〈그림 3〉 Session Hijacking 공격 수행 모델

전자결재서버(A)와 스토리지(B)는 정상적인 세션을 연결하여 프레임을 송·수신하도록 설정하였고, 공격자(C)는 Fibre Channel 트래픽 분석용 상용 툴인 Notified analyzer를 설치하여 전자결재서버(A)와 스토리지(B)가 송·수신하는 프레임의 SEQ_ID와 SEQ_CNT를 획득하였다.

획득한 정보를 이용, 동일한 SEQ_ID에 SEQ_CNT를 '1' 증가하여 정상적인 세션을 연결한 전자결재서버(A)와 스토리지(B) 사이에 프레임을 삽

입한 결과 이를 수신한 스토리지(B)는 정상적인 프레임으로 인식하여 전자결재서버(A)와 스토리지(B)간 연결된 세션이 스토리지(B)와 공격자(C)로 새롭게 연결되었다. 이러한 연결이 가능한 이유는 Fibre Channel 환경에서는 세션이 연결될 때 어떠한 인증이나 권한을 검증하지 않기 때문이다.

따라서 현재 국방에서 운용중인 전장관리체계의 스토리지 네트워크는 악의적인 내부자에 의한 Session Hijacking 공격에 취약하다고 할 수 있다.

3.2 Man-in-the-Middle(MITM) Attack

MITM 공격은 신뢰할 수 없는 제삼자가 두 명의 신뢰할 수 있는 엔티티 간에 통신을 가로채는 공격으로서, 주 목적은 스위치에서 패킷을 훔쳐보기 위한 것이다. IP 환경에서 ARP의 인증이 없는 취약점을 이용하며, 이러한 취약점은 SAN을 구성하는 Fibre Channel에서도 HBA(Host Bus Adapters)의 WWN(World Wide Name)이 인증 없이 쉽게 변경될 수 있기 때문에 동일한 취약점을 가진다고 할 수 있다. MITM의 공격 시나리오는 <그림 4>와 같이 나타낼 수 있다.

1. Cain 프로그램을 공격자(C)에 다운로드
2. 전자결재서버(A)에서 IP와 기본 게이트웨이, arp 테이블 확인
   a. ipconfig
   b. ping [default gateway]
   c. arp -a
3. 악의적인 사용자인 공격자(C)에서 Cain 프로그램을 이용해 arp response를 송신

〈그림 4〉 MITM 공격 시나리오

SAN 환경에서의 모든 노드는 24비트 fabric 주소를 가지며 이를 이용해 소스 노드와 목적지 노드를 식별하여 라우팅을 수행한다. 이러한 SAN 환경에서 공격자가 24비트 fabric 주소를 조작하여 패킷 가로채기를 시도할 수 있다. 본 실험의 주 아이디어는 24비트 fabric 주소가 SAN 스위치의 라우팅에 활용되는 과정에서 인증이나 권한을 확인하지 않는 점을 이용하였다.

fabric 통신의 정상적인 형태에서 전자결재서버(A)와 스토리지(B)가 상호 통신을 하기 위해서는 SAN 스위치에 24비트 fabric 주소를 포함한 프레임을 전송한다. 이를 수신한 스위치는 스위치네임서버의 테이블에서 포트 아이디를 확인하여 전자결재서버(A) 또는 스토리지(B)를 찾아 프레임을 전달한다. 이 과정에서 MITM 공격을 수행하기 위한 모델은 <그림 5>와 같이 나타낼 수 있다.

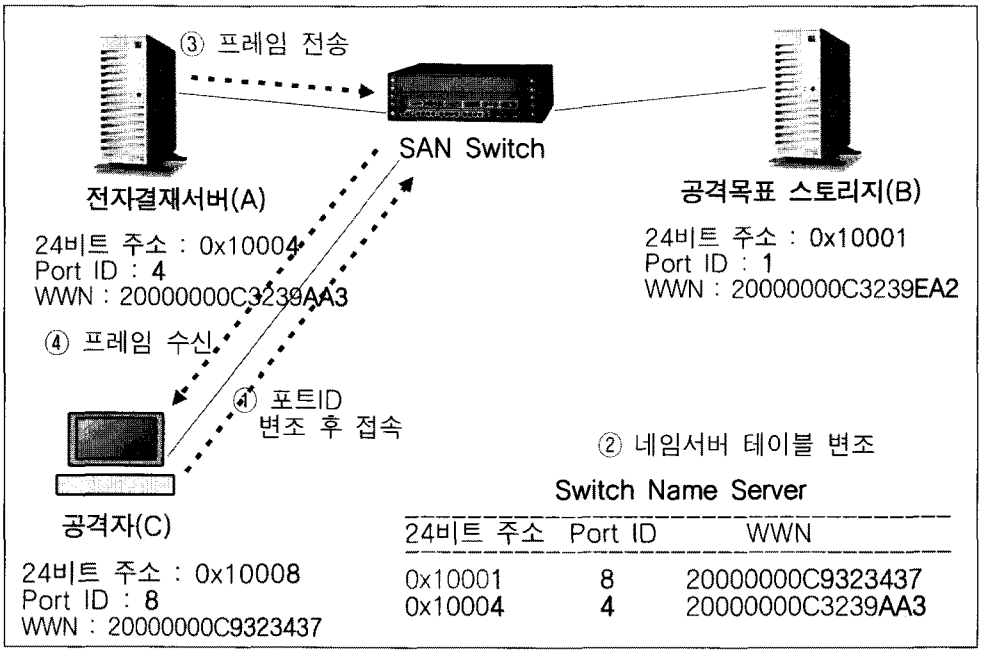
공격자(C)에 FC(Fibre Channel) 트래픽 분석용 상용 툴인 Notified analyzer를 설치하여 전자결재서버(A)와 스토리지(B)의 송·수신 프레임을 획득하였다. 이후 공격자는 자신의 포트 아이디를 8로 변조하여 스위치의 네임서버 테이블에 등록하고, 스위치가 참조하는 24비트 주소를 공격목표의 24비트 주소로 변조한 상태에서 전자결재서버(A)는 스토리지(B)로 보내는 프레임을 전송하였다. 그 결과 스위치는 새롭게 등록된 변조된 네임서버 테이블의 24비트 주소를 참조하여 원래 목적지인 스토리지(B)로 프레임을 전달하지 않고 공격자(C)로 프레임을 전달하였다.

이러한 공격이 가능한 이유는 Fibre Channel 환경에서 새로운 노드가 접속하는 과정에 인증 절차가 없기 때문이다. 이는 실제 전장환경에서 악의적인 사용자가 SAN 스위치에 MITM 공격을 가해 패킷 가로채기 시도로 중요 정보의 유출이라는 치명적인 피해를 유발할 수 있음을 의미한다.

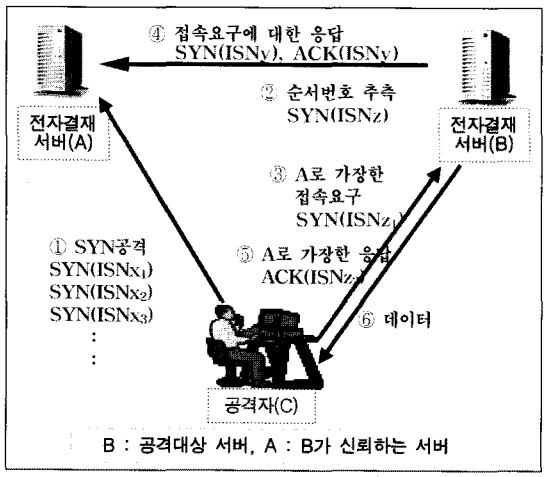
3.3 WWN Spoofing

Spoofing은 1995년 케빈 미트닉이라는 해커가 최초로 IP를 이용해 시도한 해킹방법으로 자신의 IP를 속여서 해킹을 시도하는 것이다.

IP Spoofing의 절차는 <그림 6>에서 보는 바와 같이 전자결재서버(A)와 전자결재서버(B)가 통신



〈그림 5〉 MITM 공격 수행 모델



〈그림 6〉 IP Spoofing 수행 개념

할 때 전자결재서버(A)에게는 서비스거부공격인 TCP Syn flooding 공격을 하고, 전자결재서버(B)와는 자신을 전자결재서버(A)로 위장하여 통신하며 해킹하는 것이다.

WWN은 SAN에서 HBA 정보를 이용하여 특정 노드를 식별하거나 분할하는데 사용되는 중요한 항목이지만, IP NIC(Network Interface Card)의 맥 어드레스와 같이 변조될 수 있어서 보안에 취약하다고 할 수 있다. 공격자는 별다른 방해물 없이 공격 목표 노드의 WWN을 변조할 수 있는 다양한 방법이 있다.

첫 번째 방법은 가장 단순한 방법으로 일일이 HBA에 접속할 수 있는 소프트웨어를 실행해 보는 것이다. 두 번째 방법은 SAN 스위치의 IP 인터페이스를 이용해 접속하여 SAN 스위치의 설정과 접속한 각 노드들의 WWN을 훔쳐보는 방법이다. 마지막 방법은 Brute Force 공격을 통한 패턴

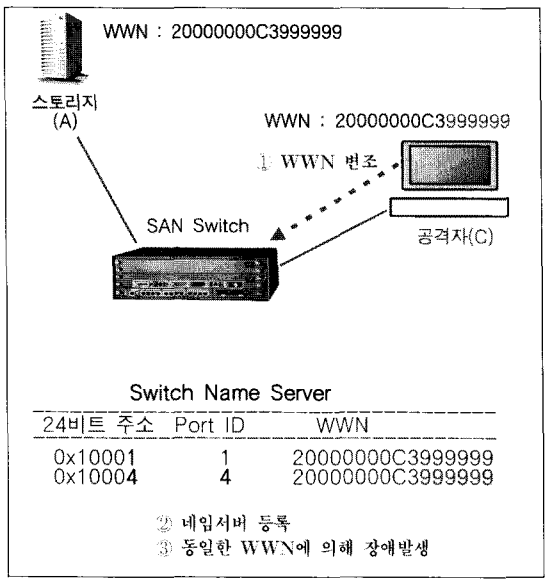
1. spoof 하고자하는 노드에 Emulex 설치
   (http://www.emulex.com/ts/dds.html)
   a. 브라우저에 Fibre Channel의 IP 입력
   b. Name Server 버튼 클릭
   c. 목표로 잡은 클라이언트 노드의 WWN 선택
2. Emulex 설정 프로그램 실행
   a. 시작 -> 프로그램 -> Emulex -> elxcfg
3. 가용한 네트워크 어댑터 선택
4. 어댑터 정보 창에서 Change Node WWN 선택
5. 공격목표의 WWN으로 수정

〈그림 7〉 WWN Spoofing 시나리오

매칭 기법을 이용하는 것이다.

WWN Spoofing의 공격 시나리오는 <그림 7>과 같이 나타낼 수 있다.

WWN Spoofing은 IP 환경에서 네트워크 인터페이스 카드의 MAC 주소가 쉽게 변조될 수 있는 것과 같이 Fibre Channel 환경에서 WWN이 쉽게 변조 될 수 있는 취약점을 이용한 공격이다[15]. SAN에서의 WWN Spoofing 공격 모델은 <그림 8>과 같이 나타낼 수 있다.



〈그림 8〉 WWN Spoofing 공격 수행 모델

우선 WWN을 변조할 공격자(C) 단말에 'Emulex' 프로그램을 설치하고 이를 이용해 WWN을 스토리지(A)의 WWN으로 변조하였다. 스위치는 변조된 WWN을 네임서버 테이블에 인증과정 없이 등록하였으며, 네임서버 테이블에는 동일한 WWN을 가진 24비트 주소가 두 개 생성되었다. 이상과 같이 Fibre Channel 환경에서는 동일한 WWN이 존재하는 경우 정상적인 서비스제공이 불가능하기 때문에 서비스거부공격이 되어 장애가 발생한다.

물론 이러한 장애를 접한 관리자는 SAN 장비를 재부팅하여 문제를 해결할 수 있다. 그러나 공격자(C)는 정상적인 스토리지(A)에 서비스거부공격을 지속적으로 가함으로써 스위치 네임서버에 등록되지 않도록 하고 결과적으로 스위치 네임서버에 등록된 장비는 정상적인 스토리지(A)가 아닌 공격자(C)가 되도록 할 수 있다.

따라서 전장 환경에서 악의적인 내부자에 의해 SAN 스위치를 대상으로 WWN Spoofing을 통한 서비스거부공격을 발생시켜 정상적인 스토리지는 대량의 정보를 이용할 수 없는 상태가 되거나 자료를 탈취 당할 수 있게 된다.

4. 역할기반 스토리지 암호화 기법 : CryptoGW

CryptoGW는 Cryptography와 GroupWare의 합성어로 본 논문에서 제안하는 역할기반의 스토리지 암호화 기법을 지칭한다. 본 장에서는 CryptoGW의 운영개념을 정의하고, 이를 기반으로 개략설계를 수행하여 현 전장관리체계에 적용 가능한 구현모델을 제안한다.

현재까지의 스토리지 암호화에 대한 연구는 외부의 침입과 내부의 공격으로 인한 데이터의 손실이나 변형 및 유출을 방지하기 위한 방법만을 중심으로 다양하게 진행되어 왔다[3]. 그러나 본 논문에서는 이러한 스토리지 암호화를 바탕으로 단순한 통신상의 기밀성을 보장하는 암호화 기법에 사용자의 접근권한 정책을 반영하여 전장관리체계 사용자 역할에 기반한 스토리지 암호화 기법으로서의 CrytpoGW를 설계한다.

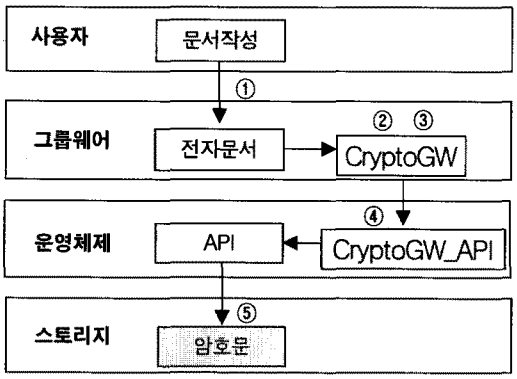
4.1 CryptoGW 운영 개념

전장관리체계의 전자결재시스템은 일반문서와 군사비밀을 유통하기 위한 기능을 수행한다. 이때 군사비밀은 사용자 레벨에서 사용자 단말의 암호화 모듈을 이용하여 PKI(Public Key Infrastruc-

ture)를 이용한 공개키 암호화 알고리즘을 사용한다.

그러나 이러한 암호화 기능은 전자결재시스템 상의 비밀문서에 한하여 적용하고 있다. 따라서 일반문서로 생성하는 모든 문서는 암호화하지 않은 평문 상태로 생성되어 스토리지에 보관되고, 원격으로 떨어진 부서에 통신망을 이용하여 전송한다. 이러한 운영환경은 3장에서 살펴본 바와 같은 보안 취약점들을 이용하여 악의적인 내부자에 의해 데이터의 손실 및 유출이 가능하다고 할 수 있다[18].

따라서 본 논문에서는 그러한 취약점을 해결하기 위한 방안으로 전장관리체계 전자결재시스템 내에 적용 가능한 CryptoGW를 제안하며, 그 운영개념은 <그림 9>와 같다.



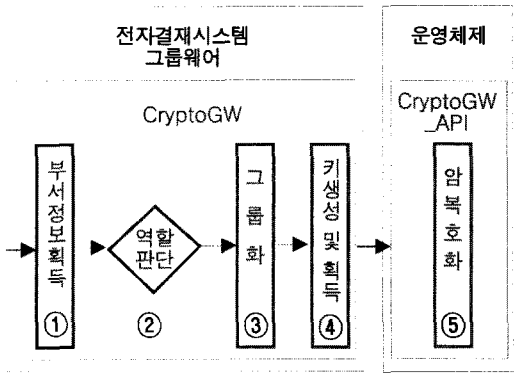
〈그림 9〉 CryptoGW 운영 개념

CryptoGW는 전자결재시스템의 그룹웨어와 함께 구성한다. 사용자는 작성하고자 하는 문서를 기안하여 그룹웨어에 처리를 요청(①)하고 그룹웨어의 CryptoGW는 부서정보를 포함하여 역할기반으로 그룹핑하며(②), 권한과 역할을 판단(③)한다. 그 결과에 따라 역할에 기반하여 암호키를 생성하고, 운영체제에서 CryptoGW_API를 이용하여 암호화(④)한다. 최종적으로 전자문서는 스토리지에 암호문으로 저장(⑤)된다.

4.2 CryptoGW의 개략 설계

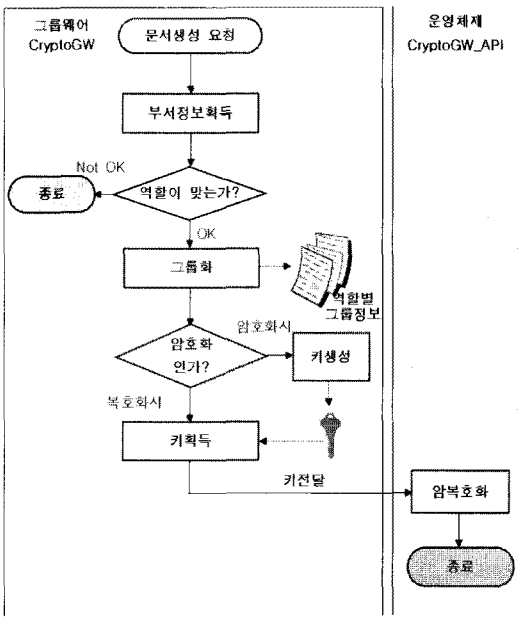
사용자의 부서정보에 따라 권한과 역할을 판단하여 암호화를 수행하는 역할기반의 CryptoGW 동작방법은 <그림 10>과 같다.

전자문서 처리 시 그룹웨어에서 사용자 부서정보를 획득(①)하여 역할을 판단(②)하고, 그 결과에 따라 역할기반으로 사용자를 그룹화(③)하여 키를 생성(④)한 후 데이터베이스에 암호화 저장한다. 보호할 파일은 스토리지에 저장하기 전 운영체제의 CryptoGW_API에서 암호화(⑤)를 수행한다.



〈그림 10〉 CryptoGW와 API의 동작방법

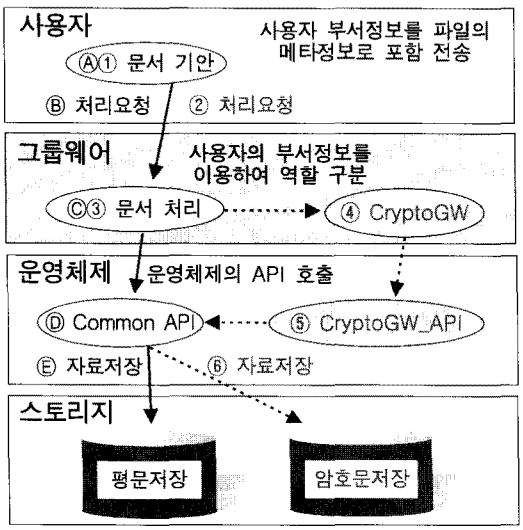
제안하는 CryptoGW의 내부 처리 흐름은 <그림 11>과 같다.



〈그림 11〉 CryptoGW 내부 처리 흐름도

4.3 구현 모델

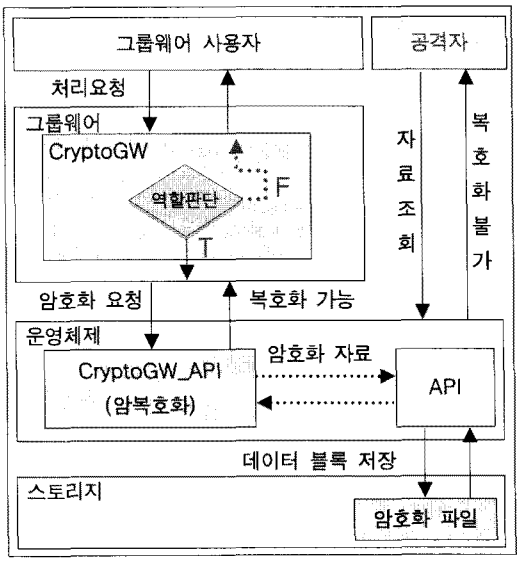
제안한 CryptoGW를 이용한 역할기반의 스토리지 암호화 기법을 전자결재시스템에 적용한 구현 모델은 <그림 12>와 같다.



〈그림 12〉 CryptoGW의 전자결재 적용 모델

<그림 12>에서 Ⓐ부터 Ⓔ까지의 흐름은 최종 저장 형태가 평문인 현재의 스토리지 저장방식을 보여주고 있다. ①부터 ⑥까지는 본 논문에서 제안하는 암호화 기법인 CryptoGW를 이용하는 경우로서, 사용자 부서정보를 이용하여 전자결재시스템 그룹웨어 내부에서 암호화에 필요한 정보를 전달하고, 운영체제에서 CryptoGW_API로 암호화하여 스토리지에 저장한다.

이와 같이 운영체제 수준에서 그룹웨어만을 위한 암호화 API로 암호화를 수행하면 일반적인 운영체제의 일반적인 API로는 암호화된 파일을 조회할 수 없다. 이러한 특성은 스토리지 네트워크 취약점을 이용한 공격들과 내부 관리자의 공격으로부터 자료유출을 방지할 수 있다. 그리고 전자결재시스템의 그룹웨어 내부에서 수행된 암호화는 그룹웨어 자체가 일반사용자나 서버 관리자는 접근할 수 없는 영역에 블랙박스화하여 관리하게 되므로 내부 관리자에 의해 암호화 키가 유출되는 사례를 방지할 수도 있게 된다. <그림 13>은 CryptoGW의 동작방법을 보여주고 있다.



〈그림 13〉 CryptoGW 동작방법

5. CryptoGW 적용 및 평가

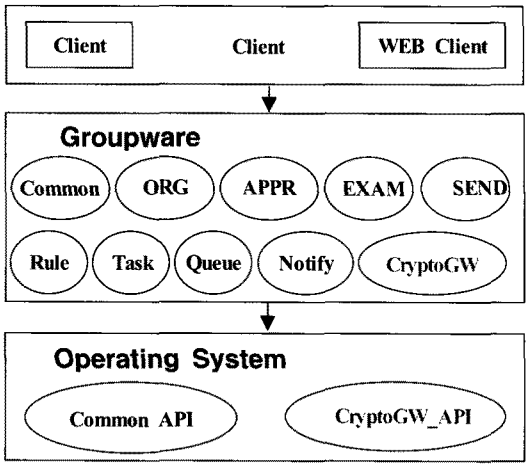
CryptoGW는 전자결재시스템 그룹웨어의 일부로서 부서정보를 이용해 역할을 식별하고, 식별된 역할을 기반으로 그룹화하여 그룹별 키를 생성하며, 그 키를 이용해 암호화를 수행한 후 스토리지에 저장한다.

이러한 CryptoGW는 기존의 스토리지 암호화 기술과 달리 응용레벨에서 사용자 중심의 역할기반 개념을 적용한 키를 생성하여 운영체제에서 암호화를 수행함으로써 보다 강화된 접근제어 기능을 구현할 수 있을 뿐만 아니라 CryptoGW를 적용하지 않은 현 전자결재시스템에서 스토리지에 평문으로 데이터가 저장되는 문제를 보완할 수 있다.

5.1 CryptoGW를 적용한 전자결재시스템 아키텍쳐

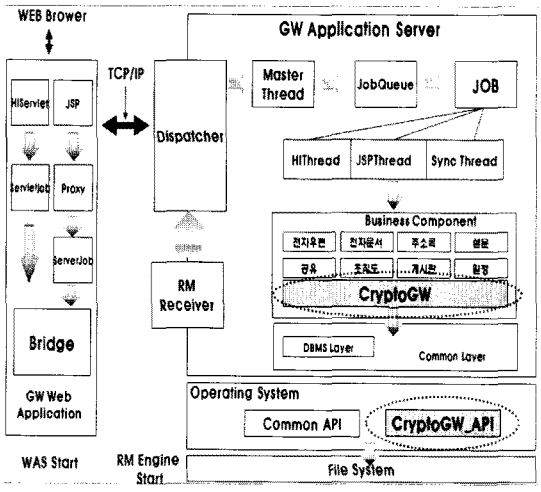
전장관리체계 전자결재시스템의 아키텍처는 사

용자, 그룹웨어, 운영체제로 구분할 수 있다. 이러한 전자결재시스템의 아키텍쳐에 CryptoGW를 추가 적용한 아키텍처는 <그림 14>와 같다.



〈그림 14〉 CryptoGW를 적용한 아키텍쳐

그룹웨어 레벨에는 기존에 Common, ORG, APPR, EXAM, SEND, RULE, TASK, QUEUE, NOTIFY가 있으며 여기에 CryptoGW를 하나의 그룹웨어 모듈로서 추가하고, 운영체제의 커널레벨에는 CryptoGW가 호출할 수 있는 CryptoGW_API를 추가하여 구성한다.



〈그림 15〉 CryptoGW를 적용한 그룹웨어 전체구조

<그림 15>는 기존의 전자결재시스템의 전체 구조도에 본 논문에서 제안하고 있는 CryptoGW를 적용한 모습을 보여준다. 웹 브라우저를 이용해 전자결재시스템의 그룹웨어 웹 어플리케이션이 동작하여 RM Receiver와 Dispatcher에 의해 그룹웨어 어플리케이션 서버로 의뢰된 처리가 컴포넌트에 의해 수행되고, 그 비즈니스 컴포넌트에 CryptoGW를 의뢰하게 된다.

5.2 기존 암호화 기법과의 비교

본 논문에서 제안한 CryptoGW를 기존 파일시스템의 암호화 키, 키 생성, 키 저장, 관리자 접근으로 구분하여 그 처리 방식을 비교하면 <표 1>과 같이 나타낼 수 있다.

〈표 1〉 암호화 키관리 방법 비교

구 분	CFS	TCFS	CryptoGW
암호키	디렉토리별 키 생성	로그인 암호	0 < 키 수 < 사용자 수
키생성 방식	사용자	표준키 관리시스템	역할 기반
키저장	-	특정파일	그룹웨어
관리자 접근	가능	가능	불가

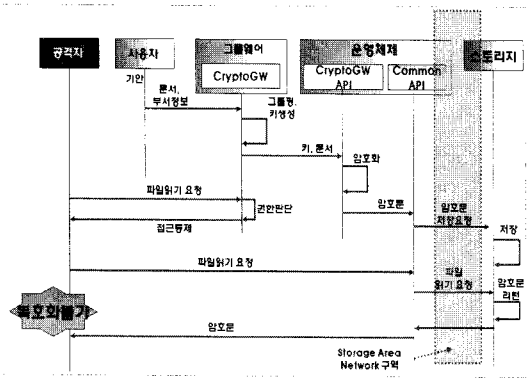
제안하는 CryptoGW는 암호키를 생성함에 있어 사용자의 역할을 부서정보로 구분하여 적정량의 키를 생성한다. 이는 너무 많은 키 생성에 따른 관리 부담을 줄여주고, 단일키로 암호화하여 키가 노출될 경우 모든 자료가 유출될 수 있는 단점을 보완한다.

키 생성 방식은 CFS나 TCFS와 달리 운영체제보다 상위의 응용레벨인 그룹웨어에서 수행함에 따라 사용자의 부서정보를 기준으로 역할을 구분하여 키를 공유한다. 이렇게 생성된 키는 그룹웨어를 통해 별도 암호화 저장함으로써 블랙박스화하여 최고 프로그램 매니저만이 접근 가능하고, 일반 서버 관리자나 지역별 전자결재시스템 관리

자에 의한 자료유출을 방지할 수 있는 장점이 있으며, CrypoGW_API라는 암호화 API를 이용하므로 관리자가 일반적인 운영체제 API를 이용해서는 복호화할 수 없는 장점이 있다. 즉, 반드시 그룹웨어의 CryptoGW를 통해서만 암·복호화가 가능하다.

5.3 안전성 평가

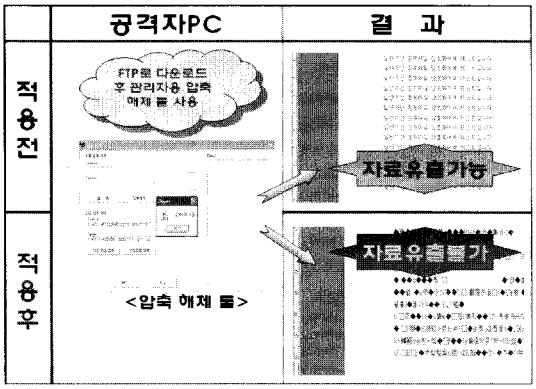
CryptoGW는 외부의 공격자가 전장관리체계 전자결재시스템의 서버 운영체제에 적절한 방해 없이 접근하였거나, 내부 관리자 권한을 획득하여 공격하는 경우에 운영체제의 일반적인 API를 이용하는 명령으로는 스토리지에 저장되어 있는 암호화 파일에 접근할 수 없도록 한다. 이는 스토리지의 중요 자료를 탈취당한 경우도 마찬가지로 운영체제 레벨에서는 암호화된 파일에 접근할 수 없음으로써 보안성을 강화할 수 있다. 이를 도식화하여 공격 및 방어 시나리오를 나타내면 <그림 16>과 같다.



〈그림 16〉 CryptoGW의 공격 및 방어 시나리오

<그림 16>의 점선으로 표시된 부분은 SAN 영역으로 본 논문에서 주로 실험을 실시한 영역이다. 이 영역은 다양한 공격들이 발생할 수 있으나 금번 실험에서는 주요한 3가지 위협인 Session Hijacking, MITM 공격, WWN Spoofing을 중심으로 CryptoGW를 이용한 방어 시나리오를 작성하고, 세부적인 안전성 평가를 수행하였다.

CryptoGW에 의한 안전성 평가를 위한 실험은 내부 공격자가 정당한 권한을 가지고 자료를 획득할 수 있다고 가정하고 CryptoGW를 적용하지 않은 파일과 CryptoGW를 적용한 파일을 각각 ftp로 획득하여 파일의 복호화 및 세부 정보 확인이 가능한지를 확인하였다. 실험 결과 CryptoGW를 적용하지 않은 파일은 스토리지에 단순 압축 파일 형태로 저장되어 있기 때문에 손쉽게 별도 압축 해제용 관리자 툴을 이용하여 압축만 해제하면 내부 공격자는 중요 자료들을 획득할 수 있었다. 그러나 CryptoGW가 적용된 상황 하에서는 <그림 17>에서 보는 바와 같이 암호화된 파일의 복호화가 불가능해져 스토리지 접근권한이 있는 사용자에 의해 자료가 유출되더라도 안전함을 확인할 수 있었다.



〈그림 17〉 CryptoGW의 적용 전과 후의 상태

이상과 같은 안전성 평가 실험결과는 3장에서 기술한 3가지의 위협을 포함하여 권한이 있는 내부자가 실행 가능한 다양한 공격들에 의해 스토리지에서 중요자료가 유출되더라도 본 논문에서 제안하는 역할기반 스토리지 암호화 기법을 이용해 안전성을 보장받을 수 있음을 의미한다.

6. 결론 및 향후 연구방향

본 논문은 전장관리체계 전자결재시스템에 적

용된 SAN 스토리지의 보안취약점을 분석하고 시나리오 기반의 실험을 통해 SAN이 내부자에 의한 정보유출이 가능할 수 있음을 검증하였다. 그리고 SAN에서 내부자에 의한 정보유출을 방지하기 위한 대책으로 사용자 역할기반의 스토리지 암호화 기법인 CryptoGW를 제안하였고, 전장관리체계 전자결재시스템 개발환경에서 구현 및 적용하여 안전성을 평가하였다.

CryptoGW는 기존의 암호화 파일시스템을 이용한 스토리지 암호화에 사용자 정보를 이용하여 역할기반의 접근제어 능력을 추가함으로써 암호키를 생성하고 저장하는 핵심적인 부분을 그룹웨어 내부에서 처리하도록 설계하였기 때문에 내부자 뿐만 아니라 외부자에 의한 정보유출을 방지할 수 있는 장점을 가진다. 그리고 운영체제의 CryptoGW_API가 암복호화를 수행케 함으로써 커널 레벨에서 암호화를 수행하는 TCFS의 장점을 그대로 유지하고 있다.

또한 안전성 평가 실험 결과 권한이 있는 내부 사용자가 제안된 CryptoGW를 이용하여 스토리지에 저장된 파일을 획득하더라도 일반적인 관리자 권한이나 운영체제 수준에서의 명령을 이용한 복호화는 불가능하여 자료유출에 대한 안전성을 보장함은 물론 전장관리체계 전자결재시스템의 보안성을 향상시킬 수 있음을 확인하였다.

향후 연구에서는 전장관리체계에 적용된 키관리 시스템 및 인증체계와의 연동성을 고려하여 중요 군사자료들을 보다 더 안전하게 저장할 수 있는 방안에 대해 연구할 계획이다.

참고문헌

[1] 한국정보보호진흥원, "2009 정보시스템 해킹·바이러스 현황 및 대응", 한국정보보호진흥원, 2009.

[2] 김성배, "스토리지 네트워크 보안현황과 스토리지 모델 비교분석", 동국대학교, 2004.12.

[3] 윤희용, 최성춘, "분산 스토리지에 대한 취약성 분석 및 공격 탐지기법 개발", 한국정보보호진흥원, 성균관대학교, 2003.12.

[4] 임재덕, 은성경, 김정녀, "데이터 보호를 위한 암호화 파일시스템의 분석", 전자통신동향분석 제16권 제4호, pp.54-66, 2001.8.

[5] Matt Blase, "A Cryptographic File System for Unix", 1993 ACM Conference on Communications and Computing Security, Fairfax, VA, November 3-5, 1993.

[6] G. Cattaneo et al., "Design and Implementation of a Transparent Cryptographic File System for Unix", Technical Report. Dip. Informatica ed Appl, Universita di Salerno, July 1997.

[7] Transparent Cryptographic File System, http://tcfs.dia.unisa.it/

[8] 임재덕, 유준석, 김정녀, "유닉스 시스템에서 다양한 접근제어 정책을 이용한 커널 수준의 자동 암호화 기법", 한국전자통신연구원, 2003.5.

[9] E. Zadok et al., "Cryptfs: A Stackable Vnode Level Encryption File System", TR CUCS-021-98. CS Department, Columbia University, 28 July 1998.

[10] Erez Zadok, "Stackable File Systems as a Security Tool", TR CUCS-036-99. CS Department, Columbia University, Dec. 1999.

[11] 김병선, "한군군 C4I체계의 실태 및 발전방안에 대한 연구", 한남대학교, 2006.12.

[12] 정태용, "전자결재시스템내 비밀문서 유통체계 설계방안", 대전대학교, 2006.2.

[13] 이민섭, "공개키 암호화 알고리즘에 관한 연구", 단국대학교, 한국전자통신연구원, 1998.6.

[14] 최일호, "전자문서 결재시스템내 비밀문서 정보유통 보안설계방안", 배재대학교, 2006.6.

[15] Himanshu Dwivedi, "Securing Storage", Addison-Wesley, 2005.

[16] http://lin.fsid.cvut.cz/~kra/#HUNT

[17] http://ettercap.sourceforge.net/

[18] Tom Olzak, "Data Storage Security", 2006.6.

저자소개

허 경 순

2009년	국방대학교 정보관리전공(공학석사)
현재	국군지휘통사령부 상호운용성센터 체계개발팀(KJCCS 전자결재운영 및 유지보수담당)
관심분야	전장관리체계, 상호운용성, 키관리, 스토리지 보안

이 수 진

1992년	육군사관학교 전산학과(이학사)
1996년	연세대학교 전산과학과(이학석사)
2006년	한국과학기술원 전자전산학과(공학박사)
2006년~현재	국방대학교 국방관리대학원 교수
관심분야	침입탐지시스템, Ad-hoc 네트워크 보안, 센서 네트워크 보안, 사이버공격 대응 기술, 암호키 관리