Web기반 초고속 통신망에서의 CALS시스템을 위한 지능형 보안시스템 개발

김동현, 권낙주, 구상엽, 왕지남

아주대학교 산업공학과

Abstract

현재 많은 기업들은 인터넷을 기반으로 Intranet, Extranet등을 구축하며 기업간 전자 상거래에 활발한 움직임이 있다. Extranet은 WWW으로 대표되는 인터넷 기술을 사용한 기업간 정보 시스템이라 할수 있고, 종래의 기업간 정보시스템 보다 훨씬 구축하기 쉽기 때문에 Extranet의 수요는 점점더 확산되고 있는 추세이다. 즉 Intranet에서 Extranet으로 기업의 정보 시스템이 확대되기 시작했다. 그러나 Extranet은 Intranet과는 달리 영업데이타가 공용 통신 회선을 타고 전송된다든지 다른 회사의 사용자가 사내 서버에 액세스해 들어오기 때문에 반드시 고려돼야 할 과제가 보안(Security) 문제이다. 즉 어떤 거래에 대한 데이터의 전달과정에서의 변조 및 누락이 없었는지 거래자가 거래사실을 부인하지 못하게 하는 조치, 혹은 제3자가 거래내용을 도청하지 못하게 하는 조치와 내부에 보관된 정보를 허가받지 않은 사용자가 알지 못하게 한다든지 하는 조치가 반드시 필요하다. 따라서 본 연구에서는 Web기반 CALS시스템 구현에 있어 보안성을 확보하기 위하여 내부 정보보호를 위한 미들웨어 구현, 인증 및 접근제어를 위한 Proxy구현 기술, 인증 및 데이터 보호를 위한 암호화 기술등을 확보하여 이에 대한 시제품의 개발과 구현에 관해 알아보고자 한다.

1. 서론

최근 급속히 확산되고 있는 기업간의 전자상거래는 정보화 사회에 필수 불가결한 요소로써 인식되고 있다. 각 기업들은 Extranet등을 기반으로 하는 CALS시스템의 구축을 통하여 보다나은 경쟁력 확보에 힘을 기울이고 있는 실정이다. 그러나 이러한 시스템은 Internet이라는 거대한 공용망에 연결돼있으므로 허가받지 않은자(침입자)가 보호해야할 내부 네트워크로 침투해 들어올수 있는 가능성을 내재하게 되었다. 즉 보호해야할 내부 네크워크의 중요한 데이터를 도난 당하거나 변조 혹은 삭제 당할수 있게 되었다. 뿐만아니라 네트워크 상에서 중요한 데이터가 도청당하거나 변조 될 수 있으며 위조된 송신자로부터의 거짓된 데이터를 받을수도 있으며 내부 네트워크가 침입자가 투입한 바이러스나 웜에 의해 감염될수 있는 가능성을 항상 가지게 된 것이다.

이러한 공격을 받게 되면 보호해야 할 자료는 물론이고 시스템 전체가 파괴될수 있으며 이것은 곧 그 기업에 막대한 해를 끼치게 될 것이다. 따라서 현재 추진되고 있거나 이미 완성된 CALS시스템에 보안대책을 강구해야 한다.

따라서 본논문에서는 Web기반 CALS시스템에서의 보안에 관한 문제점에 대한 대비책으로 외부로부터 내부 자원보호를 위한 도구로써 미들웨어의 구현과 인증 및 접근제어를 위한 프락시(proxy)구현기술과 전자서명과 인증 및 데이터 보호를 위한 암호화 기술(IDEA, RSA, MD5)에 대하여 논하며 원격 호스트간의 안전한 정보 전송을 위한 Virtual Private Network(VPN)과 네트워크 상에서 보안을 유연하게 지원하는 IPSec(Internet Protocol Security)에 대하여 고찰하여 향후 사용자 관점에서 보다 안전하게 사용할수 있는 Web환경

하에서의 인증서버 구축과 다기능 접근제어 시스템 구축등 지능형 통합 보안 시스템 구축의 연구 방향을 제시한다.

2. 암화화 알고리즘

2.1.DES(Data Encryption Standard)

DES는 대표적인 관용암호 방식(symmetric algorithm)으로써 64비트의 평문을 64비트 암호문으로 만드는 블록암호시스템으로 입력으로는 64비트 평문과 56비트키(실제로는 64비트키이다 다만 8비트는 패리티 비트나 임의의 값을 준다.)를 사용한다.

DES는 64비트 평문이 초기순열단계, 동일함수의 16회 반복단계 그리고 64비트 암호문 생성을 위한 초기 순열의 역인 역초기 순열단계를 거치게된다.

56비트 키는 순열선택에 의해 순열되며 이 결과는 28비트의 두 개의 값으로 취급된다. 28비트 두 개로 나누어진 키는 각반복단계에서 별도로 일정한 규칙에 의해 1또는 2비트씩 좌측 이동 또는 회전(rotation)하게 된다. 두 개의 28비트(56비트)키는 순열선택에 의해 48비트 출력을 생성하며 이 결과인 48비트 키는 S-box의 입력이 되기 위해 각 반복단계에서 평문의 오른쪽 32비트가 확장된 48비트와 XOR된다.

DES의 복호과정은 기본적으로 암호과정과 동일하며 암호문이 DES알고리즘의 입력으로 사용되고 다만 각 반복단계에서 사용된 키가 역순으로 사용된다. DES는 평문이나 키의 작은변화가 암호문에 많은 변화를 준다. 즉 DES는 강한 쇄도 효과를 보이고 있다.

DES의 우려사항은 DES에 사용되는 키가 56비트로 비교적 작기 때문에 키의 전수탐색공격(brute-force attack)이 가능하다는것과 DES알고리즘 자체에 사용되는 S-box에 대한 우려이다. 즉 S-box에 대한 설계 고려사항이 공개된 적이 없었기 때문에 S-box의 약점에 대해 알고 있는 공격자가 해독할 수 있을수도 있다는 우려이다. 그이외에도 Bihman과 Shamir에 의해 다수의 논문이 발표된 차분 암호 해독 공격(Defferential Cryptanalysis Attack)과 Matsui가 발표한 선형 암호 해독(Linear Cryptanalysis)방법에 의해 계속적인 우려가 있어왔다.

2.2 MD5 메시지 다이제스트 알고리즘

이 알고리즘은 임의의 길이를 가진 메시지를 입력으로 하고, 128비트 메시지 다이제스트를 출력으로 제시한다. 입력은 512비트 블록으로 처리한다.

MD5의 다이제스트 순서는 우선 메시지 길이를 표시하는 64비트와 패딩비트를 부가하여 패딩된 메시지 길이가 512비트의 정수배가 되도록 한다. 메시지 길이를 표시하는 64비트는 만일 메시지 길이가 2^{64} 보다 크다면 원메시지 길이의 64비트만이 사용되어진다. 그러므로 이것은 [원메시지길이 (mod 2^{64})]로서 원래의 길이를 표시한다.

패딩비트 = 512 − ((원메시지길이 + 64비트) (mod 512))
패딩된메시지 = 원메시지 + 패딩비트 + 64비트

128비트 버퍼는 해쉬함수의 중간과 최종결과를 보관하기 위하여 사용되어 지며 4개의 32비트 레지스터로 표현할 수 있다. 이러한 레지스터들은 정해진 16진수 값으로 초기화 되어지고 패딩된 메시지는 512비트 블록으로 나누어서 각 블록을 동일한 방법으로 마지막 블록까지 다이제스트한다. 512비트 블록은 16개의 32비트 단어로 나누어서 4개의 라운드에 동일하게 적용한다. 4개의 라운드는 각각 다른 논리 함수를 사용하며 각 라운드는 16번의 반복적인 논리함수와 mod 2^{32}에서의 덧셈과 반복적 수행시 정해진 쉬프트 연산을 하게 된다. 각 라운드가 수행된 결과는 다음 라운드의 입력값으로 사용됨으로써 해쉬함수의 결과를 보관하기 위해 사용된 4개의 32비트 레지스터에 출력되고 이것은 곧 다음의 512비트 블록의 다이

제스트에 입력으로 들어간다. 마지막 블록까지 처리되어지면 마지막 단계의 출력이 128비트 메시지 다이제스트이다.

MD5는 강도는 같은 메시지 다이제스트를 가지는 두 개의 메시지를 추적하는 어려움은 2^{64} 연산의 정도인 반면, 주어진 다이제스를 가지고 메시지를 찾는 어려움은 2^{128}연산의 정도로 써 비교적 강하다는 것을 추측할수 있다.

2.3 RSA 알고리즘

Rivest, Shamir, Adleman에 의해 개발된 공개키 암호방식의 대표적인 알고리즘이다. RSA 알고리즘은 Euler's Theorem을 기반으로 하고 있다. Euler's Theorem을 살펴보면

$\phi(n)$은 집합 $\{1,2,3,\cdots,n-1\}$ 에서 n과 서로소인 원소의 갯수를 나타낸다.

$\phi(p)=p-1$ (단 p가 소수 일때)

$\phi(pq)=(p-1)(q-1)$ (단 p, q가 소수 일때)

$a^{\phi(n)}\equiv 1 \pmod{n}$ (단 a와 n이 서로소 일때)

위의 식에서 p×q=n 이라면 p와 q를 알고있으면 ϕ(n)을 구하기 쉬우나 n이 어느정도 큰수이고 p와 q를 모른다면 ϕ(n)값을 구하기는 대단히 어렵다. 따라서 이런 성질을 이용하여 RSA알고리즘을 살펴보면 우선 두 개의 큰 소수 p와 q를 선택하여 자신의 개인키로 하고, 그다음 ϕ(n)을 구하여 ϕ(n)과 서로소인 e를 구하여 n과 e를 공개키로 한다. 그리고 e에대한 mod ϕ(n)에서의 곱셈에 대한 역원을 구한다 즉 $e \times d \equiv 1 \pmod{\phi(n)}$을 만족하는 d를 구하여 개인키로 한다.

암호화 단계를 보면 암호문 C는 평문 M에 의하여 다음과 같이 구할 수 있다.

$$C \equiv M^e \pmod{n}$$

복호화 단계에서는 다음과 같다.

$$M \equiv C^d \pmod{n}$$

이를 간단히 증명하면 다음과 같다.

$C \equiv M^e \pmod{n}$ (양변에 d제곱을 하면)

$C^d \equiv (M^e)^d \pmod{n}$

$\equiv M^{ed} \pmod{n}$

$\equiv M^{\phi(n)k+1} \pmod{n}$

$\equiv (M^{\phi(n)})^k \times P \pmod{n}$

$\equiv M \pmod{n}$ (단 P와 n이 서로소 일때)

따라서 $M \equiv C^d \pmod{n}$이 된다.

만약 n과 e를 가지고 d를 구할 수 있다면 RSA 알고리듬은 전혀 쓸모가 없게 된다. 하지만 앞에서도 밝힌바와 같이 d를 찾아 내기 위해선 ϕ(n)를 계산해야 하는데 이를 위해서는 n을 소인수 분해 해야 한다. 만약 p, q가 100자리 소수라면 n을 소인수 분해 하는 것은 거의 불가능하다고 알려져 있다. 현재 RSA 알고리즘이 사용되는 장비들은 512비트의 키를 사용하

고 있고 이것은 RSA의 속도를 늦게하는 원인이 되고 있다.

RSA암호 분석에서 가장 큰 논의는 n을 두 개의 소수로 인수분해하는 작업이다. 현재까지 매우 큰값에 대하여 인수분해 하는 방법은 알려져 있지 않다. 그러나 RSA의 안정성은 전적으로 소인수 분해의 어려움에 기인하기 때문에 다른 공격 방법이 없다고는 증명되지 않았다.

3. VPN(Virtual Private Network)과 IPSec(Internet Protocol Security)

3.1. VPN

VPN은 그림1과 같이 실제로 어떤 네트워크를 구성하는 것이 아니고, 원격의 두 네트워크 혹은 두 호스트 간의 통신에 항상 약속된 암호화(Encryption)방법을 통하여 중간에서 패킷을 도청당하더라도 그내용을 알수 없게 함으로써 마치 하나의 내부 네트워크안에서 통신을 하듯이 자유롭게 원격의 네트워크를 이용할수 있게 하는 방법이다. 따라서 VPN의 장점은 사설 전용망을 구축하는것보다 비용이 절감되며, 단시일 내에 구축이 가능하고, 회선의 유지보수에 대한 부담이 감소한다. 그러나 VPN은 고용망을 사용하는것이기 때문에 보안상의 취약점이 결정적인 약점으로 지적되고 있다. 이것은 기본적으로 암호화기법을 바탕으로 구축될수 있다.

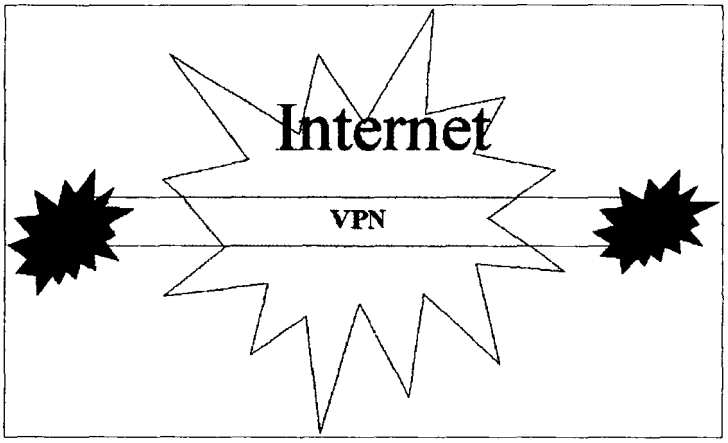

그림 1. VPN

3.2. IPSec

IPSec의 설계목적은 사용자들이 희망하는 유용하고 견고한 암호화 메카니즘을 확실하게 하는 것이다. IPSec은 IP version 4 (IPv4)와 IP version 6 (IPv6)에서 보안 서비스를 제공하는데 사용될 두 개의 독특한 header가 있다. 이 두 개의 header는 IP Authentication Header(AH)와 IP Encapsulating Security Payload(ESP) header 이다.

3.2.1. IP Authentication Header(AH)

이 header는 IP datagram에 대하여 무결성(Integrity)과 인증(Authentication)을 제공하지만 기밀성(Confidentiality)은 제공하지 못하며 traffic analysis에 대한 보호도 갖지 못한다. 기본적으로 사용되는 알고리즘은 symetric 방법인 MD5이며 따라서 그자체로는 부인방지(non-reputation)를 제공하지 못한다. Authentication Header에 IP datagrame에 대한 인증정보를 가지며 비밀키가 사용된다.

Authentication Header의 사용은 IP protocol 처리 비용과 통신 지연을 증가 시키는 결과를

가져온다. 증가하는 지연의 가장 큰 이유는 송신자(Sender)가 authentication data를 계산하고 수신자(recever)는 수신된 Authentication Header를 포함하는 IP datagram마다 authentication data를 계산하고 비교해야 하기 때문이다.

모든 IPv6가 가능한 호스트들은 적어도 128-bit 키를 사용하는 MD5 알고리듬을 가지고 IP Authentication Header를 수행해야만하며, 그 수행들은 다른 인증 알고리듬을 지원하는 것이 좋다.

3.2.2. Encapsulation Security Payload

Encapsulation Security Payload는 IP datagram에 대하여 무결성과 인증, 기밀성을 제공한다. 이방법은 IP datagram 전체를 캡슐화하는 방법(Tunnel-mode)과 단지 upper-layer 프로토콜(TCP, UDP, ICMP등)을 ESP(Encapsulation Security Payload)안에 캡슐화 하고 cleartext IP header를 덧붙이는 방법(Transport-mode)이 있다. 이러한 방법은 internetwork를 통하여 안전한 데이터를 전송하는데 쓰인다.

ESP는 각 datagram이 암호화되고 복호화 되기 때문에 통신 지연이 증가한다. 그리고 상호운용성을 위해서 CBC(Cipher-Block Chaining)모드를 사용하는 DES(Data Encryption)알고리즘을 사용한다.

IP security에서 IP Authentication 과 IP Encaptuating Security Payload는 각각 독립적으로 사용될 수 있고 두 방법이 혼합해서 사용될 수 있다. 두가지 방법을 혼합해서 사용하는 경우 IP Authentication을 IP datagram에 덧붙인다음 ESP에 의해 캡슐화 하는 방법이다. 두가지 방법을 혼합할 경우 보다 강력한 보안을 제공하게된다.

4. Proxy 서버와 보안시스템

Proxy서버는 말그대로 서비스를 대행하는 서버를 통칭한다. proxy서버의 장점중에 하나는 내부 네트워크로 통하는 하나의 병목점 역할을 할 수 있다는 점이다. 즉 외부로 부터의 접근을 통제할수 있는 하나의 방화벽(Firewall)의 기능을 갖을수 있다.

그러나 Web환경하에서 내부 네트워크를 단순히 proxy서버에게 의존할 수는 없다. 따라서 허가된 사용자는 빠르고 쉽게 접근이 가능하고 허가되지 않은 사용자나 악의 적인 침입자를 방지하며 다기능 접근 제어(허가)를 위해 사용자별, 그룹별, 서비스의 권한에 따른 접근제어 데이터 베이스를 구축할 필요가 있으며, Web서버별 자원별로 통합관리 하고, 사용자명과 그룹 과 패스워드 그리고 접근권한등을 포함하는 인증데이타의 암호화로 보안성 및 비밀성을 유지하며, Web서버는 자체의 파일 및 서비스별 접근제어를 하며 필요시 인증서버에 인증을 요구하고, 실시간으로 LOG 상태정보를 확인하며 LOG정보의 통계 및 효율적인 분석을 할수 있으며 필요시 원격에서도 관리할수 있는 보안시스템이 요구되고 있는 실정이다.

5. 결론 및 향후과제

정보화사회로 가는 길목에서 CALS시스템의 도입은 기업의 경쟁력 확보를 위하여 그 중요성이 점점더 더해가고 있다. 그러나 CALS시스템의 구축에 앞서 가장 염려되는 문제가 바로 보안이다. 우리나라의 네트워크 보안기술은 선진국에 비해 많이 뒤떨어져 있으며 더구나 전국적인 네트워크 표준 Architecture에서의 CALS와 초고속망에서 운영되는 통합 네트워크 보안에 대한 연구는 확립되지 않은 실정이다.

본논문에서는 Web기반 CALS시스템의 보안을 위하여 기본적인 암호화 알고리즘과 보안방법들에 대하여 간략히 살펴 보았고 앞으로 보안 시스템을 구축할 경우 고려해야할 사항들을 알아보았다.

앞으로 보안에 관한 여러 가지 기술들을 도입하여 초고속망에서의 Web기반 CALS시스템

에서 사용자는 보다 안전하고 편리하고 안정적인 사용을 할수 있으며 관리자는 쉽고 신뢰성 높은 운영을 할수 있는 보안시스템의 개발이 이루어 져야 할 것이다.

참고문헌

1. 하태용, 김동현, 왕지남, 신용백, "지능형 Virtual Private Network(VPN)의 서버구현", 대한산업공학회 추계 학술 대회 논문집, 대한산업공학회 1997. 10.
2. 김광배, 김 철, "정보 보호 이론의 발전", 전자공학회지, 제21권, 제5호, 한국전자공학회, 1994. 5.
3. 윤기송, 변옥환, "국내외 Internet 보안대책",전자공학회지, 제21권, 제5호, 한국전자공학회, 1994. 5.
4. 최용락, 소우영, 이재광, 이임영, "통신망 정보 보호" 도서출판 그린, 1996.
5. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security", Prentice Hall PTR, 1995.
6. Bruce Schneier, "Applied Cryptography", John Wiley & Sons, 1996.
7. Kenneth H. Rosen, "Elementary Number Theory and Its Application", ADDISON-WESLEY PUBLISHING COMPANY, 1993.