Telecommunications Review, 제 10 권, 3 호, pp.537-546, SKT, 2000.

차세대 인터넷의 보안 기술

김 광조*, 백 준상*, 이 종태**

* 한국정보통신대학원대학교, 공학부 정보보호그룹
연구관심분야 : 암호와 정보보안
대전시 유성구 화암동 58-4
전화 : 042-866-6118 Fax : 042-866-6154
** 한국전자통신연구원 차세대인터넷정보보호연구팀
대전시 유성구 가정동 161
전화 042-860-5545 Fax : 042-860-5611
E-mail : kkj@icu.ac.kr, mohi@icu.ac.kr, jtl@etri.re.kr

요약

본 논문에서는 개방성을 지향하는 현행 인터넷에서 발생가능한 보안 취약점으로 직 간접 공격 방식과 그 대책을 기술하고 이러한 위협으로부터 인터넷을 보호하기 위한 방법으로 암호 기술의 응용 방법으로 파일간, 컴퓨터 간, 통신 기기간 암호 방식을 분류하고 프로토콜을 예시한다. 또한, 통신 기기 간의 암호 방식으로 차세대 인터넷 보안 기술인 IPSec 의 보안 요구사항과 운용 특징을 고찰한다. 또한, 암호나 인증 방식을 이용하기 위하여 통신 쌍방간에 사전에 공유하여야 하는 키 관리 시스템에서의 요구 사항을 기술하고 Baek 과 Kim[4]이 최근에 제안한 안전한 키 관리 시스템을 상세히 고찰한다. 인터넷의 보급과 함께 수반되는 신규 사이버 서비스의 탄생, 이동성의 확보와 보안성의 제공 등 점차 발전된 통신 구조에서 다양한 암호 기법이 응용되리라고 예상한다.

Abstract

In this paper, after introducing the possible vulnerabilities, i.e., passive and active attacks, of the current Internet, we discuss their cryptographic countermeasures by using file-to-file, end-to-end and link-by-link encryption. schemes and give cryptographic protocols in detail.

Also, we describe security requirements and state-of-the-art of IPSec, which is security specification for next generation Internet (IPv6) to add confidentiality, authentication and integrity services to the current Internet. Since key management systems are to be one of the crucial techniques for IPSec, we discuss Baek and Kim [4]'s key management scheme in detail and suggest how to share a session key over the open Internet environment securely. Finally, we expect that the emerging cryptographic techniques will play a central role in the cyber space and mobile communications services.

I. 서론

90 년대에 들어와 정보통신망의 발전과 더불어 발전한 현행 인터넷 (IPv4)은 정보통신망을 통하여 언제든지, 누구든지, 어디에서든지 정보 교류가 가능한 정보통신 수단으로 각광을 받고 있으며 전자 우편이나 정보 수집에 이용될 뿐만 아니라, 새로운 통신 서비스로서 기업간 (B2B) 또는 기업과 소비자간 (B2C)의 전자 상거래, 전자 화폐 시스템, 전자 은행 등 다양한 사이버 사업이 전개되고 있으며, 향후 기업과 정부간 (B2G)의 전자상거래도 예측되고 있다.

이러한 인터넷은 사용자가 세계 어디에 있든지 이용할 수 있는 공개된 네트워크이므로 사용자에게 편리성을 제공하는 반면, 누구든지 접근 가능한 공개적인 통신로 상의 정보를 도청이나 감청하는 등의 제 3 자의 불법 행위와 합법적인 통신 상대방간에도 비대면이라는 네트워크 상의 특징을 이용하여 불법 접근을 시도한다거나 교신 사실을 부인하는 행위가 발생한다. 따라서 안전하게 인터넷 서비스를 이용하기 위해서는 보안이 필수 불가결하게 요구된다. 하지만, 현행 인터넷의 큰 취약점은 보안 서비스가 광범위하고 일반적으로 제공되지 않는 점에 있다. 실제로 현행 인터넷의 보안 구조상의 문제점으로 인하여 네트워크 상의 정보를 불법적으로 감청하여 정당한 통신자의 패스워드 훔쳐보기 (password sniffing)를 손쉽게 할 수 있을 뿐만 아니라, IP spoofing 공격, TCP/IP 세션 가로채기, SYN 정보를 반복적으로 특정 호스트에 주입하여 호스트의 장애를 유발시키는 서비스 부인 (denial of service) 행위 등이 가능하다 [8, 20]. 또한 현행 인터넷은 90 년대 초에 보급되기 시작하여 현재는 컴퓨터의 보급과 함께 폭발적인 증가세를 보여 고유 주소에 해당하는 IP 주소의 고갈 등의 문제점을 드러내고 있다. 현재 이런 문제점등을 고려한 새로운 인터넷과 이 새로운 인터넷의 보안 구조가 제시되고 있다. 이러한 추세를 보면 보안 기술은 모든 분야에서 선택 기술이 아니라 필수 기술로서 부각되고 있으며 특히 전자 상거래 시스템의 보급과 함께 중요성이 더욱 인식되고 있다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 개방성을 지향하는 현행 인터넷에서 발생 가능한 보안 취약점으로 직,간접 공격 방식과 그 대책을 기술한다. 제 3 장에서는 이러한 위협으로부터 인터넷을 보호하기 위한 방법으로 암호 기술의 응용 방법으로 파일 간, 컴퓨터 간, 통신 기기 간 암호 방식을 분류하고 프로토콜을 예시한다. 제 4 장에서는 통신 기기 간의 암호 방식으로 차세대 인터넷 보안 기술인 IPSec (Secure Architecture for the Internet Protocol)의 보안 요구사항, IPSec 의 보안 프로토콜인 AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 보안 특징을 고찰하고 운용 특징을 기술한다. 제 5 장에서는 암호나 인증을 이용하기 위하여 통신 쌍방간에 사전에 공유하여야 하는 키 관리 시스템에서의 요구 사항을 기술하고 Baek 과 Kim[4]이 최근에 제안한 키 관리 시스템의 안전성을 분석한다. 그리고 제 6 장에서는 끝으로 결론을 맺는다.

II. 인터넷에서의 보안 위협과 대책

1. 보안 위협

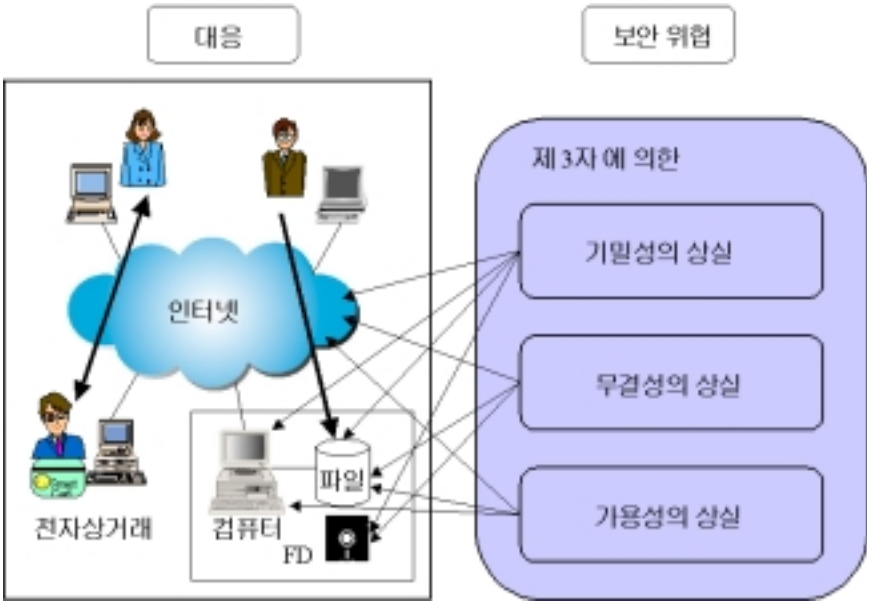
현행 인터넷 상에서의 보안 위협은 불법적인 제 3 자와 합법적인 통신 상대방에 의한 행위로 구별되며 제 3 자에 의한 보안 위협을

(1) 기밀성의 상실 : 인터넷 상의 정보가 부당하게 노출됨.

(2) 무결상의 상실 : 인터넷 상의 정보가 불법 개조, 변조됨.

(3) 가용성의 상실 : 인터넷 상의 보존된 정보나 자산이 제 3 자의 컴퓨터에 부당하게 사용됨.

등의 3 가지로 나눌 수 있다. (그림 1) 은 인터넷 상의 이런 여러 가지 위협을 나타내고 있다.



(그림 1) 인터넷 상의 보안 위협

한국정보보호센터 내의 침해사고 대응팀 [1] 의 최근 보고서에 의하면 현행 인터넷은 이와 같은 보안 위협으로 인해 불법적인 해커들이 ID 와 패스워드를 도용한다던가, 특정 해킹 프로그램 등을 이용한 정보 통신망의 해킹 행위가 점차 증가하고 있다고 한다. 이러한 행위를 하는 사람들은 (a) 크랙커 (b) 외국의 스파이 (c) 테러리스트 (d) 산업 스파이 등이라고 추정되며 이러한 네트워크 상에 공격은 다음과 같이 직접적 공격과 간접적 공격으로 구별된다.

(1) 직접적 공격: 악의의 제 3 자가 자신의 컴퓨터를 직접 조작하여 통신로를 경유를 이용하

여 네트워크에 연결된 컴퓨터로 침입하여 파일등에 피해를 준다. 또한, 보안 허점 (security hole)을 교묘히 찾아서 대상이 되는 컴퓨터에 침입하는 행위로 부정 접근이라고도 한다.
(2) 간접적 공격: 악의의 제 3 자가 부정한 소프트웨어를 목표 컴퓨터에 삽입시켜 이 소프트웨어를 이용하여 컴퓨터 내부의 파일을 공격한다. 이런 공격을 통상 컴퓨터 바이러스에 의한 공격이라고도 한다. 작년에 국내에 최초로 엄청난 피해를 CIH 바이러스의 내부 구조과 대책은 참고문헌 [2]에 자세히 기술되어 있다.

또한, 합법적인 통신 상대방에 의한 부정으로는 인증성의 상실을 들 수 있다. 즉, 통신 상대방이 계약문서 상의 일부 내용을 변조한다든가 거래 내용을 부인하는 행위가 발생할 수 있다. 예를 들어, 100,000 원을 송금하였다 하였는데 10,000 원을 수신하였다고 하는 부정한 행위에 대한 증거를 제시할 수 있는 수단이 제공되어야 한다. 이러한 송수신 사실을 부인을 방지하는 기법으로 공개키 암호 기법을 활용한 전자 서명 방식을 이용하면 효과적으로 대처할 수 있다.

2. 보안 대책

2.1 제 3 자의 위협으로부터 보안 대책

<표 1> 에서 보듯이 직접적인 대책과 간접적 대책이 분류하며 간접적 대책으로는 보안 감시, 보안 감사, 보안 평가 등이 있으며 보안 대책을 확고히 하기 의하여는 반드시 행하여야 한다.
직접적인 대책은 접근 관리 기술과 공격 대상이 되는 통신로나 파일내의 정보를 부정 접근을 방지하는 기술을 의미한다. 접근 관리가 제대로 되면 공격에 필요한 정보를 추가하는 것이 불가능하며 기밀성, 무결성, 가용성의 상실 대책 효과가 있다. 이러한 접근 관리 기술은 다음의 2 가지 기술로 분류된다.

(1) 사용자 인증 기술
사용자가 본인임을 증명하는 기술로 본인 확인 기술이라고 하며 현재는 패스워드 만을 이용한 것이 일반적이나 일방향 함수를 이용한 암호 시스템이나 해쉬 함수를 이용한 도전-응답 프로토콜에 의한 인증 방식 및 영지식 상호 대화형 증명 방식 등 강력한 암호 기술을 이용한 방식도 실용화되고 있다. 또한, 개인별 생체 정보의 유일성을 이용한 지문, 성문, 얼굴모양, DNA 정보 등을 겸용하여 인식하는 기법도 가능하다.

(2) 접근 제어 기술
이것은 사용자가 허가된 권한 이상으로 접근을 방지하는 기술로 네트워크의 연결점에 부정한 접근을 방지하기 위한 방화벽 (Firewall) 시스템을 이용하여 제어할 수 있다. 이런 접근 통제 기법은 MAC(Mandatory Access Control)과 DAC(Discretional Access Control) 기법이 있으며 최근 실체가 수행할 수 있는 역할에 기반한 RBAC(Role Based Access Control) 기법의 연구가 진행 중이다.

<표 1> 보안 위협과 대책

보안 위협		보안 대책			
		직접 대책	효과	간접 대책	효과
제3자에의한위협	(1) 기밀성의 상실	접근 제어 암호화	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
	(2) 무결성의 상실	접근 제어 암호화	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
	(3) 가용성의 상실	접근 제어	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
통신상대방의위협	(4) 증거성의 상실	디지털 서명	방지 검출		
	(5) 불법 복제			Watermarking	검출 예방

위에서 열거한 접근 관리 대책을 세웠다 하여도 제 3 자가 합법적인 타인으로 위장한다든가 보안 허점을 이용하여 침입할 가능성도 있다. 암호 기술은 접근 통제가 실패하여 제 3 자가 정보를 입수하였다고 하더라도 그 문자나 데이터를 변형하여 이해할 수 없게 하는 보호 기술이다.

2.2 통신 상대방의 위협으로부터의 보안 대책

인터넷을 이용한 거래 사실을 부인하는 등의 문제를 방지하기 위하여는 통신 쌍방이 정보 내용에 대하여 행위를 한 사실을 증명할 수 있는 수단이 필요하다. 이러한 수단으로 종래에 계약서등에 날인하는 기술이 이용되었듯이 네트워크 상에서 디지털 컨텐트에 전자적으로 서명하는 전자 인증 기법이 있다. 또한 이 전자 인증 기법을 이용하여 디지털 컨텐트의 불법 복제를 방지할 수 있으며 디지털 복제가 되었다고 하더라도 지적 소유권을 주장하게 할 수 있는 Watermarking [17] 기법도 이용된다.

III. 인터넷 상에서의 암호 기술 이용

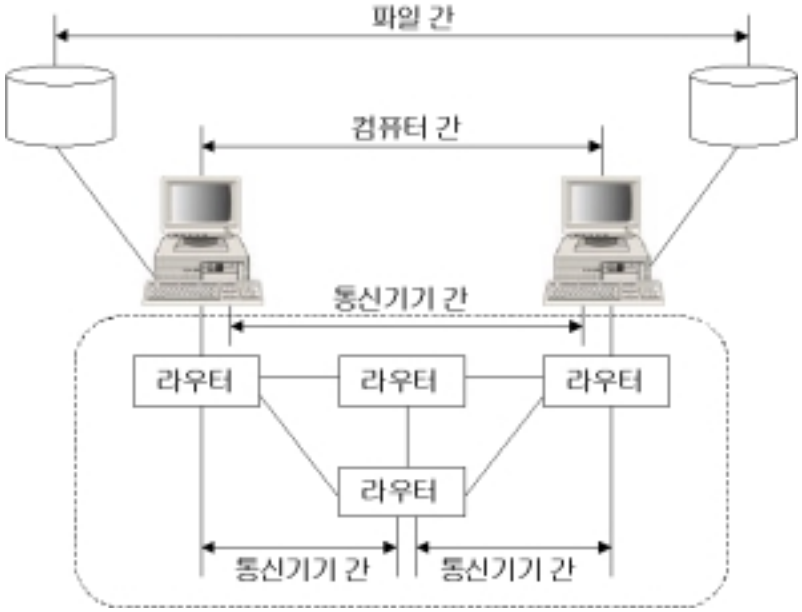
3.1 암호를 이용한 정보 보호

인터넷 상에서 정보를 보호하기 위하여는 일반적으로 실시간 처리가 가능한 암호 방식으로서 대칭키 암호 알고리즘을 이용한다. 70 년도에 미국은 연방정부의 데이터 보호를 위한 표

준 알고리즘으로서 56 비트 키를 가진 대칭키 암호 알고리즘인 DES(Data Encryption Standard)를 채택한 바가 있다. 이후 DES 는 전세계적으로 파급되어 정보 통신을 비롯한 금융 등 각 방면에 실질적으로 세계에서 가장 많이 사용된 암호 알고리즘이 되었다. 그러나, 90 년대에 들어와서 이스라엘 암호학자 Biham [3]과 일본의 암호학자 Matsui [18]가 각각 고안한 차분 해독법과 선형 해독법에 의하여 실질적으로 해독될 가능성이 제기되었고 이에 미국은 미봉책으로 키의 크기를 128 비트로 증가하기 위하여 3 중 DES 를 표준으로 잠정 채택하기에 이르렀다. 그러나 이러한 방법은 영구적인 해결책이 되지 아니하여 새로운 천년을 맞이하여 128 비트에서 256 비트의 가변 키를 가지는 새로운 블럭 암호알고리즘의 표준으로 AES(Advanced Encryption Standard) [21]가 전세계적으로 97 년도 공모 되었고 금년도 8 월이면 최종 결정하게 되어 있다. 현재까지 최종적으로 남은 5 개의 후보 알고리즘으로 MARS, RC6, Rijndael, Serpent, Twofish 가 있다.

이러한 암호 알고리즘 자체 외에 암호 시스템이 실제 구축되고 운용하기 위하여 키 관리 방법, 암호화가 행하는 통신 구간, 암호 시스템을 소프트웨어 또는 하드웨어로 할 것 인지 등 여러 가지를 결정하여야 한다.

인터넷 상의 정보를 보호하는 암호 기능을 부가하는 방법은 어느 구간을 암호화를 적용하는 가에 따라 몇 가지로 구분한다 [22].



(그림 2) 암호화 구간의 분류

(1) 파일간 암호

암호화한 파일을 그대로 송신하는 방법으로서 원래의 정보가 암호문으로 변형되었기 때문

에 인터넷 상에는 암호를 인식할 수 없다. 그러나 파일 내의 정보를 추출하여 암호화하여 파일 내로 삽입하여야 하는 처리가 필요하여 시간이 소요된다.

다른 방식으로는 인터넷의 통신 기능과 암호 기능을 조합하는 방식으로 다음과 같이 분류된다.

(2) 컴퓨터 간 암호

통신로에 정보를 발송하기 바로 전에 컴퓨터의 내부에서 암호화를 수행하고 암호문을 수신한 컴퓨터 내부에서 복호화를 하는 방법이다. 이 방법은 송신처의 컴퓨터와 최종 수신처의 컴퓨터 간에서 암호화가 수행되므로 end-to-end 암호화라고 부른다. 암호화 기능은 응용 프로그램 내부에 삽입된 경우가 많다. End-to-end 암호화의 예로서, 신용카드를 이용한 전자 지불 프로토콜인 SET (Secure Electronic Transaction) [23, 24, 25] 프로그램, 전자 우편용 PEM [15], PGP [27], S/MIME [16] 등이 있다. 이들 프로그램은 OSI 7 계층 모델 중 최 상의 층인 응용 층에서 암,복호화가 이루어 지고 있으나, 컴퓨터 내의 통신 처리용 소프트 웨어에서 암호화를 처리하는 Netscape 사가 개발한 SSL (Secure Socket Layer) 이나 TLS (Transmission Layer Security) 등은 TCP/IP 위와 응용 계층 사이에서 암호화 기능을 수행한다.

(3) 통신기기 간의 암호화

방화벽이나 라우터 사이 또는 모뎀 상에서 암호화를 수행하는 기능이 가능하다. 이는 통신업자나 ISP(Internet Service Provider)에 의해 제공되는 기능으로서 (a) 컴퓨터에 연결하지 않고 통신기 간에 행하는 경우와 (b) 직접 인접한 기기간에 행하는 경우가 있다. 어느 경우에도 암호화가 필요한 측에서 통신문을 발송하면 동작하므로 암호화 기능을 고려하지 않은 응용 프로그램을 개조하지 않고도 통신로 상에 암호화된 정보를 보내는 것이 가능하다. (a) 방식으로는 IPSec (Secure Architecture for the Internet Protocol) 이나 PTPT(Point-to-point Transfer Protocol) 등이 있으며 네트워크 층에서의 암호 기능이다. (b) 방식은 모뎀간의 암호 통신과 동일하며 데이터 링크 층에서의 암호화하므로 link-by-link 암호 방식이라고도 한다.

IV. IPSec 보안 기술

4.1 보안 요구 사항

현재 인터넷 상에는 32 비트의 제한된 어드레스 공간, 실시간 멀티 미디어 정보의 수용 불가 등의 문제점이 부각되고 있다. 특히 IP 패킷의 어드레스를 쉽게 위조할 수 있는 점, IP 패킷의 내용을 변조할 수 있는 점, 전송 중에 있는 패킷의 내용을 볼 수 있는 점, 이전에 사용한 패킷을 되풀이(reply)할 수 있는 점등은 현행 인터넷의 보안 구조상의 문제점으로 지적되고 있다 [8, 20]. 이를 바탕으로 차세대 인터넷에서는 다음과 같은 보안 사항이 요구된다.

- 데이터 근원지의 인증(data origin authentication)

- 데이터의 무결성(data integrity)
- 데이터 내용의 기밀성(data content confidentiality)
- 되풀이공격 방지(anti replay protection)

IPSec 은 위의 보안 요구 사항에 대하여 AH(Authentication Header) [10] 와 ESP(Encapsulated Security Payload) [11] 두 개의 프로토콜을 통해 기본적이면서도 강력한 보안 서비스 두 개, 즉 암호화와 인증을 IP 레벨에서 제공하는 기능을 한다. 또한 <표 2>와 같이 이 두 프로토콜 내에 서비스 방지 또는 되풀이공격(replay attack) 등을 방지하는 기능도 가지고 있다.

<표 2> AH 와 ESP 가 제공하는 보안 서비스

	AH	ESP(기밀)	ESP(기밀+인증)
Access Control	X	X	X
Connectionless Integrity	X		X
Data origin authentication	X		X
Rejection of replayed packets	X	X	X
Confidentiality		X	X
Limited Traffic flow confidentiality		X	X

AH 와 ESP 헤더 모두는 SN(Sequence Number)을 포함하고 있는데, SA 를 설정할 때 초기화된 SN 에 대해 패킷을 수신할 때마다 “sliding receive window”와 “bit masking” 기법을 적용하여 중복된 SN 이나 정해진 시간내에 패킷이 도착하였는지를 검사하여 되풀이공격 방지를 수행할 수 있게 된다. 그리고 무엇보다도 IPsec 의 터널모드 설정기능은 가상사설망 구축시 확장성 및 호환성을 보장하는 보안 메커니즘을 제공하고 있다. 이는 B2B 전자상거래를 위한 필수 보안기술로서 L2TP, PPTP 등 기존 터널링 기술을 대체하면서 미국의 VPNC(Virtual Private Network Consortium)에서는 VPN 의 보안기술 표준으로 정하고 있다.

4. 2 운용 특징

IPSec 에서의 핵심 개념은 SA(Security Association) [12]로서 논리적인 “simplex connection”으로 정의되며, 양방향 연결인 경우 적어도 두 개의 SA 가 존재해야 한다. 각 SA 는 Security Parameter Index(SPI), IP destination address 와 security protocol(AH / ESP)에 의해 유일하게 식별된다. 일반적으로 보안의 강도를 높이기 위해서는 “SA bundle”을 적용하게 되는데, 패킷전송 노드쌍 간에 서로 다른 SA 를 설정함으로서 결과적으로 분산형 다중암호와 인증이 이루어지게 할 수 있다. 이 SA 는 성능저하를 막기위해 SAD(SA Database)내에 저장되며 IPSec 엔진

에서 참조하여 실시간으로 패킷 송수신시 암복호 및 인증이 수행되도록 한다.

타 보안프로토콜에 비해 IPSec 보안기능의 우수한 점은, 사용자 보안정책에 의거하여 다양한 selector 를 선택함으로서 자유로운 granularity 조절기능을 갖고 있는데 있다. 물론 응용계층의 사용자 데이타에 대한 이중서명과 같은 경우의 보안서비스는 불가능하지만 착신주소 필터링과 포트선택 등을 통하여 개별 시스템 보호도 이루어질 수 있는 것이다. AH/ESP 의 프로토콜이 성공적인 것으로 평가 받고 있지만, IPSec 이 현실적으로 적용되기 위해서는 두 컴퓨터간 보안 연결 외에도 일명 “Road-Warriors”라 불리는 휴대용 이동 단말기를 사용하여 지역 ISP 를 통한 유선 접속 및 원격지에서 유무선 LAN 을 통한 연결 접속 시 보안 서비스를 제공하기 위한 절차 및 프로토콜에 대한 필요성도 증대하고 있는 실정이다.

보안의 우수성에도 불구하고 이제 실제 환경에서 IPSec 이 사용자에게 투명하면서 자동으로 동작하기 위해서는 보안정책서버 및 PKI 와의 연동을 고려하지 않을 수 없게 되었다. 인터넷의 활용범위가 넓어지고 글로벌화 되면서 사용자인증을 원활하기 위한 공개키 기반구조 구축 및 인증서버 간 상호인증, 그리고 지역 보안정책 서버간 정책매핑 등이 필수적으로 뒷받침되어야 하는 것이다. 이러한 추가 요구 사항들은 IETF 에서도 IPSec WG 과 별도로 추진되고 있으며, PKIX, IPsra, IPsp 에 대한 표준작업이 활발히 진행중에 있다.

V. 키 관리 기술

IPSec 자체의 내용은 아니지만 IPSec 을 구현하는 데는 부가적으로 가장 중요한 것이 키 관리 방법이다. IPSec 은 대칭키 암호 알고리즘을 이용하여 데이터를 암호화하고 인증성을 제공하기 위하여 HMAC 같은 메시지 인증 코드를 사용하는데 이를 위해서는 통신을 시작하기 전에 각 실체 간에 같은 키를 공유하고 있어야 하기 때문이다. RFC 2401[12]에서는 두 가지 종류의 키 관리를 요구하고 있다. 하나는 수동키 교환(manual key exchange)이며 다른 하나는 자동키 교환(automated key exchange)인데, 수동키 교환이란 전화로 키의 초기값 (seed)을 알려준다든지 키를 디스켓에 넣어 직접 전하든지 하여 안전한 통신을 원하는 실체와 직접 키 교환을 하는 것이다. 하지만, 실체가 많아지거나 효율적인 관리를 위해서는 자동키 교환 프로토콜을 사용하는 것이 좋다고 하겠다. 자동키 교환을 위한 대표적 프로토콜로 IKE (Internet Key Exchange) [14]가 제안되어 있다. IKE 는 SA 의 설정, 협상등에 대하여 다루고 있는 ISAKMP (Internet Security Association and Key Management Protocol) [13]와 Diffie-Hellman 키 교환을 다루고 있는 OAKLEY 키 결정 프로토콜(OAKLEY Key Determination Protocol)을 합친 것이다.

본 장에서는 키 교환 프로토콜에 요구되는 보안 요구 사항을 정리하고 각종 공격에 안전한 대한 최근의 연구 결과를 제시 한다.

5.1 키 교환 프로토콜의 보안 요구 사항

키 교환 프로토콜의 궁극적인 목표는 세션키로 사용될 데이터를 안전하게 합의하는 것이며

이상적으로는 대면에 의한 키 교환과 똑같은 특성을 가져야 한다. 즉, 세션키는 합법적인 실체들 간에만 공유되어야 하고, 난수적으로 선택되어야 하며, 불법적인 실체는 키에 대한 어떠한 부분정보도 획득할 수 없어야 한다. 이 절에서는 키 교환 프로토콜의 보안 요구사항을 기본적 보안 요구사항, 추가적 보안 요구사항, 기타 요구 사항 등의 세 가지로 구분하여 기술한다 [5, 19].

가. 기본적 보안 요구사항

키 교환 프로토콜의 기본적 보안 요구사항은 키 교환 프로토콜이 반드시 제공해야 하는 기본적인 보안특성을 말한다. 이 후, A 와 B 는 프로토콜을 수행하는 합법적인 두 실체라고 가정하자.

- 함축적 키 인증성 (IKA, Implicit Key Authentication)

A 가 B 이외에 어느 누구도 세션키를 생성할 수 없다는 확신을 가질 수 있을 경우 키 교환 프로토콜은 A 에게 B 에 대한 함축적 키 인증성(IKA)을 제공한다고 말한다. 이것은 B 가 실제로 키를 소유함을 확신하는 것은 아니다. IKA 를 제공하는 키 교환 프로토콜을 AK(authenticated key exchange) 프로토콜이라고 한다.

- 명시적 키 인증성 (EKA, Explicit Key Authentication)

실체 B 가 실제로 공유키를 계산하여 소유함을 실체 A 가 확신할 수 있을 경우 프로토콜은 A 에게 B 에 대한 명시적 키 인증성 (EKA)을 제공한다고 말한다. EKA 는 IKA 보다 더 강력한 인증성을 제공하며 EKA 는 IKA 를 포함한다. EKA 를 제공하는 키 교환 프로토콜을 AKC (authenticated key exchange with key confirmation) 프로토콜이라고 한다.

나. 추가적 보안 요구사항

이것은 응용분야에 따라서 추가적으로 요구되는 보안 요구사항을 말한다. 다음은 키 교환 프로토콜의 추가적인 보안 요구사항을 열거한 것이다.

- 알려진 키에 대한 보안성 (Known-key security)

이전의 다른 세션키가 공격자에게 노출되었을 경우에도 프로토콜의 안전성이 보장될 수 있어야 한다.

- 전향적 보안성 (Forward secrecy)

하나 또는 그 이상의 실체들의 장기적인 개인키(long-term private key)가 노출되었을 경우에도 이전에 합의한 세션키들에 대한 안전성이 제공되어야 한다.

- 키 노출에 의한 위장 (Key-compromise impersonation)에 대한 안전성

A 의 장기적인 개인키가 공격자에게 노출되었을 경우 공격자는 A 로 위장할 수 있다. 그러나 이러한 경우에도 공격자는 A 에게 다른 실체로 위장할 수 없어야 한다.

- 미지의 키 공유(UKS, Unknown Key-Share)에 대한 안전성

실체 B 는 실체 C 와 키를 공유하고 있다고 믿고 있지만 자신도 모르는 사이에 실체 A 와 키를 공유하게 되며 객체 A 는 B 와 키를 공유하고 있다고 믿는 경우를 말한다. 만일 실체

B 가 은행 지점이며 A 는 고객이라고 가정해 보자. 이와 같은 공격이 성공적으로 이루어졌다고 하면 은행 B 는 고객 A 의 계좌 대신에 C 의 계좌에 돈을 입금하게 될 것이다.

다. 기타 보안 요구사항

기타 보안 요구 사항으로는 프로토콜에 참여하는 객체의 익명성, 프로토콜상의 역할의 대칭성(role symmetry), 프로토콜 메시지간의 상호 연관성 감소, 암호화 알고리즘, 해쉬 알고리즘, 타임스탬핑 기법에의 무의존성 등을 들 수 있다.

5.2 UKS 공격에 대한 자세한 고찰

본 절에서는 앞서 언급한 키 교환 프로토콜의 UKS 공격에 대한 안전성에 대하여 좀 더 자세히 다룬다. UKS 공격의 대표적인 예로서 STS(Station-to-Station) 키 교환 프로토콜에 대한 UKS 공격을 들 수 있다 [7]. 논의에 앞서 다음의 기호들을 정의하자.

기호

→ : 공격자가 정상적으로 메시지를 되풀이함

➥ : 공격자가 실체 사이의 메시지를 가로챔

A : 실체 A

B : 실체 B

I_A, I_B, I_E : A, B,C 의 식별정보

CertA , CertB , CertE : A,B,C 의 인증서

Sig_A , Sig_B : A, B 의 서명

MAC_K : $K = g^{ab}$ 를 키로 하는 메시지 인증 코드(Message Authentication Code)

(그림 3)은 STS 프로토콜에 대한 UKS 공격을 기술한 것이다.

(1a) A→ B I_A, g^A

(1'a)E➥ B I_E, g^A

(2a) E←B CertB, g^b, $Sig_B(g^b, g^a)$, $MAC_K(Sig_B(g^b, g^a))$

(2'a)A←E CertB, g^b, $Sig_B(g^b, g^a)$, $MAC_K(Sig_B(g^b, g^a))$

(3a) A➥B CertA, $Sig_A(g^a, g^b)$, $MAC_K(Sig_A(g^a, g^b))$

(3'a)E →B CertE, $Sig_A(g^a, g^b)$, $MAC_K(Sig_A(g^a, g^b))$

(그림 3) STS 프로토콜에 대한 UKS 공격

먼저 (1a) 에서 공격자 E 는 A 의 메시지를 가로채어 I_A 를 자신의 식별정보 I_E 로 바꾸어 (1'a) 의 과정에서 B 에게 전송한다. B 가 (2a)의 과정에서 E 에게 자신의 인증서, g^b, 그리고 이 전에 받은 g^a 에 서명하고 서명에 대한 MAC 값을 E 에게 보내면 E 는 (2'a)의 과정

에서 B 로부터 받은 메시지들을 A 에게 그대로 되풀이한다. (3'a)의 과정에서 E 는 A 의 인증서를 가로채서 자신의 인증서로 바꾼 다음 B 에게 보낸다. 프로토콜이 끝나면 A 는 B 하고 통신하고 있다고 믿고 있지만 B 는 E 하고 통신하고 있게 된다.

따라서, UKS 공격을 방지하는 방법은 첫째, 인증서를 키 교환 프로토콜의 수행 전에 각 실체가 교환하는 것이다. 하지만, 적은 대역폭 (bandwidth)을 요하는 통신로에서 이 방법은 효율적이지 못하다.

둘째, CA 가 인증서를 발행할 때 각 실체가 공개키에 해당하는 비밀키를 가지고 있는 지 확인하는 것이다. 그러나 모든 CA 가 그러한 확인 작업을 수행하는 것을 기대하기도 어려운 일이거니와 최근 PKC'99 에 발표된 Blake-Wilson 의 논문 [6] 에서는 각 실체가 공개키에 해당하는 비밀키를 가지고 있다는 사실을 확인하는 것만으로는 UKS 공격을 방지하기 어렵다는 것이 성질을 통해 밝혀졌다. Blake-Wilson 과 Menezes 는 서명 알고리즘이 가지고 있는 DSKS (Duplicate- Signature Key Selection)을 지적 하였는데, DSKS 성질이란 주어진 서명에 대하여, 그 서명에 상응하는 공개키를 여러 개 선택할 수 있다는 성질 이다. 예를 들어, 키 교환 프로토콜에 인증성을 제공하기 위한 서명 방법이 ElGamal 서명 [9]이라고 가정하자. 그리고 서명을 생성하는 데 이용한 공개키를 $y = g^x$ 라고 하고 서명 값을 (r,s) 라고 가정하자. 이 때, $r = g^k \bmod p$, s 는 $ar + ks = h(m) \bmod p\text{-}1$ 를 만족한다. (h 는 해쉬 함수이며, m 은 메시지이다.) 이제 공격자가 생성원 g 대신, $g' = (r^s)^{t^{-1}}$ (단 t 와 c 는 $t = h(m)\text{-}cr \bmod (p\text{-}1)$ 를 만족하는 임의의 정수) 를 새로운 생성원으로, 새로운 자신의 공개키를 $y' = g'^c$ 로 선택한다면, (p,g,y) 대신 (p,g',y') 을 공개키 파라미터로 전송 받은 실체는 $g'^{-h(m)} y'^r r^s = g'^{-h(m)+cr} r^s = g'^{-t} r^s = (r^s)^{-t^{-1}t} r^s = 1 \bmod p$ 를 계산하게 되어 서명 값은 항상 옳은 값으로 검증되게 된다. 즉, 공격자가 ElGamal 서명 (r,s) 에 대하여 서명 검증에 문제가 없는 공개키를 임의로 생성할 수 있는 것이다. 비록 CA 가 키 교환 프로토콜에 참여하는 각 실체가 공개키에 해당되는 비밀키를 소유하고 있다는 것을 확인한다 해도 공격자는 아무 문제없이 자신이 비밀키를 소유하고 있음을 밝힐 수 있다.

셋째, 키 교환 프로토콜에서 서명 되는 메시지에 각 실체의 ID 정보와 flow number 를 포함시키는 것이다. 이 방법이 UKS 공격을 방지하는 효율적인 방법으로서 많이 이용되어 왔지만, 최근에 Baek 과 Kim [4]은 이 방법을 이용하여 Blake-Wilson 과 Menezes 에 의하여 재설계된 STS-MAC (Station-to-Station Message Authentication Code) 프로토콜이 DSKS 성질을 이용한 UKS 공격에 약함을 보였다: 그림 3 의 (3a) 에서 A 와 B 의 ID 정보가 서명되는 메시지 안에 포함되었더라도, (즉, A→B CertA, Sig_A (**3**, $g^a, g^b, \text{I}_A, \text{I}_B$), MAC_K (Sig_A (**3**, $g^a, g^b, \text{I}_A, \text{I}_B$)) 공격자는 $h' = h(3, g^a, g^b, \text{I}_E, \text{I}_B)$ 를 먼저 계산한 후 $t' = h' - a'r$ 을 계산하여, 새로운 공개키 파라미터들을 $(p, \overline{g}, \overline{y})$ 를, $\overline{g} = (r^s)^{t'^{-1}}$, $\overline{y} = \overline{g}^{a'}$ 로 선택한다면,

$$
\begin{aligned}
&\overline{g}^{(-h')}\overline{y}^{r} r^{s} \bmod p \\
&= (r^{st^{r-1}})^{(-h')} (r^{st^{r-1}})^{a'r} r^{s} \\
&= (r^{s/(h'-a'r)})^{(-h')} (r^{s/(h'-a'r)})^{a'r} r^{s} \\
&= r^{(-sh'+sa'r+sh'-sa'r)/(h'-a'r)} \\
&= r^{0} \\
&= 1
\end{aligned}
$$

이 되므로 B 는 공격자 E 의 공개키를 이용하여 주어진 서명 (r,s) 를 항상 옳은 것으로 검증할 수 있다.

따라서 Baek 과 Kim 은 MAC 을 사용하는 키 교환 프로토콜의 UKS 공격에 대한 안전성을 보장하기 위한 방법으로 서명 되는 메시지 뿐만이 아니라 MAC 이 취해지는 메시지에도 각 실체의 ID 와 flow number 를 포함시킬 것을 제안하였다. 이 방법을 이용하여 재구성된 STS-MAC 프로토콜은 다음과 같다.

(1b)A→ B $\quad I_A,\ g^A$

(2b)A←B CertB, g^b,Sig_B (**2**, g^b, g^a, I_B, I_A), MAC_K(Sig_B (g^b, g^a, I_B, I_A), **2**, I_A, I_B)

(3b)A→B CertA, Sig_A (**3**, g^a, g^b, I_A, I_B), MAC_K (Sig_A (**3**, g^a, g^b, I_A, I_B), **3**, I_A, I_B)

(그림 4) UKS 공격에 안전한 STS-MAC 프로토콜

VI. 결론

본 논문에서는 급증하고 있는 차세대 인터넷에서 요구되는 보안 요구 사항과 암호 기술의 응용 방법, IPSec 의 보안 특징 등을 살펴 본 뒤, 암호 기술의 사용에 가장 중요한 키 관리 시스템으로 요구 사항과 UKS 에 의한 공격 방법과 대처 방안을 기술하였다. 보안 기술은 과거에는 시스템이 보급된 후, 특수한 환경에서 선별적으로 후속적인 서비스 기능으로 이용되어 왔으나, 인터넷 상에서의 보안 위협과 특징에서 보듯이 시스템을 구축하는 데 반드시 선행적으로 해결하여야 하는 필수적인 기법으로 인식되고 있다. 현행 가용한 보안 기술을 차세대 인터넷의 보안 기술로 구현할 때에는 특별한 문제점은 없으나, 중요한 정보인 사용자 키를 관리하는 기법으로 본 논문에서 취급한 UKS 에 대한 대비책을 고려한 인터넷 프로토콜을 이용하여 보다 강력한 보안 서비스를 제공할 수 있다.

인터넷의 보급과 함께 수반되는 통신 인프라의 발전과 정비, 그리고 신규 사이버 서비스의 탄생, 이동성의 확보와 보안성의 제공 등 점차 발전된 통신 구조에서 다양한 암호 기법

이 응용되리라고 예상한다.

참고문헌

[1] CERTCC-KR, "'99 국내외 해킹 현황 분석", http://www.certcc.or.kr/statistics/hack/1999/99-hack.htm

[2] 황규범, 김광조, 안철수, "CIH 바이러스 분석 및 대책", KIISC 논문지, Vol 9, No 4, pp.49-60, 1999.12

[3] E.Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology – Proceedings of Crypto '90, LNCS 537, pp. 2-21, Springer-Verlag, 1991

[4] J. Baek, and K. Kim, "Remarks on the Unknown Key- Share Attack", To appear in Trans. on IEICE, 2000

[5] S. Blake-Wilson and A. Menezes, "Authenticated Diffie-Hellman Key Agreement Protocols", Proceeding of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), LNCS1556, pp.339-361, 1999.

[6] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station(STS) Protocol", Public Key Cryptography - Proceedings of PKC'99, LNCS1560, pp.26-45, Springer-Verlag, 1999.

[7] W. Diffie, P. van Oorschot, and M. Wiener, " Authentication and Authenticated Key Exchanges", Designs, Codes and Cryptography, Vol.2, pp.107-125, 1992.

[8] N. Doraswamy and D. Harkins, *IPSec*, Prentice Hall,1999.

[9] T. ElGamal, "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. on Information Theory, IT-31(4), pp.489-472, July, 1985.

[10] IETF IPSec WG, "IP Authentication Header (AH)", RFC 2402, November 1998.

[11] IETF IPSec WG, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[12] IETF IPSec WG, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[13] IETF IPSec WG, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[14] IETF IPSec WG, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[15] IETF PEM WG, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures". RFC 1421, 1993.

[16] IETF Network, WG, "S/MIME Version 2 Message Specification", RFC 2311, 1998.

[17] S. Katzenbeiser and F. A. Peticolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, pp. 95-145, Artech House, 2000.

[18] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology –

Eurocrypt ’93, LNCS 765, pp. 386-397, Springer-Verlag, 1993

[19] A. Menezes, P. C. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, pp. 489- 586, CRC Press, 1996.

[20] M. W. Murhammer, O. Atakan, S. Bretz, L. R. Pugh, K. Suzuki, and D. H. Wood, *TCP/IP Tutorial and Technical Overview*, pp. 263-355, IBM Red Book, 1998, available at http://www.redbooks.ibm.com

[21] NIST,“Advanced Encryption Standard(AES) Development Effort”, http://csrc.nist.gov/encryption /aes/

[22] R. Sasaki, “Internet and Security”, J. of IEICE Vol.83, No.2, pp.107-111, 2000.2.

[23] SETco, SET(Secure Electronic Transaction) Specification, Standard Book 1: Business Description, 1997.

[24] SETco, SET(Secure Electronic Transaction) Specification, Standard Book 2: Programmer’s Guide, 1997

[25] SETco, SET(Secure Electronic Transaction) Specification, Standard Book 3: Formal Protocol Definitions, 1997

[26] W. Stalling, *Cryptography and Network Security*, 2nd Edition, pp. 399-433, Prentice Hall, 1999.

[27] P.R. Zimmerman, *The Official PGP User’s Guide*, MIT press, 1995.