패스워드 기반 인증 프로토콜의 무선 VPN 적용에 관한 연구

김현택° 송주석
연세대학교 컴퓨터과학과
{motorio°, jssong}@emerald.yonsei.ac.kr

A study on the application for the mobile VPN using password-based authentication protocol

Hyuntaek Kim° Jooseok Song
Dept. of Computer Science, Yonsei University

요 약

근래 휴대폰과 PDA등의 대중적인 보급과 동시에 기업체의 유무선 VPN 구축도 활기를 띄고 있다. 유선환경에서의 VPN은 보안적인 측면에서 무선환경보다 비교적 안전하다고 할 수 있다. 그러나 무선환경은 유선환경과 달리 능동적인 공격자뿐만 아니라 수동적인 공격자에 대해서도 보안상 취약한 면을 가지고 있다. 또한 무선 VPN에서 사용하는 단말기인 PDA, 휴대폰 등의 하드웨어적 제약 또한 무선 VPN 구축시 반드시 고려하여야 한다. 따라서 본 논문에서는 이러한 무선환경에서의 하드웨어적 제약 및 보안 취약성을 보완할 수 있도록 패스워드 기반 인증 프로토콜을 무선 VPN에 적용하고자 한다.

1. 서 론

최근에 기업체의 시설 확장, 국내 및 해외 지점간 업무분담과 외부 협력 업체 수의 증가 등에 따라 막대한 시설 투자비가 드는 자체 전용망 이용을 지양하는 반면 ISP(Internet Service Provider)에서 제공하는 공중망인 인터넷망을 이용한 가상사설망(VPN : Virtual Private Network)을 이용하여 네트워크를 구성하는 기업이 많아지고 있다. 기존의 전용망은 공중망에 비해 상대적으로 안전하지만 초기 투자비용을 제외하더라도 운영과 관리에 큰 문제점을 내포하고 있다. 이러한 전용망을 이용한 사설망(Private Network)의 부담을 덜기 위해 많은 기업에서 공중망을 이용하는 VPN을 도입하고 있다.

최근 휴대폰과 PDA 등이 급속도로 보급되고 기업 활동에서 정보의 신속하고 정확한 이동은 필연적인 요소가 되었다. 본점과 지점, 국내 본점 및 지점과 해외지점, 국내외 협력업체로의 유선 환경에서의 VPN 연결은 상당부분 많은 가시적인 결과를 가져왔지만 무선 환경에서의 VPN 이용은 무선망의 특수성으로 인하여 유선환경에서의 VPN에 비해서 진행 속도가 느리다. 무선환경은 유선환경에 비해 높은 패킷 손실률, 보안취약성 및 단말기의 하드웨어적 제약을 가진다. 그러므로 유선환경에서 사용하는 VPN을 무선환경에 그대로 적용하기는 어렵다.

본 논문에서는 무선환경이 가지는 취약점 중 보안취약점을 보완하기 위하여 패스워드 기반 인증 프로토콜을 무선 VPN에 적용하고자 한다. 2장에서는 VPN과 본론에서 다루게 될 DH-EKE에 대해 살펴보고, 3장에서는 VPN에의 적용에 대해 살펴보며, 4장에서는 향후 연구방향에 대해 밝히고 결론을 맺도록 하겠다.

2. 관련연구

2.1 VPN(Virtual Private Network)[1]

VPN은 물리적으로 존재하지 않는 사설망(Private Network)을 가상(Virtual)으로 구축하여 별도의 전용망처럼 사용하는 것을 말한다. 즉, 사설망을 물리적으로 구축하지 않고 기존의 인터넷과 같은 공중망(Public Network)을 이용해 특정 사용자 그룹이 사설로 이용하는 형태를 말한다.

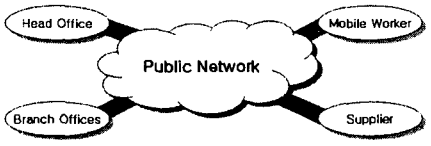

그림 1 가상사설망(VPN)

VPN 연결은 사용자로 하여금 원거리에서 회사 VPN 서버로의 원격 접속을 가능하게 한다. 또한 회사가 지리적으로 떨어져 있는 사무실이나 다른 회사와 보안이 유지된 상태에서 각종 정보의 전송이 가능하게 해준다.

2.2 DH-EKE[2][3]

1992년 Bellovin과 Merritt는 대칭키 암호와 공개키 암호를 결합하여 공격자가 유추한 패스워드의 정당성을 검증할 정보가 불충분한 EKE(Encrypted Key Exchange)라는 새로운 프로토콜을 제안하였다. EKE는 두 당사자들이

패스워드에서 비롯된 대칭키를 이용하여 그들의 임시 공개키로 암호화하는 형태이며 여러 변형된 형태로 발전되었고 가장 단순한 형태가 DH-EKE이다.

DH-EKE는 전송되는 공개키 속성들을 인증정보인 패스워드로 암호화하여 중간자 공격 및 오프라인 사전공격을 예방한다. 프로토콜 수행 절차는 다음과 같다.

가. $A \rightarrow B$: $A, P(g^{R_A} (\mathrm{mod} p))$

A는 난수 R_A을 생성하고 패스워드 P를 대칭키 암호시스템의 암호화키로 사용하여 $g^{R_A} (\mathrm{mod} p)$를 암호화한 값 $P(g^{R_A} (\mathrm{mod} p))$를 전송한다.

나. $B \rightarrow A$: $P(g^{R_B} (\mathrm{mod} p)), R(challenge_B)$

B는 R_B를 생성하고 $g^{R_B} (\mathrm{mod} p)$를 계산한다. 또한 $P(g^{R_A} (\mathrm{mod} p))$를 P를 복호화하여 $R = g^{R_A R_B} (\mathrm{mod} p)$ 를 계산하고, 상호인증을 위해 $challenge_B$를 생성하여 R을 개칭키 암호시스템의 암호화키로 사용하여 암호화한 값 $R(challenge_B)$을 전송한다.

다. $A \rightarrow B$: $R(challenge_B, challenge_A)$

A는 P를 사용하여 $g^{R_B} (\mathrm{mod} p)$를 복호화하고 R을 생성하여 $R(challenge_B)$을 복호화 할 수 있다. A는 임의의 $challenge_A$를 생성하여 $R(challenge_B, challenge_A)$ 을 전송한다.

라. $B \rightarrow A$: $R(challenge_A)$

B는 $R(challenge_B, challenge_A)$ 을 복호화하여 $challenge_B$가 제대로 돌아왔는지 검증하고 $R(challenge_A)$을 전송하여 상호인증을 완성한다.

DH-EKE를 사용할 경우 공격자가 임의로 유추한 P'에 대한 정당성을 검증할 수 있는 유용한 정보를 획득할 수 없다. 따라서 평문으로 전송되는 A에 대한 정보를 공격자가 획득하더라도 난수 R_A을 모르면 $challenge_B$에 대한 답을 할 수 없게 된다. 또한 공격자가 패스워드를 정확히 유추하더라도 $g^{R_A} (\mathrm{mod} p)$와 $g^{R_B} (\mathrm{mod} p)$ 각각에 대한 정보만을 가지고 있으므로 세션키 R에 대한 정보를 획득할 수 없다.

DH-EKE는 RSA나 ElGamal과 같은 다른 암호시스템을 이용하여 EKE를 구현할 경우와는 다르게 키 협상과정 자체가 무작위의 세션키를 생성하므로 세션키를 전송하는 과정이 별도로 고려되지 않아도 된다.

3. 본 론

MN(Mobile Node)의 Mobile IP는 VPN 망에서 현재 지원되지 못한다. 그 이유는 MN이 외부 네트워크로 이동하였을 경우 VPN 내에 있는 HA(Home Agent)로 등록을 하여야 하는데 이 과정에서 VPN Gateway가 MN의 새로운 주소에 대하여 접근을 거부하기 때문이다. Mobile VPN을 사용하기 위하여 이 문제가 먼저 해결되어야 한다.

3.1 암호화된 인증코드 이미지 등록

먼저 Mobile VPN을 사용하기를 희망하는 사람은 최초 자신의 HA 관리자에게서 하나의 인증코드를 다운받아야 한다. 이때 인증코드는 관리자가 임의로 부여하는 것이 아니라 사용자의 ID, Time Stamp 그리고 사용자가 직접 입력한 One-time Password를 이용하여 암호화된다. 관리자는 암호화된 인증코드의 이미지를 HA(Home Agent)와 Gateway에 등록하고 사용자의 단말기에도 동일한 이미지를 전송한다. 그림 2는 이를 도식화 한 것이다.

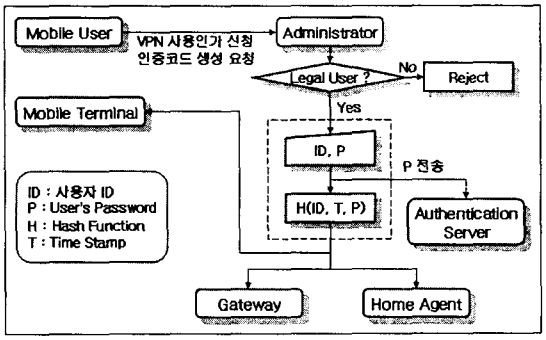

그림 2 암호화된 인증코드 이미지의 등록

위 그림에서 ID 및 사용자의 P(Password)를 사용자가 직접 입력하는 방법을 택해 관리자로부터 보안을 유지할 수 있게 한다. 관리자는 사용자의 ID, P, T(Time Stamp)를 이용하여 해쉬값을 구하여 이를 사용자의 단말기에 전송하고 Gateway 및 Home Agent에 등록한다. Gateway에 인증코드 이미지를 등록함으로써 사용자의 단말기가 외부에서 접속을 할 시 단말기의 인증코드 이미지와 Gateway의 인증코드 이미지를 비교함으로써 등록된 사용자임을 확인할 수 있다. 또한 인증서버에 사용자의 P를 전송하여 차후의 패스워드 기반 인증에 사용토록 한다.

3.2 패스워드 인증 프로토콜을 이용한 사용자 인증

최초 VPN 접속 시 Gateway를 통과한 후 2.2에서 언급한 DH-EKE 기법을 이용하여 인증서버를 통해 정당성을 검증한다.

3.2.1 표기법

A, AS	정당한 사용자와 인증서버
P	사용자의 패스워드
g	유한체 $GF(P)$의 원시근
p	큰 소수(1024비트 이상)
R	세션키

3.2.2 인증절차

1단계 : $A \rightarrow AS$: $ID_A, P(g^{R_A}(\bmod p))$

2단계 : $AS \rightarrow A$: $P(g^{R_{AS}}(\bmod p)), R(challenge_{AS})$

3단계 : $A \rightarrow AS$: $R(challenge_{AS}, challenge_A)$

4단계 : $AS \rightarrow A$: $R(challenge_A)$

가. 1단계 : 사용자(A)는 인증서버(AS)에게 사용자 정보를 나타내는 ID_A와 사용자의 P(패스워드)를 대칭키 시스템의 암호화키로 이용하여 $g^{R_A}(\bmod p)$를 암호화한 $P(g^{R_A}(\bmod p))$를 인증서버에 전송한다.

나. 2단계 : 인증서버는 세션키 R_{AS}를 생성하고 $g^{R_{AS}}(\bmod p)$를 계산한다. 인증서버에 등록된 사용자의 키인 P를 이용하여 이를 암호화한다. 그리고 A에게서 받은 $P(g^{R_A}(\bmod p))$를 P로 복호화하여 $R = g^{R_A R_{AS}}(\bmod p)$ 를 계산하고 상호인증을 위한 $R(challenge_{AS})$를 생성하여 R로 암화화한다. 인증서버는 $P(g^{R_{AS}}(\bmod p)), R(challenge_{AS})$ 를 A에게 전송한다.

다. 3단계 : A는 P를 이용하여 $P(g^{R_{AS}}(\bmod p))$를 복호화하여 $R = g^{R_A R_{AS}}(\bmod p)$ 을 생성한다. 물론 R을 구할 수 있으므로 $R(challenge_{AS})$를 복호화 할 수 있다. A는 임의의 $challenge_A$를 생성하여 $R(challenge_{AS}, challenge_A)$ 를 생성하여 전송한다.

라. 4단계 : 인증서버는 $R(challenge_{AS}, challenge_A)$ 를 복호화 하여 $challenge_{AS}$가 제대로 돌아왔는지 검증한다. 검증이 이루어진 후 $R(challenge_A)$를 전송한다. A는 $challenge_A$가 제대로 돌아왔는지 검증하여 상호인증을 종료한다.

3.2.2 분석

무선 VPN을 사용하고자 하는 사용자를 VPN 관리자가 오프라인 상에서 확인하는 절차를 둠으로써 1차적인 보안을 유지할 수 있다. 사용 등록시 입력한 패스워드를 인증서버에 전송하므로 별도의 패스워드 지정절차가 필요 없다. 인증코드의 이미지를 단말기 및 Gateway에 등록하여 무선 VPN의 문제점인 외부 네트워크에서의 접속시 접속을 거부하는 문제를 어느 정도 해결하였다.

또한 무선 단말기의 하드웨어적인 제약을 고려하여 부하가 가장 많은 메시지 교환과정이 간략한 DH-EKE 기법을 사용하였다. 표 1은 다른 프로토콜과의 메시지 교환 횟수를 비교한 것이다.[3][4]

표 1 각 프로토콜의 메시지 교환 횟수

프로토콜	SRP	A-EKE	DH-EKE
메시지 교환 횟수	6	7	4

4. 결론 및 향후 연구 과제

논문은 무선 VPN 환경에서 상용자를 인증함에 있어 무선환경의 특수성을 고려하고 다른 프로토콜에 비해 메시지 교환 횟수가 현저히 적은 DH-EKE 기법을 이용하였다. 무선 VPN에서 외부 네트워크에서의 접속시 Gateway에서 접속을 거부하는 문제를 인증코드의 이미지 등록 및 비교를 통하여 해결할 수 있다. 그러나 DH-EKE 기법은 패스워드를 서버에 평문의 형태로 저장을 하므로 서버 자체가 공격받을 시 패스워드의 도난 우려가 있다.

본 논문의 향후 연구과제를 살펴보면 인증코드 이미지의 사용 활성화 방안과 단말기에서 행해지는 모듈러 지수승의 신뢰할 수 있는 제3의 기관 이양 방안 등이 있다.

5. 참고문헌

[1] Ruixi Yuan and W.Timothy Strayer, "Virtual Private Networks: Technologies and Solutions," Addison-Wesley, 2001, pp.4 - 21

[2] S.M.Bellovin and M.Merritt, "Encrypted Key Exchange: Efficiently Preventing Password Chaining and Dictionary Attacks," Six USENIX UNIX Security Symposium, July 1996

[3] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이영한 패스워드 기반의 원거리 사용자 인증 프로토콜," 정보과학회논문지 : 정보통신 제 30권 제 1호 pp.75 - 81, 2003년

[4] Steven M.Bellovin, Michael Merritt, "Argumented Encrypted Key and Exchange: a Password-Based Protocol Secure Against Dictiona교 Attacks Password File Compromise," ACM Conference on Computer and Communications Security, 1993.