무선 네트워크 환경에서 일회용 패스워드를 이용한 사용자 인증방식의 안전성 분석

김일곤[0], 이지연, 손은경, 한근희, 최진영
고려대학교 컴퓨터학과
{igkim[0], jylee, choi, sonems, khhan}@formal.korea.ac.kr

The Safety Analysis of a User Authentication Method using One-Time Password in Wireless Networks

Il-Gon Kim[0], Ji-Yeon Lee, Eun-Kyoung Son, Keun-Hee Han, Jin-Young Choi,
Dept of Computer Science & Engineering, Korea University

요약

무선 인터넷의 활성화와 더불어, 사용자 인증을 위해 801.1x EAP, CHAP 및 PAP를 이용한 다양한 인증 방식이 사용되고 있다. 그 중에서도 RADIUS 및 CiscoSecure ACS와 같은 인증 서버에서는 RSA의 SecureID 및 S/Key와 같은 일회용 패스워드 방식을 지원하고 있다. 본 논문에서는 Casper 도구를 사용하여 CiscoSecure ACS 환경에서 동작하는 일회용 패스워드 방식을 명세하고, 모델체킹 도구인 FDR을 이용하여 안전성을 분석하였다.

1. 서론

무선 인터넷의 활성화와 더불어, 기존의 무선랜 시스템이 초고속 무선 공중망의 기반구조로 부각되고 있다. 무선랜 시스템의 활발한 보급을 위해서는 무선랜 사용자의 안전한 통신을 보장하는 것이 중요 과제로 남아 있다. 무선랜의 보안을 위해 WEP, SSID, MAC 필터링과 같은 보안방식이 사용되어 왔으나, 이 방식들에 대한 보안 취약점들이 점차 발견되어지고 있다. 현재 무선랜 보안은 크게 두 가지 방식을 이용하고 있다. 첫째는 무선 뿐만 아니라 기존의 이더넷 및 토큰링에서 사용되는 포트 기반의 접근제어 표준인 IEEE 802.1x을 이용한 사용자 인증 방식이다(예, EAP-MD5, EAP-TTLS 등)[1]. 두번째는 IEEE 802.11b, IEEE 802.11i 등과 같은 무선랜 표준인 IEEE 802.11 계열을 이용한 인증방식이다(예, WEP, MAC 인증 등)[2]. 무선랜 환경의 경우, 현재까지는 무선랜 보안 표준이 제안되고는 있으나, 밴더들이 개발한 장비마다 보안 기능을 지원함에 있어 다소 차이가 나타나고 있다.

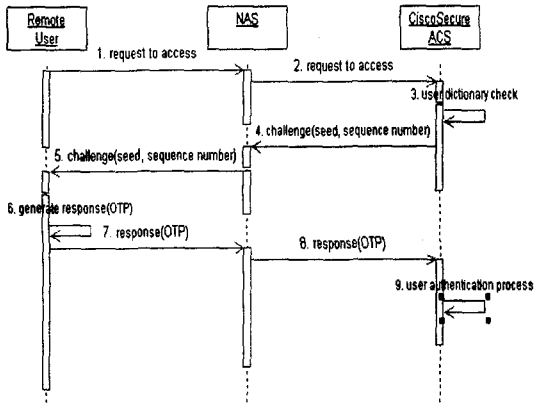
보안 장비 및 프로토콜들은 그 특성상 보안상 안전성을 분석하기 위해 다양한 연구가 진행되어오고 있다. 이런 연구는 크게 정리 증명과 모델체킹 기법으로 나누어 볼 수 있다. 첫번째 방법의 경우, BAN, GNY와 같은 보안 로직을 이용하여 정해진 규칙에 따라 상호 호스트간의 신뢰성을 증명하게 된다. 두번째 방법의 경우, 해당 프로토콜의 인증 동작을 정형 명세 언어로 설계 한 후, 다양한 보안 속성을 만족시키는지 체크하게 된다. ESTELLE, Murphi, NRL Protocol Analyser와 FDR은 위와 같은 방법을 이용하게 된다[3]. 특히 FDR 도구의 경우, 프로세스 알제브라 언어의 일종인 CSP[4]로 기술된 모델을 입력으로 받아 보안 프로토콜의 안전성을 분석하기 위해 널리 사용되어오고 있는 방법이다. 하지만, CSP로 모델을 명세하기는 매우 어려운 과정이여서, CSP로 기술된 모델을 보다 쉽게 자동으로 생성해 줄 수 있는 Casper 도구가 개발되게 되었다[5]. 초창기 개발된 Casper 도구에서는 단지 공격자의 악의적인 스니핑(sniffing) 및 스푸핑(spoofing) 행위만을 찾아낼 수 있었지만, 새로 개발된 Casper 도구에서는 패스워드에 대한 공격자의 추측공격(guessing attack)도 자동적으로 찾아낼 수 있도록 명세할 수 있어서, 보안 프로토콜에 대한 보다 다양한 안전성 분석을 가능하게 해준다.

본 논문에서는 Casper를 이용하여 Cisco의 CiscoSecure ACS 서버에서 사용되는 S/Key 일회용 패스워드 방식의 동작행위를 명세하고, FDR[6] 도구를 이용하여 그 안전성을 분석해 보고자 한다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 Casper, CSP 언어와 FDR 도구에 대해 각각 간략히 설명하고, 제 3장에서는 CiscoSecure ACS 서버의 S/Key 일회용 패스워드를 이용한 사용자 인증 방식에 대해 언급하고, 제 4장에서는 Casper와 FDR을 이용한 안전성 분석 결과를 보여주고, 마지막으로 제 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. CiscoSecure ACS 서버 환경에서의 S/Key 일회용 패스워드 인증방식

CiscoSecure ACS(Access Control Server)[7]는 Cisco 사에서 개발한 사용자 인증 서버를 의미한다. CiscoSecure ACS는 S/Key[8] 방식과 더불어, RSA의 SecureID 일회용 패스워드 방식을 지원해 준다. 하지만 본 논문에서는 S/Key 일회용 패스워드 인증 방식을 기준으로 추상화 모델을 설계하였다. 본 논문에서 다루고 있는 CiscoSecure ACS 기반의 일회용 패스워드 인증방식은 [그림 1]에 나타나 있다.



[그림 1]. 일회용 패스워드를 이용한 CiscoSecure ACS 기반의 사용자인증방식에 대한 메세지 순서도

위의 [그림 1]에서 사용자는 CiscoSecure ACS에 인증을 받기 위해 무선 환경에서 NAS에 접속을 시도하게 되며, NAS는 사용자의 접속 요청을 인증서버에 알려주게 된다. 인증서버에서는 서버의 데이터베이스에 등록되어 있는 사용자 사전목록 정보를 비교한 후, 이미 등록되어 있는 사용자이면 challenge 정보를 NAS를 통해 사용자에게 전달하게 된다. 기본적으로 S/Key 일회용 패스워드 방식은 challenge & response 프로토콜을 기반으로 하고 있기 때문에 사용자가 일회용 패스워드를 생성할 수 있도록 기반 정보를 알려주게 된다.

즉, challenge 정보에는 시드(seed)와 순서번호(sequence number)와 같은 정보를 사용자에게 알려준다. 예를 들어, "sue" 라는 사용자가 접속을 하게 되었을 경우, "97 fr09072" 정보를 사용자에게 전달해 준다.

여기서, "97"은 순서번호이고 "fr09072" 시드정보를 나타낸다. 사용자는 NAS로부터 수신받은 "97 fr09072", challenge 정보와 함께 인증서버와의 공유키인 사용자 패스워드를 일회용 패스워드 생성기에 입력하게 된다.

challenge와 사용자 패스워드 정보의 조합은 해쉬함수를 통해 64 비트로 출여지게 되며, 사용자가 일회용 패스워드를 쉽게 인식할 수 있도록 6자리의 짧은 워드 형태로 보여지게 된다. 예를 들어, 일회용 패스워드 생성기에 "97 fr09072"와 사용자의 패스워드 "password"를 입력하게 되면, "YES LOW MET NU FOLD PEA"의 일회용 패스워드가 생성되게 된다. 사용자는 생성된 일회용 패스워드를 NAS를 통해 인증서버에 전달하게 되고, 일회용 패스워드 서버에서 생성한 패스워드와 일치하면 사용자는 인증을 허가 하게 되며, 다음번에 사용자게 인증을 요청하게 되면 순서번호는 1만큼 감소된 "96"이 전달되게 된다.

3. Casper, CSP 와 FDR

3.1 Casper(A Compile for the Analysis of Security Protocols)

기존의 CSP를 이용하여 보안 프로토콜의 동작을 명세하고 분석하는 방식은 매우 복잡하여 CSP 명세 전문가 조차도 사소한 실수나 에러를 야기시킴으로써, 보다 정확한 분석을 어렵게 만들었었다. 이에 따라 보안 프로토콜을 보다 쉽게 명세할 수 있고, 자동으로 CSP 명세 소스를 생성할 수 있도록 개발된 도구가 바로 Casper이다. Casper를 이용하여 보안 프로토콜에서 사용되는 각종 키 타입, 동작 절차, 보안 속성, 공격자 모델등을 8개 영역으로 나누어 명세할 수 있다. 초기에 개발된 Casper 도구는 공격자의 스니핑(sniffing) 및 스푸핑(spoofing) 행위를 찾아내는데만 국한되었으나, 최신 버전의 도구에서는 패스워드에 대한 추측공격(guessing attack)도 찾아낼 수 있도록 개선되었다.

3.2 CSP(Communicating Sequential Process)

CSP는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신 프로토콜의 동작을 효율적으로 명세하기 위해 제작되어졌다. 처음에는 일반적인 통신 프로토콜과 제어 시스템을 명세하기 위해 사용되어졌지만, 점차 보안 프로토콜을 명세하기 위한 영역으로도 확대되어 오고 있다. CSP에서 제공하는 pure synchronization(|||)과 interleaving parallelism(||) 개념을 사용하여 분산 시스템 환경에서 동작하는 클라이언트 서버, 공격자 모델을 정형적으로 표현할 수 있다는 장점을 갖고 있다. 예를 들면, 분산시스템 환경에서 동작하는 보안 시스템은 다음과 같이 간략히 표현될 수 있다.

SYSTEM = CLIENT1 ||| CLIENT2||| SERVER ||
INTRUDER

3.3 FDR(Failure Divergence Refinements)

FDR은 모델체킹 도구로서, CSP 언어로 구현된 보안 모델이 안전성(safety), 인증(authentication)과 같은 보안 속성을 만족시키는지 체크하게 되며, 만일 해당 속성을 만족시키지 않을 경우 반례를 보여주어, 어떤 공격 시나리오가 가능한지 분석하도록 도와준다. 기본적으로 trace, failure, failure and divergence 이 세가지 동치성 검사 방법을 제공하며, trace는 시스템의 safety, failure는 deadlock, failure and divergence는 livelock을 검사하기 위해 각각 사용되어 진다.

4 Casper 명세 및 FDR 검증

본 논문에서는 CiscoSecure ACS 서버에서 사용되는 S/Key 인증 방식을 Casper로 명세하였다. [그림 2]에서는 제 2장에서 언급한 S/Key 인증방식에 대한 자연어 명세를 바탕으로 무선환경에서 동작하는 S/Key 인증 방식의 동작절차와 요구사항에 대한 명세를 보여주고 있다.

[그림 2]는 논문의 페이지 사정상 Casper의 8개의 섹션 영역중에서 #free variable과 #protocol description, #specification, #intruder information 명세 부분만 보여주고 있다.

```
#Free variables
A, B : Agent
S: Server
seed, sequence : Nonce
passwd : Password
f : HashFunction
InverseKeys = (f, f), (passwd, passwd))
#Protocol description
0.  -> A : B
1. A -> S : A
2. S -> B : S
3. B -> S : seed, sequence
4. S -> A : seed, sequence
5. A -> S : f(passwd,seed,sequence)%v2
6. S -> B : v2%f(passwd,seed,sequence)
#Specification
Secret(A, passwd, [S, B])
#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, Sam}
```

[그림 2]. Casper를 이용한 무선 네트워크 환경에서의 S/ Key 인증 명세

#Free variables 명세 부분에서, A, B는 각각 사용자와 ACS 인증서버를 의미하며, S는 NAS를 나타낸다. seed와 sequence는 난수 타입으로서 매번 임의 난수를 생성하도록 명세하였다. passwd는 사용자가 일회용패스워드 생성기에 입력하는 패스워드를 의미한다. f는 MD5 해쉬함수로서 사용자의 패스워드, 시드와 순서번호를 암호화 하는데 사용된다. #Protocol description는 프로토콜의 인증 동작 절차를 순차적으로 나타내고 있다. 0번은 사용자 A가 결국 최종적으로 인증서버 B에게 메시지를 보내고자 함을 명시한 것이다. 나머지는 매우 평이한 기호를 사용하여 이해하기 쉬울 것이다. 하지만 5, 6번 메시지의 경우에는 % 기호를 사용하고 있다. 예를 들어, m%v 표현의 경우, m은 메시지를 의미하고 v는 변수를 나타내게 된다. 즉, 5번 메시지의 경우, 사용자 A는 f(passwd,seed,sequence) 메시지를 변수 v2에 담아 보내게 되며, 6번 메시지에서 NAS인 S는 이 메시지를 복호화 하지 않고, 인증서버인 B에게 전달하게 된다. 이 논문에서 공격자인 Mallory 는 단지 A(Alice), S(Sam), B(Bob) 그리고 M(Mallory)에 대한 호스트 식별자만을 알고 있다고 가정한다. #Specification 부분은 S/Key 인증 시스템이 반드시 만족시켜야 하는 보안요구사항을 나타내고 있다. 'Secret(A, passwd, [S, B])'은 "사용자 A와 NAS인 B 그리고 인증서버 B 사이에 전송되는 패스워드 passwd는 안전하게 메시지가 전송된다"는 의미이다. 즉, passwd에 대한 비밀성을 나타내기 위한 표현이다. 본 논문에서는 일회용 패스워드를 생성하기 위한 사용자의 패스워드가 안전하게 전송되는지 FDR 도구를 통해 검증해 보았다. [그림 2]의 명세를 FDR 도구에 입력하여 검증해 본 결과, 패스워드인 passwd에 대한 비밀성이 보장된다고 결과가 나왔다. 하지만, 이 경우에는 공격자가 단지 각 사용자의 호스트 식별자만을 알고 있고, 공격자의 행위는 메시지를 스니핑하고 호스트를 스푸핑하는 능력만을 갖추고 있다고 가정한 경우였다. 다음 [그림 2]의 #Intruder Information 부분에서 맨 밑줄 다음에 'Guessable = Password' 라는 코드를 추가하였다. 이 코드는 공격자가 패스워드에 대한 사전공격 능력도 갖고 있음을 의미한다. 위 코드를 추가한 다음 FDR 도구를 통해 검증해 본 결과 무선환경에서 동작하는 S/Key 인증 시스템의 경우, seed와 sequence 정보를 공격자가 스니핑한 후, 사용자의 패스워드인 passwd를 추측해 낼 수 있다는 사실을 확인할 수 있었다.

5. 결론 및 향후 연구 방향

본 논문에서는 Casper, CSP/FDR을 이용하여 무선환경에서 Cisco ACS 서버의 S/Key 인증 방식의 비밀성을 분석해 보았다. 분석해 본 결과, 일회용 패스워드를 생성하는 사용자의 패스워드를 추측공격할 수 있는 가능성이 존재함을 재확인 할 수 있었다. 패스워드 추측공격을 방지하기 위해선 무엇보다 사용자가 패스워드를 주기적으로 교체하는 것이 가장 안전한 방법이며, 두 번째 방법으로는 사용자간의 통신 채널에 대한 암호화가 필요하겠다. 무선통신의 환경상, 현재 출시된 몇몇 NAS 장치만이 이런 암호화 방식을 지원하기 때문에 첫번째 대응책이 가장 효율적인 대안이라 사료된다. 향후 연구방향으로는 Casper 명세의 표현력을 확장시켜 보다 다양한 공격을 탐지해 내는 방법을 연구하고자 한다.

6. 참고문헌

[1] A. Mishra and W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", available from http://www.cs.umd.edu/waa/lx.pdf, February 2002.

[2] A. Stubblefield, J. Ioannidis, and A. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", Aug. 2001.

[3] Philip E. Varner, Formal Methods as an Environmental Catalyst for Emergent Security in System Design and Construction, December 12, 2002.

[4] C.A.R. Hoare, *Communicating Sequential Processes*, Prentice-Hall, 1985.

[5] G. Lowe. Casper: A compiler for the analysis of security protocols. 10th IEEE Computer Security Foundations Workshop, 1997.

[6] Formal Systems(Europe) Ltd. Failure Divergence Refinement-FDR2 User Manual, Aug. 1999.

[7] Cisco ACS, http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/

[8] N. M. Haller, "THE S/KeyTM ONE-TIME PASSWORD SYSTEM", Proceedings of the Symposium on Network and Distributed System Security, 1994.