# SPEAR를 이용한 SSL 상의 RADIUS 보안 프로토콜 명세 및 분석

김일곤[0], 이지연, 최진영
고려 대학교 컴퓨터학과
(igkim[0], jylee, choi)@formal.korea.ac.kr

# The Formal Specification and Analysis of RADIUS security protocol over SSL using SPEAR

Il-Gon Kim[0], Ji-Yeon Lee, Jin-Young Choi
Dept of Computer Science & Engineering, Korea University

요약

최근 사용자 정보의 안전한 정보 전송 및 네트워크 시스템의 안전성을 보장하기 위한 방법으로 각종 보안 인증 프로토콜에 대한 연구가 진행 중에 있다. 그 중에서 AAA 는 다중 네트워크와 플랫폼에서 인증(Authentication), 권한 부여(Authorization), 자원 체크(Accounting)의 기능들을 제공하는 모든 프로토콜을 말한다. 이 논문에서는 AAA 프로토콜의 대표적인 예인 RADIUS(Remote Authentication Dial_In User Service)를 보안 프로토콜 디자인 및 분석 도구인 SPEAR(Security Protocol Engineering & Analysis Resource)를 이용해 SSL 상에서 동작하는 RADIUS 보안 프로토콜의 문제점 및 성능을 디자인 단계에서 부터 분석하여 보안 프로토콜의 안전성을 보다 향상시키고자 하였다

## 1. 서론

최근 사용자 정보의 안전한 정보 전송 및 네트워크 시스템의 안전성을 보장하기 위한 방법으로 각종 보안 인증 프로토콜에 대한 연구가 진행중에 있다. 이중에서도 AAA[1]는 다중 네트워크와 플랫폼에서 인증(Authentication), 권한부여(Authorization), 자원체크(Accounting) 의 기능들을 제공하는 모든 프로토콜을 지칭한다. RADIUS(Remote Authenntication Dial In User Service)[2] 프로토콜은 이런 AAA 서비스를 제공하는 대표적인 프로토콜로 이미 마이크로소프트 Windows 2000 프로토콜에 내장되어 있을 정도로 오래전부터 사용되고 있는 프로토콜 이다. 만일 이러한 보안 프로토콜에서 아무도 예상치 못한 보안 헛점이 발견된다면 어떻게 될까? 사실, 소위 말하는 해커들은 이러한 프로토콜상의 취약점을 이용하여 시스템을 공격하여 시스템에 막대한 손실과 피해를 입힐 수 있다. 과연 그렇다면, 어떻게 하면 보안 프로토콜의 안전성을 분석하고 보장할 수 있을 것인가? 이러한 보안 암호 프로토콜을 디자인하여 실제 시스템에 적용하려고 할 때, 과연 그 안전성을 어떻게 보장하고, 이 복잡한 프로토콜이 제대로 그 보안 성능을 만족하는지 분석하는 일은 그리 간단한 작업이 아니다. 이미 유럽을 주축으로한 보안 선진국들은 오래전부터 모델체킹, 정리 증명등의 정형기법을 이용하여 보안 프로토콜을 분석하고 검증하는 방법을 사용해 오고 있다. 이 논문에서는 BAN 로직의 변형인 GNY[3] 로직을 바탕으로 보안 프로토콜을 디자인하고 분석하는데 사용되는 SPEAR (Security Protocol Engineering and Analysis Resource) II[4]를 이용하여 RADIUS 프로토콜의 보안기능을 분석하고자 한다. 사실, 대부분의 숙련된 공격자들은 네트워크 패킷 스니퍼링 도구를 사용하여 TCP/IP 를 통해 전달되는 모든 패킷을 분석할 수 있기 때문에, RADIUS 프로토콜 또한 안전하지 않은 방법이다. 따라서 본 논문에서는 RADIUS 프로토콜이 SSL(Secure Socket Layer)[5] 상에서 상호 키 교환을 한다는 가정아래 전체 프로토콜을 디자인하고 분석하고자 한다. 이 논문의 2 장에서는 RADIUS 프로토콜의 동작 원리 및 보안 기능을 보여주고, 3 장에서는 SPEAR II 도구의기능에 대해 설명하며, 4 장에서는 SPEAR II 도구를 사용하여 디자인한 RADIUS 의 보안 프로토콜을 분석하고, 마지막으로 5 장에서는 결론 및 향후 연구방향을 제시하고자 한다.

## 2. RADIUS

RADIUS(Remote Authentication Dial In User Service) 프로토콜은 원격지 이용자의 접속 요구시 이용자 ID 나 패스워드, IP 주소 등의 정보를 인증 서버에 보내어 이용자에 대한 인증 및 식별 작업을 해서, 만일 적합한 사용자 이면 인증 서버의 접속을 허가하고, 그렇지 않을 경우는 인증이 실패했다는 메시지를 클라이언트에 보내주게 된다. [그림 1]에서 보듯이 RADIUS 서버와 통신하게 되는 클라이언트는 NAS(Network Access Server)가 된다. 사용자(User)는 NAS 의 데이터베이스에 사용자의 아이디, 네트워크 주소, 패스워드, 통신 방식(PPP telnet, rlogin 등)의 서비스 정보를 저장하게 되며, 이런 정보를 바탕으로 RADIUS 서버에 인증을 요구하게 된다.

클라이언트(NAS)와 서버(RADIUS)의 통신은 상호간의 공유 패스워드를 사용하여 인증이 이루어지게 되며, 전체적인 통신 방식은 도전/응답 방식을 사용하고 있다. 이 도전/응답 인증 방식에 대해 간략히 설명하면, 클라이언트가 서버에 접속 요청을 하게 되면, 서버는 클라이언트에 아무도 예측할 수 없는 난수를 보내주게 된다.

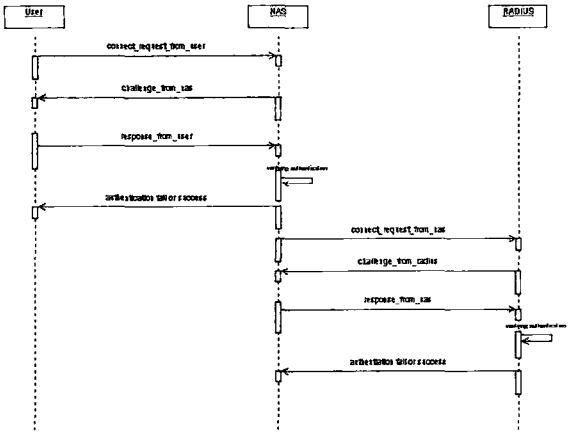


그림 1. RADIUS 프로토콜의 순차도

키 생성기를 이용하여 서버에 인증받기 위한 응답 정보를 생성하게 된다. 예를 들어, NAS 가 RADIUS 서버에 접속허가 요청 패킷을 보내게 되면, 서버는 Challenge 12345678 과 같은 정보를 보내주며, 사용자 응답정보 와 함께, NAS_Identifier, NAS_Port, NAS_Name 정보를 보내게 된다. 단, 사용자의 패스워드는 MD5 를 이용하여 해쉬화되어 전송되어 지게 된다. 아래 [그림 2]는 실제 RADIUS 제품을 이용하여 인증하였을 경우의 정보를 보여주고 있다.

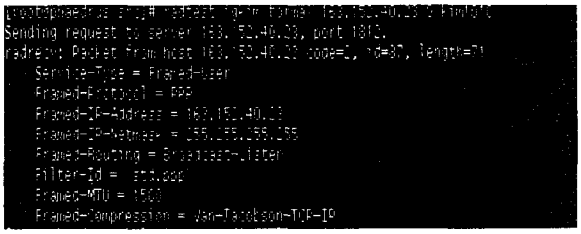


그림 2. RADIUS 서버에 대한 인증 예제

## 3. SPEAR, SPEAR II

SPEAR(Security Protocol Engineering and Analysis Resource)는 특히 보안 프로토콜을 위해서 만들어진 프로토콜 엔지니어링 도구로, 보안과 효율적인 디자인 및 분석 기능을 제공한다. 이미 오래전부터 암호화 알고리즘을 명확히 명세하고 분석하기 위한 연구가 진행되어 왔으며 이런 방법으로, MSC(Mssage Sequence Chart), SDL(Specification and Description Language)와 같은 방법을 이용하다가, 암호화 알고리즘들을 로직에 기반을 두고 명세하고 분석하자는 방법이 대두되게 되었다. 그 대표적인 예가 바로 BAN[6] 로직이다. 이런 BAN 로직을 변형한 형태가 GNY, SVO[7] 로직이다. SPEAR, SPEAR II 도구 모두 GNY 로직을 바탕으로 프로토콜을 분석한다. SPEAR , SPEAR II 도구가 개발되었으며 하지만 이 두 버전은 도구의 기능상 큰 차이점을 보여주고 있다. SPEAR 에서는 자바 코드 생성, 메타 실행등의 기능을 제공한 반면, SPEAR II 에서는 GNY 로직을 이용한 프로토콜 분석에 중점을 두도록 만들어 졌다. 아래 [그림 3]은 SPEAR 과 SPEAR II 의 기능상 차이점을 보여주고 있다.

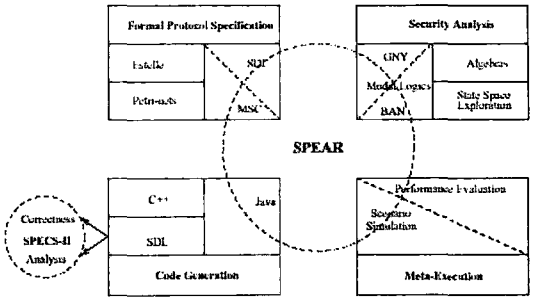


그림 3. SPEAR 와 SPEAR II 동작 범위

본 논문에서는 SPEAR 를 이용하여 RADIUS 를 디자인 하여 자바 코드를 생성해 보았을 뿐만 아니라, SPEAR II 도구를 이용하여 RADIUS 프로토콜을 GYN 로직으로 표현하고 분석하였다.

## 4. SPEAR, SPEAR II 도구를 이용한 RADIUS 프로토콜 디자인 및 분석

### 4.1 디자인

RADIUS 프로토콜을 이용하여 전달되어지는 패킷을 공격자가 패킷 스니퍼링 도구를 이용하여 쉽게 분석할 위험성이 있다. 따라서 본 논문에서는 보다 안전한 통신을 위해 RADIUS + SSL 을 이용한 통신 프로토콜을 SPEAR 를 통해 디자인 하고 분석해 보았다.

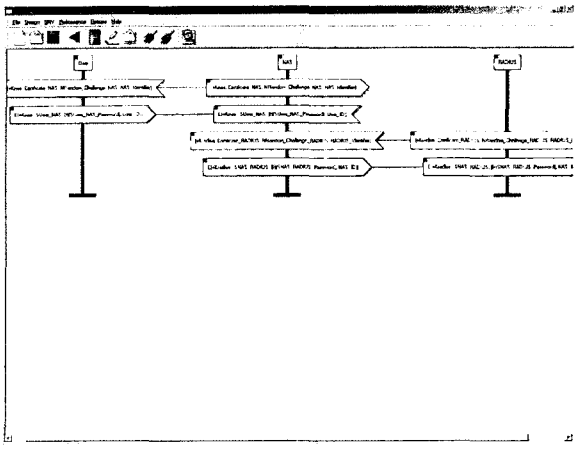

그림 4. SPEAR II 를 이용한 SSL 상의 RADIUS 프로토콜

위의 [그림 4] 에서 볼 수 있는 바와 같이 SSL 상에서 동작하는 RADIUS 프로토콜을 SPEAR II 도구를 이용하여 디자인하였다. 이 그림은 앞의 <그림 1>에서 본 순차도와 유사한 형태를 취하고 있으며, 프로토콜상의 키 교환에 중점을 두고 있다.

### 4.2 분석

[1] Proof for RADIUS possesses SNAS_RADIUS:

1. RADIUS possesses SNAS_RADIUS. {Assumption}

[2] Proof for RADIUS possesses SNAS_RADIUS_Password:

1. RADIUS possesses SNAS_RADIUS_Password. {Assumption}

[3] Proof for User possesses SUser_NAS_Password:

1. User possesses SUser_NAS_Password. {Assumption}

.....

NAS believes that SNAS_RADIUS_Password is a suitable secret for use between NAS and RADIUS.

NAS believes that SUser_NAS_Password is a suitable secret for use between NAS and User.

NAS believes that SUser_NAS is a suitable secret for use between NAS and User.

그림 5. GNY 로직을 이용한 RADIUS 프로토콜 분석결과

[그림 5]에 나타나 바와 같아. GNY 로직을 통해 RADIUS 프로토콜을 분석한 결과 아래에서 보듯이 User, NAS, RADIUS 사이에 안전한 통신을 위해 다음과 같은 키 교환이 이루어짐을 증명할 수 있었다.

1. User ↔ NAS
   Suser_NAS
   Suser_NAS_Password

2. NAS ↔ RADIUS
   SNAS_RADIUS
   SNAS_RADIUS_Password

- SUser_NAS : User 와 NAS 간에 SSL 을 통해 전달되는 세션키,
- SUser_NAS_Password; User 와 NAS 간에 RADIUS 프로토콜 인증을 위해 사용되는 세션키
- SNAS_RADIUS : NAS 와 RADIUS 간에 SSL 을 통해 전달되는 세션키,
- Suser_NAS_RADIUS; NAS 와 RADIUS 간에 RADIUS 프로토콜 인증을 위해 사용되는 세션키

### 5. 결론 및 향후 연구 방향

점차적으로 보안 프로토콜을 이용한 전자상거래 시장이나 보안 시장이 매우 활성화 되어 가고 있는 추세이다. 이에 따라, 그 안전성을 보증하기 위해 보안 프로토콜에 대한 검증이 절실히 요구되는 시기이다. 본 논문에서는 SSL 상에서 동작하는 RADIUS 보안 프로토콜을 SPEAR , SPEAR II 도구를 이용하여 디자인하고 GNY 로직을 이용하여 프로토콜을 분석하여 봄으로써 설계 단계에서부터 프로토콜의 안전성을 진단해 보았을 뿐만 아니라, 소스 코드 생성 자동화 기능을 이용하여 자바 코드를 산출할 수 있었다. 그러나 SPEAR 도구를 이용한 자동화된 소스코드 생성 기능은 SPEAR II 에서는 지원되지 않고 있는 상태이다. 향후 연구과제로는 RADIUS 프로토콜을 변형하여 , 모바일 환경에서 동작하도록 제안된 DIAMETER [8] 프로토콜을 Murphi[9]와 같은 정형 검증 도구를 이용하여 명세하고 검증하고자 한다.

### 6. 참고문헌


[1] AAA Working Group INTERNET-DRAFT, draft-ietf-aaa-transport-0.5.txtAuhentication, Authorization and Accounting(AAA) Transport Profile.

[2] RFC 2138, Remote Authentication Dial In User Service (RADIUS).

[3] Li Gong, Roger Needham, and Raphael Yahalom Reasoning about Belief in Cryptographic Protocols

[4] E. Saul and A.C.M. Hutchison. SPEAR II: The Security Protocol Engineering and Analysis Resource. In Second Annual South African Telecommunications, Networks and Applications Conference, pages 171-177, Durban, South Africa, September 1999.

[5] D. Wagner and B. Schneier. Analysis of the SSL 3.0 Protocol.. In Proceeding of the Second USENIX Workshop on Electronic Commerce, November 1996.

[6] M. Burrows, M. Abadi , and R. Needham, "A Logic of Authentication", in Proceedings of the 12th ACM Symposium on Operating Systems Principles.

[7] P. Syverson and P. van Oorschot. On unifying some cryptographic protocol logics. In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 14-28, 1994.

[8] Pat R. Calhoun, "DIAMETER Base Protocol," draft_calhoun-diameter-15.txt, IETF work in progress, June 2000.

[9] Automated analysis of cryptographic protocols using Murphi, John C. Mitchell, Mark Mitchell, and Ulrich Stern, IEEE Symposium on Security and Privacy, 1997