한국사물인터넷학회논문지 Vol. 2, No. 1, pp. 1-6, 2016 http://dx.doi.org/10.20465/KIOTS.2016.2.1.001

사물인터넷 환경에서 RADIUS 프로토콜의 향상된 인증기법

김영세[1], 한근희[2*], 김기천[3]
[1]건국대학교 IT융합정보보호학과, [2]고려대학교 정보보호대학원, [3]건국대학교 컴퓨터공학과

Improved authentication mechanism of the RADIUS protocol in the Internet of Things

Young-Se Kim[1], Keun-hee Han[2*], Kee-cheon Kim[3]
[1]Division of IT Convergence Information Security, Konkuk University
[2]Graduate School of Information Security, Korea University
[3]Division of Computer Science, Konkuk University

요 약 사물인터넷은 네트워크에 연결된 사람, 사물, 공간 등 모든 것들(Things)이 실시간으로 데이터를 생성하고 해당 객체간의 정보가 수집, 공유, 활용되는 기술이나 환경을 일컫는다. 현재 헬스케어, 스마트홈 등 다양한 분야에서 연구가 진행이며 사물인터넷 환경에 지리적 공간과 인터넷 간의 연결성을 강조한 만물인터넷의 개념도 등장했다. 사람, 사물 등 각 객체간의 연결성이 중요하게 부각되면서 효율적이고 안전한 인증기술에 대한 연구가 진행 중이다. 이 논문에서는 사물인터넷 환경에서 사람, 사물 등 객체간의 상호인증을 위한 개선된 RADIUS(Remote Authentication Dial In User Service) 프로토콜을 제안한다.

주제어 : RADIUS(Remote Authentication Dial-In User Service), SCTP(Stream Control Transmission Protocol), Authentication, URI Signing, MD5 Hash

Abstract The IOT environment, people connected to the network, object, everything such as space (Things) generates data in real time. The information between the object collecting, sharing, are utilized. Currently health care, research in various fields such as smart home has been promoted. Also appeared concepts emphasized all things(IOE) Internet connection between the geographic space and the Internet. Human, while important connections between the objects, such as objects, studies of efficient and secure authentication technologies have been developed.
In this paper, we propose a RADIUS (Remote Authentication Dial In User Service) protocol for improved mutual authentication between each object in the IOT environment.

Key Words : RADIUS(Remote Authentication Dial-In User Service), SCTP(Stream Control Transmission Protocol), Authentication, URI Signing, MD5 Hash

1. 서론

네트워크에 연결된 사람, 사물, 공간 등 모든 것들(Things)이 실시간으로 데이터를 생성하고 해당 객체간의 정보가 수집, 공유, 활용되는 사물인터넷 환경에서는 각 객체간의 상호인증 프로세스가 빈번하게 발생한다.

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업(IITP-2016-H8501161012000l002) 및 글로벌 딜리버리 클라우드 플랫폼의 대규모 OTT 서비스 적용을 위한 방송·통신 사업자 공동의 시범 사업의 연구결과로 수행되었음(No.B0511-15-0001)."
*교신저자 : 김기천(kckim@konkuk.ac.kr), 한근희(khhan@formal.korea.ac.kr)
접수일 : 2016년 3월 10일, 수정완료 : 2016년 3월 20일, 최종게재확정 : 2016년 3월 30일

전통적인 AAA(Authentication, Authorization, and Accounting) 프레임 워크 기반의 인증프로토콜인 RADIUS(Remote Authentication Dial-In User Service)는 다이얼업 네트워킹을 이용하는 사용자들을 인증하기 위해서 표준인증 방식으로 UDP를 사용하고 있다[1].

본 논문에서는 IOT환경에서 SCTP(Stream Control Transmission Protocol)전송방식을 RADIUS에 적용해서 송/수신 두 객체간의 데이터 교환 시, 각 경로별 전송 데이터의 무결성을 유지할 수 있는 방안을 제시하고 개선된 User-Password 해시기법을 제안한다.

본 논문에서 제안한 방식을 통해서 송/수신 두 객체간의 데이터 교환 시, 각 경로별 전송 데이터의 무결성을 유지할 수 있었으며, 평가결과 인증을 위한 식별정보 전송 시, 랜덤하게 생성된 임의의 nonce를 첨부하여 해시하는 것이 기존방식보다 보안성의 측면에서 보다 유리함을 알 수 있었다.

2. 관련 연구

2.1 RADIUS 인증

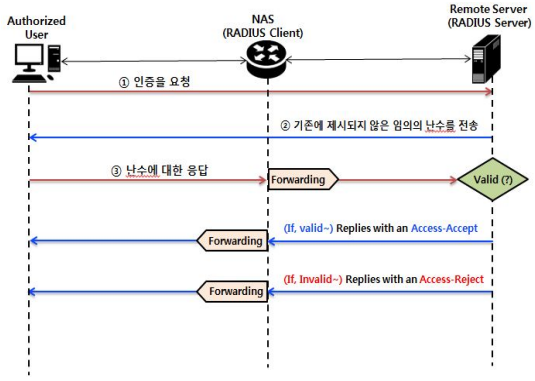
RADIUS은 AAA 프레임워크 기반의 인증 프로토콜로서 사용자들이 특정 네트워크/시스템에 접속을 요청할 때, 인증 서버에서 사용자의 ID, 패스워드 등의 정보를 검증한 후 인증 및 식별 작업을 수행한다.

인증 서버는 수신한 식별정보를 근거로 적합한 사용자일 경우에는 원격접속을 허가하고, 그렇지 않을 경우에는 인증실패 메시지를 클라이언트에 반환한다[1].

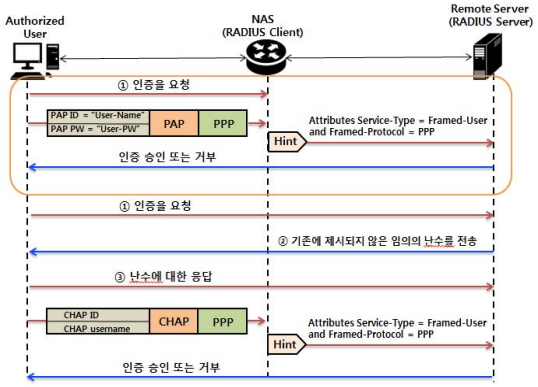
RADIUS 프로토콜에서 사용되는 메시지는 기본적으로 TCP대신 UDP프로토콜을 사용한다. 또한 RADIUS 프로토콜은 다양한 인증 방식을 지원하며, 일반적으로 PAP(Password Authentication Protocol)와 CHAP(Challenge Handshake Authentication Protocol) 인증 방식을 사용한다.

두 인증방식은 모두 PPP(Point to Point Protocol) 인증용 프로토콜이다. PAP는 클라이언트의 평문 ID, 암호를 그대로 전송하며, 인증요청 및 인증응답 2개 절차만 있어서 보안상 취약한 구조의 방식이고, CHAP는 클라이언트가 인증을 요청하면 인증 서버가 클라이언트에게 Challenge 메시지를 보낸 후, 응답을 수신하는 Three-way Hand shaking방식이다.

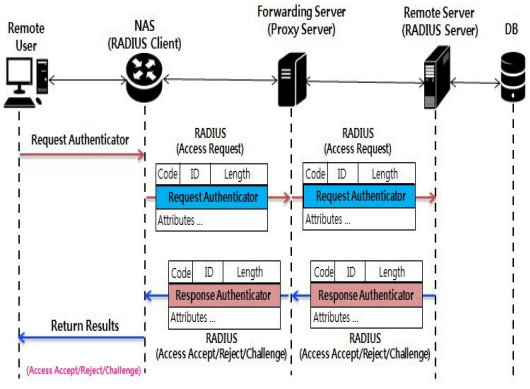
[Fig. 1]은 CHAP 인증의 기본구조인 Challenge&Response 과정을 보여주고 있으며, [Fig. 2]는 PAP와 CHAP의 인증과정을 비교해서 보여주고 있다.



[Fig. 1] Challenge & Response 방식



[Fig. 2] PAP & CHAP 방식



[Fig. 3] 인증(Authentication) & 권한부여(Authorization)

RADIUS 프로토콜의 사용자 인증과 권한부여과정은 최초 클라이언트가 인증요청을 할 때, RADIUS 서버에 의해서 동시에 수행되고 자원체크는 사용자의 네트워크 접근이 허용된 이후에 자원사용 시작/종료시점과 주기적인 상태 업데이트를 통해서 이뤄진다. [Fig. 3]는 RADIUS 프로토콜의 사용자 인증과 권한부여 과정을 보여주고 있다[3].

3. IOT환경에서 개선된 패킷 인증 방식

3.1 SCTP방식을 활용한 인증

SCTP(Stream Control Transmission Protocol)는 데이터 통신을 위한 전송계층 프로토콜로서 혼잡제어를 통해 경로장애 복구기능을 제공하는 'multi-homing', 하나의 Association을 설정하여 다양한 종류의 데이터를 여러 개의 스트림으로 분리하여 독립적으로 전송할 수 있는 'multi-streaming'의 특징이 있다[2].

RADIUS는 현재 표준인증 방식으로 UDP를 사용하고 있으며, 이로 인해 다음과 같은 문제가 발생하고 있다[6].

(1) 메인 서버의 이상여부 탐지불가
(2) 제한적인 혼잡제어
(3) 비 신뢰적인 데이터 전송

위와 같은 단점에도 불구하고 메인서버에 장애가 발생 시, 대체 서버를 신속하게 이용하기 위해서 RADIUS는 UDP 전송방식을 최초에 채택했다. 결국, 신뢰성 있는 데이터 전송보다 빠르고 효율적인 데이터 전송에 의미를 두었다.

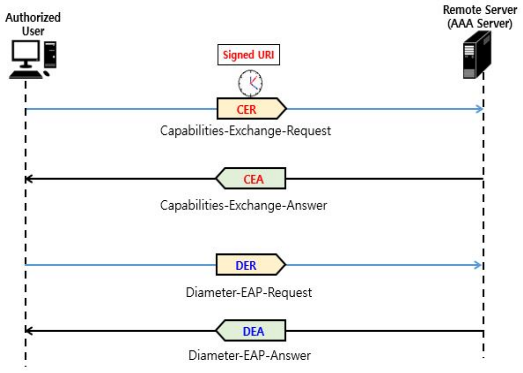
하지만 IOT환경에서는 Device간의 인증 프로세스가 빈번하게 발생하고, 인증 메시지에 보안을 위한 속성이 추가되면서 신뢰성 있는 데이터의 전송을 무시할 수 없는 상황이다.

따라서 빠르고 효율적인 데이터 전송을 하면서, 혼잡제어를 통한 경로 장애 복구를 할 수 있는 SCTP방식을 RADIUS에 적용하는 것을 고려해 볼 수 있다.

SCTP는 송/수신 객체간의 associations을 설정한 후, 데이터 전송을 위한 메인 경로를 지정한다. 그 이외의 다른 경로들은 예비 경로로 지정하고, 메인경로에 장애 발생 시 대체경로로 활용한다. 또한 여러 stream에서 동시에 데이터를 전송할 수 있는데, 특정 stream에서 전송이 지연될 경우 다른 stream에 영향을 주지 않고 독립적으로 데이터를 전송한다[2].

결국, RADIUS에 SCTP방식을 사용해서 Device간의 인증절차를 수행할 경우, 각 경로별 전송 데이터의 무결성을 유지해야만 송/수신 객체간의 신뢰가 확보되게 된다.

따라서 본 논문은 송신 객체의 URI 서명 정보를 인코딩해서 request 패킷의 속성으로 저장한 후, 데이터를 전송하는 방식을 통해서 각 경로별 전송 데이터의 무결성을 유지하는 방안을 제안한다. [Fig. 4]는 URI 서명 정보를 인코딩해서 request 패킷의 속성으로 저장한 후 인증을 요청하는 과정을 보여주고 있다.



[Fig. 4] URI 서명 정보를 활용한 인증과정

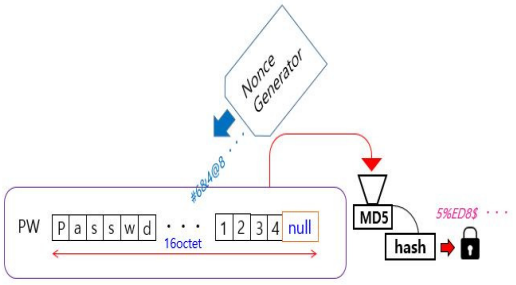
위의 인증과정은 SCTP방식을 사용하는 DIAMETER 프로토콜의 인증 노드 탐지과정을 기반으로 하고 있다[4]. 최초 인증을 요청하는 송신객체는 Capabilities-Exchange-Request (CER) package를 전송할 때, 자신의 URI정보를 전자서명 한다. 이 때, 해당 메시지의 요청시간을 근거로 응답유효 시간이 설정된다. 이는 서명된 URI에 유효시간을 부여하여 Reply 공격을 방지하기 위함이다. 그 이후에 수신객체에서 송신객체의 URI서명 정보의 유효성을 검증한 후, 인증과정을 수행하게 된다.

3.2 개선된 User-Password Hashing

송신객체는 인증요청을 시도하면서, 자신의 ID, 패스워드 등의 정보를 전송하게 된다. 기존 RADIUS에서는 User-Password 필드 128비트 부분을 MD5 hash 처리해서 전송하고 있다.

하지만 MD5 hash 대상 메시지의 길이가 128비트(RADIUS의 User-Password 할당 길이)라면 공격자는 해시충돌을 찾기 위해서 2^64개의 메시지만 필요하게 된다[5].

기존 RADIUS 프로토콜의 User-Password MD5 Hash는 SHA-1방식을 사용하고 있는데 현재 메시지 다이제스트 크기의 제한으로 인한 보안상의 취약점이 발견된 상황이다. 따라서 32비트의 nonce를 임의로 생성해서, 기존 User-Password에 첨부한 후 MD5 Hash과정을 수행하는 것이 좀 더 보안성을 향상하기 위한 방안이 될 수 있다[6]. [Fig. 5]는 개선된 User-Password Hashing 과정을 보여주고 있다.



[Fig. 5] 개선된 User-Password Hashing 과정

4. 성능평가

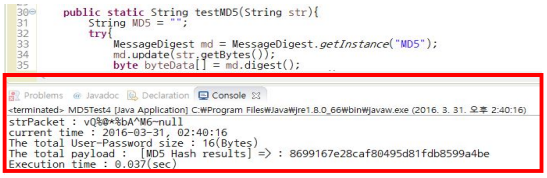
본 논문에서 제안하는 방식의 시뮬레이션을 위한 시스템 사양은 다음과 같다.

- CPU : Intel(R) Core(TM) i5-4590, 3.3GHz
- RAM 8G
- HDD 500G
- OS : Windows 7 professional k 64bit version

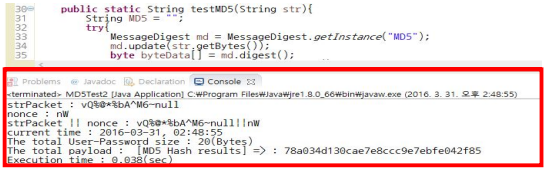
시뮬레이션은 JAVA에서 제공하는 MessageDigest, SecretKeySpec 클래스를 이용해서 MD5 Hash 기능을 구현했다.

시뮬레이션 내용은 다음과 같다.

(1) User-Password 필드 128비트 부분을 MD5 hash (기존, User-Password Hashing 과정)
(2) 32비트의 nonce를 임의로 생성한 후, User-Password 필드 128비트 부분에 첨부해서 MD5 hash (제안방식)



[Fig. 6] 기존 User-Password Hashing 과정



[Fig. 7] nonce를 활용한 개선된 User-Password Hashing 과정

[Table 1] 시뮬레이션 결과

단위 (sec)	1회	2회	3회	4회	5회	평균
기존방식	0.037	0.035	0.041	0.036	0.038	0.0374
제안방식	0.038	0.035	0.038	0.038	0.039	0.0376

[Fig. 8] 시뮬레이션 결과

[Fig. 6, 7]은 각각 User-Password 필드 128비트 부분을 단순하게 MD5 hash 처리하는 기존방식과 nonce를 활용해서 보안성을 높인 hash방식의 결과화면이다. 시뮬레이션 결과, 기존방식과 32비트의 nonce를 추가해서 hash하는 방식은 속도 면에서 큰 차이가 없었다.

사용자들이 보유한 Device간의 재인증이 빈번하게 발생하는 IOT환경에서 단순하게 Password필드만을 Hash하는 것은 중간자 공격 (man in the middle attack, MITM)으로 인해 보안상 취약한 문제가 발생할 수 있다.

따라서, 송신객체가 RADIUS 서버에 인증 패킷을 전송할 경우, nonce를 활용해서 해시충돌 경우의 수를 증가시키는 방식이 효율적인 프로세스가 될 수 있다.

5. 결론 및 향후 연구 방향

본 논문에서는 기존 RADIUS 프로토콜의 인증방식을 분석한 후, IOT환경에서 좀 더 신뢰성을 보장하면서 효율적인 전송방식에 대해 연구했다. 기존의 UDP방식과 비교를 통해 IOT환경에서 개선된 패킷 인증 방식으로서 메시지 지향(message-oriented)방식과 연결 지향(connection-oriented)방식의 특성을 지닌 SCTP전송방식이 좀 더 적합한 전송방식임을 알 수 있었다.

또한, 송/수신 두 객체간의 데이터 교환 시, 각 경로별 전송 데이터의 무결성을 유지할 수 있는 방안으로 송신 객체의 URI 서명 정보를 인코딩하는 방안에 대해 연구했다.

Device간의 상호연결성이 강조되는 IOT환경에서 중요 정보를 단순 Hash해서 전송하기 보다는 임의로 생성된 nonce를 활용해서 보안성을 향상시키는 것이 조금 더 합리적일 수 있다.

향후 연구과제로는 Cloud 환경에서 효율적으로 Private Data와 Public Data를 구분해서 전송하기 위한 방안으로 Diameter 프레임워크 기반의 SCTP전송방식을 활용해서 연구하고자 한다.

ACKNOWLEDGMENTS

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.B0511-15-0001, 글로벌 딜리버리 클라우드 플랫폼의 대규모 OTT 서비스 적용을 위한 방송·통신 사업자 공동의 시범 사업)과 2016년도 한국인터넷진흥원의 지원을 받아 고용계약형 정보보호 석사과정 인력양성사업의 일환으로 수행된 연구임.

REFERENCES

[1] C. Rigney, S. Willens, A. Rubens, W. Simpson. “Remote Authentication Dial In User Service (RADIUS)”. RFC 2865. June 2000

[2] RFC2960, Stream Control Transmission Protocol, October 2000

[3] A. DeKok. “RADIUS over TCP”. RFC 6613. May 2012

[4] Mladen Stanke, Mile Sikic. “Comparison of the RADIUS and Diameter Protocols”. Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on, pp. 893-898, June 2008

[5] M Iwamoto, T Peyrin, Y Sasaki, ″ Limited-Birthday Distinguishers for Hash Functions″. ASIACRYPT, 2013 - Citeseer

[6] Youngse Kim, Keecheon Kim, ″The RADIUS protocol Improved packet encryption and transmission method of Larger packets″ The 2015 Fall Conference of the korea information processing society.

김 영 세(Young-Se Kim) [준회원]

- 2013년 2월 : 영산대학교 사이버경찰학과 (학사)
- 2015년 2월 ~ 현재 : 건국대학교 일반대학원 IT융합정보보호학과 석사과정

<관심분야>
사물인터넷 보안, 네트워크 보안, 개인정보보호

한 근 희(Keun-Hee Han) [종신회원]

- 서울과학기술대학교 컴퓨터공학과 졸업
- 한양대학교 공학대학원 공학석사
- 고려대학교 대학원 이학박사
- 현재 : 고려대학교 융합소프트웨어전문대학원 산학교수

<관심분야>
소프트웨어 보증, 시큐어 코딩, 정보보호관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 자동차 보안 등

김 기 천(Keecheon Kim) [정회원]

- 1988년 : 서울대학교 계산통계학 (공학사)
- 1992년 : 미국 Northwestern Univ. (공학박사)
- 1992년 ~ 1996년 : 한국통신기술(주) 선임연구원
- 1996년 ~ 1998년 : 신세기 통신(주) 책임연구원
- 1998년 ~ 현재 : 건국대학교 컴퓨터공학과 교수

<관심분야>

mobile wireless network, 미래인터넷보안, sensor network, 네트워크 보안, 사물인터넷