

한국정보보호학회 충청지부

제 23회 정기총회 및 정보보호학술논문발표회

2019년 10월 18일 – 19일
대전, 한남대학교(공과대학-9호관)

Organized by

한국정보보호학회 충청지부



대신정보통신(주)



13:30-14:30 Poster A KIISC-CC 2019

(공과대학 9호관-디자인씽킹 스튜디오(90524))

(좌장: 강정민 박사(국가보안기술연구소))

1. Siemens S7 PLC 프로토콜 통신 및 취약점 분석을 통한 재전송 공격 기법 연구
- 김준원, 최현표, 이주찬, 김장훈, 정다운, 서정택 (순천향대학교)
2. 드론을 이용한 기반시설 공격 가능 시나리오 및 파급영향 분석
- 김장훈, 이주찬, 서정택 (순천향대학교)
3. 개인정보 노출 방지를 위한 오프라인 문서 보호 방법
- 한진희, 김건우 (한국전자통신연구원)
4. ARM Cortex-M4에서의 ECDSA p-256 스칼라 곱셈 최적화 구현 및 성능 비교분석
- 오진혁, 한주홍, 윤승환, 이옥연 (국민대학교)
5. 암호화폐용 콜드월렛의 단일파형 부채널 취약점 조사
- 박동준, 김희석, 홍석희 (고려대학교)
6. 프록시 재암호화 기법을 활용한 CCTV 영상 암호화에 관한 연구
- 강주영, 황용운, 이임영 (순천향대학교)
7. 경량·저전력 환경에서의 보안성 향상을 위한 블록체인 기반 드론 데이터 분할 분산 저장 기술
김지수, 신충용, 김태성, 조성현
8. QR코드 및 스마트 글래스를 활용한 개인 정보 보호 블록체인 택배 시스템
- 최승주, 장경배, 김현지, 서화정 (한성대학교)
9. DNS와 SNI를 이용한 인터넷 검열
- 윤재웅, 김경호, 서화정 (한성대학교)
10. 실제 IT 환경에서의 로컬 차분 프라이버시 적용 사례 연구
- 정수용, 홍도원, 서창호 (공주대학교)
11. 위치정보보호를 위한 Geo-Indistinguishability에 대한 연구
- 강준영, 홍도원, 서창호 (공주대학교)
12. 스마트기기를 통한 영상 서비스의 프라이버시 보호를 위한 속성기반 키 관리 기술 개발
- 허영준, 김건우 (한국전자통신연구원)
13. 클라우드 환경에서의 티켓 기반 인증 기법
- 조정석, 김득훈, 곽진 (아주대학교)
14. 마우스행위 중 뇌파데이터 기반 사용자인증 연구
- 남승수, 최대선 (공주대학교)

클라우드 환경에서의 티켓 기반 인증 기법

조정석*, 김득훈*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실, **아주대학교 사이버보안학과

Ticket-Based Authentication Scheme in Cloud Environments

Jeong-Seok Jo*, Deuk-Hun Kim*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요약

클라우드 네트워크는 다양한 서비스 제공을 위해 다수의 서버가 존재한다. 이와 동시에, 서비스 사용자 수가 증가하면서, 다양한 서버에서의 사용자 인증에 대한 중요성이 증가하였다. 다양한 서버에서의 사용자 인증을 위해 사용되던 ID/PW 기반 인증 기법의 문제점들을 보완하기 위해 SSO 기술과 같은 인증 기법에 관한 연구가 다수 진행되고 있다. 따라서, 본 논문에서는 클라우드 환경에서의 사용자 인증을 위해, 사용자 지문 정보와 티켓을 활용한 인증 기법을 제시하고자 한다.

I. 서론

클라우드 네트워크를 활용한 서비스 제공 분야가 확대되고 있다. European Banking Authority의 “FinTech and cloud in banking”에 따르면 금융 분야에서 클라우드 서비스를 활용함으로써, 고객 요구에 대한 향상된 응답 속도, 위험 분리, 비용의 효율성 등의 장점을 확보할 수 있다고 제시하였으며, 사용자 인증의 중요성에 대해서도 언급하였다[1]. 이러한 사용자 인증의 중요성이 증가하면서, Gartner는 ID/PW뿐만 아니라 생체 정보와 같은 추가적인 정보를 활용한 인증 방식이 확대될 것으로 예상했다[2].

이에 따라, 본 논문에서는 클라우드 환경에서의 사용자 인증을 위해, 사용자의 지문 정보와 티켓을 활용한 사용자 인증 기법을 제시하고자 한다.

II. 제안 기법

S.M. Bellovin, M. Merritt의 “Limitations of the Kerberos Protocol”에서는 Kerberos 기술의 한계에 대해 제시하였다. 해당 논문에서는 티켓 유효성 검증을 위한 시간 값 동기화와 같은 시스템 문제와 함께, Password Guessing 공격과 같은 보안 위협을 제시하였다[3]. 이에 대응하기 위해,

본 논문에서는 클라우드 환경에서의 지문 정보를 활용한 티켓 기반 인증 기법을 제안하고자 한다.

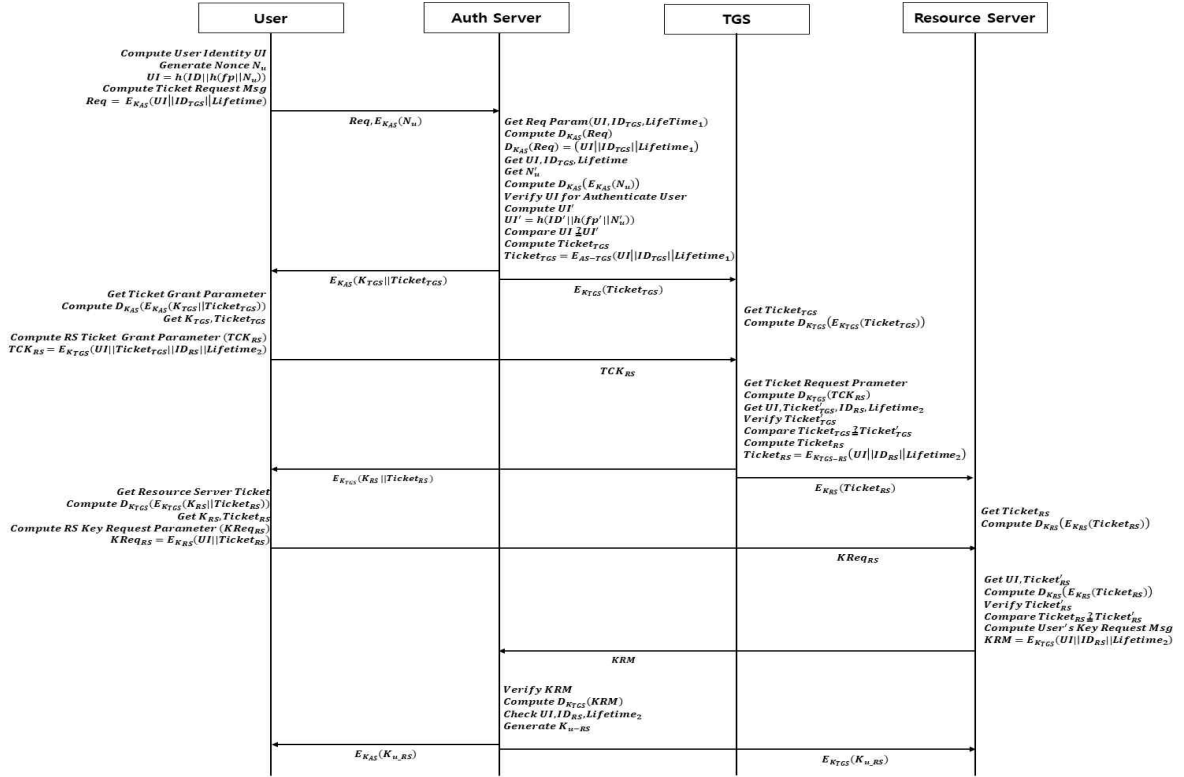
2.1 제안 기법

본 논문에서는 지문 정보를 활용한 사용자 정보 생성 및 티켓을 활용한 사용자 인증을 수행한다. 제안 기법은 사용자(User)와 Authentication Server(Auth Server) 사이의 사전 인증을 통한 Session Key E_{AS} 가 상호 간에 전달되었고, 사용자의 ID와 지문 정보 fp 를 Auth Server가 확보하고 있다. 제안 기법은 사용자, 사용자의 정보(ID, fp) 및 각 구성요소의 키를 생성하고 보관하는 Auth Server, 다양한 서버의 티켓을 발부하는 Ticket-Granting Server(TGS), 사용자에게 서비스를 제공하는 Resource Server(RS)로 구성된다. 제안하고자하는 인증 기법은 (그림 1)과 같으며, 구체적인 인증 단계는 다음과 같다.

Step 1. Send Request Message for TGS Ticket

사용자는 난수 N_u 를 생성하고, 생성된 난수와 함께 지문 정보를 이용하여 사용자 개개인의 특징 값($UI = h(ID || h(fp || N_u))$)을 생성한다. UI 와 TGS의 ID, 티켓 유효 시간 값들로 구성된 Request Message(Req)를 Auth Server에게 전송한다.

Step 2. Verify User & Send TGS's Key and TGS Ticket



(그림 1) 제안 기법

Auth Server는 수신한 UI 값을 통해 User를 인증하고, User와 Auth Server의 세션키를 활용하여 TGS의 키와 TGS 티켓을 전송한다. 동시에, Auth Server는 생성한 티켓을 TGS에게도 전송한다.

Step 3. Send RS Ticket Request Message

User는 Step 2.에서 확보한 TGS의 키를 활용하여, TGS에게 Ticket Request Message를 전송한다.

Step 4. Verify User's TGS Ticket & Send RS's Key and RS Ticket

TGS는 Step 3.에서 수신한 User의 TGS 티켓을 검증하고, User와 TGS의 키를 활용하여, RS의 키와 RS 티켓을 전송한다. 동시에, TGS는 생성한 티켓을 RS에게도 전송한다.

Step 5. Send RS Key Request Message

User는 RS에게 Step 4.에서 수신한 RS의 키를 활용하여 RS 티켓을 RS에게 전송한다.

Step 6. Verify User's RS Ticket & Send Key Request Message

RS는 User의 티켓을 검증하고 Auth Server에게 키 생성 요청 메시지를 전송한다.

Step 7. Auth Sever Generate User-RS Key

Auth Server는 Step 6.에서 수신한 요청 메시지의 UI , 티켓 유효 시간 값들을 검증하고 타당하다면,

User와 RS의 키(K_{U-RS})를 생성하여 User에게 세션키(E_{AS})를 이용해 전송한다. 동시에, TGS의 키를 활용해 RS에게 키 K_{U-RS} 를 전송한다.

III. 결론

본 논문은 클라우드 네트워크에서의 사용자 인증을 위해 지문 정보와 티켓을 활용한 인증 기법을 제시하였다. 제시된 인증 기법은 ID/PW 기반의 티켓 인증 기법의 보안 위협인 Password Guessing 공격 완화를 위해 지문 정보를 활용하여 티켓을 생성하였다.

제시된 인증 기법은 사용자 인증을 위해 각 구성요소의 키를 Auth Server와 TGS가 사전에 가지고 있어야 한다. 따라서, 향후 안전한 키 분배 과정을 포함한 SSO 인증 기법 연구를 진행할 예정이다.

[참고문헌]

- [1] European Banking Authority, "FinTech and cloud in banking", Jul. 2017
- [2] Gartner, "Predicts 2019: Identity and Access Management", Dec. 2018
- [3] S.M. Bellovin and M. Merritt, "Limitations of Kerberos Protocol", ACM SIGCOMM Computer Communication Review, Vol. 20, No.5, pp.119-132, Oct. 1990