지문을 이용한 보안 토큰생성과 전파공격 보호 개선 기법

이수연*, 홍지훈*, 김진우*, 전유부**, 이근호*
*백석대학교 정보통신학부 ,
**순천향대학교 컴퓨터소프트웨어공학과
e-mail : lsuy0530@naver.com, acx12343@naver.com, dosnzmffjq@gmail.com,
jeonyb@sch.ac.kr, root1004@bu.ac.kr

A Scheme of Improving Propagation Attack Protection and Generating Security Token using Fingerprint

Su-Yeon Lee*, Hong ji hun*, Kim Jin Woo*, Yoo-Boo Jeon**, Keun-Ho Lee*
*Dept. of Information Communication, BaekSeok University
Dept. of Computer Software Engineering, Soonchunhyang University

요 약

급격한 전파를 이용하는 기기의 다양화와 대중화로 인해 많은 전파 관련 보안 문제들이 일어나고 있다. 전파와 생활에서의 안전은 매우 밀접한데 전파의 방해와 교란은 단순 생활의 불편뿐 아니라 신체의 직접적인 피해를 입힐 수도 있기 때문에 전파보호는 매우 중요한 과제이다. 본 내용에서는 그 대안으로 본문의 전파 교란과 교섭을 막기 위한 방안으로 생체정보인 지문을 이용한 암호화된 토큰을 만들어 토큰링을 통한 정보의 수신여부를 결정 하여 인증 강도, 호출자의 정보 등이 포함된 동적 보안 속성을 가진 수평 전파를 전송하고 java직렬화와 직렬화 해제 기능을 이용하여 토큰의 고유성을 확인 수평전파를 송·수신 하여 해당 문제점을 해결 하고자 제안하였다.

1. 서론

스마트폰, 자동차, 네비게이션 시스템, 드론과 같이 개인 소형 기기 종류와 이용자가 기하급수적으로 늘어나면서 전파 피해, 전파이용과 보호의 중요성이 대두대고 있다. 간단하게는 드론이나 네비게이션 등은 위성으로부터 발신되는 신호를 받아 위치를 파악하고, 스마트기기들은 GPS를 이용하여 위치기반 서비스와 통신서비스를 제공하고 있다. 공격은 수신기에 대한 교란전파 공격을 의미하며, 크게는 국가 간의 전파 교란공격이나 정보 취득의 목적으로 무선 전파를 이용해 국가의 정보를 취득하기도 하며, 민간 항공기의 전파 교란으로 안전의 위협을 가하는 실제 사례들이 있었으며 작게는 개인의 통신이용을 방해하고 재머 등을 사용해 생활의 불편함을 주는 등 여러 가지 방법으로 피해를 주고 있다.

위에서 언급한 다양한 문제점들 중 개인사용자의 전파 이용 시 발생하는 문제점들을 미연에 방지하고자 본 내용에서는 실생활에서 가장 접근성이 뛰어난 사용자 고유의 생체정보인 지문으로 생성한 키로 생산된 보안토큰 접목한 전파의 보안을 제안하고자 한다.

2. 관련연구

2.1 피해사례

전파교란으로 인한 피해사례로는 일상생활에서의 위협뿐만 아니라 크게는 국가간의 갈등의 요인이 되기도 한다. 아래의 상황들을 경험한다면 GPS 교란 시 나타나는 현상으로 의심되기 때문에 즉시 보호가 필요하다.

- 차량 내비게이션 작동 불가
- 항공기 자동 비행 불가능
- 휴대전화 자주 끊기거나 통화 불능
- 현금자동입출금기 오작동
- GPS를 사용한 측량 불가능
- 선박 항로 이탈

2.2 전파공격 종류 및 탐지방법

- 재밍(jamming)

전파 방해 행위인 재밍(jamming)은 전파가 강한 주파수를 이용해 기계가 기존 주파수를 대신 강한 전파의 주파수를 수신하면서 순간적으로 먹통이 되거나 오작동을 일으키는 것으로 신호가 위성으로부터 받은 신호보다 더 강하기 때문에 위성으로부터 받은 신호를 복원하지 못해 정

확한 위치와 시간을 계산하는데 영향을 줄 수 있다.

재밍은 노이즈 신호가 들어와 위치를 계산할 수 없게 되면 공격으로 탐지한다. 재밍을 방어하기 위한 항재밍를 위해서는 지향성 안테나를 사용하는 방법이 있으나 수신 할 수 있는 위성의 수가 제한될 수 있어 수신기의 성능에 문제를 줄 수 있다.

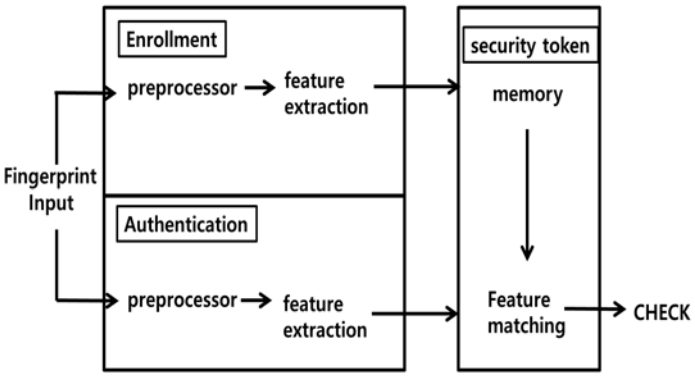
- 전파 위조 공격

위조 공격은 미리 확인된 위성의 위치와 시간을 계산해 위성이 보낸 신호와 같은 신호를 보낸 후 원하는 위치로 위성을 이동하거나 시간을 변경시켜 수신기가 위성으로 받은 신호를 선택하지 않고 공격자가 보낸 신호를 선택하도록 시간과 위치를 조작한다. 이런 공격은 시뮬레이터나 무선 통신 연구용으로 사용되고 있는 USRP와 같은 소프트웨어 라디오 장비를 이용해 비교적 쉽게 구현할 수 있다.

위조 공격의 경우 탐지하기가 어렵기 때문에 다양한 수신기가 수신 정보를 공유함으로써 가능하다고 이론적으로 알려져 있으나 실제 위조 공격 방지는 현재까지 암호화가 가장 많이 사용되는 거의 유일한 수단이다. 복호화용 키가 모든 수신기에 설치되어야 하며, 키가 유출될 위험이 있어 키 관리의 문제가 있다. 때문에 정보의 변경이 불가한 이용자의 생체정보 중 지문을 이용한 암호화 방법을 다음과 같이 제안 하고자 한다.

3. 지문을 이용한 보안 토큰 생성 기법

3.1 보안 토큰 생성 과정

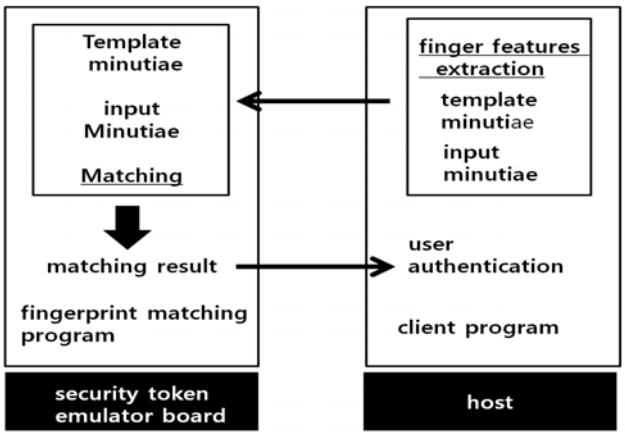


(그림 1) 지문 토큰 시스템

암호화 토큰 생성 시 개인 사용자의 지문 정보를 이용하여 생성을 한다. 지문의 융선과 두 융선 사이의 골을 입력받아 상을 기반으로 하여 높은 보안을 제공하기 위해 인증 과정 자체가 한 보안 토큰 내부에서 수행되어지는 시스템인 Match-on-Token을 이용하여 사용자의 특징을 기반으로 작성된 인증 보안 토큰 시스템을 사용한다.

지문을 사용한 특징 기반의 인증 시스템은 사용자 인증 과정과 사용자 등록과정을 수행한다. 등록은 획득 된 지문 상에서 특징 정보들을 추출하고, 인증 과정은 특징 정보를 입력한 지문영상에서 추출한 후 미리 장된 특징점과 matching을 수행함으로써 저장된 지문과 입력된 지문이 동일한 지문인지를 판단하여 등록, 처리과정을 거친다. 이후 특징을 추출하는 과정을 호스트 컴퓨터에서 수행하고, 등록된 특징을 인증해 새로 입력된 특징 사이의 유사도를 측정하는 특징 매칭 과정을 보안 토큰 내부에서 수행한다. 처리 과정과 특징 추출 과정은 많은 메모리 사용과 명령어 수를 요구 하여 보안 토큰과 같은 제한인 환경에서는 수행이 불가능하다.

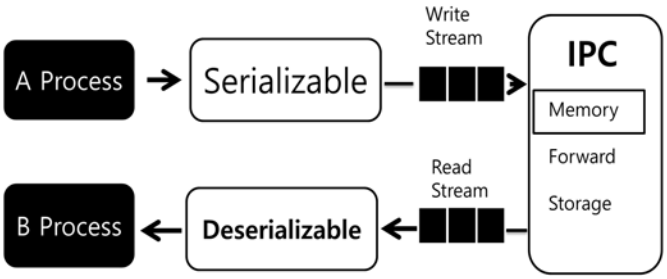
정보보호를 위해 외부로 유출되지 않아야 할 지문으로부터 추출된 특징 정보는 등록 과정에서 보안 토큰에 저장된 특징 정보는 외부로 전달하지 않고 보안토큰 내부에서 정합 과정을 수행한 후 최종 인증 결과만을 호스트로 전송하기여 고유한 개인의 생체 정보가 외부로 유출되지 않도록 한다.



(그림 2) 보안 토큰 시스템 동작도

3.2 보안 토큰 활용 방안

- 보안 전파



(그림 3) Java 직렬화

보안 속성 전파를 사용하면 보안 속성을 전송할 수 있다. WebSphere Application Server는 정적 속성이나 동적 속성을 조회할 수 있는 사용자 모듈에서 보안 속성을 가져올 수 있다. 동적 보안 속성은 연결에 사용할 인증 강도, 호출자의 정보 등을 포함한다. 보안 속성 전파는 Java직렬화 방법에 대한 규칙을 지정, 전파 서비스를 제공한다. 서로 다른 플랫폼 및 소프트웨어 버전을 처리할 때 문제가 발생할 수 있으므로 사용자 정의 직렬화 기능을 사용가능하게 하는 프레임워크를 제공한다. 프레임워크는 만들어진 토큰의 고유성을 식별할 수 있다.

인증할 때는 로그인 모듈에서 로그인 여부를 판별한다. 사용자 정보(지문)를 인증한 후 원격 사용자 레지스트리를 호출하여 사용자 액세스 권한을 표시하는 보안 속성을 찾는 프로세스를 사용 전파 로그인은 사용자 정보의 유효성을 검증한 다음 WebSphere Application Server에 알려진 사용자 정의 오브젝트와 프레임워크를 구성하는 일련의 토큰 직렬화 해제한다. 사용자 정의 토큰의 직렬화 및 직렬화 해제는 구현을 통해 수행되고 사용자 정의 로그인 모듈에 의해 처리되며 접근의 여부를 결정하고자 한다.

- 수평전파

수평 전파에서 직렬화된 보안 속성(전파 토큰)에는 정적 속성과 동적 속성이 포함된다. SSO토큰은 수평 전파에 필요한 시스템 특정 정보를 저장한다. SSO 토큰에 포함된 정보는 위치와 해당 서버와 통신하는 방법을 수신 서버에 알려주며, 직렬화된 속성을 찾기 위한 키도 포함된다. 수평 전파를 사용하려면 SSO토큰 및 보안 속성 전파 기능을 구성해야 하며, 관리 콘솔에서 두 기능을 모두 구성할 수 있다.

수평 전파에서 보안 속성은 서버 간에 전파가 된다. 직렬화된 보안 속성(내용 및 전파 토큰)에는 정적 속성과 동적 속성이 포함되어있다. SSO 토큰은 수평 전파에 필요한 추가 시스템 특정 정보를 저장한다. SSO 토큰에 포함된 정보는 원래 서버가 있는 위치와 해당 서버와 통신하는 방법을 수신 서버에 알려준다. 또한 SSO 토큰에는 직렬화된 속성을 찾기 위한 키를 가지고 있으며, 수평 전파를 사용하려면 SSO 토큰 및 웹 인바운드 보안 속성 전파 기능을 구성해야 한다. 관리 콘솔에서 두 기능을 모두 구성할 수 있다.

주제에 추가된 사용자 정의 SSO토큰은 자동으로 응답에 쿠키로 추가되며 브라우저로 다시 전송되는 속성을 포함한다. 토큰 인터페이스 getName 메소드는 getVersion 메소드와 함께 쿠키 이름을 정의한다. 중요한 정보, 기밀 정보 또는 암호화되지 않은 데이터를 응답 쿠키에 추가하지 않아야 한다.

사용자는 SSO 토큰을 사용하여 한 번의 인증으로 여러 WebSphere Application Server의 자원에 액세스할 수 있다. 사용자 정의 SSO 토큰은 사용자 정의 처리를 SSO 시나리오에 추가하여 이 기능을 확장한다. SSO 토큰에 대한 자세한 정보는 웹 사용자 인증을 최소화하기 위해 싱글 사인온 구현의 내용을 참조할 수 있다.

4. 결론

전파를 직접적으로 이용 하는 사용자들이 급격히 늘면서 집단의 의해서가 아닌 개인 사용자들끼리의 전파 방해 간섭 교란 등 일어나면서 각종 사고들이 빈번하게 일어나고 있지만 개인 사용자들의 가이드라인이나 미흡하여 많은 문제를 야기하고 있다. 문제의 종류와 인과 관계를 통해 이를 보호하고자 하였다. 그 대안으로 본문의 전파 교란과 교섭을 막기 위한 방안으로 생체정보인 지문을 이용한 암호화된 토큰을 만들어 토큰링을 통한 정보의 수신여부를 결정 하여 인증 강도, 호출자의 정보 등을 포함한 동적 보안 속성을 가진 수평 전파를 전송하고 java직렬화와 직렬화 해제 기능을 사용하여 토큰의 고유성 여부를 확인하여 수평전파를 송·수신 해당 문제점을 해결 하고자 제안했다. 하지만 다양한 기기들의 각기 다른 전파의 위협을 모두 충족하기에는 여러 전파 종류와 각기 다른 기기들을 모두 부합하기에는 아직 미흡한 부분이 있어 추후 세밀한 방안을 모색하고 제안하고자 한다.

감사의 글

2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2016R1D1A3B03935976)과 2018년도 산학협동재단 학술연구비 지원사업으로 수행한 결과물임

참고문헌

[1] Dae-Sung Moon, Youn-Hee Gil, Do-Sung Ahn, Sung-Bum Pan, Yong-Wha Chung and Kyo-Il Chung, "Implementation of A Security Token System using Fingerprint Verification," Journal of the Korea Institute of Information Security & Cryptology, Vol. 13, No. 4, pp. 63~70.

[2] Lim, Deok Won,"Case Study of Incidents by GPS Interferences and Trend for Monitoring Techniques," Current Industrial and Technological Trends in Aerospace, Vol. 11, No. 1, pp. 169~176.

[3] Kim Gi Gan, Kim do San and ,"An Analysis of Anti-jamming Capability of Frequency Hopping Satellite Communication Systems", The Journal of Korean Institute of Communications and Information Sciences, Vol. 26, No. 1, pp. 34~41.

[4] Sang-Ho Han, "A Study on certification plan on Radio Frequency Identification for Airplane Use," Aerospace Engineering and Technology, Vol. 7, No. 1, pp. 236~244.