전자 인증에 관한 보증 레벨 요구사항 분석

김준섭*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail:jskim0911@sch.ac.kr, jkwak@sch.ac.kr

Assurance Level Requirement Analysis on Electronic Authentication

Jun-Sub Kim*, Jin Kwak**
*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University
**Department of Information Security Engineering, Soonchunhyang University

요 약

디지털 ID는 온라인 환경에서 사용자를 식별하기 위한 수단으로 사용되고 있다. 하지만 온라인상에 저장된 개인정보 노출뿐만 아니라 신원도용에 따른 사용자의 프라이버시 침해 및 금전적 피해 등으로 이어질 수 있어 이에 대한 관심과 중요성이 높아지고 있다. 따라서 본 논문에서는 전자적인 수단을 통해 정보 시스템에 제시되는 사용자 신원을 확인하는 전자 인증 과정과 신원 인증에 대한 보증 레벨별 요구사항을 마련하고 있는 NIST SP 800-63을 분석하고자 한다.

1. 서론

최근 발생한 7.7 DDoS 사이버 침해사고의 피해에 따른 사회적 파장이 커지면서 사이버 보안의 중요성 및 사이버 테러 대응방안의 필요성이 요구되고 있다. 사이버 위협은 21세기 경제와 국가안보에 대한 가장 심각한 위협요인 중 하나로 등장하고 있다. 이에 따라 미국, 영국, 일본 등 전 세계적으로 사이버 보안 및 정보보호의 중요성에 대한 인식이 확산되고 있으며, 해외 주요국은 강력한 정부 리더십을 강조하면서 종합적인 사이버보안 국가 전략을 수립하고 있다.

또한 디지털 환경의 급속한 발달과 함께 개인 신원을 식별하기 위한 수단으로 디지털 ID를 사용하게 되면서 사용자의 프라이버시 침해, 신원도용 등 피해가 확산되고 있다. 이에 따라 디지털 ID에 대한 피해 방지를 위해 디지털 ID 관리 기술이 대두되고 있으며, 디지털 ID 관리 서비스에 대한 강한 인증 기술 개발이 활발하게 진행되고 있다[1].

NIST SP 800-63(전자 인증 지침)에서는 전자 인증 과정, 토큰 및 인증에 대한 위협요소, 인증 메커니즘에 대한 레벨별 요구사항을 정의하고 있다. 또한 크리덴셜 발급기관의 신뢰성 평가, 크리덴셜 발급 및 검증 솔루션에 대한 상호운용 시험을 수행한다[2].

따라서 본 논문에서는 전자 인증에 관한 보증 레벨 요구사항을 분석하기 위해서 2장에서 전자 인증의 개요에 대해서 기술하고, 3장에서는 인증 메커니즘의 보증 레벨 요구사항을 기술한다. 마지막으로 4장에서 결론을 맺는다.

2. 전자 인증

전자 인증은 전자적인 수단을 통해 정보 시스템에 제시되는 사용자 신원의 신용을 확인하는 과정이다. OMB 지침에서는 인증 에러와 크리덴셜(Credential)의 오용 결과에 따라 레벨 1~4의 4가지 보증레벨을 정의하고 있다. 레벨 1은 최소 보증 레벨이며, 레벨 4는 최고 보증 레벨이다[3].

신청자는 등록기관(RA : Registration Authority)에 등록 신청을 하고, RA는 해당 신청자에 대한 신원 검증(Identity proofing)을 실시한다. 신원 검증의 결과에 문제가 없으면, 신청자는 RA와 연계하고 있는 크리덴셜 서비스 제공자(CSP : Credential Service Provider)의 가입자가 되어 크리덴셜과 비밀 토큰을 가입자 정보에 등록하게 된다. 가입자는 트랜잭션(Transaction)을 수행하기 위한 인증을 필요로 할 때, 검증자(Verifier)에 대한 인증 요청자(Claimant)가 된다. 인증 요청자는 검증자에게 인증 프로토콜을 통해 자신이 토큰을 관리하고 있다는 것을 증명한다. 검증자가 RP(Relying Party)에서 분리되어 있는 경우, 검증자는 인증 요청자에 관한 검증조건(Assertion)을 RP에게 제공한다[4].

3. 인증 메커니즘의 보증 레벨 요구사항

SP 800-63에서는 4개의 보증 레벨을 정의하고 있다. 레벨 4가 가장 높은 레벨의 인증 보증을 제공하고, 레벨 1은 가장 낮은 레벨의 인증 보증을 제공한다. 다음 <표 1>과 <표 2>는 보증 레벨에서 사용할 수 있는 토큰의 유형과 보증 레벨에 따른 공격별 보호 수준을 나타낸다.

<표 1> 보증 레벨에서 사용할 수 있는 토큰 유형

토큰 유형	레벨 1	레벨 2	레벨 3	레벨 4
하드웨어 암호 토큰	√	√	√	√
1회용 패스워드 장치	√	√	√	
소프트 암호 토큰	√	√	√	
패스워드 및 개인 식별 번호	√	√		

<표 2> 보증 레벨에 따른 공격별 보호 수준

공격 유형	레벨 1	레벨 2	레벨 3	레벨 4
온라인 추측 공격	√	√	√	√
재생 공격	√	√	√	√
도청 공격		√	√	√
검증자로 위장 공격			√	√
중간자 공격			√	√
세션 하이재킹 공격				√

3.1 레벨 1

레벨 1에서는 다양한 인증 기술을 사용할 수 있고, 레벨 2, 3, 4의 토큰 방식을 이용하는 것이 허용된다. 인증을 성공하기 위해서는 보안 인증 프로토콜을 통해 인증 요청자가 토큰을 관리하고 있다는 것을 증명해야 한다. 레벨 1의 요구사항을 충족시키는 일반적인 프로토콜은 APOP [RFC 1939], S/KEY [SKEY], Kerberos [KERB]가 있다.

구분	설명
검증조건	· 신뢰할 수 있는 엔티티에 의해 디지털 서명된 것 · 신뢰할 수 있는 엔티티가 직접 가져온 것
공유 비밀정보 보호	· 패스워드 파일에 일방향 해시 처리 · 레벨 2, 3, 4에서 보호 수단으로 허용되는 모든 방법을 사용 가능
패스워드 강도	2^{-10}(1,024분의 1)

3.2 레벨 2

레벨 2에서는 다양한 인증 기술을 사용할 수 있고, 레벨 3, 4의 토큰 방식을 이용하는 것이 허용된다. 패스워드의 사용도 마찬가지이다. 인증 요청자가 인증에 성공하려면, 보안 인증 프로토콜을 통해 인증 요청자가 토큰을 관리하고 있다는 것을 증명해야 한다.

구분	설명
크리덴셜/토큰의 유효기간, 상태, 폐기	· CSP는 크리덴셜/토큰이 유효여부를 통지하고, 72시간 이내에 크리덴셜/토큰을 폐기 · 검증자 또는 RP는 사용하는 크리덴셜이 유효여부를 검증
검증조건	레벨 1과 동일 (검증자에 의해 생성된 검증조건은 12시간 후 만료)
공유 비밀정보 보호	· 패스워드를 salt 등에 연결한 후 해시함수 처리 · 승인된 암호 알고리즘을 사용하여 암호화된 형태로 저장
패스워드 강도	2^{-14}(16,384분의 1)

3.3 레벨 3

레벨 3의 인증은 암호화 프로토콜을 사용하여 암호 키를 가지고 있다는 것을 증명한다. 레벨 3의 인증 보증은 기본 인증 토큰을 다양한 프로토콜 위협에 의한 위험으로부터 보호하는 높은 강도를 가진 암호 메커니즘이 필요하다. 또한 레벨 3에서는 2가지 요소의 인증도 필요하다. 키 이외에 사용자는 키를 활성화하기 위하여 패스워드 또는 바이오인식 정보를 이용해야 한다.

구분	설명
크리덴셜/토큰의 유효기간, 상태, 폐기	· CSP는 크리덴셜/토큰을 24시간 이내에 폐기시키는 절차에 대비 · 검증자는 크리덴셜/토큰이 새로 발급되거나 유효여부를 검증
검증조건	레벨 1과 동일 (검증자에 의해 생성된 검증조건은 2시간 후 만료)
공유 비밀정보 보호	· 암호키는 FIPS 140-2 레벨 2이상을 충족 · 공유 비밀정보는 FIPS 140-2 레벨 2이상을 충족

3.4 레벨 4

레벨 4는 원격 네트워크 인증에 대한 최대 보증을 제공하는 것을 목적으로 한다. 레벨 4의 인증은 암호 프로토콜을 통해 키 소지를 증명한다. 레벨 4는 레벨 3과 비슷하지만, 하드웨어 암호 토큰만 허용된다.

구분	설명
크리덴셜/토큰의 유효기간, 상태, 폐기	· CSP는 크리덴셜을 24시간 이내에 폐기시키는 절차에 대비 · 검증자 또는 RP는 크리덴셜이 새로 발급되거나 유효여부를 검증
공유 비밀정보 보호	레벨 3과 동일

4. 결론

본 논문에서는 NIST SP 800-63에 제시된 전자 인증 과정, 보증 레벨에서 사용할 수 있는 토큰 유형, 보증 레벨에 따른 공격별 보호 수준, 인증 메커니즘의 보증 레벨 요구사항을 분석하였다.

인증 메커니즘의 보증 레벨은 전자 인증에 사용되는 크리덴셜, 검증조건, 비밀정보 등의 정보와 신원 인증 방식에 따라 다양한 프로토콜 위협을 방지하고 있다. 디지털 ID 관리 서비스에 인증 메커니즘의 보증 레벨 요구사항을 도입하여, 신원 인증 방식에 따른 레벨별 기준을 마련함으로써 사용자의 프라이버시 침해, 신원도용 등 물리적·금전적 피해를 줄이는데 도움이 될 것이다.

참고문헌

[1] 진승헌외, “인터넷 ID 관리 서비스-2006년 기술 백서”, ETRI 디지털ID 보안연구팀, 2006.

[2] 진승헌외, “Digital Identity Management-2007년 기술 백서”, ETRI 디지털ID 보안연구팀, 2007.

[3] OMB, M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003.

[4] NIST, SP 800-63, Electronic Authentication Guideline, April 2006.