情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

One-time 템플릿 기반의 바이오 인증 프레임워크 표준

정 윤 수*, 이 용 진**, 이 형 우***, 문 기 영****

요 약

최근 인터넷에 의한 전자 상거래, 전자 정부 등 정보통신 인프라가 널리 보급되고, 이를 통한 서비스가 보편화됨에 따라 패스워드나 PIN을 대신할 수 있는 바이오인식 기술에 대한 관심이 증대되고 있다. 하지만, 개방형 네트워크 환경에서 바이오 인식 기술은 바이오 정보의 유출/오용등 기존 시스템에서와 다른 문제들을 내포하고 있다. 특히, 바이오인식 정보는 비밀 번호나 PIN과 같이 사용자가 임의로 변경할 수 없으므로 외부로 유출된다면 심각한 문제가 발생할 수 있다. 본고에서는 네트워크를 통해 전송되는 바이오인식 정보를 안전하게 보호하고, 전송 도중 유출된 템플릿을 이용한 재사용 공격을 막기 위한 한 방법으로써 One-time 템플릿에 기반한 바이오 인증 서비스 프레임워크 표준에 관해 소개 한다.

Ⅰ. 서 론

바이오 인식은 개인의 신체적/행동학적 특징을 이용하는 사용자 인증 기술이다. 사용자 인증에 사용되는 바이오 인식 데이터는 개인마다 고유하며, 오랜 시간 동안 변하지 않으며, 타인과 공유할 수 없다는 특성이 있어, 바이오 인식은 가장 이상적인 인증 기술이라고 볼 수 있다. 하지만 동전의 양면처럼, 바이오 인식 데이터의 이러한 장점은 다른 한편으로는 치명적인 약점이 될 수도 있다. 바이오 인식 정보는 개인의 고유한 정보이므로 유출 시 심각한 프라이버시 침해를 가져 올 수 있다. 또한 매우 적은 수의 대체 정보만이 존재하기 때문에, 일반적인 비밀 번호 유출과 달리, 유출된 바이오 인식 정보를 대신하여 적법한 형태의 새로운 바이오인식 정보를 생성/변경하는 것은 매우 힘들다.

특히 인터넷과 같은 네트워크 기반 서비스 환경으로 발전하면서, 바이오 인식 시스템 또한 단일 시스템으로 구성되는 방식에서, 서버와 클라이언트로 구성되는 방식으로 변경되는 추세이다. 하지만, 인터넷 같은 네트워크는 개방성을 추구하여 누구나 쉽게 접속할 수 있기 때문에, 전송 도중에 데이터가 유출 될 수 있을 뿐만 아니라, 보안에 많은 허점이 생길 수 있다. 일례로, 클라이언트나 서버를 직접 해킹하지 않고, 인터넷을 통해 전송되는 비밀 번호를 중간에 획득하여 추후에 이를 이용하여 불법적으로 사용자 인증을 받는데 사용할 수도 있다. 이러한 재전송 공격(replay attack)은 네트워크를 통해 전송되는 바이오인식 정보에도 그대로 적용될 수 있으며, 앞서 언급하였듯이 그 결과는 일반적인 비밀번호 유출보다 더욱 심각하고 위협적이라고 할 수 있다.

본 표준에서는 클라이언트에서 서버로 전송되는 사용자의 바이오 인식 템플릿 보호하고 보다 안전한 사용자 인증이 이루어 질 수 있도록, One-time 템플릿 기반의 바이오 인증 프레임워크를 정의한다. One-time 템플릿은 매 인증 시마다 새로운 변환된 템플릿을 네트워크 전송 및 사용자 인증에 사용한다. 따라서 원본 템플릿의 노출을 최소화할 뿐만 아니라, 재전송 공격을 효과적으로 방지할 수 있다.

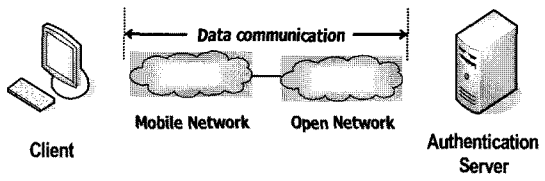
This work was supported by the IT R&D program of MKE/IITA [2007-S-020-02, Development of Privacy Enhanced Biometric System]

* 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀 (yoonsu@etri.re.kr)
** 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀 (solarone@etri.re.kr)
*** 한신대학교 소프트웨어학과 (hwlee@hs.ac.kr)
**** 한국전자통신연구원 융합보안그룹 바이오인식기술연구팀 (kymoon@etri.re.kr)

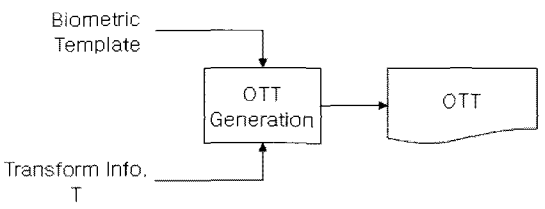
Ⅱ. One-time 템플릿을 이용한 바이오인식 프레임워크

본 표준의 One-time 템플릿 기술은 바이오 인식 템플릿을 네트워크를 통해 전송할 때 발생할 수 있는 보안 취약점을 보강하는데 있다. 즉, 인증 시스템은 [그림 1]과 같이 인증 클라이언트와 인증 서버로 이루어져 있다고 가정한다.

인증 템플릿은 클라이언트에서 생성되어 네트워크를 통해 인증 서버로 전송되고, 사용자 인증을 위한 템플릿 매칭, 즉 인증 템플릿과 등록 템플릿 비교는 인증 서버에서 이루어진다. 따라서 네트워크를 통해 전송되던 사용자의 바이오인식 템플릿이 유출될 경우, 사용자 바이오 인식 정보 노출로 인한 프라이버시 침해가 발생할 수 있으며 유출된 템플릿은 재사용 공격(replay attack)에 이용될 수 있다. 따라서 사용자 바이오 인식 정보 노출을 최소화하기 위해, 클라이언트는 변환함수를 이용하여 원본 템플릿을 변형하고, 변환된 템플릿(transformed template)을 인증 서버에 전송한다. 그리고 인증서버는 클라이언트로부터 수신된 변환된 템플릿과 인증 서버에 저장된 변환된 템플릿을 비교하여 사용자 인증을 수행한다. 즉, 인증서버에는 원본 템플릿이 아닌 변환된 등록 템플릿이 저장되어 있어야 하며, 인증서버에는 원본 템플릿을 복원할 수 있는 어떠한 정보도 저장되어 있어서는 안 된다. 또한, 매 인증 시 마다, 새로운 변환 함수를 이용하여 새로운 템플릿을 생성하여 사용자 인증에 이용함으로써, 유출된 템플릿을 이용한 재사용 공격을 방지 한다.



〔그림 1〕 One-time 템플릿 동작 환경

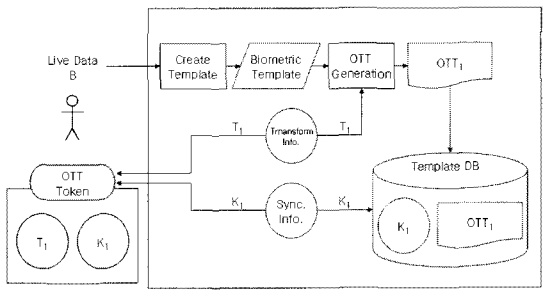


〔그림 2〕 One-time 템플릿 생성

변형된 템플릿 또는 One-time 템플릿은 입력 템플릿으로부터 변환 함수를 이용하여 생성되며, 동일한 입력 템플릿이 사용된다 하더라도, 변환 함수에 따라 서로 다른 템플릿이 생성된다. 매 인증 시 마다, 새로운 변환 함수를 이용하여 새로운 템플릿을 생성함으로써, One-time 템플릿을 생성할 수 있다. One-time 템플릿은 [그림 2]와 같이 바이오 인식 템플릿과 변환 함수 정보에 의해 생성된다. 사용자 인증 시, 유효한 One-time 템플릿을 생성하여 정당한 사용자로 인증 받기 위해서, 사용자는 자신의 바이오 인식정보와 함께 변환 함수 정보를 같이 제공해야 한다.

- Biometric Template : 사용자의 바이오 인식 특징 값을 담고 있다.
- Transform Info. : 사용자 바이오 인식 정보 노출을 최소화하기 위해, 사용자 바이오 인식 정보로부터 직접 생성된 원본 템플릿 대신, 원본 템플릿으로부터 생성된 변환된 템플릿(transformed template)을 네트워크 전송 및 사용자 인증에 사용한다. Transform Info.는 원본 템플릿을 보호하기 위한 변환 함수 생성에 관련된 정보를 의미한다.
- OTT Generation : 입력 템플릿과 변환 함수 정보를 이용하여 변환된 템플릿 또는 One-time 템플릿을 생성한다.

[그림 3]은 사용자 등록 과정 또는 사용자(또는 클라이언트)와 인증 서버 사이의 초기 동기화 과정을 나타낸다. 사용자는 자신의 바이오 인식 데이터를 제공하고, 시스템은 무작위로 서로 독립되게 Transform Info.와 Sync. Info.를 생성한다. 그리고 바이오 인식 데이터와 Transform Info.를 이용하여 등록용 One-time 템플릿을 생성하고, Sync. Info와 함께 Template DB에 저장

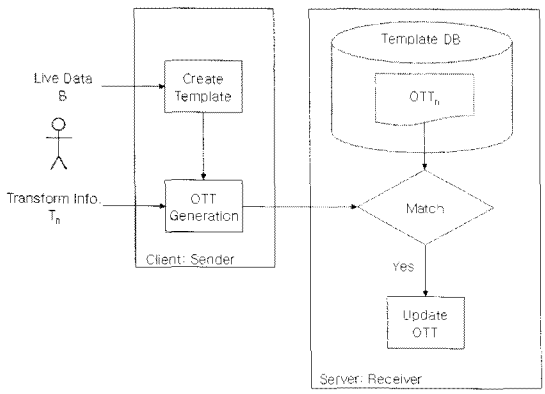


〔그림 3〕 사용자 등록 및 초기화

한다. 그리고 시스템은 사용자에게 Transform Info.와 Sync. Info.가 저장된 개인용 토큰(token)을 발급한다. 이 때, 서버에 저장된 Sync. Info.와 One-time 템플릿으로부터 사용자의 원본 템플릿(Biometric Template)을 유추할 수 없어야 한다.

- Live Data : 사용자로부터 제공된 원본 바이오 인식 데이터(raw biometric data)를 의미한다.
- Create Template : 사용자로부터 취득된 바이오 인식 데이터로부터 바이오 인식 템플릿을 생성한다.
- Sync. Info. : 클라이언트와 서버 사이의 동기화를 위한 정보이다. 인증이 성공적으로 완료 될 때마다, 이 정보를 이용하여 새로운 Transform. Info.와 One-time 템플릿을 생성한다.
- Template DB : One-time 템플릿과 Sync. Info.를 저장하는 데이터베이스로, 서버 측에 속한다.
- OTT Token : Transform Info.와 Sync. Info.를 저장하는 장치로 사용자 또는 클라이언트 측에 속한다.

[그림 4]는 One-time 템플릿을 이용한 n번째 인증 과정을 나타낸다. 사용자는 자신의 바이오 인식 데이터를 변환 함수 정보가 저장된 개인 토큰과 함께 클라이언트에 제공한다. 클라이언트는 사용자로부터 제공 받은 정보를 이용하여 One-time 템플릿을 생성하여 서버에 전송한다. 서버는 클라이언트로부터 전송 받은 One-time 템플릿과 Template DB에 저장된 템플릿을 비교하여 사용자 인증을 수행한다. 템플릿 비교를 통해 정당한 사용자로 인증되면, 서버는 Template DB에 저장된 One-time 템플릿을 새로운 템플릿으로 갱신한다.

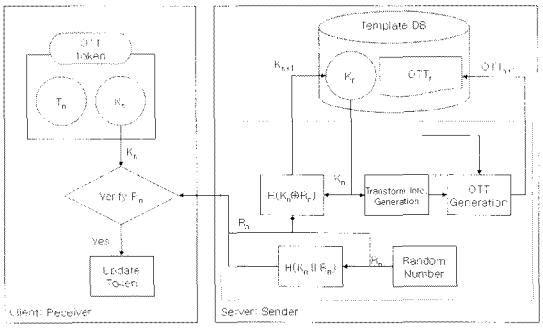


〔그림 4〕 One-Time 템플릿을 이용한 사용자 인

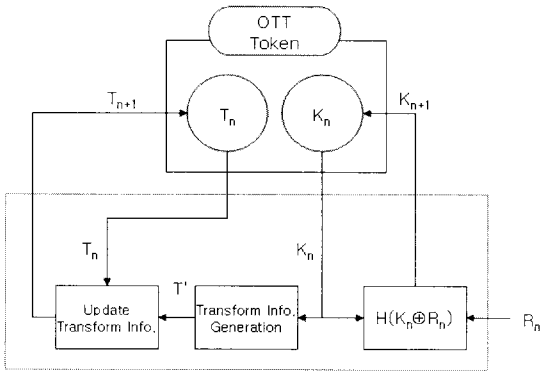
- Match : 클라이언트로부터 전송 받은 템플릿과 Template DB에 저장된 템플릿을 비교하여 사용자 인증을 수행한다.
- Update OTT : 템플릿 비교를 통해 정당한 사용자로 인정되면, Template DB에 저장된 One-Time 템플릿과 Sync. Info.를 갱신한다.

[그림 5]는 n번째 인증이 성공적으로 이루어졌을 경우, Template DB에 저장된 Sync. Info. Kn을 K_{n+1}로, One-time 템플릿 OTT_n을 OTT_{n+1}로 갱신하는 과정을 나타낸 것이다. 새로운 One-time 템플릿 OTT_{n+1}은 Sync. Info. K_n로부터 생성된 변환함수 정보 T'와 이전 인증에 사용된 One-time 템플릿 OTT_n으로부터 생성된다. 그리고 난수 R_n을 이용하여 Sync. Info. K_n를 갱신하고, R_n을 클라이언트로 전송한다. 클라이언트는 전송 받은 R_n의 유효성을 검사한 다음, OTT Token에 저장된 정보를 갱신한다.

- Transform Info. Generation : Sync. Info. K_n으로부터 Transform Info. T'를 생성한다.
- Random Number : 난수를 나타내며, K_n를 갱신하는데 이용된다.
- $H(Kn \oplus Rn)$: K_n와 R_n의 배타적 합(Exclusive OR)에 대한 해시 값을 나타난다. K_n를 $H(K_n \oplus R_n)$로 대체한다. K_{n+1} : $=H(K_n \oplus R_n)$.
- $H(Kn \| Rn)$: 서버에서 클라이언트로 전송된 R_n에 대한 유효성을 검사하기 위한 정보로 K_n와 R_n의 연결 연산(Concatenation) 값에 대한 해시 값을 나타낸다.
- Verify R_n : 클라이언트는 OTT Token에 저장된 K_n와 서버로부터 전송 받은 R_n을 이용하여 $H(K_n \| R_n)$를 계산하고, 이를 서버로부터 전송 받은



〔그림 5〕 One-Time 템플릿 갱신



〔그림 6〕 OTT Token 갱신

$H(K_n \| R_n)$와 비교하여 Rn의 유효성을 검사한다.

- Update Token : R_n이 정당한 서버로부터 전송된 것이 확인 되면, OTT Token에 저장된 정보를 갱신한다.

[그림 6]은 사용자 인증이 성공적으로 이루어졌을 경우, OTT Token에 저장된 Transform Info. T_n와 Sync. Info. K_n를 갱신하는 과정을 나타낸 것이다.

- Update Transform Info. : OTT Token에 저장된 T_n그리고 K_n로부터 생성된 T'를 이용하여 T_{n+1}을 생성하고 기존 값을 대체한다.

Ⅲ. 템플릿 기반 사용자 인증에 대한 보안 요구 사항

본 장에서는 One-time template을 이용한 사용자 등록과 인증 그리고 시스템 환경 및 운영에 관한 보안 요구 사항을 기술한다.

- 최초 사용자 등록은 관리자와의 직접 대면을 통해 오프라인(off-line)으로 이루어지도록 한다.
- 정당한 사용자로 인증 받기 위해서, 사용자는 본인의 바이오 인증 정보와 토큰을 인증 시스템에 함께 제공해야 한다.
- 사용자 토큰이 유실되었다 하더라도, 사용자 인증에 대한 오수락 가능성이 높아져서는 안 된다.
- 클라이언트와 서버 사이에서 전송되는 one-time 템플릿과 데이터로부터 사용자의 원본 템플릿을 유추할 수 없어야 한다.
- 이전 one-time template은 더 이상 인증에 사용될 수 없도록, 매 인증 시 새로운 템플릿을 생성해야 한다.
- 서로 다른 변환 함수 정보가 사용될 경우, 동일한 입력 템플릿으로부터 전혀 다른 one-time 템플릿이 생성되어야 한다.
- 클라이언트 또는 사용자 측의 one-time 템플릿은 가능하면 사용자 토큰 내에서 생성되도록 한다.
- 사용자 토큰은 토큰에 저장되는 데이터에 대한 적절한 보호 기능을 갖추고 있어야 한다.
- 클라이언트는 사용자의 바이오 정보와 기타 사용자 정보 및 서버로부터 전송된 데이터를 저장해서는 안 된다.
- 클라이언트는 사용자 인증을 종료한 즉시, 관련 모든 데이터를 삭제해야 한다.
- 인증 서버는 사용자의 원본 바이오 템플릿을 보관 및 저장해서는 안 된다.
- 인증 서버에 등록된 템플릿과 기타 데이터로부터 사용자의 원본 템플릿을 유추할 수 없어야 한다. 사용자의 원본 템플릿을 직접적으로 유추할 수 있는 데이터를 저장해서는 안 된다.

Ⅳ. 결 론

본 고에서는 네트워크를 통해 전송되는 바이오인식 정보를 안전하게 보호하고, 전송 도중 유출된 템플릿을 이용한 재사용 공격을 막기 위한 한 방법으로써 One-time 템플릿에 기반한 바이오 인증 서비스 프레임워크 표준에 관해 소개 하였다. 그리고 one-time 템플릿의 생성, 갱신, 운용 방법 등에 대한 모델 제시뿐만 아니라, 이를 이용한 사용자 인증시의 보안 요구사항을 함께 기술하였다. 이러한 관련 기술/표준들은 개방형 네트워크 환경에서 바이오인식기술의 응용시 발생할 수 있는 많은 보안상의 문제들을 해결할 수 있을 뿐만 아니라, 관련 산업의 활성화에도 기여할 수 있을 것으로 사료된다.

참고문헌

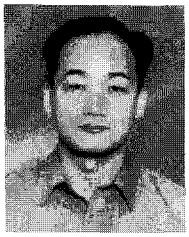
[1] 이용진, 이형우, 정윤수, "X.ott : Biometric Authentication Framework Based on One-time Template", ITU-T, 2008년 4월

[2] TTA PG505 바이오인식 프로젝트그룹, "One-time 템플릿 기반 바이오 인증 프레임워크", 2008년 7월

[3] 정윤수, 정성욱, 문기영, "개방형 네트워크 환경에

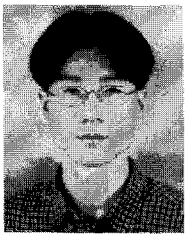
서의 바이오인식 융합 기술", 정보보호학회 학회지, 2007년 10월
[4] 정윤수, "텔레바이오인식 융합기술 및 국제 표준화 동향", IT Forum 2007, TTA, 2007.04.19
[5] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems : Issues and challenges", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, vol. 92, no. 6, pp.948-960, June 2004.

〈著者紹介〉



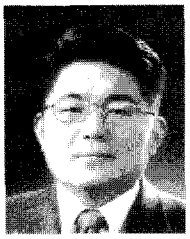
정 윤 수 (Yun Su Chung)
정회원

1993년 2월 : 경북대학교 전자공학과 졸업
1995년 2월 : 경북대학교 전자공학과 석사
1998년 8월 : 경북대학교 전자공학과 박사
1999년~현재 : 한국전자통신연구원 바이오인식기술연구팀, 선임연구원
<관심분야> 바이오인식, 정보보호, 영상처리



이 용 진 (Yongjin Lee)
비회원

2002년 2월 : 한양대학교 전자·컴퓨터·전기·제어공학부 졸업
2004년 2월 : 포항공과대학교 컴퓨터공학과 석사
2004년 3월~현재 : 한국전자통신연구원 바이오인식기술연구팀, 연구원
<관심분야> 바이오인식, 패턴인식, 기계학습



이 형 우(Hyung-Woo Lee)
회원

1994년 2월 : 고려대학교 컴퓨터학과 졸업
1996년 2월 : 고려대학교 컴퓨터학과 석사
1999년 2월 : 고려대학교 컴퓨터학과 박사
2003년 3월~현재 : 한신대학교 소프트웨어학과 부교수
<관심분야> 바이오인식, 정보보호, 바이오정보 보호

문 기 영 (Ki Young Moon)
종신회원

1986년 2월 : 경북대학교 전자공학과 학사
1989년 2월 : 경북대학교 전산학 석사
2006년 2월 : 충남대학교 전산학 박사
1994년~현재 : 한국전자통신연구원 바이오인식기술연구팀, 팀장
<관심분야> 바이오인식, 정보보호, 웹서비스보안