情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

바이오메트릭스 정보보호 가이드라인

김 재 성*, 신 용 녀*, 김 학 일**

요 약

신원확인을 위하여 생체정보를 수집하거나, 이용하는 데 있어서 준수하여야 할 생체정보 보호대책에 관한 중요사항을 정함으로써 생체정보의 안전한 이용 환경을 조성하고, 개인의 권리와 이익을 보호하는 것을 목적으로 한다. 본고에서는 유무선 통신환경에서 생체정보가 수집·저장·전송·폐기 전 과정에서 발생 가능한 취약점과 위협을 정의하고, 이에 대한 기술적·관리적 보호대책에 대한 가이드라인을 제시하고자 한다. 한편, ITU-T, ISO 등 국제 표준 및 국내 TTA 단체 규격 등과 호환 가능하도록 보안대책을 제시함으로서 국가 간의 생체정보에 대한 보호조치 방안에 관하여 상호 연동성을 보장한다. 본고는 유비쿼터스 환경에서 생체인식 국가인프라가 구축되는 시점에서 발생할 수 있는 생체정보에 대한 불신감과 인권침해 등의 사회적인 논란을 최소화하고 개인의 생체정보 보호기술의 발전과 관련 응용서비스 활성화에 기여할 것이다. 또한 전자여권·선원신분증·국제운전면허증·전자주민증 등 공항·항만·육로의 출입국관리에 생체정보의 활용이 전 세계적으로 보급 확산되는 시점에서 생체정보 활용 및 생체인식시스템에 대한 신뢰성을 제공함으로서 국내 생체인식산업의 활성화에 기여할 수 있다고 기대한다.

Ⅰ. 서 론

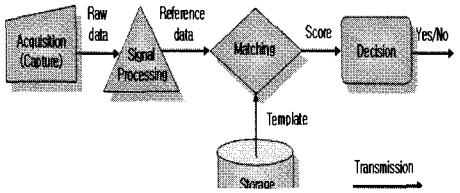
최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다. 최근 들어 개인정보의 유출과 남용 등 피해가 잇따라 생체정보를 포함한 개인정보 보호의 중요성에 대한 사회적 인식이 커지고 있다. 동시에 국내외적으로 개인정보를 이용한 산업부문이 확대돼 가고 있어 산업발전이라는 측면에서 이를 뒷받침해 줄 수 있는 적절한 법적·제도적 장치가 시급한 실정이다. 사이버 공간이 안전지대가 아니라는 사실을 우리는 수차례의 인터넷 뱅킹 사고, 사이버머니 해킹 등을 통해서 알고 있다. 그런 위험을 해소하기 위해 우리는 정보보호시스템을 구축해왔고 특히 전자거래에서 스마트카드나 전자서명을 이용한 공인인증서 등을 사용하고 있다.

더 나아가 안전성을 더욱 강화하기 위하여, 생체인식 기술이 최근 각광을 받고 있는 것이 보안 분야의 한 추세다. 지문·홍채·얼굴인식 등 생체인식 기술은 사람의 고유한 신체적 특징을 이용하기 때문에 기존 신원확인 수단보다 정확하고 편리하다는 장점이 있다. 선진국에서는 국가 및 국방 등 주요시설에 대한 출입통제 목적으로 활용된 지 오래되었으며 점차 상업목적으로 근태관리, 의료 정보관리 등 정확한 신원확인절차가 필요한 분야로도 활용되고 있다. 다방면에서 생체인식기술의 활용이 필요하게 됨에 따라 이에 적극대처하기 위해 KISA에서는 신속히 민·관·산·학·연이 참여하는 생체인식 실무협의회를 구성·운영 중에 있고, 이를 통하여 정보통신부에서는 생체인식 관련 법제도 정비, 한국생체인식시스템시험센터(K-NBTC) 설립·운영, 기술개발 및 표준화 로드맵, 시범사업 발굴 등을 위한 「생체인식 종합인프라 구축 계획」을 수립하고 있다. 특히, 서울대 기술사 정맥인식기 도입, 전북학교 급식시설에 지문인식기 설치 등 생체정보의 무분별한 수집과 오·남용에 대한 우려에 대하여 근원적인 보호대책 마련이 필요하다.

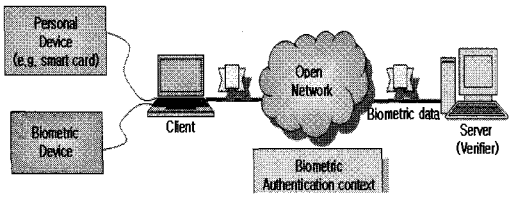
Ⅱ. 델리바이오메트릭시스템 취약점과 위협

생체정보를 위한 기술적 보호조치를 취하는 첫 단계는 보호하고자 하는 대상과 규모를 정확하게 파악하는

* 한국정보보호진흥원 (jskim ynshin ychungy@korea.ac.kr)
** 인하대학교 정보통신공학과 (hikim@inha.ac.kr)



〔그림 1〕 생체인식시스템의 프로세스

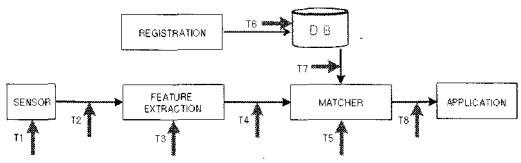


〔그림 2〕 통신상의 텔리바이오메트릭시스템 구성

것이다. 보호하고자하는 대상과 규모를 정확히 파악한 후, 생체정보 정책을 수립하는 것이 두 번째 단계라고 볼 수 있다. 기술적 보호조치가 보호정책에 반영되기 위해서는 제안된 정책을 모두 이해하고 이를 구현할 수 있는 기술요원과 이 정책을 시행할 권한을 가지고 있는 의사 결정자가 함께 참여하여 작업하여야 한다.

개인의 생체정보는 영원히 변하지 않는다는 것이 프라이버시 문제의 시작이다. 즉, 한번 유출된 생체정보에 대한 피해의 심각성이 크기 때문에, 가능한 모든 공격에 대해서 강인성(Robust)을 가져야 하는 반면에 생체정보 변형에 따른 복잡성으로 인해 성능에 현격한 저하가 없어야 한다. 생체정보의 강인성이란 다양한 입력 장치를 고려한 환경 변화 및 주위 잡음 그리고 연령 및 세월의 변화에 강인함을 가져야 함을 의미한다. 생체정보 유출 방지 차원에서 생체인식시스템을 설치하거나 구성하는데 있어 원래 계획되었던 검증 또는 인증 관련 기능보다 더 복잡하거나 광범위한 범위를 수행하고자 할 경우 생체정보 감사자의 감사하에 이루어지도록 하고 그 결과 또한 외부에 공개하는 것이 좋다. 일반적인 생체인식시스템의 프로세스는 다음의 그림 1과 같다.

센서 등의 생체 디바이스에서 생체정보를 획득한 후 신호처리를 통하여 특징을 추출하는 단계가 공통적으로 포함된다. 이를 기반으로 사전에 동일한 단계를 통하여 변환되어 저장된 데이터베이스 내의 생체정보와 비교하여 결과를 결정하는 단계로 구성된다. 그림 2는 네트워크망을 통한 텔리바이오메트릭시스템(Tele-biometric System)을 설명한 것으로 클라이언트에서는 개인의 정보와 생체정보를 획득하여 위에서 설명된 생체인식 단계가 탑재된 서버로 전송하는 구성도를 나타낸 것이다.



〔그림 3〕 텔리바이오메트릭시스템의 위협요소

1. 텔리바이오메트릭시스템 취약점과 위협요소

상기에 설명된 텔리바이오메트릭시스템의 처리 단계에서 발생가능한 위협요소를 도식화하면 그림 3과 같다.

텔리바이오메트릭시스템의 처리 단계에서 발생 가능한 위협요소(Threat)를 다음과 같이 정의하고자 한다.

T1 : 생체 입력 디바이스 공격
T2 : 생체인식 샘플을 생체인식 템플릿 추출부로 전송하는 과정간의 공격
T3 : 생체인식 템플릿 추출부 공격
T4 : 추출된 생체인식 템플릿을 인증부로 전송하는 과정간의 공격
T5 : 인증부 공격
T6 : 생체정보 데이터베이스 공격
T7 : 생체정보 데이터베이스를 인증부로 전송하는 과정간의 공격
T8 : 인증부로부터 나온 결과를 전송하는 과정간의 공격

한편, 그림 3의 텔리바이오메트릭시스템 구성요소에 있어서 다음과 같은 취약점(Weakness)이 있을 수 있다.

W1 : 생체정보 입력장치(Device)
W2 : 텔리바이오메트릭시스템 전송(Transmmision)
W3 : 텔리바이오메트릭시스템(System)
W4 : 생체정보 저장(Collection)
W5 : 생체정보 DB 사용자 인증(Authentication)
W6 : 생체정보 DB의 조작 및 변경(DB Manipulation & Alternation)
W7 : 생체정보 특징점 추출(Feature Extractor)
W8 : 생체정보 인식알고리즘(Matcher)
W9 : 생체정보 특징점 전송(Feature Transmmision)

W10 : 생체정보 위변조 체크(Checking)
W11 : 생체정보 암호화(Encryption)
W12 : 생체인식 템플릿(Biometric Template)
W13 : 키관리(Key Management)
W14 : 생체정보 파기(Destruction)

2. 생체인식 프로세스와 연관관계

상기에서 정의한 텔리바이오메트릭시스템 구성요소에 있어서의 위협요소와 그림 1의 생체인식시스템 프로세스간의 연관성에 관하여 표 1에서 나타내고 있다.

한편, 상기에서 정의한 텔리바이오메트릭시스템 구성요소에 있어서의 취약점과 그림 1의 생체인식시스템 프로세스간의 연관성에 관하여 표 2에서 나타내고 있다.

Ⅲ. 텔리바이오메트릭시스템 보안대책

1. 생체정보 입력장치(Device) 보호대책

(1) 생체인식시스템은 현재 사용되고 있는 디바이스에 고유한 값을 저장해 두거나 하는 방법을 이용해 사용하기 전에 그 값을 검사해 디바이스가 다른 외부의 누군가에 의해 교체된 것이 아닌지를 확인 할 수 있는 기능이 제공되어져 비 인가된 불법 디바이스가 사용되는 것을 막을 수 있어야 한다.

(2) 디바이스 또는 생체인식시스템은 현재 입력된 정보가 실제 사용자에 의해 입력된 라이브 생체정보인지를 알 수 있는 방법을 제공하여야 하며 라이브 생체정보가 아닌 경우에는 데이터 입력을 받지 않거나 획득된 데이터를 무시 할 수 있어야 한다. 지문인식 디바이스의 경우 입력되는 지문이 실제 라이브 지문에 의해 입력되는 것인지를 확인 할 수 있는 장치를 추가하는 방법 등을 사용할 수 있으며, 홍채 인식의 경우 홍채의 적녹 현상에 대한 검사나 반사광의 각도 등을 분석하여 실제 사람에 의한 생체정보인지 또는 사진과 같은 모조 정보인지를 구분 할 수 있는 방법 등을 제공할 수 있다. 디바이스 차원에서 실제 라이브 생체 데이터인지를 판별하는 기능을 가지도록 하는 것이 바람직하며, 보안성을 높이기 위해서는 라이브 생체정보가 아닐 경우에는 획득조차 하지 않도록 해야 한다.

(3) 생체정보를 획득하는 디바이스는 외부로부터 안전하게 보호받을 수 있는 형태로 구성되어야 하며 외부의 분해나 조작 등으로부터 쉽게 노출되지 않는 형태로 만들어 져야 한다. 또한 외부의 침입으로부터 안전한 곳에 디바이스가 설치되도록 하여야 한다.

(4) 생체인식시스템은 현재 사용되고 있는 디바이스가 정상적으로 동작중인지를 항상 검사할 수 있도록 하는 기능을 제공해 디바이스의 오작동 여부를 탐지 할 수 있도록 하는 것이 좋다.

2. 생체인식 샘플을 생체인식 템플릿 추출부로 전송하는 과정간의 보안대책

(1) 디바이스로부터 넘어오는 데이터에 대해 무결성 검사를 통해 안전한 데이터가 전송되어져 왔다는 것을 알 수 있는 방법을 제공하여야 한

〔표 1〕 생체인식 프로세스와 위협요소간의 연관관계

Treats	획득	수집	인증	파기	전송
T1	√				
T2	√				√
T3			√		
T4			√		√
T5			√		
T6		√	√		
T7		√	√		√
T8			√		√
T9				√	

〔표 2〕 생체인식 프로세스와 취약점간의 연관관계

Weakness	획득	수집	인증	파기	전송
W1	√				
W2					√
W3	√	√	√	√	√
W4		√			
W5	√	√	√	√	
W6	√	√	√	√	√
W7			√		√
W8			√		
W9			√		√
W10			√		√
W11		√	√		√
W12		√	√	√	√
W13		√	√		√
W14			√	√	

다. 이를 위해 디바이스에 특정 암호화 키를 제공하고 디바이스는 획득된 생체정보를 전달받은 암호화 키를 이용해 암호화 해 전송하는 방법 등을 사용 할 수 있다. 이렇게 할 경우 외부에 의해 다른 데이터가 들어오더라도 암호화 방식이 다름으로 인해 인증시스템에 영향을 주지 않게 된다. 무선 통신을 통한 전송일 경우 반드시 무선 통신에 적합한 암호화 방식을 사용해 전송되는 데이터를 보호하는 것이 필요하다. 또한 디바이스와 생체인증 시스템간의 전송되는 라인이나 방식이 외부의 물리적 침해로부터 안전하게 보호되어질 필요도 있다.

(2) 디바이스에서 획득된 데이터가 암호화 된 후 전송되어져 다른 곳으로 유출되더라도 사용 할 수 없도록 해야 한다.

(3) 전송되어지는 데이터의 유효성을 판별 할 수 있는 기능이 필요 할 수 있다. 전송상의 데이터 오류를 검출하기 위한 작업이 수반되어질 수 있고 해쉬 함수와 같은 암호화 기법을 이용해 전송된 생체 정보가 손상되지 않았음을 확인 할 수 있는 방법이 제공되어야 한다.

(4) 시스템과 디바이스가 연결된 상태가 물리적으로 충분히 가까워 실제적으로 외부로부터의 침입이 불가능 할 경우, 이 부분에 대해서는 안전한 전송이 이루어진다고 가정할 수 있다.

3. 생체인식 템플릿 추출부 보안대책

(1) 생체인식 템플릿 추출을 위해 입력된 생체정보가 라이브 생체정보임을 확인 할 수 있는 방법이 제공되어 지는 것이 필요하다. 모조 데이터는 항상 동일한 형태의 입력만을 제공함으로 추출되어 지는 생체인식 템플릿도 항상 동일하게 될 가능성이 있다. 이 때문에 외부 공격자는 모조 데이터에 대한 입력 값을 동일하게 하여, 결과로 생성되는 생체인식 템플릿을 분석할 수 있는 정보를 가질 수 있다. 또한 모조데이터로 인해 생체인식시스템이 무력화될 수 있으므로, 이를 막을 수 있는 대책이 제공되어져야 한다.

(2) 생체정보로부터 추출된 생체인식 템플릿은 반드시 암호화 되어 처리되어야 한다. 암호화 되지 않은 생체인식 템플릿은 내부의 정보가 외부 공격자에게 노출되어져 조작되거나 분석될 가능성이 있고 가공된 새로운 생체인식 템플릿으로 인증요청이 되어질 가능성도 가지고 있다. 이를 위해 암호화 된 생체인식 템플릿을 출력 할 수 있도록 생체인식 템플릿 추출부가 만들어질 필요가 있다.

(3) 생체데이터 인증시스템에는 여러 가지 다양한 프로그램을 설치하지 말고 가능하면 생체데이터만을 취급하는 시스템으로 관리하여 시스템의 안정성을 유지해 나가는 것이 필요하다. 많은 프로그램들을 설치하게 되면 전반적인 시스템의 안정성이 침해받게 될 가능성이 있으며 프로그램간의 오류로 인해 생체데이터의 보안에 영향을 줄 수도 있다.

(4) 생체데이터 인증시스템에 접근 할 수 있는 권한의 사용자를 지정하고 이 사용자만이 시스템에 접근할 수 있는 통제 시스템을 갖추는 것이 좋다. 또한 관리자 계정을 가진 자는 생체인식 시스템에 접근한 모든 행위에 대해 책임이 있다는 것을 인식하여야 하며, 생체인식시스템 접근에 대한 권한 부여를 통제하기 위하여 이에 대한 공식적인 비밀번호 등의 관리절차를 수립하여 이행하도록 한다.

4. 생체인식 템플릿 인증부 보안대책

(1) 일반적으로 두개의 생체인식 템플릿을 입력받아 유사도를 비교하는 인증부의 경우 입력되는 생체인식 템플릿이 유효한지를 검사할 수 있는 방법을 제공해야 한다. 생체인식 템플릿에 대해서는 자체적으로 암호화 되어 있어야 하고 암호화한 데이터에 대해서도 일방향 해쉬 함수와 같은 방법 등을 통해 입력되는 생체인식 템플릿이 변조된 것이 아닌지를 검사하고 유효성을 판단하는 것이 좋다. 입력된 데이터가 유효하지 않을 경우 결과로 출력되는 유사도 값은 의미를 가질 수 없으며 만약 그러한 검사 없이 사용된 유사도 결과 값은 전체 인증 시스템에 치명적인 영향을 미칠 수 있게 되므로 입력 값에 대한 검사는 꼭 필요하다고 할 수 있다.

(2) 라이브 생체정보로부터 얻어지는 원본 데이터는 생체정보의 특징상 항상 조금씩 다른 원본 데이터가 얻어지게 되고 그로 인해 생체인식 템플릿도 미세하지만 항상 조금씩 달라진다고 볼 수 있다. 하지만 라이브 생체정보가 아닌 가공된 생체정보로부터 얻어진 원본데이터로 생체인식 템플릿을 추출하게 될 경우 항상 동

일한 원본데이터가 입력되므로 수학적 특징에 의해 항상 동일한 생체인식 템플릿이 출력되게 된다. 그러므로 인증부에서는 이전과 완전히 동일한 생체인식 템플릿이 연속적으로 입력되어지는 경우에는 정상적인 인증이 아닌 외부로부터의 인가되지 않은 입력으로 판단하는 것이 좋다. 또한 생체인식 템플릿에 타임스탬프 정보를 삽입하여 유효한 정보를 판단하는 방법을 사용 할 수도 있다.

(3) 인증을 위해서는 안전한 프로세스를 통해 인증을 처리하는 것이 필요하다. 인증을 위해 내부적인 초기화 및 정확한 값의 할당이 끝난 후 인증 요청이 수행되지 않고 안전하지 않은 상태에서 인증 요청이 들어오는 경우에는 인증처리를 하지 않는 것이 좋다. 인증에 대한 결과도 안전한 절차에 의해 전달되어져야 한다. 시스템에 따라 명확한 인증 절차를 확립하고 그 절차에 의해서만 인증 처리가 루어 질 수 있도록 하는 것이 중요하다.

5. 생체정보 등록과정 보안대책

(1) 온라인상의 침입뿐만 아니라 오프라인 상에서도 물리적인 접근통제를 하는 것이 필요할 수 있다. 등록 시스템에 아무나 접근해 작업을 할 수 있게 되면 내부에 등록된 생체정보가 쉽게 외부로 유출되거나 조작되어질 수 있다. 이것은 바이러스 백신이나 스파이웨어 탐지기, 또는 방화벽을 설치해 둔다하더라도 막을 수 없는 상황이므로 더욱 심각하다고 할 수 있다. 보안 담당자를 두고 생체정보 등록시스템에 접근 할 수 있는 사용자를 엄격히 제한하는 것이 필요하다.

(2) 마찬가지로 인가되지 않은 사용자에 의한 생체정보 등록을 제한하는 것이 필요하다. 온라인 상에서는 개인의 신분을 확인 할 수 있는 확실한 방법이 부족하므로 공개키 기반의 서명 등을 통한 방법으로 개인의 신분을 확인하는 것이 필요하고 오프라인 상에서는 보안관리자를 통해 인가되고 확인된 사용자에 한해 생체정보를 등록 할 수 있도록 제한하여야 한다.

(3) 인가된 사용자라 하더라도 자신의 실제 데이터가 아닌 모조 데이터를 이용해 등록을 하게 될 경우(예를 들어 모조 지문을 통한 지문 등록, 얼굴 사진을 이용한 얼굴 등록, 녹음기를 이용한 음성 등록 등) 실제 등록된 데이터가 본인의 것이 아님으로 인해 이후 인증시 원래 등록자와 다른 사람을 인증해 주거나 또는 본인 인증을 거부 할 수 있다. 이를 막기 위해 디바이스로부터 라이브 생체정보가 입력되는지를 등록과정에 확인하는 것이 필요하고 보안 담당자에 의해 본인이 정상적으로 등록하는지를 확인하는 것이 필요하다. 등록된 데이터에 대해서도 실제 원본데이터를 직접 확인하여 모조 데이터에 의한 것이 아닌지를 실제로 판단하는 작업도 필요하다.

(4) 생체정보의 등록은 일반적으로 패스워드를 등록하는 것과는 다르게 사용자들이 익숙한 작업이 아니다. 특히 가장 익숙하지 않은 때가 처음 생체정보를 등록하는 과정이라고 할 수 있다. 일정 시간 생체 인증 시스템을 사용할 경우 생체 입력 디바이스와도 익숙해지고 정확한 데이터를 입력하기 위해 의도적으로라도 행동하게 되지만 처음 생체정보를 등록하는 과정에서는 처음 접하는 생체 인증 시스템과 디바이스에 적응되지 않은 상황이라 인증되기 어려운 잘못된 데이터가 입력되는 빈도가 가장 높을 수 있다. 문제는 이렇게 잘못된 생체정보가 등록정보로 입력되어 이후 인증 시 계속 사용이 되면서 인증율을 떨어뜨리게 된다는데 있다. 한번 잘못 입력된 데이터가 이후 계속적으로 인증 실패의 원인이 될 수도 있다는 것이다. 때문에 가능하면 처음 등록 시에 자세한 가이드를 미리 사용자에게 주는 과정이 필요하며 등록 시에도 여러 번의 생체정보를 입력받아 서로 유사도를 비교해 문제가 없을 경우 등록을 허용하고 그중에서 가장 품질이 좋은 데이터를 저장하도록 하는 것이 좋다. 또한 가능한 한 많은 데이터를 등록데이터로 사용하여 이후 인증 시 등록된 여러 개의 데이터와의 인증을 통해 인증율을 높이도록 해야 한다.

6. 생체정보 파기관련 보안대책

(1) 생체정보 취급자는 생체정보를 파기 했을 때 파기한 사실을 명확히 개인에게 통보하여 확인해 줄 수 있어야 한다. 이 후 파기되었다고 통보된 생체정보가 파기되지 않고 불법적으로 남용되어질 경우에는 생체정보 취급자가 그 책임을 지도록 한다.

(2) 파기된 생체정보가 복원되지 않도록 적절한 기술적 조치를 취하는 것이 필요하다. 일반적으로 하드디스크에 저장된 파일의 경우 그냥 삭제하는 것만으로는 파일이 완전히 삭제되지 않으며 다시 복구되어질 수 있다. 이것을 방지하기 위해 그 파일에 여러 번 다시 덮어써주어 복구를 완전히 불가능하게 하거나 완전 삭제 프로그램 등을 이용해 복구가 불가능하게 완전히 삭제를 해 주는 작업이 필요하다. 또한 하드디스크를 물리적으로 파괴하는 방법도 사용되어 질 수 있으나 이 경우 완전히 파괴되었음을 확인할 수 없어 가능하면 전자의 방법을 이용해 생체정보를 파괴하는 것이 좋다.

(3) 생체정보가 디바이스를 통해 입력되어 추출부로 전송된 후 생체 인식 템플릿으로 처리되는 과정에서 원본 생체정보(지문 이미지, 얼굴 화상, 홍채 이미지 등)는 메모리 상에서만 존재했다가 처리 후 완전 삭제되어 지는 것이 좋다. 원본 생체정보의 경우 언제고 다시 추출되어질 가능성이 있고 개인 프라이버시의 문제를 일으킬 수 있는 소지가 있기 때문에 가능한 따로 저장하지 않는 것이 좋으며 만약 감사목적으로 저장해 둘 경우라면 반드시 변형해 저장하거나 암호화 알고리즘을 통해 암호화 한 후 저장하여 유출의 위험으로부터 보호하는 것이 필요하다.

Ⅵ. 결 론

본고에서는 생체정보의 수집·저장·전송·폐기 등 전 과정에서 발생가능한 통신상의 텔리바이오메트릭시스템에 대한 위협요소와 취약점을 분석하였고, 텔리바이오메트릭시스템의 구성요소별로 생체정보에 대한 기술적·관리적 보안대책을 제시하였다. 이러한 연구결과는 현재, "생체정보 보안대책 가이드라인"이라 표준과제로 TTA PG103(생체인식프로젝트그룹)에 상정되어 올해말 TTA 단체표준으로 제정을 목표로 하고 있다. 또한, 국제적으로는 "기술적·관리적 생체정보 보안대책 가이드라인(x.tpp)"이란 국제표준과제로 ITU-T SG17 Q8에서 채택되어, 10월 스위스 회의에서 일본, 중국과 이메일그룹을 통한 의견교류키로 결정되었으며, '07년 12월에 국제표준으로 제정을 검토하기로 의결되었다.

참 고 문 헌

[1] Enhancing Security and Privacy in biometrics-based authentication systems," Ratha, Connell and Bolle, IBM System Journal, Vol. 40, No 3, 2001

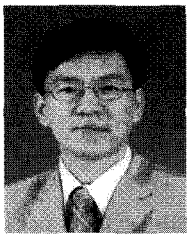
[2] S.Liu and M.Silverman, "A Practical Guide to Biometric Security Technology", IEEE Computer Society, IT Prosecurity, Jan-Feb, 2001.

[3] ANSI, X9.84:Bioemtric Information Management and Security, American National Standards Institute.

[4] 인하대 정보통신대학원 공학박사학위논문, "생체인식시스템 표준적합성 및 보안성 평가모델", 2005. 8

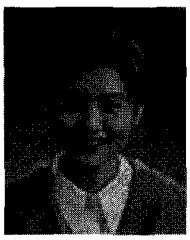
[5] 정보통신부, 서혜석 의원실 주관, KISA 주최 제2차 "생체정보보호 가이드라인 제정" 공청회, 2005. 10. 31

〈著 者 紹 介〉



김 재 성 (Jason Kim)
정회원

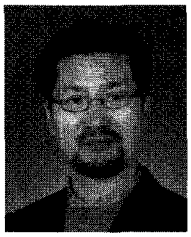
1989년 2월 : 인하대학교 전산학과 석사 졸업
2005년 8월 : 인하대학교 정보통신대학원 공학박사 졸업
1996년 7월~현재 : 한국정보보호진흥원 생체인식 TFT 팀장
2002년 12월~현재 : TTA PG103(바이오인식) 국내표준화 의장, 산자부 기표원 품질인증 표준화위원장
2003년 8월~현재 : ITU-T SG17, ISO/IEC JTC1 SC37 국제표준과제 에디터 활동
〈관심분야〉 생체인식시스템 시험기술 및 국제표준화, 정보보호제품 시험평가



신 용 녀 (Anne Shin)

2001년 9월 : 고려대학교 컴퓨터학과 석사 졸업
2005년 11월 : 고려대학교 컴퓨터학과 박사 과정
2002년 1월~현재 : 한국정보보호

진홍원 기술표준팀 연구원
〈관심분야〉 생체인식, 정형기법, 정보보호



김 학 일 (Hakil Kim)
종신회원

1983년 2월: 서울대학교 제어계측공학과 (학사)
1985년 8월: (미)퍼듀대학교 전기컴퓨터공학과 (석사)
1990년 8월: (미)퍼듀대학교 전기컴퓨터공학과 (박사)
1990년 9월~현재: 인하대학교 공과대학 교수
2001년 2월~현재: 한국생체인식포럼 시험평가분과 위원장
2002년 1월~현재: 한국정보보호학회 생체인증연구회 위원장
2003년 3월~현재: ISO/IEC JTC1/SC37(생체인식) WG5(성능평가) Rapporteur Group
2005년 4월~현재: ITU-T SG17 Q.8 (Telebiometrics) Associate Editor