情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

ITU-T SG17/Q.8 X.tpp-1 국제표준화 (텔레바이오메트릭스 환경의 바이오정보 보안대책) 현황

전 인 자*, 김 재 성**, 하 도 윤***, 최 재 유****

요 약

바이오인식기술을 이용하는 개인인증을 수행하는 바이오인식 시스템으로 구성되어 물리적 접근제어, 인터넷 접근제어, 전자여권 등 다양한 장소에서 신원확인의 수단으로 이용되어지고 있다. 바이오인식 시스템은 다양한 장소에서 사용되므로, 바이오정보획득, 처리, 정합 등을 수행하는 시스템이 분리되어 구축된다. 이때 각 시스템 및 시스템에서 사용/전달되어지는 정보의 변환, 도용, 훼손에 대한 보호 및 시스템에서 비인가자의 불법적인 원격침입 가능성이 발생한다. 이와같은 공격의 취약성을 방지하기 위하여 텔레바이오메트릭 시스템에 대한 보호절차를 구성하였다. 개인인증을 위하여 생체정보를 수집하거나, 이용하는데 있어서 준수하여야 하는 바이오정보보호에 대한 중요사항을 제시하고, 안전한 이용환경을 제공하기 위하여 네트워크상에서 시스템이 수행될 때 발생하는 공격 취약점을 정의하였으며, 이를 보호하기 위한 가이드라인을 구성하였다. 텔레바이오인식 시스템보호 절차에서 제시하는 가이드라인은 바이오정보 보호 정책 개발방법, 위험분석, 바이오인식 시스템 운영 및 기술 개발시에 활용할수 있다. 본고는 현재 ITU-T SG17 Q.8(Telebiometrics)에서 KISA가 추진하여 년내에 X.tpp로 제정이 예상되는 국제표준을 상세히 설명하고 있으며, 이는 곧 바이오인식 시스템을 이용한 작은규모의 물리적 접근 제어 시스템으로부터 국가적 규모의 바이오인증 시스템까지 응용가능한 텔레바이오인식 시스템 전반에 적극 활용할 수 있다.

Ⅰ. 서 론

개인인증을 위하여 사용하는 다양한 방법중 개인만이 유일무이하게 가지고 있는 바이오정보를 이용하는 바이오인식 시스템이 다양한 응용환경에서 사용되어지고 있다. 바이오인식 시스템은 작은규모의 접근제어시스템에서부터 국가적 규모의 바이오인증을 위하여 구축 사용되어지고 있다. 최근 유무선 환경에서의 바이오인식 시스템 또한 구성되어지고 있다. 네트워크 환경에서 이용되는 바이오인식 시스템인 텔레바이오메트릭스(Telebiometrics)의 응용분야가 확대되어짐에 따라서 시스템에서의 공격 가능성 또한 확장되어지고 있다. 바이오정보의 안전한 이용환경을 조성하고, 개인 정보를 보호하기 위하여 공격취약점에 대하여 정의하고, 각 단계에서의 공격 취약성을 예방하기 위한 가이드라인을 제시한다.

Ⅱ. 텔레바이오메트릭 시스템상에서의 공격 취약점

바이오메트릭 시스템은 바이오정보의 획득, 정보처리, 정합 과정등을 거치게 되며, 개인정보의 등록 및 인증과정을 통하여 개인인증이 이루어진다. 현재 다양한 응용을 위하여 바이오메트릭 시스템은 네트워크 환경에서 구축이 이루어지며, 텔레바이오메트릭 시스템이라고 한다. 텔레바이오메트릭스 환경에서는 획득되어지고 처리되어지는 바이오정보가 전달매체를 통하여 다음 단계의 처리시스템으로 전송되어진다. 정보의 처리 및 전송의 단계에서 외부의 악의적인 공격이 발생한다. 외부 공격에 대하여 인적 보안, 물리적 보안, 시스템 개발보안, 암호통제, 접근통제, 운영관리, 전자거래 보안, 보안사

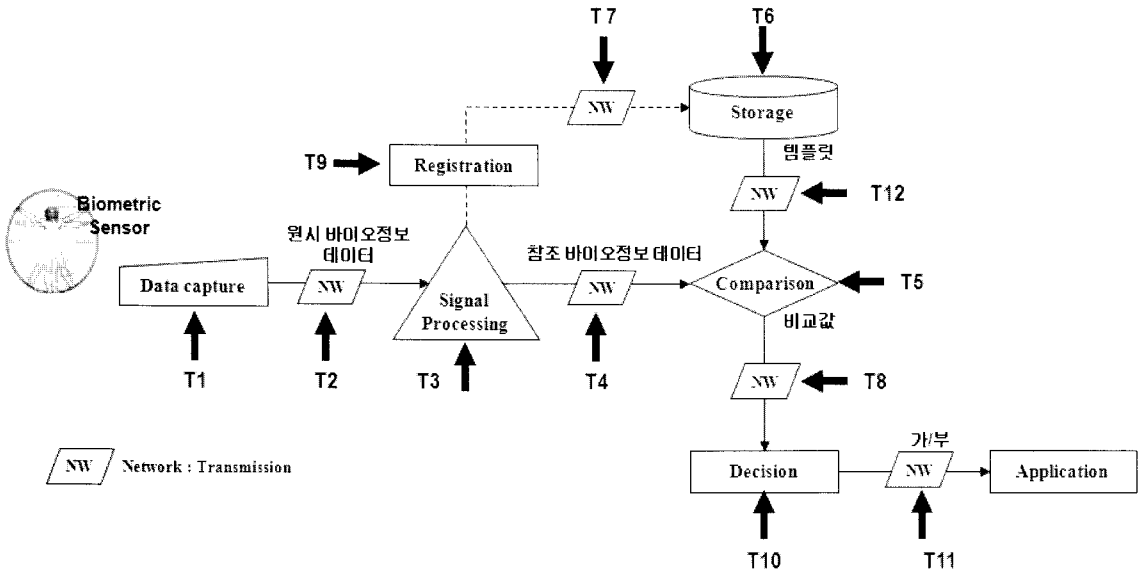
* 인하대학교
** 한국정보보호진흥원 국가사이버안전센터(NCSC) 파견 팀장 (jskim@kisa.or.kr)
*** 한국정보보호진흥원 국가사이버안전센터(NCSC) 파견 연구원 (dyha@kisa.or.kr)
**** 방송통신위원회(KCC) NCSC 파견 국장

고 관리, 모니터링등을 이용하여 시스템의 운영적 보호 조치가 필요하게 된다. 또한 바이오정보의 보호정책, 외부자 보안등의 관리적 보호조치 또한 필요할 것이다.

바이오정보의 기술적 조치를 위하여 보호하고자 하는 대상과 규모를 정확히 파악한 후, 바이오정보를 보호하고자 하는 정책을 수립하여야 할 것이다. 기술적 보호조치를 위하여 구축된 보호정책이 반영되어지기 위하여 이를 구현하는 기술요원 및 시행 권한을 가지고 있는 의사 결정자 모두 제안된 정책을 숙지하고 있어야 할 것이다.

바이오정보는 변화하지 않는다는 장점 때문에 개인 인증을 위한 유일무이한 데이터로 이용되어지고 있다. 그러나 등록 및 인증을 위하여 사용되는 정보가 유출된다면 그 피해의 심각성은 이루말할 수 없을 것이다. 이와같은 피해를 줄이기 위하여 텔레바이오메트릭 시스템은 다양한 공격에 대하여 강인성을 가져야 하며, 생체정보의 변형을 방지하기 위한 복잡한 처리등에서 발생하는 성능 저하가 없어야 할 것이다.

텔레바이오인식 시스템은 바이오인식 시스템이 네트워크 환경에서 구축되는 것이므로, 운용시스템상에서 원시 바이오정보 및 처리된 정보가 외부로부터의 공격에 노출되지 않도록 각 지점에서의 보호 가이드라인을 구성할수 있다. 텔레바이오인식 시스템에서 발생가능한 공격은 바이오인식 시스템의 각 컴포넌트와 정보전송단계에서 이루어진다. 아래 [그림 1]은 텔레바이오메트릭 시스템의 처리 단계에서 해킹 등의 원인으로 발생하는 정보의 취약성을 보호하고자 정의한 12가지 공격취약지점을 포함한 텔레바이오인식 시스템의 구성도이다.



〔그림 1〕 텔레바이오메트릭 시스템의 공격취약점

각 부분별 공격취약점에 대한 기술은 아래와 같다.

T1 : 바이오정보 입력 단계에서의 공격
T2 : 획득된 원시바이오 정보의 정보처리단계로의 전송에서의 공격
T3 : 원시바이오정보의 처리단계에서의 공격
T4 : 처리된 참조 바이오정보가 비교를 위하여 전송되어지는 단계에서의 공격
T5 : 비교를 위하여 획득한 참조 바이오정보의 데이터와 저장소로부터 전송된 템플릿의 비교 단계에서의 공격
T6 : 바이오정보 저장소에서의 공격
T7 : 등록을 위하여 구축된 개인정보의 전달과정에서의 공격
T8 : 참조바이오정보 데이터와 템플릿의 비교과정을 거친후에 발생한 비교값을 전달할 때 발생하는 공격
T9 : 등록 단계에서 발생하는 공격
T10 : 결정 단계에서 발생하는 공격
T11 : 결정된 값이 어플리케이션으로 전송될 때 발생하는 공격
T12 : 정보저장소로부터 비교를 위하여 전달되는 템플릿정보에 대한 공격

Ⅲ. 구성된 공격취약점에서의 보호 가이드라인

3.1 T1 : 바이오정보 입력단계에서의 공격

바이오정보를 취급하는 시스템에서 사용자의 바이오정보를 입력받는 작업은 매우중요하다. 획득되는 바이오정보의 품질이 어떠한가에 의해 바이오정보를 취급하는 전체 시스템의 성능이 결정되어지기도 한다. 획득되는 바이오정보는 외부로 유출되어 인가되지 않은 곳에서 무단으로 사용되거나 부정한 방법으로 이용되어지지 못하도록 하여야 한다. 이상과 같은 이유 때문에 바이오정보를 획득하는 장비에 대한 보호는 반드시 이루어져야 한다.

(가) 공격 취약점
- 비인가된 불법 디바이스에 의해 사용자의 원본 생체정보가 아닌 조작된 생체정보가 입력 되어질 수 있다.
- 라이브정보가 획득되지 않고 모조지문이나 얼굴사진, 녹음기 등을 통하여 가짜 정보가 입력 되어질 수 있다.
- 장치로부터 획득된 정보가 안전한 전송이 이루어지기 전에 외부로부터 침입을 당해 유출되어질 수 있다.

(나) 가이드라인
- 바이오인식 시스템은 현재 입력된 정보가 실제 사용자에 의해 입력된 라이브 바이오정보인지를 알수 있는 방법을 제공해야 한다. 라이브 바이오정보가 아닌 경우 데이터 입력을 받지 않거나 데이터를 무시할 수 있어야 한다.
- 바이오정보를 획득하는 장치는 외부로부터 안전하게 보호받을수 있는 형태로 구성되어야 한다. 외부의 분해나 조작등으로부터 쉽게 노출되지 않는 형태로 만들어져야 한다.
- 외부의 침입으로부터 안전한 곳에 시스템이 설치되도록 하여야 한다.

3.2 T2 : 획득된 원시바이오 정보의 정보처리단계로의 전송에서의 공격

바이오정보는 데이터 처리를 위하여 바이오메트릭 시스템으로부터 안전하게 전송되어야 할 것이다. 만약 획득된 바이오정보가 정확하게 입력되었다 하더라도 장치가 획득된 바이오정보를 정합 시스템에 전송하는 도중 오류가 발생하거나, 데이터가 외부 침입에 의하여 훼손되어진다면 정확한 바이오정보의 전송은 불가능하게 될 것이다.

특히, 바이오정보가 유선 네트워크나 무선 네트워크 등을 통하여 전송하게 된다면 바이오정보의 보호에 심각한 문제가 발생할 것이다. 또한 바이오정보는 개인의 프라이버시를 침해받을수 있는 정보이기 때문에, 장치로부터 획득된 정보는 다른 곳에서 불법 유출되는 문제에 대한 보호도 반드시 필요하다.

(가) 공격 취약점
- 장치로부터 입력되어진 생체정보가 정상적으로 정보처리 시스템으로 전송되지 않고, 외부에서 변형되어진 정보를 전송할수 있다.
- 바이오 정보 전송상의 오류로 인하여 전송되어진 정보가 손상되어 인증을 방해할 수 있다.

(나) 가이드라인
- 장치로부터 전송되는 데이터에 대하여 무결성 검사를 통하여 안전한 데이터가 전송되어져 왔다는 것을 알수 있는 방법을 제공하여야 한다.
- 장치와 인증시스템간의 전송되는 라인이나 방식이 외부의 물리적 침해로부터 안전하게 보호되어질 필요도 있다.
- 장치에서 획득된 바이오정보가 암호화 된후 전송되어져 다른 곳으로 유출되더라도 사용할수 없도록 해야한다.
- 전송되어지는 바이오정보의 유효성을 판별할 수 있는 기능이 필요할 수 있다.

3.3 T3 : 원시바이오정보의 처리단계에서의 공격

바이오정보 획득 장비로부터 얻어진 원시 바이오정보는 특징추출과정을 거쳐 인식하기에 적합한 형태인 바이오데이터(Reference data) 또는 셈플(Sample)로 구성된다. 이때 바이오정보가 정보처리단계에서 유출될수 있다는 가정을 전제로, 이와같은 정보유출의 취약부분에 대비하는 것이 필요한다. 또한 구성된 참조데이터의 구조가 외부로 유출되더라도, 불법적으로 저작되어 바이오인식 시스템에 사용될 경우, 인증시스템이 오동작할 수 있기 때문에 모든 바이오인식을 위한 참조데이터는 암호화하여 처리되도록 해야한다.

(가) 공격 취약점
- 라이브정보가 아닌 보조데이터에 의하여 정보가 추출될 수 있다.
- 바이오인식시스템이 바이러스나 스파이웨어와 같은 악성프로그램에 의해 래퍼런스 데이터가

유실되거나 조작되거나 유출되어질 수 있다.
- 바이오인식 시스템이 시스템 자체 오류에 의해 오작동 되거나 시스템에 문제가 발생할 수 있다.

(나) 가이드라인
- 레퍼런스데이터를 구성하기 위하여 입력된 바이오정보가 라이브 정보임을 확인할 수 있는 방법이 제공되어야 한다.
- 모조데이터로 인하여 바이오인식 시스템이 무력화될수 있으므로, 이를 막을수 있는 대책이 제공되어져야 한다.
- 원시 바이오정보로부터 추출된 레퍼런스 데이터는 반드시 암호화 되어 처리되어야 한다.

3.4 T4 : 처리된 참조 바이오정보가 비교를 위하여 전송되어지는 단계에서의 공격

구성되는 레퍼런스 데이터는 비교단계로 전송하게 되어지며, 이때 안전하게 정보의 전송이 이루어져야 한다. 구축된 레퍼런스 데이터는 전송상의 보호뿐만 아니라, 시스템간 정보 전송에도 강력한 보호가 필요하다.

(가) 공격 취약점
- 레퍼런스 데이터가 전송되는 도중 외부 침입자에 의해 가로채어져 다른 부정적인 용도로 사용되어질 수 있다.
- 전송상의 오류로 레퍼런스 데이터가 손상되어 전송되어질 수 있다.

(나) 가이드라인
- 외부에 의하여 불법적으로 유출되더라도 다른곳에서 사용할 수 없도록 암호화하여 전송하여야 하며, 전송상의 키는 매번 다른 키를 사용하여 암호화 하거나 PKI등의 방법을 이용하여 전송중의 정보가 위변조 되는 것을 막도록 한다.
- 전송되는 레퍼런스데이터가 전송오류나 기타 이유로 인하여 변경되었음을 탐지 할수 있는 기능이 제공되어야 한다.

3.5 T5 : 비교를 위하여 획득한 참조 바이오정보의 데이터와 저장소로부터 전송된 템플릿의 비교 단계에서의 공격

바이오인식 시스템에서 레퍼런스 데이터를 이용한 인식 알고리즘의 비교부는 가장 중요한 요소이다. 비교시스템은 두 개의 바이오정보를 입력받아 그 둘의 유사도를 확률적으로 비교하여 그 결과를 알려주는 역할을 한다. 인식시스템은 외부로부터 인가되지 않은 접근을 방지해야할 핵심적인 부분이며, 비교결과에 대한 유효성이 판단 될 수 있는 방법이 필요하다.

(가) 공격 취약점
- 변경된 레퍼런스 데이터나 템플릿을 이용하는 경우 잘못된 비교 결과를 도출할 수 있다.
- 안전하지 않은 비교처리 과정에 의하여 비교가 수행되거나, 비교 결과가 외부로 유출 또는 외부 요인에 의하여 절차가 변경되어 질 수 있다.

(나) 가이드라인
- 레퍼런스 데이터와 템플릿을 이용하여 유사도를 비교하는 시스템에서, 입력되는 정보가 유효한지를 검사할 수 있는 방법이 제공되어야 한다.
- 비교시스템에서는 안전한 처리를 통하여 비교를 처리할 수 있도록 명확한 절차를 확립하고, 그 절차에 의해서만 비교처리가 수행되도록 구성되어야 한다.
- 가능한 많은 데이터를 등록 데이터로 사용하여 이를 비교시 여러개의 데이터와의 비교를 통하여 인증률을 높이도록 해야한다.

3.6 T6 : 바이오정보 저장소에서의 공격

바이오인식 시스템에서 사용자의 바이오정보는 하나 이상의 정보저장소에 저장되고, 인증요청시 저장된 템플릿데이터와의 비교를 통하여 비교처리를 수행하게 된다. 바이오정보를 저장하는 저장소가 외부의 침입에 노출될 위험성을 가질수 있기 때문에 정보저장소에 대한 보호는 매우 중요하다.

(가) 공격 취약점
- 모든 정보 및 바이오데이터는 단일/다중 데이터베이스에 저장된다. 이때 등록된 바이오정보는 불법적인 침입에 의하여 모든 사용자의 바이오정보가 노출되어질 수 있다.
- 인가되지 않은 사용자가 정보저장소에 대한 접근이 가능하다면 데이터가 훼손되거나 손상되어질 수 있으므로 이에 대한 예방이 필요하다.

(나) 가이드라인
- 바이오정보는 다른 정보와 구분되어 저장되는 것

이 좋다. 이를 위하여 데이터베이스를 따로 구성하여, 독립된 시스템을 통하여 정보저장소를 관리하도록 하여야 한다.
- 어떠한 방식으로든 매체에 저장된 개인정보는 암호화를 통하여 저장되어야 한다.
- 정보저장소에는 관리자 만이 접근할수 있도록 접근제한을 해야 한다.

3.7 T7 : 등록을 위하여 구축된 개인정보의 전달과정에서의 공격

개인정보의 등록을 위하여 구성된 정보를 저장하기 위하여 독립된 정보저장소로 전송되어질 경우, 정보 훼손 가능성이 발생하게 된다.

(가) 공격 취약점
- 불법적인 바이오정보가 실제 바이오정보를 대신하여 저장될 수 있다. 암호화 되지 않은 데이터가 전송될 경우 외부의 공격에 노출될 수 있다.
- 만약 스마트카드나 USB 메모리등을 사용하는 경우 데이터는 비인가된 시스템에서 전송되어지거나 복제된 장치들로부터 전송이 시도될 수 있다.

(나) 가이드라인
- 전송되는 개인 정보는 전송되는 각 유형에서 암호화 된후에 전송되어야 한다.
- 스마트카드나 USB 메모리 로부터 전송되어지는 경우, 시스템은 외부의 공격에 대비하여 물리적인 연결시스템을 구성해야 할 것이다.

3.8 T8 : 참조바이오정보 데이터와 템플릿의 비교과정을 거친후에 발생한 비교값을 전달할 때 발생하는 공격

비교시스템으로부터 전송되는 결과값은 외부 공격에 의하여 변경이 이루어질 수 있다. 마지막 결과 전송을 위한 단계에서의 공격 취약 지점 또한 발생하게 된다.

(가) 공격 취약점
- 비교결과가 점수로 나올 경우 여러번의 공격을 통해 비교 결과의 판단 임계점을 파악해 낼 수 있다. 이 경우 비교 점수를 통해 비교를 요청한 템플릿의 유사도를 유추할 수 있으므로 주의해야 한다.

(나) 가이드라인
- 비교 결과값을 전송하기 전에 반드시 암호화를 통해 전송하여야 하며, 중간에 가로채어져 바뀌는 것을 방지해야 한다.

3.9 T9 : 등록 단계에서 발생하는 공격

개인정보를 등록하는 과정에서 바이오정보는 유일한 등록 처리 과정을 가진다. 일반적으로 개인정보는 암호화된 정보의 구성을 필요로 한다. 바이오정보의 등록을 위하여 반복적으로 입력이 이루어진다면 암호화된 등록 처리와 좀더 세밀한 처리절차를 필요로 할 것이다.

(가) 공격 취약점
- 등록을 위한 바이오정보는 비인가된 사용자에 의하여 훼손되어질 가능성이 있다.
- 만약 비인가된 사용자가 등록하거나 바이오정보가 사용되어진다면, 시스템의 공격과 접속에 대하여 좀더 강력한 처리가 필요로 할 것이다.
- 만약 모방된 바이오정보에 의하여 등록된 데이터가 허가된다면, 비합법적인 데이터를 이용한 비교 처리가 이루어질 것이다.

(나) 가이드라인
- 비 인가된 사용자에 의한 바이오정보의 등록은 강력하게 이루어져야 한다.
- 등록 처리에서 라이브 바이오인식 데이터가 장치를 통하여 입력되어 지는 것을 점검해야 한다.
- 처리는 등록된 데이터는 실제 원본 데이터를 점검하는 것에 의하여 모조된 데이터로부터 결정되도록 요구되어질 것이다.

3.10 T10 : 결정 단계에서 발생하는 공격

네트워크에 연결된 바이오인식 시스템에서 전송된 결과값의 가/부 결정에 올바르게 이루어지기 위하여 잘못된 프로그램이나 잘못된 함수로부터 안전하게 구축되어야 할 것이다.

(가) 공격 취약점
- 시스템의 에러나 문제 때문에 잘못된 결과가 전송될수 없도록 구성해야 할 것이다.
- 비인가된 사용자가 바이오인식 시스템을 처리하기 위하여 처리를 요청할 경우, 즉시 이를 발견할

수 있어야 한다.

(나) 가이드라인

- 바이오인식 시스템은 외부로부터의 공격이나 불법적인 사용에 대응하기 위하여 방화벽 및 바이러스백신 등의 프로그램을 사용하여야 한다.
- 바이오인식 시스템은 가능한 한가지 용도로 이용되어지도록 구성되어야한다. 다양한 종류의 프로그램을 이용하는 불법적인 외부로부터의 침입이 이루어질 수 있다.
- 바이오인식 시스템에서 내부적인 위험이 감지되었을 경우 시스템에서 위험에 대한 잠재적인 가능성을 측정할 수 있어야 한다.

3.11 T11 : 결정된 값이 어플리케이션으로 전송될 때 발생하는 공격

결정은 비교단계로부터 마지막 결과값이 공격을 당하였기 때문에 최종 결과는 변화될 수 있다. 비인가된 사용자가 마지막 결과값의 전송단에서의 전송에 대한 공격이 이루어져서 인가된 사용자에 대한 결과가 변화될 수 있다.

(가) 공격 취약점

- 가/부에 대한 마지막 결과값은 결정된 결과값에 따라 변화되어질 수도 있다.
- 결정을 위한 판단 임계값은 다양한 공격의 대상이 될 수 있다.

(나) 가이드라인

- 결정된 결과값은 응용요소에서 가/부를 표현하게 된다. 전송되는 가/부의 요소가 전송되는 도중에 외부의 요인에 의하여 변화되어질 수 있다.
- 라우터나 다른 시스템에서 결과값이 전송되어질 때, 사용하는 시스템이 비인가된 시스템인지 인가된 시스템인지에 대한 카테고리가 구성 되어져야 할 것이다.

3.12 T12 : 정보저장소로부터 비교를 위하여 전달되는 템플릿정보에 대한 공격

저장된 데이터가 저장소에서 비교시스템으로 전송되어질 때, 데이터는 외부의 공격에 노출되어질 수 있다. 전송되는 템플릿은 비교단계로 전송되어질 때 암호화되어져 있어야 할 것이다. 강력한 보호 처리는 저장소로부터 저장된 템플릿의 전송뿐만 아니라 저장된 템플릿의 시스템 사이에서의 전송에 대하여도 제공되어야 할 것이다.

(가) 공격 취약점

- 저장된 템플릿은 비교처리를 위하여 전송되어지며, 이때 침입자에 의하여 변화가 이루어진 템플릿은 비교를 위하여 전송될 것이다.

(나) 가이드라인

- 저장소에서 전송되는 템플릿은 전송되어질 때 반드시 암호화 되어져야만 한다. 템플릿을 전송하기 위한 전송라인은 외부의 공격에 노출되지 않아야 한다.
- 전송을 위하여 라우터나 다른 시스템을 사용할 경우, 외부의 공격을 대비하기 위하여 비인가된 시스템과 인가된 시스템에서 사용되어지기 위하여 구조화 되어져야 할 것이다.

Ⅳ. 결 론

바이오인식 시스템의 안전한 구축을 위하여 본 고에서는 유무선 네트워크 환경에서 운영되어지는 텔레바이오메트릭 시스템의 공격취약점에 대한 보호 절차에 대한 구성을 제시하였다. 본 고에서 제시하는 보호 절차는 텔레바이오인식 시스템을 수행하는 도중 발생하는 취약사항에 대한 기술과 각 취약사항을 보호하기 위한 기술적, · 운영적 보안대책 가이드라인으로서 금년말 ITU-T SG17 Q.8분과에서 X.tpp(에디터 : 김재성 팀장/KISA) 국제표준으로 제정될 전망이다. 이러한 국제표준은 텔레바이오메트릭스 시스템을 필요로 하는 모든 응용환경에서 시스템을 구축하는 개발자 및 운영자, 시스템을 사용하는 사용자들이 시스템의 공격취약점을 알고 이를 예방하는 요소를 사용하게 된다면, 보다 안전한 시스템의 운영에 기여할 것으로 전망된다.

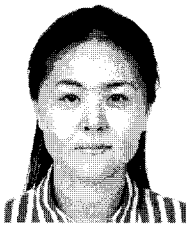
참고문헌

[1] 김재성, "생체인식시스템 표준적합성 및 보안성 평가모델", 인하대 정보통신대학원 공학박사 학위논문, 2005. 8.

[2] 특허청, "BioAPI 프레임워크와 독립적인 BSP기반

의 표준적합성 시험방법", 특허 제10-0750629호, 2007. 8.
[3] 김재성, X.tpp-1 : Guideline for Technical and Managerial Countermeasures of Biometric Data Security, ITU-T SG17/Q.8, 2008. 4.
[4] 김재성 외 3인, 생체정보보호 가이드라인, 정통부, 2005. 12.
[5] 김재성, Conformance Testing for BioAPI - Part1 : Methods & Procedures, ISO/IEC 24709-1, 2007. 1.
[6] TTA IT839 전략 표준화로드맵, "바이오인식", 2007. 12.

〈著者紹介〉

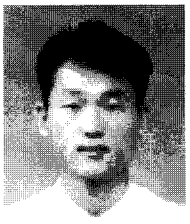


전 인 자 (Inja Jun)

1999년 2월 : 동양대학교 전산학과 학사
2001년 2월 : 인하대학교 이학석사
2005년 8월 : 인하대학교 공학박사
2005년 9월~2007년 8월 : 인하대학교 SITC 연구수 전임연구원
2006년 2월~2008년 2월 : 인하대학교 강의전임강사
<관심분야> 바이오인식, 영상처리, 상황인식

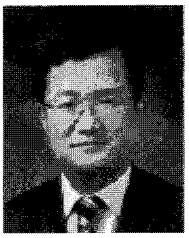
김 재 성 (Jason Kim)
정회원

1986년 2월 : 인하대학교 전산학과 학사
1989년 2월 : 인하대학교 이학석사
2005년 8월 : 인하대학교 공학박사
1996년 7월~현재 : 한국정보보호진흥원(KISA) 국가사이버안전센터(NCSC) 파견 팀장
2001년 2월~2007년 11월 : TTA PG103(바이오인식) 국내표준화 의장, JTC1 SC37 전문위원, KBA 사무국장
2007년 9월~현재 : 아시아바이오인식컨소시움(ABC) 사무국장, ITU-T SG17 · JTC1 SC37 에디터
<관심분야> 바이오인식, 정보보호 표준화, 금융 · 의료보안



하 도 윤 (Doyoon Ha)

1998년 2월 : 동아대학교 환경공학과 학사
2006년 2월 : 전남대학교 정보보호학과 석사
2005년 8월 : 전남대학교 박사과정
2000년 2월~현재 : 한국정보보호진흥원(KISA) NCSC 파견연구원
<관심분야> 정보보호, 시스템보안, 침해사고대응



최 재 유 (Jaeyou Choi)

1984년 2월 : 연세대학교 경영학과 학사
2000년 5월 : 미시간주립대학교 정보통신정책 석사
2008년3월~현재 : 방송통신위원회(KCC) NCSC 파견 국장
<관심분야> 정보보호, 방송통신 소비자보호, 네트워크 보안