情 報 保 護 學 會 誌
第 13 券 第 6 號, 2003. 12

지문인식시스템 보안기능 평가 방법론 연구

염 흥 렬*, 박 준 우**, 심 상 옥**

요 약

생체정보를 이용한 인식 기술의 사회적 요구가 빠르게 증대함에 따라 생체인식 기술에 대한 신뢰성에 대한 요구 역시 급속하게 증대되고 있다. 생체인식 기술에 대한 신뢰성은 생체인식시스템의 인식률에 대한 시험과 생체인식시스템에 대한 보안성 시험을 통해 보장될 수 있다. 보안성 시험은 크게 시스템 내부 및 외부 공격에 대한 안전성 등에 대한 일련의 항목들에 대해 시험을 한다. 이러한 보안성 시험에 대해 국외의 경우 자국기준 또는 공통평가기준에 따라 지문인식시스템을 포함한 생체인식시스템에 대한 보안성 시험을 수행되고 있으나 국내에서는 이에 대한 연구가 아직 미진한 상태이다. 본 연구에서는 제시하는 지문인식시스템의 보안성 평가 방법론은 지문인식시스템을 시험할 때 어떤 면을 고려하여 시험해야 하는지에 대한 지침을 제공하기 위한 것이라 할 수 있다.

Ⅰ. 서 론

신분확인은 정보보호 시스템을 통하여 내부 또는 외부의 객체에 대한 접근을 시도하는 사용자의 신분을 인증하고 인식하는 것이다. 대부분의 신분확인을 지원하는 시스템은 어떤 중요한 자산을 불특정 다수의 사용자들이 직접 접속을 하지 못하도록 하는 것이 목적이다. 여기에 사용하는 용어 중, 인증은 사용자 자신이 누구인지를 알리는 과정을 의미하고, 인식은 사용자가 정당한 사용자인지를 확인하는 과정으로 주로 인증 메커니즘이 사용된다. 여기에 사용되는 인증메커니즘 기술로는 일회용 패스워드, 암호기법을 이용한 인증방식, 생체특징을 이용한 생체인식방식 등이 다양하게 사용되고 있다. 여기에서 패스워드와 관련한 인증방식의 경우 현재 사용자 인증 방법 등에 많이 사용되고 있지만 패스워드의 분실이 쉽고 타인에게 노출되기 쉬워 언제라도 허점이나 취약한 구조를 통해서 개인을 안전하게 인증하는 수단으로써 문제가 있어 왔다. 이러한 문제점을 해결하기 위한 방법으로 개개인의 고유한 신체의 생리학적이고 행위학적인 생체인식방식이 사용되기 시작하였다.

또한 최근 생체인식기술에 대한 관심이 크게 높아지면서 보안성이 우수하고 사용이 간편한 생체인식기술 및 이를 이용한 보안장비의 개발이 활기를 띄고 있다. 이에 따라 국내에서도 지문, 정맥, 홍채, 음성 등 다양한 생체인식기술을 이용한 보안시스템이 개발 및 상용화되고 있다. 또한 생체인식기술의 응용분야도 단순한 오프라인상태의 물리적 보안장비에서 전자상거래 인증시스템 등 인터넷 보안시스템으로 점차 확산되어 가고 있는 추세이다. 특히 국내의 경우, 생체인식제품 시장이 활성화 된 것은 불과 2~3년 사이이지만 급속한 성장을 거듭하고 있다. 또한 아시아 및 국내시장의 경우 지문인식제품이 전체 생체인식기술 중 반 이상을 차지하고 있는 실정이다. 하지만, 이러한 빠른 성장에도 불구하고 제품에 대한 신뢰성이나 정확성 및 안전성을 보장하는 제도나 연구가 국외 기관이나 연구단체에 비해 활성화되지 못했다.

생체인식제품의 신뢰성이나 정확성 및 안전성을 보장하기 위해서는 생체인식시스템의 시험에 대한 기술이 필요하다. 생체인식시스템의 시험의 필요성은 크게 시장활성화 및 기술력향상이라는 측면에서 매우 중요하다. 전자는 사용자에게 신뢰성을 보장하는 것을 말하며 후자는 신뢰성 있는 수준의 성능 및 안전성을 요구하는 기준을 만족함으로써 경쟁력 있는 제품을 만들

* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)
** 한국정보보호진흥원 산업지원단 평가1팀({junupark, sangok}@kisa.or.kr)

수 있음을 말한다. 즉, 지문인식시스템들의 기술을 향상시키고 상업적으로 성공하기 위해서는 일반사용자가 지문인식시스템을 사용함에 있어서 편리성, 친근감, 경제성, 안전성, 정확성, 성능 등을 고려해야한다. 이렇게 함으로써 생체인식시스템의 상용화 초기단계에서 생체인식기술의 신뢰성을 확보하여 시장성을 보호할 수 있다.

본 연구에서는 생체인식시스템 중 지문인식시스템의 보안기능 시험방법론을 제시한다. 본 시험방법론은 침입차단시스템이나 침입탐지시스템과 달리 지문인식시스템에만 특화된 부분을 중점으로 위협에 대한 정의, 보안기능 시험방법, 기능강도 측정, 취약성시험 방법에 대해서 제시함으로서 지문인식시스템을 시험할 때 어떤 면을 고려하여 시험해야 하는지에 대한 체계성 있는 지침을 제공하기 위한 방법론이라 할 수 있다.

본고의 구성의 2장에서 먼저 국외의 지문인식시스템을 포함한 생체인식시스템의 평가동향을 살펴본 후, 본 연구에서 다루고자 하는 지문인식시스템에 대한 개요를 3장에서 설명한다. 4장에서는 지문인식시스템의 보안성 시험방법론을 그리고 마지막으로 5장에서는 결론을 기술한다.

Ⅱ. 국외 평가 동향

생체인식시스템에 대한 대표적인 연구 현황 및 프로젝트를 간단히 살펴보면, 현재 미 국방부 소속의 BMO(Biometrics Management Office)에서 생체인식시스템 평가 센터인 BFC (Biometric Fusion Center)를 군대 내에서 생체인식 기술을 사용하기 위하여 설립되어 운영중이다. BFC는 제품 평가를 수행함에 있어서 실내와 실외, 네트워크형태와 독립형태, 인증과 인식으로 구분하는 환경 테스트와 실제 환경에서의 필드테스트를 수행하고 있다.

영국에서는 정보보호 분야에 대한 인증기관 역할을 수행하는 CESG(Computer Electronic Security Establishment)가 생체인식시스템에 대한 성능뿐 아니라 보안성을 측정할 수 있는 기준개발이나 방법론을 개발하기 위하여 BWG (Biometrics Working Group)을 설립하였으며 독일, 이탈리아, 네덜란드 등이 참여하고 있다. BWG에서는 공통평가기준에 따른 생체인식시스템의 보안성 세부평가기준인 BDPP (Biometric Device Protection Profile)을 개발하고 개정중이다.[1]

독일의 경우는 정부산하 정보보호기관이 주관이 되어 생체인식시스템에 대한 보안성 평가에 대해서 연구하고 있으나 미국이나 영국의 경우에서처럼 공통평가기준에 따른 생체인식시스템 세부평가기준을 개발하여 평가하는 것이 아니라, 독일 자체의 평가기준을 통해서 평가한다는 점이 차이점이라 할 수 있다. GISA (German Information Security Agency)는 정보보호시스템 평가기준, 절차 및 도구개발, 평가시행 및 인증서 교부 등에 대한 정책적 규정, 국가정보보호기관으로서 암호, 정보시스템 보안 및 전자파 보안등의 보안업무 수행을 하는 기관으로서 생체인식시스템의 성능 및 보안성평가를 위해서 EvalKrit라는 프로젝트를 진행하였으며, 이 프로젝트를 통하여 시험과정을 일반적 평가, 인식률의 신뢰성, 보안성 등 3단계로 구분하여 시험 할 수 있도록 자체 기준을 제시하였다.[2]

Ⅲ. 지문인식시스템의 개요

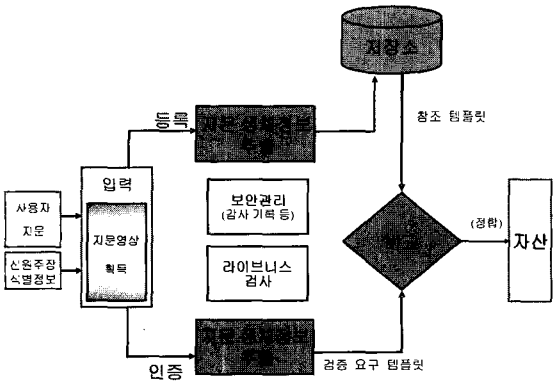
지문인식시스템의 주요 구성요소는 지문정보 입력, 인증, 관리, 저장, 전송으로 나눌 수 있다.[3] 또한 지문인식시스템이 운영되기 위해서는 두 가지의 처리절차를 가지고 있어야 한다. 첫 번째는 지문정보를 지문인식시스템에 등록하기 위한 등록처리과정이며, 두 번째는 등록된 지문정보를 바탕으로 하여 인증기능을 수행하는 인증처리과정이 있다. 참고로 인증처리과정의 경우 시스템의 사용분야에 따라 등록된 사용자의 지문정보와 신원확인을 요구하는 사용자에 해당하는 등록된 사용자와 1:1 비교 확인하는 인증(Verification) 시스템과 신원확인을 요구하는 사용자에 대해서 등록된 모든 사용자의 생체정보를 1:N 형식으로 비교 확인하는 인식(Identification) 시스템이 있다.[4]

[그림 1]은 앞서 설명한 바와 같이 지문인식시스템의 구성도를 나타낸다.

1. 지문인식시스템 구성요소

지문인식시스템은 입력, 인증, 관리, 저장, 전송으로 구성된 주요구성요소를 통하여 등록과 인증처리과정을 수행한다.

등록처리과정은 지문인식시스템에 사용자의 지문정보를 입력장치를 통하여 입력하여 입력된 지문영상으로부터 특징점을 추출하여 템플릿을 생성하고 저장장치에 사용자의 부가정보와 같이 저장하는 과정을 의미한다. 이렇게 저장된 템플릿은 인증처리과정에서



〔그림 1〕 지문인식시스템 구성도

사용된다. 저장 과정에서 입력부분과 저장장치가 분리되어있는 경우 전송과정이 요구되기도 한다. 또한 템플릿이 저장되는 매체의 경우 대규모 분산환경에서 사용되는 집중화된 데이터베이스에 저장 될 수도 있고, 스마트카드와 같은 이동식 저장매체에 등록이 가능하다.

인증처리과정은 등록된 템플릿과 신원확인을 요구하는 사용자의 템플릿을 비교하여 사용자의 신분확인을 수행한다.

1.1 입력

입력 구성요소는 사용자의 지문 특징을 수집할 수 있는 입력 장치를 포함한다. 이들 입력 장치는 사용자의 지문영상으로부터 특징정보를 읽고 이 정보를 지문인식시스템의 나머지 구성요소들이 처리하기에 적절한 형태로 변형한다. 이 구성요소의 출력물은 인증이나 전송 등의 구성요소로 전달되며 이 구성요소에서 지문인식시스템의 성능이나 보안에 영향을 주는 사항으로는 지문입력방식, 입력장치에 의해서 수집된 지문영상 표현, 입력장치 자체 성능, 주변의 환경 등이다.

1.2 인증

인증 구성요소는 입력 구성요소로부터 지문영상을 받아서 사용하기에 적당한지를 결정하기 위해 영상 품질을 분석하는 기능을 수행한다. 만약 분석결과가 적합하지 않다고 판단되면, 처리되지 않을 것이며, 적합하다고 판단되면, 비교를 하기 위한 템플릿 형태로 변환 할 것이다. 특히, 품질을 분석하는 기능에서는 입력되는 지문영상에 대한 불필요한 잡음이나 값들을 제거한다.

비교를 하기 위한 템플릿 형태로 변환하게되면, 등록된 템플릿과 비교기능을 수행하게된다. 비교기능을 수행 시 비교 값에 따른 스코어를 산출하게되고 이것은 정책에 따라 정해진 임계값에 의해서 사용자의 신원을 확인할 수 있다. 만약 정해진 임계 값이 너무 낮게 되면, 잘못 인식될 확률인 FAR (False Acceptance Rate)이 높아져서 시스템의 성능이 저하되는 요인을 제공하고, 임계값이 너무 높게 되면, 특정 환경변수에 의한 값이나, 영향요소에 의해서 정당한 사용자의 인식이 거부되는 FRR (False Rejection Rate)이 높아져 시스템의 성능이 저하되는 요인을 제공할 수 있다[4]. 그러므로 관리구성요소에서 시스템과 환경에 적절한 임계값 설정의 정책이 요구된다.

1.3 관리

관리 구성요소는 지문인식시스템에서 사용되는 보안 매개변수, 사용자 등록 및 관리, 사용자 데이터관리, 시스템 로그관리 등을 지원하는 요소를 지원한다. 사용자 등록 및 관리에서 사용자는 보안관련데이터를 접근할 수 있는 권한을 가진 관리자 그룹의 설정 및 관리를 수행하도록 할 수 있고 일반사용자는 신분확인에 필요한 기능을 사용하도록 결정할 수 있다. 또한 임계값과 같은 보안 매개변수에 대한 조정 및 수정을 할 수 있고, 사용자 정보 및 시스템의 인증결과처리 로그데이터를 관리할 수 있는 기능을 제공한다.

1.4 저장

저장 구성요소는 기본적으로 등록된 사용자의 템플릿을 유지한다. 만약 저장 구성요소가 템플릿을 저장하는 이외의 기능을 제공해야 한다면 등록된 템플릿의 추가, 삭제 그리고 복구 기능을 제공할 수도 있다. 저장 구성요소는 단일 사용자를 위한 단일 템플릿만을 저장할 수도 있고, 많은 사용자를 대상으로 수천 개의 템플릿들을 저장할 수도 있다. 템플릿들은 지문인식시스템 자체에 물리적으로 보호된 저장 장소에 저장될 수 있고, 시스템 내에 일반적인 데이터베이스에 저장될 수도 있다. 또한 휴대가 가능한 이동식 저장매체인 스마트카드에도 저장이 가능하다. 기본적으로 각 저장소에 저장된 데이터는 기본적으로 사용자의 템플릿을 포함하지만, 필요 시 다른 정보 또한 포함될 수 있다.

1.5 전송

전송 구성요소는 구성요소들 간의 정보 전송 기능을 제공한다. 시스템 구성요소들은 단일 보안 시스템

으로 구성되거나 원격지로 분리되어 구성될 수 있다. 전송 구성요소는 하나의 전송 매체만을 이용할 필요는 없다. 여러 종류의 다양한 전송 매체로 구성될 수도 있다. 이러한 매체들은 연결된 구성요소 간에 신뢰성, 무결성, 인증과 같은 보안 서비스를 제공할 수도, 제공하지 않을 수도 있다.

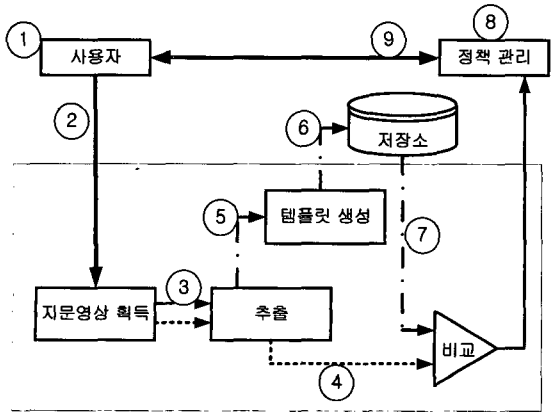
Ⅳ. 지문인식시스템 보안기능 평가 방법론

지문인식시스템에 존재하는 위협이 어떤 것이냐에 따라 지문인식시스템에 구현해야 될 보안기능과 그 시험 방법론이 달라지기 때문에 먼저 지문인식시스템에 존재하는 위협을 정의하고 각 위협을 막기 위해 구현해야 될 보안기능을 나열한 후, 각 보안기능에 대한 시험방법론을 정의한다.

1. 위협

지문인식시스템에 존재하는 위협을 분류하면 크게 지문인식시스템에 자체에 대한 위협과 지문인식시스템의 운영환경에 따른 위협으로 분류할 수 있다. 그리고 지문인식시스템 자체에 대한 위협은 또 다시 등록된 사용자로 가장하여 자산에 접근을 시도하는 사칭 관련 위협과 지문인식시스템 자체의 취약성을 이용한 취약성 관련 위협이 있다. 본 연구에서는 지문인식시스템 자체에 대한 위협에 대해서만 다루기로 한다. 〔그림 2〕는 지문인식시스템에서 이러한 위협들이 발생할 수 있는 위치를 나타낸 것이다.

사칭 관련 위협의 대표적인 예로서는 첫 번째 공격자가 접근권한을 획득하기 위해 인가된 사용자의 지문과 유사한 인공물을 제작하여 인증을 성공하는 위협을



〔그림 2〕 지문인식시스템에서의 위협

들 수 있다. 이 위협은 특히, 지문에 대한 인공물 제작을 쉽게 할 수 있는 장비가 있어 공격이 용이하기 때문에 지문인식시스템에서 인공물에 대한 위협으로 잘 알려져 있다. 두 번째로 지문인식시스템은 지문영상 입력장치와 물리적인 접촉이 요구되기 때문에 지문영상 입력장치에 잔존하는 영상에 취약하다. 지문영상 입력장치에 잔존하는 이미지를 남긴 채 떠난 인가된 사용자의 지문이 바로 뒤따라서 접근권한을 획득하고자하는 공격자에게 이용될 수 있는 위협을 가지고 있다.

지문인식시스템 취약성 관련 위협으로는 먼저 인식률에 관련된 위협으로는 공격자가 인가된 사용자와 비슷한 지문특징을 가지고 인증을 시도하는 등 단순히 인식률의 성능에 의존하여 인증시도를 성공할 수 있는 위협이 있다. 이 위협은 지문인식시스템의 낮은 인식률 때문에 유사한 지문특징을 구별하지 못하여 사칭자가 자산에 대한 접근권한을 얻을 수 있는 위험을 야기시킨다. 그리고 지문인식시스템의 구성요소간의 전송 시 전송되는 데이터를 조작하여 발생시키는 위협을 들 수 있다. 지문인식시스템은 앞서 설명하였듯이 크게 입력, 인증, 관리, 저장 등으로 구분 지을 수 있는데, 전송 시의 위협은 이 들 각각의 구성요소들 간의 전송 시 발생한다. 먼저 입력과 인증 구성요소간의 전송 시 위협으로는 지문영상 획득장치로부터 획득된 지문영상이 인증구성요소로 전송 시 이에 잡음 등을 첨가하여 불안정한 정보로 조작을 하여 인가된 사용자의 서비스를 막을 수 있다. 그리고 인증구성요소와 관리구성요소간의 전달되는 인증결과에 대한 조작 위협이 있는데 공격자는 인증구성요소에 의해서 인증 처리된 결과를 설계과정의 취약점을 이용하여 변경할 가능성이 있다. 마지막으로 입력/인증 구성요소와 저장구성요소사이에 전달되는 템플릿의 조작 위협이 존재한다. 공격자는 등록단계에서 입력구성요소를 통하여 인증구성요소에 전달된 템플릿을 저장장치에 전달하는 과정에서 조작될 가능성이 있고, 인증단계에서 인증구성요소에 의해서 저장된 템플릿을 저장장치로부터 전달받는 과정에서 템플릿의 조작가능성이 존재한다.

이 외에도 관리상의 실수 때문에 발생할 수 있는 위협들이 있다. 예를 들어, 적당하지 못한 FAR이나 FRR 값의 설정으로 공격자의 인증시도가 성공하거나 정규 사용자의 인증시도가 실패할 수 있고, 관리자가 정규 사용자에게 추가적인 권한을 부여할 경우 실수로 적절치 않은 권한을 부여함으로서 야기될 수 있는 위협을 가지고 있다. 그리고 지문인식시스템은 다른 정보보호제품과는 달리 사용자 인증을 하기 위해서 지문

영상 입력장치가 외부로 노출되어 있어 이러한 지문영상 입력장치는 공격자에게 일차적으로 공격대상이 될 수 있다.

마지막으로 저장소와 관련된 위협을 살펴보면, 저장소가 안전하게 유지·관리되지 않을 경우, 공격자가 지문템플릿과 사용자 정보가 저장되어 있는 저장소를 공격하여 필요로 하는 정보를 수정, 추가, 삭제 등을 할 수 있으며 이를 후에 인증 시 사용하여 서비스 거부나 인가되지 않은 사용자의 인증 성공 등을 야기 시킬 수 있다. 그리고 사용자가 스마트 카드와 같은 이동식 저장매체에 자신의 정보를 소유하고 있다면, 동일한 형태의 저장소에 사칭자가 자신의 정보를 저장하여 인증을 시도하는 위협이 존재한다.

2. 보안기능

앞서 나열한 위협들을 막기 위해서는 여러 보안기능들이 필요하다. 이 중에서는 지문인식시스템과 관련이 있는 보안기능들만 살펴보기로 한다.

먼저 암호화 지원을 들 수 있는데, 일반적으로, 생체인식 시스템은 참조 템플릿을 자체 시스템 또는 사용자가 항시 휴대하는 이동식 저장매체(예, 스마트카드)나 템플릿의 중앙 집중화 데이터베이스에 저장할 수 있다. 자체 시스템에 저장하거나 이동식 저장매체에 저장하는 경우에는 설계 시 템플릿을 보호할 수 있도록 보장될 수 있다. 그러나 아키텍처의 개념에 중앙 집중화 데이터베이스로부터의 템플릿 검색 또는 템플릿을 공공 영역 내에서의 전송이 포함되는 경우, 템플릿을 보호하기 위한 수단이 필요하다. 암호화는 안전한 경로와 채널, 그리고 생체인식 템플릿의 프라이버시와 보호를 보장하기 위해 일부 생체인식 시스템에서 사용되는 수단이다. 이는 특정한 어플리케이션에 맞는 사용자 데이터를 위해 사용되는 경우도 있다. 템플릿이 보호된 환경 밖에 상주하고 있는 동안 변조 또는 교체로부터 이를 보호하기 위해, 일부 시스템들은 템플릿에 내부적으로 생성되는 형태의 암호화키를 이용하여 암호화하고, 보호된 환경 내에서 복호화하게 된다. 이러한 방법을 이용하면 기술이 사회적으로 수용될 중요한 원인이 되는 문제를 해결할 수 있으며 사용자의 생체인식 템플릿의 프라이버시를 보장할 수 있다. 이러한 기능들은 템플릿의 생성, 저장, 전송 기능에 적용할 수 있다.

인증기능은 각 사용자가 주장하는 신분을 확인하고 각 사용자가 자신이 주장하는 신분과 일치함을 검증하기 위한 기능이다. 지문인식시스템에서는 본 기능은 인식률과 관계가 있다. 암묵적으로 지문인식시스템은 100% 완벽한 것은 아니고 특성이 중복 될 수 있다. 인간의 특성이 유일할 수는 있더라도, 이들 특성을 측정하기 위한 기술과 기법에는 편차가 내재되어 있다. 이유는 응용 기술이 부정확할 수도 있고, 특성들이 표현되고 측정되는 환경이 부정확할 수 있기 때문이다. 이러한 오차에 의해 FAR과 FRR의 결과가 나타난다. 이 두 가지 비율간에는 상반된 관계가 존재하는데, FAR의 비율이 낮아질수록 FRR이 높아지게 되며, 그 역도 성립한다. 따라서 이 보안기능에 대해 "분명한 인증"이라는 요구사항에 근접하기 위해, FAR과 FRR의 비율에 대해 정해져야 한다.

사용자데이터 보호기능은 사용자 데이터를 보호하기 위해 사용자 데이터의 송신, 수신 및 저장 시, 지문인식시스템 내에서 사용자 데이터와 직접적으로 관련이 있는 보안속성과 사용자 데이터 보호를 위한 기능이다. 이 기능은 템플릿 생성 과정의 역추적과 본래 지문 영상으로의 재구성을 막아야 하며 템플릿에 대한 불법 변조, 지문인식시스템 외부에서의 불법적 사용을 위한 템플릿의 복제, 지문인식시스템내의 템플릿을 공격자의 템플릿으로 교체를 막아야 한다.

지문인식시스템의 인식률을 높이기 위해서는 지문영상 품질제어기능은 있어야 한다. 지문영상 품질은 특징점을 추출하는데 영향을 주며, 나쁜 품질의 영상은 등록실패나 지문인식시스템의 안전성에 위협을 줄 수 있다. 지문영상의 품질은 크게 날씨, 온도, 습도, 압력 등의 환경적 요인과 손가락의 손상정도, 주름 정도 등의 사용자적 요인에 의해 영향을 받는다.

마지막으로 Liveness Detection 기능을 들 수 있다. Liveness Detection 기능은 인공물 제작을 통하여 사칭자가 인가된 사용자로 인증되는 취약성을 확인하기 위한 기능이다. 다시 말해 지문인식시스템이 지문을 입력하는 것이 사람의 진짜 손가락인지 아니면 인조 손가락인지를 알아내는 기능이다. 이러한 취약성은 대부분의 지문인식시스템이 가지고 있는 문제 중 가장 큰 문제이다. 이러한 문제를 해결하기 위한 방법으로는 획득된 지문영상을 처리하여 검사하는 소프트웨어 방법과, 다른 하드웨어를 추가하여 지문영상 획득 시 지문을 입력하는 손가락을 검사하는 하드웨어 방법이 있다. 소프트웨어 방법의 기본 원리는 사람의 손가락의 경우 지문 입력시 시간이 지남에 따라 지문의 상태가 땀 등에 의해 변한다는 원리를 이용하여 소프트웨어적으로 일정한 시간마다 지문의 상태 변화를

통해 검사하는 방법이다.[6] 그리고 하드웨어 방법은 하드웨어를 이용하여 손가락의 온도를 확인하거나, 손가락이 전기가 통한다는 전기적 성질을 이용하거나, 아니면 맥박의 산소농도, 맥박 등을 하드웨어로 검사하는 방법을 말한다.

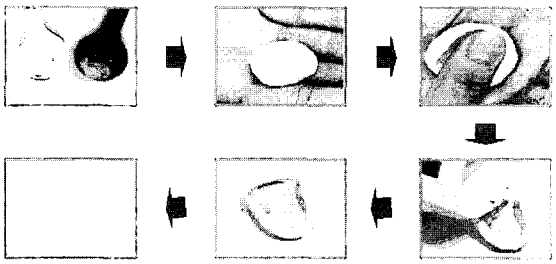
3. 보안기능 평가 방법

보안성 시험은 시스템 성능평가도 아니고, 어떤 기술이 최고인지를 판단하는 척도도 아니며 특정 어플리케이션에 어떤 시스템이 가장 적합한지를 판정하기 위한 시험도 아니다. 이는 시스템이 보안기능 및 보증요구사항을 충족하는 정도를 판정하기 위한 시험이다.

보안성 시험은 크게 입력구성요소에서 기만성 시험과 인증구성요소의 취약성 시험을 들 수 있다.

3.1 기만성 시험

기만성 시험은 Liveness Detection 기능에 대한 시험을 말하며 Liveness Detection 기능에 대해 시험을 하기 위해서는 실제 지문 인공물을 제작하여 해당 시스템이 이를 감지하는지에 대하여 시험을 수행하여야 한다. 지문인공물을 제작하는 대표적인 방법으로는 젤라틴과 실리콘을 이용하여 제작하는 방법이다. 그림 3은 지문 인공물을 제작하는 과정을 나타내고 있다.[7]



〔그림 3〕 지문 인공물 제작과정

이렇게 제작된 인공물을 이용한 기만성 시험방법으로는 표 1과 같이 인공물과 실제 손가락을 등록 시켜놓고 인증 시에 다시 인공물과 실제 손가락으로 시도해가며 시험을 수행한다.[10]

기만성 시험 시 주의할 점은 인공물의 굳음에 따라 인식률이 달라진다는 것이다. 따라서 인공물 제작 직후, 제작 후 6시간 경과 후, 12시간 경과 후, 24시간 경과 후 등으로 제작완료 후 일정 시간대별로 기만성 시험을 하는 것이 좀 더 정확한 결과를 얻을 수 있다.

〔표 2〕 시험 타입

형태	등록	인증
L-L	실제손가락(L)	실제손가락(L)
L-G	실제손가락(L)	인공물(G)
G-L	인공물(G)	실제손가락(L)
G-G	인공물(G)	인공물(G)

본 시험이 모든 인공적인 지문을 찾아낼 수 있는 완벽한 기법은 되지 못한다. 때문에 그 원리를 알면 우회 방법이 존재 할 수 있다. 따라서 이에 대한 지속적인 연구가 필요하다.

3.2 취약성 시험

취약성 시험은 지문인식시스템의 오용이나 부정확한 구성, 확률 메커니즘이 파괴될 가능성, 그리고 악용 가능한 취약성이 개발이나 운영 중에 나타날 가능성을 다루며, 크게 오용시험, 보안기능강도 시험, 취약성 분석 등으로 나눈다.[11]

3.2.1 오용시험

오용 시험이라 함은 지문인식시스템이 잘못된 환경설정이나 이로 인한 잘못된 사용이 되는지 시험하는 것으로 운영 시 사람이나 기타 오류에 의해 보안기능을 비활성화 시키거나, 무력화하거나, 활성화하지 못하여 탐지하지 못한 안전하지 않은 상태가 될 위협을 최소화하는 것에 그 목적이 있다.

오용 시험의 방법으로는 먼저 지문영상 품질제어를 들 수 있는데 등록을 위해서 부적당한 지문영상 품질제어 기준을 설정한다면 지문인식시스템이 취약한 지문영상을 받아들여서 안전성에 위협을 받을 수 있기 때문이다. 이러한 지문영상 품질제어에 대해 시험하기 위해서는 인위적으로 나쁜 품질의 영상을 수집하여 시험을 수행하여야 한다. 지문영상 수집 시 영상의 품질에 영향을 미치는 온도, 습도, 그리고 압력 등의 환경적 요인을 고려하여 수집하여야 한다. 그 온도와 압력에 대한 예시로는 표 3,4와 같다.

〔표 3〕 온도에 따른 분류

온도	상태
0도 이하	겨울
0도 ~ 10도	초봄, 늦가을
10도 ~ 20도	봄, 가을
20도 ~ 30도	상온
30도 이상	여름

〔표 4〕 압력에 따른 분류

압력	상태
저압	살짝 얹어 놓은 상태
중압	일반적인 상태
고압	강한 압력을 가한 상태

습도에 대하여 고려할 시에는 피부 습도와 대기 습도를 같이 고려하여 지문영상을 수집하여야 한다.

3.2.2 기능강도 시험

기능강도 시험은 지문인식시스템의 시험 중 가장 중요한 부분이다. 기능강도와 밀접한 관련이 있는 요소는 FAR이나 FMR과 같은 측정치이다. 하지만, 이러한 수치에 대한 기준은 명확히 정해진 바가 없다. 이러한 기능강도에 대한 측정을 위해서는 지문인식시스템의 인식률 측정이 선행되어야 하고, 측정을 위해서는 적절한 시험 데이터가 필요하다. 시험 데이터의 중요한 특성은 다음과 같다.

- 데이터는 지문인식시스템의 "정상적인" 또는 예상되는 운영 조건(조명, 기후, 이동, 주변 환경 등과 같은 환경적 조건 등)을 대표해야 한다.
- 데이터는 FAR 비율을 정확하게 측정할 수 있을 만큼의 충분한 크기여야 한다.
- 그리고 데이터는 수집된 표본(예, 성별, 연령, 직업 및 기타 생체인식 정보)의 형태를 대표해야 한다.

지문인식시스템의 성능 시험과 관련한 현행 참고 문헌들에 따르면, 시험 결과에 대한 "통계적 신뢰"를 갖기 위해 대략적이라도 몇 회가 적정한 지를 예측하기가 어렵다고 주장한다. 즉, 임의의 어플리케이션에서 지문인식시스템의 특성을 적절하게 규명하는데 필요한 시험 횟수를 정확하게 예측할 수 있는 방법은 현재로는 없는 셈이다. 그러나 다음과 같은 사항들을 고려 할 수는 있다.

"Doddington의 법칙"에 의하면 요구되는 비교 회수와 시험 주제는 30회 오류를 기초로 한다고 한다. 시험 횟수가 30회의 오류를 발생할 만큼 많다면, 에러율의 수치가 측정치의 약 40%의 범위에 드는 95% 신뢰 수준에 있다. 실제로 시험할 때는 가능한 실질적으로 활용될 수 있는 많은 사용자들을 이용해야 한다. 그리고 각 사용자들은 가능한 많은 시간에 의해서 구분된 여러 개의 표본을 제공한다. 수집된 데이터는 사용될 응용프로그램과 대상 모집단과 상당히 유사해야 한다.[8]

시험 데이터의 품질과 시험 데이터가 수집된 조건은 FAR 비율 예상 결과에 영향을 미친다. 저질의 시험 데이터들은 지문인식시스템의 진정한 능력을 반영한 결과를 산출해 내지 못할 수도 있다. 이와 마찬가지로, 대단히 양질의 데이터 역시 정확히 의도된 운영 환경을 반영하지는 않기 때문에 자동화 시스템의 진정한 성능을 나타낼 수 없기는 마찬가지이다.

표본 추출에 관한 또 다른 접근 방법을 보면, FAR 비율 예측은 실험 결과 수집에 기초한 값들을 통해 최상의 값을 만드는 것이며, 예상 값에 대한 신뢰 정도를 인식하는 것이라고 언급하였다. 시험 또는 실험할 때 동일하고 독립적인 시도들을 반복하였고, 각각은 결과를 산출한다. 각 시험 시도를 통해 획득한 결과는 이전의 결과 혹은 이후의 결과 어느 것에도 의존하지 않는 것이며, 이러한 것들은 독립적인 시도이다. 독립적인 시도의 횟수가 증가하면, 시험 결과 역시 더 의미 있는 결과를 도출하게 될 것이다. 자동화 생체인식 기반 인식 및 검증 시스템에 대한 예상은 반복적인 베르누이 실험 결과를 바탕으로 파라미터 예상 값으로 공식화될 수 있다.[9]

세 번째로 제시되는 접근 방법은 지문인식시스템의 기능강도와 FAR 비율을 산출하기 위해 사용된 표본 크기/유형 사이의 균형을 맞추는 것이다. FAR 비율은 본질적으로 측정된 특성의 유일성을 나타낸다. 그러나 통계적으로 대표성을 지니는 표본 크기는 생체인식 장비 측정에 대한 모든 변수들을 입증하기 위하여 필요하다. 생체인식정보의 유일성이 중요한 자료로 입증된다면, 유일성에 대한 입증 자료가 부족한 지문정보이기 보다는 FAR 비율을 계산하기 위해 보다 적은 수의 표본을 수용하는 것이 합리적일 수 있다(이 경우 통계적으로 대표성을 지닌 크기가 FAR 비율을 제공하기 위하여 사용되어야 한다). 그러나 이러한 접근 방법은 예측과 관련한 신뢰성을 측정할 방법을 갖추고 있지 않다.

지문인식시스템 기능강도를 산출하기 위해 사용되는 마지막으로 제안하는 방법은 시뮬레이션방법이다. 성능은 정확하게 시뮬레이션을 하기 어려운 요소들에 대단히 의존적이기 때문에 시뮬레이션은 성능 시험 관점에서는 일반적으로 사용되지 않는다. 그러나 보안성 평가의 측면에서 볼 때, 이 접근 방법은 적절하다고 할 수 있다. 이러한 방법은 이전에 수집한 템플릿이 정확한 일치성 여부와 FAR을 검토하기 위하여 각 템

플릿과 모든 다른 템플릿을 비교할 수 있는 일치 알고리즘에 오프라인으로 제시하는 경우에 사용하도록 제안하고 있다. 이는 낮은 수준의 오류 비율을 검증하기 위해 필요한 일대다 교차 비교를 하기에는 실용적이다. 비록 복잡하고 어렵기는 하지만, 생체인식정보의 각 변형 단계에서 변형 효과를 평가하기 위한 시도, 그리고 각각의 고유한 독자성에 대하여 얼마나 효과적으로 유지되는가를 평가하기 위한 시도는 또 다른 접근 방법일 수 있다. 시뮬레이션은 살아 있는 표본 대신 특정 기계에 맞는 파일을 사용할 수 있다. 그러나 이 접근법은 일치 알고리즘만을 검증하는 것이며 장비의 생체인식 수집 메커니즘을 검증하지는 않는다. 그러므로, 시뮬레이션 시험 횟수를 늘이고 이를 적절한 방법으로 지원하기 위해서는 수집 메커니즘에 대한 추가적인 실험이 필요하다.

3.2.3 취약성 분석

취약성 분석은 개발, 구조, 지문인식시스템 보안정책을 위반하는 사용자들을 허용하는지에 대한 것들과 같은 취약성들을 확인하기 위해 시험하는 것이다. 지문인식시스템의 취약성 분석은 기타 정보보호제품들에 비하여 독창적이거나 크게 다르지 않다.

V. 결 론

지금까지 본 연구에서 지문인식시스템에 존재하는 위협들과 각 위협에 해당하는 보안기능들 그리고 그 보안기능들을 시험할 수 있는 시험 방법론에 대하여 제시하였다.

지문인식시스템이 다른 정보보호제품과 다른 대표적인 위협으로는 사칭관련 위협과 인식률 관련 위협을 들 수 있다. 사칭관련 위협으로는 인가된 사용자의 지문과 유사한 인공물을 제작하여 인증을 시도하는 위협과 지문영상 입력장치에 잔존하는 이미지를 이용하여 인증을 시도하는 위협 등이 있다. 인식률 관련 위협으로는 공격자가 인가된 사용자와 비슷한 지문특징을 가지고 인증을 시도하는 등 단순히 인식률의 성능에 의존하여 인증을 시도하는 위협이 있다.

제시된 주요 지문인식시스템 시험방법론으로는 기만성 시험, 지문영상 품질 제어 시험, 그리고 기능강도 시험이 있다. 기만성 시험은 젤라틴이나 실리콘 등으로 직접 지문 인공물을 제작하여 시험을 수행하는 방법을 기술하였으며, 취약한 지문영상을 받아들여서 안전성에 위협을 주는 것을 막기 위한 지문영상 품질 제어 시험에 대해서도 설명을 하였다. 그리고 지문인식시스템의 시험 중 가장 중요한 부분인 기능강도 시험에 대해서 제시하였다. 기능강도 시험을 수행하기 위해서는 적절한 시험 데이터가 필요하다. 기능강도는 시험데이터에 의해서 기능강도가 달리 나타날 수 있기 때문에 시험데이터 수집 시에는 운영조건과 데이터의 크기, 데이터의 수집된 표본을 충분히 고려하여야 한다.

본 연구에서 제안된 지문인식시스템 보안성 시험방법론을 바탕으로 지문인식시스템의 보안성을 개선시키고, 시험 결과의 투명성, 객관성, 재현성을 확보하여 시스템에 대한 사용자의 안전성 및 신뢰성을 향상시키며, 지문인식기술의 공인된 검증으로 인한 기술 개발에 많은 효과를 가져올 수 있으며, 이를 통해 국내 생체인식 산업 전반에 걸쳐 기술 경쟁력 확보 및 국외 시장 개척에도 기여 할 수 있을 것이다.

참고문헌

[1] BWG, "Biometric Device Protection Profile", BWG, October 26, 2000.

[2] GISA, "Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems", GISA, June 8, 2001.

[3] American Banking Association, "ANSI X9.84-2000, Biometric Information Management and Security for the Financial Services Industry", ANSI, 2000.

[4] "Glossary : Defense Acquisition Acronyms and Terms", Eighth edition, (U.S.) Department of Defense, Defense Systems Management College, Acquisition Policy Department, May, 1997.

[5] CSE, "Biometric Technology Security Evaluation Under The Common Criteria", CSE, September, 2001.

[6] Stephanie Schuckers, "Issues for Liveness Detection in Biometrics", Proceedings of the Biometric Consortium Conference, Vol.1, 2002.

[7] Tsutomu M., Hiroyuki M., Koji Y., and Satoshi H., "Impact of Artificial Gummy Fingers on Fingerprint Systme", Optical Security and Counterfeit Deterrence Techniques IV, Vol.4677, pp275-289, 2002.

[8] Wayman, J. L., Biometric Technology Testing, Evaluation, Results, CTST 99, May 1999.
[9] Shen, W., Surette, M., Khanna R.," Evaluation of Automated Biometrics -Based Identification and Verification Systems", IEEE, Vol 85, No. 9, September 1997.
[10] 한국정보보호진흥원, "Biometric 인증시스템 보안성 평가기술 개발", 한국정보보호진흥원, pp.330-332, 2003.
[11] 한국정보보호진흥원, "정보보호시스템 공통평가기준", 정보통신부, 2002.

〈著 者 紹 介〉

염 흥 열 (HeungYoul Youm) 종신회원

1981년 : 한양대학교 전자공학과 졸업
1983년 : 한양대학교 대학원 전자공학과 석사
1990년 : 한양대학교 대학원 전자공학과 박사
1982년~1990년 : 한국전자통신연구소 선임연구원
1990년~현재 : 순천향대학교 공과대학 정보기술공학부 교수, 정보보호학과 학과장
1997년~2000년 : 순천향대학교 산업기술연구소 소장
2000년~현재 : 순천향대 산학연컨소시엄센터 소장
1997년~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안

박 준 우 (Jun-Woo Park)

1999년 2월 : 경성대학교 수학과 이학사
2002년 2월 : 인하대학교 전자계산공학과 공학석사
2002년 1월~현재 : 한국정보보호진흥원 평가1팀 연구원
〈관심분야〉 정보보호시스템 평가, 생체인식, 네트워크 및 시스템 보안

심 상 옥 (Sang-Ok Shim)

1997년 2월 : 중앙대학교 컴퓨터공학과 공학사
1999년 2월 : 중앙대학교 컴퓨터공학과 공학석사
1999년 2월~2001년 10월 : GIS 소프트 대리
2001년 11월~현재 : 한국정보보호진흥원 평가1팀 연구원
〈관심분야〉 정보보호시스템 평가, 생체인식, 네트워크 및 시스템 보안