다중사용자인증시스템에서의 인증신뢰지수 적용에 대한 연구1)

박선호*, 김희승*, 한영주*, 정태명**
*성균관대학교 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:*{shpark, hskim, yjhan}@imtl.skku.ac.kr,
**tmchung@ece.skku.ac.kr

A Study on Applying a Calculation Method of the Authentication Trust Index for Multiple User Authentication Systems

Seon-Ho Park*, Hee-Seung Kim*,Young-Ju Han*,
Tai-Myoung, Chung**
*Department of Computer Engineering, SungKyunKwan University
**School of Information & Communication Engineering, SungKyunKwan University

요 약

다양해진 응용서비스들만큼이나 다양해진 사용자 인증 메커니즘들이 등장하였다. 이들은 강한 인증 기능을 제공하기 위해 종종 여러 메커니즘들이 혼합되어 사용되기도 한다. 각기 다른 인증메커니즘들은 각각의 특성에 따라 다른 신뢰수준을 갖기 때문에 여러 인증방식들 간의 신뢰수준을 비교할 수 있는 지표가 필요하다. 본 논문은 사용자인증 수단의 신뢰도를 가늠하기 위해 인증신뢰지수를 적용하는 방안과 다중사용자인증시스템에서 인증신뢰지수를 계산하는 알고리즘에 대해 제안한다.

1. 서론

전자정부와 전자상거래 등과 같이 인터넷을 이용하여 이루어지는 많은 서비스들은 정당한 서비스 주체만이 서비스를 이용할 수 있도록 하기 위해 다양한 사용자 인증 메커니즘을 사용한다. 다양해진 인터넷 서비스만큼이나 다양한 사용자 인증 메커니즘들이 등장했다. 보통 전자상거래나 전자정부서비스 이용 등은 패스워드나 공인인증서 등을 이용한 사용자 인증만으로도 안전하게 서비스 주체를 인증할 수 있다. 하지만 최근 대두되고 있는 유비쿼터스 센서 네트워크 기술 기반의 서비스들은 산재되어 있는 다양한 기기들에 인증을 받아야 할 필요가 있으며 이러한 다양한 기기들은 그 사용방법 및 목적에 따라 다양한 사용자 인증 방식을 사용하게 된다. 즉 하나의 서비스를 받기 위해 종종 여러 기기들에 인증을 받아야 하는 경우가 생기며 이에 따라 다양한 사용자 인증 메커니즘들이 혼합되어 사용되는 것이다.

사용자인증 방식에는 전통적인 패스워드 방식에서 스마트카드나 공인인증서를 이용하는 방식, 그리고 생체정보를 이용하는 방식 등 다양한 메커니즘들이 존재한다[1][2]. 이들 인증 메커니즘들은 인증방식에 따라 각기 다른 인증 수단을 갖고 있으며 따라서 인증 수단의 특성에 따라 각 인증 메커니즘들의 신뢰도가 다르다. 즉, 인증 정보로서 이용되는 수단에 따라 인증정보의 도난, 위조, 분실 등의 위험률이 다르기 때문에 각 인증 방식의 에러 확률이 다르게 나타나는 것이다. 안전한 사용자 인증을 위해 인증의 에러 확률이 낮은 메커니즘들만을 사용하면 되겠지만

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성・지원사업의 연구결과로 수행되었음

인증방식의 편의성이나 보편성 등의 요소도 또한 인증방식 선택의 주요 요소로 작용되기 때문에 상황에 적절하게 인증 방식을 선택해야 할 필요가 있다. 본 논문은 사용자인증 메커니즘들의 에러 확률을 바탕으로 인증신뢰지수를 설정하고 혼합인증 환경에서 여러 인증 메커니즘들이 동시에 이용될 경우 인증신뢰지수를 계산하기 위한 알고리즘을 제안한다. 2장에서는 인증신뢰지수의 개요를 살펴본 뒤 단일 사용자인증에서의 인증신뢰지수적용에 대해 살펴본다. 3장에서는 단일 인증방식의 인증신뢰지수를 이용하여 혼합인증 환경에서의 인증신뢰지수 계산 방식에 대해 살펴본다. 마지막으로 4장에서는 결론 및 향후 연구 계획에 대해 언급하며 본 논문을 마친다.

2. 인증신뢰지수의 적용

2.1 인증신뢰지수의 개요

여러 사용자인증 방식은 각각의 특징에 따라 신뢰할 수 있는 수준에서 차이가 존재한다. 예를 들어 지문과 같은 생체 정보를 통한 인증 방식은 타인에 의한 도용가능성이 있는 패스워드나 분실가능성이 높은 스마트카드를 통한 인증 방식보다 신뢰성이 높다고 볼 수 있다. 따라서 이러한 차이를 반영하여 각 인증 방식에 차별화된 인증신뢰지수를 적용하면 여러 인증방식의 신뢰도를 비교할 수 있게 된다. 즉, 사용자가 특정 인증방식을 통해 시스템에 인증할 때 그 인증 방식의 인증신뢰지수는 인증을 수행한 시스템의 인증방식에 대한 신뢰도로서 이용되는 것이다. 이러한 인증신뢰지수는 응용 프로그램과 서비스 등에서 접근 제어 결정과정에도 반영될 수 있다. 높은 보안성을 요구하는 응용프로그램은 인증을 통해 특정 신뢰 수치 이상을 수여받은 클라이언트에게만 접근을 허용하는 방식으로 사용될 수 있는데, 예를 들어, 서비스의 핵심 기능의 시작 및 중지와 같은 중요 업무는 높은 사용자 신뢰 수치를 요구하고, 날씨정보 추출과 같은 누구나 접근할 수 있을만한 서비스를 제공하는 응용프로그램에 대한 접근 요구 신뢰수치는 낮을 수 있다. 2.2장에서 사용자인증 방식의 특성에 따라 인증신뢰지수를 적용하는 것을 살펴본다.

2.2 단일 사용자 인증에서의 인증신뢰지수 적용

인증신뢰지수는 인증의 에러 확률을 바탕으로 결정이 된다. 즉, 인증에 사용되는 정보의 분실(망각) 위험 가능성, 복제 위험 가능성, 도난 위험 가능성 등에 기반을 두어 인증신뢰지수를 설정한다. 인증신뢰지수는 0부터 1사이의 수로서 표현되는 인증신뢰지수 C라는 값으로 표현된다. 인증신뢰지수는 분실 위험 가능성, 복제 위험 가능성, 도난 위험 가능성의 3가지 인증 에러 요소들을 바탕으로 0부터 1사이의 수치를 적용하도록 한다. 1에 가까울수록 신뢰수준이 높다는 것을 의미한다. 만일 3가지 인증 에러 요소들을 모두 갖추고 있다면 0.3, 2가지 요소들을 가지고 있다면 0.6, 1가지 요소를 가지고 있다면 0.9의 인증신뢰지수를 적용하도록 한다. 많이 사용되는 대표적인 인증 방식인 생체인식기술, 스마트카드 방식, 패스워드 방식 등에 인증신뢰지수를 적용하여 각각의 신뢰수준을 비교하여 보자.

㉮ 생체인식기술

생체인식기술은 분실, 도난 등의 위험이 다른 인증 방식들에 비해 상당히 낮기 때문에 인증신뢰지수가 높게 설정될 수 있다[3],[4]. 하지만 이용되는 신체 부위에 따라 모방의 위험 정도가 있기 때문에 다양한 생체 정보들이 모두 동일하게 높은 수준의 인증신뢰지수를 갖지는 않는다. 따라서 생체인식기술은 도난, 분실 등의 위험 정도를 반영하여 0.9의 인증신뢰지수를 공통적으로 설정하고 각각의 생체인식기술들에 생체 부위에 따른 모방 가능성 정도를 가감하는 방식으로 인증신뢰지수를 설정한다.

◦ 지문인식기술

지문인식기술은 초기에 지문의 위조를 통한 공격에 취약했다. 하지만 현재 지문인식기술은 지문의 형태뿐만 아니라 온도, 적외선 투과 반응 등을 적용하여 위조된 지문인지를 판단하는 정도까지 기술이 발전했다[5]. 따라서 지문인식기술은 다른 생체인식기술에 비해 모방의 위험 정도가 낮다. 따라서 지문인식기술의 인증신뢰지수는 C=0.90으로 설정한다.

◦ 얼굴인식기술

얼굴인식기술은 95~98%의 정확성을 갖지만 주변 환경에 따른 변화에 취약하며 얼굴의 각도, 표정, 나이에 따라 얼굴의 형태가 변하기 때문에 정확한 인식에 어려움이 있다[6]. 따라서 얼굴인식기술의 인증신뢰지수는 C=0.85로 설정한다.

◦ 망막, 홍채 인식기술

망막과 홍채인식도 초기에는 지문인식과 같이 위조를 통한 공격에 취약했다. 안구를 정확히 본뜬 가짜 안구를 이용해 인증시스템을 통과하는 사례도 있었으며 눈의 사진을 안경에 붙이거나 홍채 모양을

본뜬 렌즈를 이용하여 인증이 가능하기도 했다. 하지만 최근에는 이러한 모방에 의한 공격에 대응할 수 있도록 망막, 홍채 인식기술이 발전하였다. 따라서 망막, 홍채 인식기술은 지문인식기술과 같이 C = 0.90의 인증신뢰지수를 설정한다.

◦ 손등, 손목 정맥(vein) 인식기술

정맥인식은 피부 안에 존재하는 정맥의 패턴을 이용하므로 분실, 도난의 위험이 적을 뿐만 아니라 모방의 위험도 매우 낮다[6]. 따라서 정맥인식기술의 인증신뢰지수는 C=0.95로 설정한다.

㈏ 스마트카드 기술

스마트카드 기술은 소유에 의한 인증 방식으로서 사용자가 분실하거나 도난당하지만 않는다면 편리하고 높은 수준의 보안성을 갖는 인증 방식이다. 하지만 분실, 도난의 위험은 다른 인식기술들에 비해 높다. 따라서 스마트카드 기술의 인증신뢰지수는 C=0.6으로 설정할 수 있다.

㈐ 패스워드 인증기술

패스워드 방식은 인증정보가 사용자의 기억에 의존한다. 사용자가 패스워드를 기억하지 못할 경우 이용할 수 없으며, 또한 사전공격이나 재전송공격 등을 이용하여 쉽게 공격당할 수 있는 특징을 갖는다. 패스워드 방식은 도난, 분실, 모방 등의 위험에 가장 크게 노출되어 있기 때문에 인증신뢰지수를 C=0.3으로 설정할 수 있다.

지금까지 살펴본 단일 사용자인증 메커니즘에서의 인증신뢰지수 적용 방식은 인증 에러의 요소를 3가지로 분류하였을 경우에 한해 적용되는 것이다. 따라서 더 다양한 에러 요소를 적용하여 인증신뢰지수를 설정할 수 있지만 본 논문은 혼합사용자인증에서의 인증신뢰지수 적용에 초점을 맞추고 있으므로 단일 사용자 인증의 인증신뢰지수 적용은 3가지 요소에 의한 인증신뢰지수 설정만을 다룬다. 3장에서는 혼합사용자인증에서의 인증신뢰지수 계산 알고리즘을 소개하고 이 알고리즘에 따라 다양한 혼합사용자 인증 방식에 인증신뢰지수를 적용하도록 한다.

3. 혼합 사용자 인증에서의 인증신뢰지수

2장에서 대표적인 사용자인증 메커니즘에 인증신뢰지수를 적용해보았다. 이들 사용자 인증 메커니즘들이 동시에 2개 이상 적용될 경우에는 각 인증방식들의 인증신뢰지수들을 이용하여 혼합사용자인증을 위한 새로운 인증신뢰지수를 구해야 한다. 인증신뢰지수는 인증 에러율을 반영하는 수치이므로 각 인증방식들이 동시에 사용될 경우 각 인증방식들의 인증 에러율의 곱이 인증신뢰지수에 적용되어야 한다. 따라서 2가지 이상의 인증 방식을 사용할 경우 인증신뢰지수는 다음과 같이 계산하여 설정한다.

- $C_{net} = 1-(1-C_1)(1-C_2)\cdots(1-C_n)$
  (n은 사용되는 인증방식의 수)

C_{net}은 다중사용자인증의 인증신뢰지수이며 C_1, C_2, …, C_n은 n개의 인증방식이 사용될 경우 각각의 인증신뢰지수이다. 그리고 $(1-C_i)$는 C_i의 인증신뢰지수를 갖는 사용자인증방식이 부정확하게 인증될 가능성 즉, 에러율이 된다. 여러 가지 인증 방식이 동시에 사용되므로 각 인증 방식에 의해 부정확하게 인증될 가능성을 서로 곱하면 각 인증 방식이 동시에 사용될 경우 부정확하게 인증될 가능성이 나오게 된다. 이 결과를 1에서 뺄 경우 여러 가지 인증 방식을 동시에 사용할 때의 인증신뢰지수를 구할 수 있게 된다. 2가지 이상의 인증 기술을 같이 사용할 경우 2장에서 설정한 각각의 인증기술들의 인증신뢰지수를 이용하여 각 인증기술들을 혼합해서 사용할 경우의 인증신뢰지수를 계산할 수 있다. 2장에서 살펴본 대표적인 사용자인증 메커니즘들을 혼합해서 사용할 경우의 인증신뢰지수를 계산해보자. 우선 2가지 방식을 혼합할 경우이다.

◦ 스마트카드기술과 패스워드기술

스마트카드기술의 인증신뢰지수는 0.6, 패스워드기술의 인증신뢰지수는 0.3이다. 따라서 다음과 같은 결과를 얻을 수 있다.

- C = 1 - (1-0.6)(1-0.3) = 0.72

◦ 지문인식기술과 패스워드기술

지문인식기술의 인증신뢰지수는 0.9, 패스워드기술의 인증신뢰지수는 0.3이다. 따라서 다음과 같은 결과를 얻을 수 있다.

- C = 1 - (1-0.9)(1-0.3) = 0.93

◦ 지문인식기술과 스마트카드기술

지문인식기술의 인증신뢰지수는 0.9, 스마트카드기술의 인증신뢰지수는 0.6이다. 따라서 다음과 같은 결과를 얻을 수 있다.

- C = 1 - (1-0.9)(1-0.6) = 0.96

◦ 정맥인식기술과 스마트카드기술

스마트카드기술의 인증신뢰지수는 0.6이며 정맥인식기술의 인증신뢰지수는 0.95이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.6)(1-0.95) = 0.98

◦ 정맥인식기술과 패스워드기술

패스워드기술의 인증신뢰지수는 0.3이며 정맥인식기술의 인증신뢰지수는 0.95이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.3)(1-0.95) = 0.965

◦ 얼굴인식기술과 스마트카드기술

스마트카드기술의 인증신뢰지수는 0.6이며 얼굴인식기술의 인증신뢰지수는 0.85이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.6)(1-0.85) = 0.94

◦ 얼굴인식기술과 패스워드기술

패스워드기술의 인증신뢰지수는 0.3이며 얼굴인식기술의 인증신뢰지수는 0.85이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.3)(1-0.85) = 0.895

◦ 홍채인식기술과 스마트카드기술

스마트카드기술의 인증신뢰지수는 0.6이며 홍채인식기술의 인증신뢰지수는 0.9이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.6)(1-0.9) = 0.96

◦ 홍채인식기술과 패스워드기술

패스워드기술의 인증신뢰지수는 0.3이며 홍채인식기술의 인증신뢰지수는 0.9이다. 따라서 다음의 결과를 얻는다.

- C = 1 - (1-0.3)(1-0.9) = 0.93

2가지 인증 방식이 혼합된 경우의 인증신뢰지수를 살펴보면 한 가지 인증방식에서의 인증신뢰지수보다 인증신뢰지수가 높아진 것을 볼 수 있다. 다음은 3가지 인증 방식을 혼합할 경우의 인증신뢰지수를 계산해보자.

◦ 패스워드기술, 스마트카드기술, 지문인식기술

지문인식기술의 인증신뢰지수는 0.9, 스마트카드기술의 인증신뢰지수는 0.6, 패스워드기술의 인증신뢰지수는 0.3이다. 따라서 다음과 같은 결과를 얻을 수 있다.

- C = 1 - (1-0.9)(1-0.6)(1-0.3) = 0.972

패스워드기술, 스마트카드기술, 지문인식기술이 혼합된 경우의 인증신뢰지수는 0.972로서 패스워드와 스마트카드(C=0.72), 패스워드와 지문인식(C=0.93), 스마트카드와 지문인식(C=0.96)에서의 인증신뢰지수들보다 높아진 것을 볼 수 있다. 이상의 결과를 살펴보면 2가지 방식을 같이 사용할 경우 각각의 인증신뢰지수보다 혼합방식의 인증신뢰지수가 높아지는 것을 확인할 수 있으며 또한 3가지 방식을 사용할 경우 인증신뢰지수가 더 높아진 것을 확인할 수 있다.

4. 결론 및 향후연구

본 논문은 다양한 인증기술들이 부정확하게 인증될 가능성 즉, 인증 에러율을 반영하는 수치인 인증신뢰지수를 다중 사용자인증 환경에 적용하는 알고리즘에 대해 제안하였다. 본 논문에서 사용한 단일 사용자인증 메커니즘의 인증신뢰지수 적용은 분실위험 가능성, 도난 위험 가능성, 모방(위조) 위험 가능성 등의 3가지 요소를 바탕으로 이루어졌다. 하지만 부정확하게 인증될 가능성은 이보다 더 다양한 요소들에 의해 영향 받을 수 있다. 따라서 사용자인증의 신뢰지수를 정확히 적용하기 위해서는 더 다양한 인증실패요인의 적용이 필요하다. 또한 인증의 에러율을 실제인증실패 빈도수에 의한 확률 값이 아닌 인증메커니즘이 지니고 있는 특성에 따라 결정하기 때문에 애매모호한 사실을 수학적으로 접근하기 용이한 퍼지이론을 사용한 신뢰지수 설정방식이 필요하다. 본 논문은 정확한 단일 사용자인증의 신뢰지수를 전제로 다중 사용자인증 환경에서의 신뢰지수 계산에 초점을 맞췄으므로 위에서 언급한 다양한 인증실패요인의 적용과 퍼지이론을 사용한 신뢰지수 설정은 향후연구과제로 남긴다.

참고문헌

[1] 이만영, 김지홍, 송유진, 염흥열, 이임영, “인터넷 보안 기술”, 생능출판사, 2002.

[2] 원동호, “현대 암호학”, 도서출판 그린, 2004.

[3] 송영기, “금융서비스산업에서의 생체인식 기술 적용방안”, 시큐리티월드, 2004

[4] http://eevision1.sogang.ac.kr/home_coming_day/pansb.pdf

[5] http://www.supremainc.com/kr/bbs/zboard.php?id=k_news&page=1&sn1=&divpage=1&sn=off&ss=on&sc=on&select_arrange=headnum&desc=asc&no=18&PHPSESSID=db40a681cfdfd06d9415826df26068da

[6] http://www.kisa.or.kr/K_trend/KisaNews/200112/special_report_01.html