사용자 인증 소프트웨어 개발 프로세스에 관한 연구

A Study on the Development Process of User Authentication Software

이상준(Sang-Jun Lee)*, 배석찬(Suck-Chan Bae)**

초 록

컴퓨터 로그인이나 인터넷 뱅킹에서 사용자 인증은 필수적인 요소이다. 사용자 인증 소프트웨어에서 보안성은 당연히 중요할뿐 아니라 사용하기도 쉬워야 한다. 소프트웨어 개발을 체계적으로 진행하기 위해서는 개발 프로세스가 정의되어 있어야 하고, 개발 프로세스는 소프트웨어 성숙도를 향상시킬 수 있다.

본 논문에서는 비주얼 패스워드 입력 소프트웨어를 개발한 사례를 통하여 사용자 인증 소프트웨어를 체계적으로 개발할 수 있는 프로세스를 제안한다. 제안한 프로세스는 6단계, 15개 활동으로 구성된다. 제안한 프로세스는 사용성 요구분석, 계획수립, 통합시험, 인수시험 활동을 통하여 사용성을 향상시킬 수 있다.

ABSTRACT

User authentication is indispensable in computer login and internet banking. Usability as well as security is needed in user authentication software. To develop the software systematically, development process must be defined, and it can result in the improvement of software maturity.

In this paper, a process needed to develop user authentication software systematically is proposed from experience of developing visual password input software. This process is composed of 6 phases and 15 activities. It is able to improve usability with its requirement analysis, planning, integration testing, and acceptance testing activity

키워드 : 사용자 인증, 소프트웨어 프로세스

User Authentication, Software Process

본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구지원사업의(03-기초-0057) 연구결과입니다.

* 서남대학교 컴퓨터정보통신학과

** 군산대학교 컴퓨터정보과학과

1. 서 론

세계 정보보호 시장은 2002년에 200억 달러를 넘어섰으며 연평균 20% 이상의 성장률 기록하여 2007년에는 600억 달러 이상의 규모를 형성할 것으로 예측된다. 국내 시장규모는 2002년 3800억원대를 넘어섰으며 연평균 25% 이상의 성장하여 2007년 1조원대에 이를 것으로 전망된다[8]. 최근 소프트웨어 사용 환경은 언제 어디서나 어느 기기를 이용해서도 컴퓨팅할 수 있는 유비쿼터스(Ubiqitous)을 고려해야 한다[5]. 유비쿼터스 환경은 "AnyTime, AnyWhere, AnyDevice, AnyThing, AnyNetwork"에서 정보가 유출될 가능성이 있음을 의미한다. 따라서 유비쿼터스 컴퓨팅 시대에는 보다 철저한 보안기술이 요구된다[15]. 다양한 기기를 통해 각종 데이터들이 무선으로 송·수신되는 환경에서는 정보에 대한 해킹이 더 쉬워져 보안 문제가 더 심각해지기 때문에 보안시스템과 유비쿼터스 환경 구축은 처음부터 같이 시작되어야 한다. 유비쿼터스 환경에서는 컴퓨터, 네트워크, 어플리케이션, 인간으로 대변되는 유비쿼터스 컴퓨팅 분야의 4대 기술중 컴퓨터 기반기술에 해당하는 사용자 인증 기술과 보안기술이 더욱 강화되어야 한다.

특정 시스템에 로그인하기 위하여 사용자의 신원을 확인하는 절차를 신원 확인(Identification) 과정 또는 인증(Authentication) 과정이라고 하며[6], 시스템 접근자가 인가된 사용자인가를 확인하는 것을 사용자 인증이라 한다. 사용자 인증은 전용망 환경 시스템, 출입통제 시스템, 인터넷 솔루션, 시스템, 자원 접근 제어와 같은 실용적인 부분에 활용된다.

사용자가 서버에게 자신의 신원을 증명하는 방법으로는 스마트카드나 토큰과 같이 사용자가 가지고 있는 것을 이용하는 방식과, 사용자의 지문이나 음성과 같은 생체 인식을 이용하는 방식, 그리고 혼합방식이 있다. 사용자가 가지고 있는 것을 이용한 사용자 인증의 전형적인 사용법에는 세가지가 체계가 있다. 첫째는 패스워드 기반 체계, 둘째는 대칭키 암호를 이용한 시도-응답 방식 체계, 셋째는 개인/공개키를 이용한 디지털 서명이나, 영-지식 기반 체계가 있다. 패스워드 방식은 사용자의 이름과 더불어 사용자만이 알고 있는 패스워드외에는 수반하거나 기억할 것이 필요없이 인증할 수 있어서 현재 가장 많이 쓰이는 방식이다.

고품질의 소프트웨어를 체계적으로 개발하기 위해서는 소프트웨어 개발 프로세스가 꼭 필요하다[7]. 건축분야에서 정해진 개발 공정도 없이 상황, 기분, 당일 근무자에 따라 매번 다른 순서로 만들어진 주택이 태풍으로부터 안전하지 못한 것처럼, 프로세스를 준수하지 않고 개발된 소프트웨어는 생명력이 짧게되며 환경의 변화에 대응하지 못한다.

보안 소프트웨어는 수학이라는 학문적인 배경을 기술 요소로 발굴하고 이를 소프트웨어로 구현하고 있는데, 이때 기술적인 측면을 소프트웨어 개발 측면보다 상대적으로 중요하게 다루고 있는 실정이다. 보안의 기술적 요소가 확립되어 있는 상태에서 다양한 분야, 다양한 플랫폼, 다양한 사용자 환경에 맞춰 보안 소프트웨어 사업 분야에 진출하기 위해서는 기술적 요소를 소프트웨어 개발 프로세

스 및 개발 방법론과 잘 조화를 이루도록 해야 한다. 하지만 보안 소프트웨어 산업의 성숙도가 낮아서 아직까지 소프트웨어 개발 프로세스나 개발 방법론의 도입 및 적용 사례가 보고된 바 없는 실정이다.

사용자 인증 소프트웨어의 산업화에서 소프트웨어 보안성이 가장 중요하며, 보안성이 유지되는 상태에서 사용성이 좋아야 한다. 아무리 기능적으로 우수한 소프트웨어라도 사용하기 어려운 경우에는 사용자로부터 외면당하게 된다. 사용성 확보를 위해서는 개발 프로세스에 사용성을 측정하고, 평가하고 향상시키는 활동이 통합되어야 좋다[11].

본 논문에서는 비주얼 패스워드 입력 소프트웨어를 개발한 사례를 통하여 사용자 인증 소프트웨어를 체계적으로 개발할 수 있는 프로세스를 제안하며, 이 프로세스는 익스트림 프로그래밍의 사용성을 향상시킬수 있는 프로세스이다.

2. 관련연구

21 사용자 인증 소프트웨어 기술 현황

사용자 인증 기술은 패스워드를 기반 방식과 생체인식 기반 방식, 혼합 방식이 있다. 패스워드 기반 방식은 쉽게 사용가능하며 효율성이 탁월하나, 훔쳐보기 공격에 취약하여 최근에는 생체인식 기반 방식에 관한 연구가 많이 진행되고 있다. 생체인식 기반 방식은 가격, 처리시간, 메모리 요구량, 구현의 용이성, 시스템간 호환성 등에서 패스워드 방식에 상대적으로 열등하고, 특히 개인의 생체정보가 노출되는 단점이 있다. 훔쳐보기 공격에 안전한 패스워드 기반 방식의 인증 방법을 연구할 필요가 있다.

패스워드 길이를 늘려서 훔쳐보기가 어렵게 만든 연구가 있다. UNIX 버전 7 이후에 MD5 암호화 방식을 도입하여 8 문자로 한정된 패스워드 길이를 256문자까지 길게 만들어 사용할 수 있도록 하였지만[16], 적법한 사용자조차도 자신의 긴 패스워드를 외우기도 어렵고 정확하게 입력하는데 어려움을 겪고 있다.

사용자 인증 기술에는 프론트엔드에 사용되는 인증 매체로서 패스워드 방식과 생체인식 방식, 특정 하드웨어 방식(스마트카드 등) 있으며, 백엔드에는 사용자에 고유한 정보를 암호화하는 알고리즘으로 DES, RSA 등이 이용된다. 단말 노드와 서버간에는 패스워드를 이용한 인증 메카니즘, 시도-응답 개인 식별 프로토콜이나 영지식 개인 식별 프로토콜을 이용한 인증 메커니즘이 필요하다[6].

실생활에서 쉽게 접하는 패스워드를 기반으로 하는 사용자 인증으로는 컴퓨터 로그인, 인터넷 뱅킹, 디지털 도어락 등으로 너무 알려진 모습들을 갖고 있어서, 최근에 이론적으로 발표된 개선된 사용자 인증 방법을 Microsoft 사례와 듀얼패스워드 시스템으로 한정하여 살펴본다.

Microsoft사는 2003년 3월에 시각 패스워드 시스템을 시연하였다[21]. 시각 패스워드 시스템에서의 패스워드 입력 방법은 다음과 같다.

① 사용자는 몇 개 나라 국기를 순서대로 기억하고 있다. 여기에서는 사용자가 네개 나라 국기를 기억하고 있다고 가정

한다.

② 시스템을 부팅하면 40개 나라의 국기가 모니터 상에 나타난다.

③ 사용자는 기억하고 있는 첫 번째 나라 국기를 마우스로 선택한다.

④ 시스템은 40개 나라의 국기를 재배열하여 모니터 상에 나타낸다.

⑤ 사용자는 기억하고 있는 두 번째 나라 국기를 선택한다.

⑥ 단계 ④와 단계 ⑤가 두 번 반복된다. 이때, 사용자는 단계 ⑤에서 기억하고 있는 세 번째 나라와 네 번째 나라의 국기를 차례로 선택한다.

Microsoft사가 제안한 사각 패스워드 시스템은 하나의 국기는 여러 글자의 나라 이름에 대응한다는 점을 이용하고 있다. 예를 들어, 사용자는 '태극기'를 선택하지만 다른 사람은 '대한민국'이라는 나라 이름을 외워야 한다는 점을 이용하고 있다. 현재까지 세계적으로 훔쳐보기로부터 안전하기 위한 패스워드 시스템을 개발하기 위하여 Microsoft사와 같이 긴 길이의 문자열을 기억하는 것이 어렵다는 사실에 기초한 방법들이 개발되고 있다.

타인의 관찰에 의한 패스워드 노출로부터 안전한 패스워드 시스템에서는 듀얼 패스워드 시스템을 이론적으로 정의하고, 훔쳐본 패스워드를 이용해 인증받을 수 있는 확률과 과거의 패스워드를 이용하여 연속적으로 정확한 패스워드를 입력시킬수 있는 확률등을 제시하였다[3].

본 논문에서는 참고문헌[3]의 듀얼 패스워드 시스템을 비주얼 패스워드 입력 소프트웨어로 개발한 사례를 통하여 사용자 인증 소프트웨어를 체계적으로 개발할 수 있는 프로세스를 제안한다.

2.2 사용자 인증 소프트웨어의 품질 요구사항

인증 기술을 위협하는 온라인 추측 공격, 훔쳐보기 공격, 가로채기 공격, 오프라인 추측 공격, 재시도 공격, 서버상의 비밀정보를 이용한 공격과 같은 많은 공격들이 있다. 사용자 인증 소프트웨어의 우수성은 이와 같은 여러 가지 공격에 대해 안전한가 즉, 보안성으로 평가한다.

ISO/IEC 9126 소프트웨어 품질 특성에 따르면 소프트웨어의 품질은 기능성, 신뢰성, 사용성, 효율성, 유지보수성, 이식성의 6가지 품질 특성으로 표현할 수 있다[18]. 모든 품질 특성이 좋아야 하지만, 본 논문에서는 기능성의 품질 부특성인 보안성과 사용성이 향상된 사용자 인증 소프트웨어를 개발하는 것에 초점을 두고 연구하였다.

2.3 소프트웨어 개발 프로세스 현황

소프트웨어 프로세스란 고품질의 소프트웨어를 구축하는데 요구되는 태스크에 대한 프레임워크로 정의한다. 소프트웨어 프로세스에 대한 일반적 모델로 폭포 모델, 프로토타이핑 모델, RAD 모델, 단계적 소프트웨어 프로세스 모델 유형인 점진적 모델, 나선형 모델, 컴포넌트 기반 모델, 컨커런트 개발 모델 등이 있다[23]. 컴포넌트 기반 모델은 컴포넌트를 새롭게 개발하는 프로세스, 기존 소프트

웨어를 컴포넌트로 변환시키는 프로세스, 컴포넌트를 저장소에 보관하는 프로세스, 컴포넌트를 조립하여 새로운 소프트웨어를 개발하는 프로세스들이 연결된 형태를 갖는다[1]. 객체지향 개발 표준 표기법인 UML(Unified Modeling Language)와 연결되어 산업계에서 널리 알려진 RUP(Rational Unified Process)는 시작, 상세화, 구축, 전이의 4단계와 요구분석, 분석, 설계, 구현, 테스트의 5개 핵심 워크플로우를 점진 반복적으로 수행하도록 하였다[19].

최근 "인터넷 시간"에 소프트웨어를 개발할 수 있는 더 가벼우며 빠르고 민첩한 소프트웨어 개발 프로세스를 제공하는 애자일 소프트웨어 개발 방법론(Agile Software Development Methodology)이 대두되었다[12,13]. 2002년 3월 Giga Information Group Inc.는 응용 소프트웨어 개발 컨퍼런스에서 18개월 이내에 전세계 IT 기업의 2/3 이상이 일종의 애자일 방법론(Agile Methodology)를 사용하게 될 것이라고 예측했다[17]. 2002년 11월부터 2003년 1월 동안에 Shine Technology에서 애자일 방법론에 대한 시장 관심을 측정하기 위해 웹기반 조사를 실시하였다. 10개의 질문에 정확하게 응답한 131개의 타당한 결과를 분석한 결과 애자일 방법론이 생산성에 도움이 됐다는 응답이 93%, 품질이 향상되었다는 응답이 88%, 비용이적게들었다가 49%, 사업적 만족도 83%, 2003년에 적용할 것인가에 94.7%로 응답하였다[10]. 설문 조사에 의하면 응답자의 59%가10여개의 애자일 개발 방법론중에서 극한 프로그래밍(XP:eXtreme Programming) 프로젝트를 가장 많이 사용하고 있었다[9].

사용자 인증 소프트웨어는 내부적인 보안기술이 확보되어있는 상태에서, 적용되는 분야에 따라 사용자 인터페이스와 같은 요구사항이 달라지며 여러 가지 버전이 만들어지기 때문에 애자일 소프트웨어 개발 프로세스를 이용하는 것이 좋다. 극한 프로그래밍(eXtreme Programming:XP)에서는 사용성에 대한 고려가 미비하며[14], 이를 개선할 수 있는 노력이 필요하다. 극한 프로그래밍 프로젝트에서는 사용자 스토리 작성, 계획 작성, 반복, 인수 시험과 같은 활동을 수행하도록 하였다[24].

3. 비주얼 패스워드 입력 소프트웨어 사례

본 논문에서는 사용자 인증을 위한 안전하고 효율적인 패스워드 시스템 개발에 관심을 갖고, 참고문헌[3]의 듀얼 패스워드 시스템을 비주얼 패스워드 입력 소프트웨어로 개발한 사례를 통하여 사용자 인증 소프트웨어를 체계적으로 개발할 수 있는 프로세스를 제안한다.

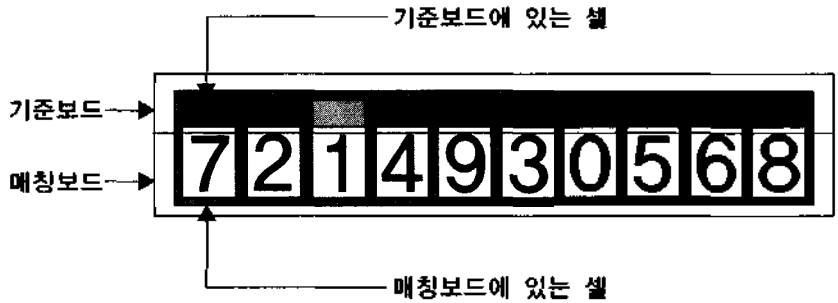
훔쳐보기 공격에 안전한 패스워드 시스템의 기술적인 요소는 인지공학에 기초한다. 인간이 눈으로 보고, 지각하고, 인지하는 과정과 능력의 한계치를 웃도는 환경을 구성한다. 실험적으로 3행 4열로 배열된 12개의 문자를 50msec 순간 노출하여 지각된 문자를 행단위로 보고하도록 해본 결과, 즉시 보고하도록 하는 경우는 4.5문자를, 보고할 행을 잠시후에 지정한 경우에 따라 기억할 수 있는 문자의 수가 3문자로 인지할 수 있는 능력의 한계가

있다. 이 결과를 기초로 시작 정보 저장의 존속시간을 약 0.25초로 추정하고 있다[4].

본 논문에서는 10개의 서로 다른 숫자가 하나의 화면에 나와서 패스워드 1자리를 입력하고, 이런 화면을 4개 조합하여 4자리의 패스워드를 입력할 수 있는 사용자 인터페이스를 갖추도록 하였는데, 각 숫자가 나오는 영역을 표시하는 부분과 나타난 숫자의 위치를 매칭해야 한다는 의미로 매칭에 기반한 패스워드 시스템이라 명명한다.

매칭에 기반한 패스워드 시스템의 인터페이스는 기준보드와 매칭보드로 구성되어 있고, 각 보드는 10개의 셀영역으로 이루어져 있다. 그리고, 〈그림 1-a〉와 같이 기준보드에 있는 셀에는 색이 부여되어 있고, 매칭보드에 있는 셀들은 숫자를 포함하고 있다. 예를 들어 패스워드를 "1835"로 갖고 있는 사용자는 기준보드의 왼쪽 3번째 숫자 "1"에 특별한 손의 움직임 없이 선택한 보드 상의 위치를 잊지 않도록 집중해서 쳐다보고, 엔터키를 눌러서 첫 번째 패스워드를 선택함을 알리고, 새롭게 나오는 수의 배열중 3번째로 나온 숫자가 "8"이 되도록 "up-down 키"로 조정한 후, "엔터키"로 선택한다. 다음에도 보드의 왼쪽 3번째에 숫자 "3"과 "5"가 순서대로 나오도록 "up-down 키"와 "엔터키"로 선택하고, 마지막에 "*"키를 선택하고 엔터키를 입력함으로서 4자리 패스워드 입력을 마친다.

매칭에 기반한 패스워드 시스템의 장점은 패스워드를 입력할 때 누군가가 바로 옆 의자에 앉아서 보더라도, 패스워드를 알 수 없다는 것이다. 이와 같은 비주얼 패스워드 입력



〈그림 1-a〉 매칭에 기반한 패스워드 시스템

보드에 맞출 숫자										이벤트
4	9		1	6	0	7	2	3	5	↑ ↓ ↵
9	4		6	1	5	2	7	8	0	↑ ↓ ↵
1	6		8	3	7	4	9	0	2	↑ ↓ ↵

〈그림 1-b〉 매칭에 기반한 패스워드 시스템의 3번째 보드에 "1835"숫자는 맞추는 과정

시스템 개발 사례를 통해 다음과 같은 개발 프로세스를 제안한다.

4. 프로세스의 제안

4.1 프로세스 구성 고려사항

비주얼 패스워드 입력 시스템에서 사용자가 비밀번호를 입력하는 방법은 다양할 수 있다. 예를 들어, 시스템이 자동으로 매칭보드에 있는 숫자들의 값을 증가시키고, 사용자는 자신이 선택한 셀에 입력하고자 하는 숫자가 나타났을 때 엔터키를 치는 방법이 있을 수 있다. 비주얼 패스워드 입력 시스템에서 매칭보드에 숫자들이 나타나는 방법은 다양할 수 있다. 예를 들어, 시스템이 매칭보드에 숫자들을 한번만 나타내어도, 사용자는 결정한 셀에 비밀번호를 입력할 수 있다. 또한, 이용되는 플랫폼에 따라 입력 방법등이 다양하다. 예를 들어 PC, PDA, ATM 각각의 경우에 사용할 수 있는 입력키가 서로 달라 입력 방법이 다양하다.

사용자가 비밀번호를 입력하는 새로운 방법, 매칭보드에 숫자들을 나타내는 새로운 방법, 숫자를 선택할 수 있는 새로운 방법이 있을 수 있다는 변화 요인은 소프트웨어 개발에서의 요구사항 변경으로 받아들일 수 있다. 요구사항의 잦은 변경은 체계적인 소프트웨어 공학 측면의 접근을 요구한다. 이때, 최근 연구되고 있는 극한 프로그래밍 개발 프로세스를 개선하여 사용할 수 있다.

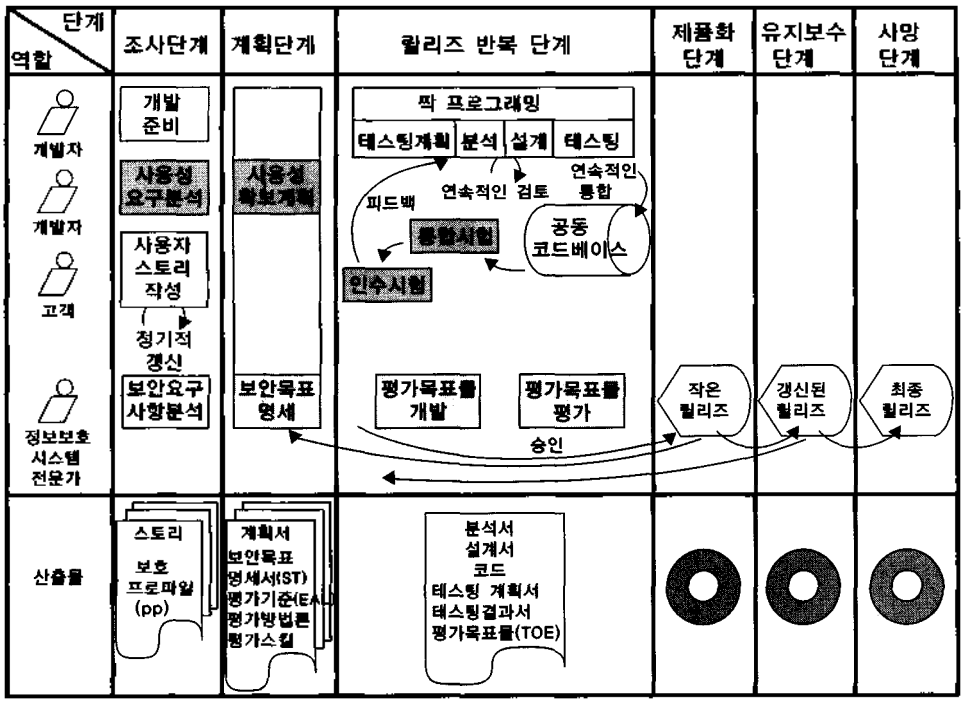
비주얼 패스워드 입력 시스템과 같은 좋은 보안 기술을 다양한 환경에 맞게 사용할 수 있도록 소프트웨어로 개발하는 프로세스에 관한 연구가 필요하다.

4.2 프로세스 구성

소프트웨어 프로세스는 여러개의 활동, 태스크, 산출물 등으로 구성된다[23]. 본 논문에서는 프로세스를 <그림 2>와 같이 소프트웨어 개발 단계, 단계별 활동, 단계별 산출물로 정의하였다. <그림 2>에는 사용성 향상을 위한 활동은 사용성 전문가가 특별히 다루는 부분과 정보보호시스템 전문가가의 활동이 정의되어 있다. 본 논문에서는 사용성 향상을 위한 활동은 자세히 정의하고, 일반적인 소프트웨어 개발 활동과 정보보호시스템 전문가의 활동들은 간단히 소개하고자 한다. 전체 생명주기는 조사단계, 계획단계, 릴리즈 반복 단계, 제품화 단계, 유지보수 단계, 사망 단계의 6 단계로 구성되었다.

4.2.1 조사 단계

조사단계에서는 개발준비, 사용성 요구분석, 사용자 스토리 작성의 활동을 수행하여 스토리 산출물을 생성한다. 조사 단계에서 개발자는 소프트웨어 개발에 사용될 도구, 기술, 실무에 친숙하도록 개발 준비한다. 고객은 자신이 원하는 소프트웨어에 대한 요구사항을 사용자 스토리라는 카드에 작성한다. 사용성 전문가는 희망하는 학습시간, 실행시간, 사용성 정도를 스토리 카드에 명시하도록 한다. 정보보호시스템 전문가는 보안 요구사항을 분석하여 보호 프로파일(Protection Profile)을 작성한다.



〈그림 2〉 제안한 프로세스

4.2.2 계획 단계

계획단계에서는 계획수립 활동을 수행하여 계획서 산출물을 생성한다. 계획 단계에서는 개발자, 고객, 사용성 전문가가 함께 모여 사용자 스토리의 우선순위를 결정하고, 각 릴리즈에 포함될 내용을 선정한다. 개발자는 독립적으로 각각의 사용자 스토리를 소프트웨어로 구현하기 위해 얼마나 많은 노력이 필요한가 예상하고, 개발 비용과 일정을 계획서에 명시한다. 정보보호시스템 전문가는 보안 목표 명세서(Security Target)를 작성하며, 평가기준(Evaluation Assurance Level), 평가 방법론, 평가 스킴을 정의한다.

4.2.3 릴리즈 반복 단계

릴리즈 반복 단계에서는 테스팅 계획 작성, 분석, 설계, 짝 프로그래밍, 단위테스팅, 통합시험, 인수시험을 수행하며, 분석서, 설계서, 코드, 테스팅 계획서, 테스팅 결과서 산출물을 생성한다. 릴리즈를 위한 반복 단계에서는 계획서에 근거하여 계획을 나누고 각각이 1주에서 4주내에 구현될 수 있도록 한다. 일반적인 소프트웨어 개발 과정과 마찬가지로, 분석, 설계, 구현, 테스팅 활동이 필요하고, 특히 우선적으로 테스팅 계획을 수립하는 일이 선행되도록 한다. 특정 버전의 릴리즈를 생성하기 위해서는 몇 번의 반복이 있게되며, 각 반복

의 끝에는 기능시험을 수행한다. 본 논문에서는 기능시험외에 사용성 시험의 필요성을 인식하고, 사용성 평가 방법중 학문적으로 가장 정리가 잘 되어있으며 사용성 평가 결과를 이용하여 설계를 수정할 수 있는 가이드라인까지 제공하는 GOMS를 이용한 모델 기반 방법을 통합시험에 도입하고, 사용자의 느낌을 가장 쉽게 평가할 수 있는 질문지 방법과 전문가에 의해 숨겨진 문제점까지 찾아내올 수 있는 휴리스틱 평가 방법을 인수시험에 도입하고자 한다[2].

통합시험에 적용하는 GOMS(Goals, Operators, Methods, Selection rules)란 목표, 조작자, 방법 및 선택 규칙에 기초를 두고 컴퓨터 시스템과 함께 업무를 수행할 때의 사용자 지식과 작업을 기술하는 것이다. 이 방법은 전문가를 참가자 대상으로 하며 수행능력과 수행시간을 정밀하게 검사한다. 논리적인 수행 과정을 검증하고자 하거나 반복적인 사용 시간을 단축시키는 것이 목적일 경우에 매우 유용한 방법이다[20].

GOMS 방법에 인지복잡도 이론을 근거로 한 NGOMSL(Natural GOMS Language)이 있다. NGOMSL은 모형 구축에 필요한 규칙과 용어를 단순화하고, 모형 구축을 용이하게 하며, 사용성 관련 자료를 수치적으로 예측할 수 있도록 하였다. NGOMSL에 의한 예측 결과를 이용하여 설계를 수정할 수 있고, 수정한 후 성능예측을 다시 계산할 수 있다. GOMS 방법은 다른 사용성 평가 방법에 비해, 설계 과정에서 평가가 가능하며, 사용성을 향상시킬수 있는 7개의 가이드라인을 제공한다. 원시연산자를 이용하여 예상되는 실행시간과 사용자 학습 시간을 간단한 공식을 이용하여 계산 가능하다.

인수시험에 적용하는 질문지 이용 평가 방법은 사람들이 가지고 있는 일반적인 생각과 그 변화를 이해하는데 효율적이어서 시스템이나 서비스에 대한 사용자들의 만족도, 불편사항, 건의사항 등을 파악할 때 가장 많이 사용되는 방법이다. 질문조사의 결과는 중요한 요인 항목을 찾아내고, 그 항목들간의 상관관계를 밝히는 것 이상의 세부적인 사용성 정보를 주지 못하는 문제점도 있다. 하지만 개발에 참여하는 사용자에게 사용하기에 편리한가라는 개괄적이고 단편적인 질의 응답보다는, 척도가 있어야 상태를 알 수 있는 품질 평가의 기본 특성을 구체적인 질문으로 정량적으로 사용성을 평가할 수 있기에 질문지를 이용하고자 한다. 특히, 개발과정의 요구분석 단계와 자격시험, 고품질 레벨이 요구되는 평가에 우수한 방법이다.

인수시험에 적용하는 휴리스틱 평가는 주로 4-5명 정도의 소수의 평가 전문가가 사용성 평가 대상 시스템(또는 시제품)에 대한 사용평가를 수행하여 그 인터페이스가 사용성 원칙에 따르는지 등의 문제점을 도출한 후, 모여서 수합하는 방식으로 진행된다. 일반적으로 평가자가 많을수록 더 많은 사용성 문제를 탐지하지만 그 부가적 효율성은 5명 이상이 되면 급감한다.

휴리스틱 평가는 UI 전문가들이 UI의 각 요소가 확립된 사용성 원칙을 따르고 있는지 판단할 수 있는 사용성 검증법 중 하나이다. 각 프로젝트에 맞게 구성된 전문가 집단은 휴리스틱 평가 항목에 의해 가시적인 평가를 하

고 이것을 수치적으로 나타날 수 있다. 전문가의 검증이 필요한 기초 분석단계 또는 프로젝트 수행 마지막 단계에 효과적이다. 휴리스틱 평가 방법을 제안한 Nielson의 10개 평가 항목은 참고문헌 [22]에 제시되어 있다.

릴리즈 반복 단계에서는 정보보호시스템 전문가 입장에서는 평가목표물(Target of Evaluation)이 개발되고 있으며, 평가목표물에 대한 평가가 수행된다.

4.2.4 제품화 단계, 유지보수 단계, 사망 단계

제품화 단계에서는 릴리즈된 소프트웨어가 실제 사용 현장에서 문제 없는지 추가적인 테스팅을 수행하고 문제가 없을시 수행가능한 형태의 릴리즈가 가능하다. 지연된 아이디어나 제안을 추후 구현을 위해 문서화한다.

유지보수 단계에서는 아직 반영되지 않은 사용자 스토리 및 요구사항을 새로운 릴리즈로 개발하기 위하여, 현재의 릴리즈를 고객이 계속 사용할 수 있도록 지원하는 과정이다. 조직이나 조직구성요원이 변화될 가능성이 있다.

사망 단계는 어떤 스토리도 사용하지 않으며, 사용자의 기대와 같은 결과를 만들지 못할 때 더 이상 해당 소프트웨어를 사용하지 않는 상태이다.

4.3 제안한 프로세스의 평가

제안한 프로세스를 평가하기 위하여 기존 애자일 방법론과 제안한 프로세스를 정성적으로 비교하는 방법과, 비주얼 패스워드 입력 시스템에 프로세스를 적용한 결과를 보이는 방법을 사용한다.

〈표 1〉에서 기존의 애자일 방법론인, ASD(Adaptive Software Development), AM(Agile Modeling), Crystal, DSDM(Dynamic Systems Development Method), XP(eXtreme Programming), FDD(Feature Driven Development), OSS(Open Source Software development), PP(Pragmatic Programming), RUP(Rational Unified Process), Scrum 애자일 방법론과 제안한 프로세스의 핵심, 특징, 단점을 정리 비교하였다.

비주얼 패스워드 입력 시스템을 팬티엄III-700MHz 컴퓨터에 Windows 2000 서버상에서 자바로 구현하였다. 4자리 패스워드를 입력시간, 입력정확도, 패스워드 알아내는 확률을 프로세스 적용전과 적용후로 구분하여 〈표 2〉에 정리하였다.

5. 결 론

사용자 인증 소프트웨어는 우선적으로 보안성이 우수하도록 기술적인 연구가 있어야 하며, 어려운 기술이더라도 사용자는 사용하기 쉬워야 한다.

본 논문에서는 비주얼 패스워드 입력 시스템을 개발하는 사례를 통해서 사용자 인증 소프트웨어 개발 프로세스로 제안하였다. 비주얼 패스워드 입력 소프트웨어는 패스워드를 정확히 입력하는것과 쉽게 입력하는 것이 중요하며, 패스워드의 보관이나, 패스워드의 전송등을 고려하지 않기 때문에 핵심은 사용성

〈표 1〉 애자일 소프트웨어 개발 방법과 제안한 프로세스의 특징 비교

개발 방법	핵 심	특 징	단 점
ASD	적응할 수 있는 문화,협동, 임무중심의 컴포넌트기반 반복 개발	조직이 적응적인 시스템으로 간주됨. 상호연결된 개인들간의 웹외의 불시의 요구를 생성	소프트웨어 실무보다는 개념과 문화에 대한것
AM	애자일 원리를 모델링에 적용:애자일 문화, 통신과 단순성을 제공하기 위한 작업 조직	기민한 생각을 모델링에 적용	모델링 전문가를 위한 좋은 부가 철학. 다른 방법 내에서 사용됨.
Crystal	메소드 집합. 각 메소드는 동일한 현행 핵심 가치와 원칙을 갖음. 기법, 역할, 도구, 표준이 다름	방법 설계 원칙. 프로젝트 크기와 치명성에 기반한 대부분의 적당한 방법을 선택할 수 있는 능력	아직 평가하기 이름 : 제안된 방법 4개중에서 2개만 존재.
DSDM	RAD에 대한 제어응용. 타임박스의 이용, 보강된 DSDM 팀, 메소드 개발을 이끄는 활동적인 컨소시엄.	최초의 진정한 기민한 소프트웨어 개발 방법, 프로토타이핑 사용. 여러 개의 사용자 역할:특사, 공상가,충고자	메소드가 이용가능하나, 메소드의 실제 사용을 처리할 수 있는 백서는 컨소시움 멤버만이 접근가능하다.
XP	고객 기반 개발, 소규모팀, 매일 구축	리팩토링-성능을 향상하고 변화에 바로 응답하기 위해 시스템을 재설계	개별 실무가 많은 상황에 적합하지만, 전체적인 뷰와 관리 실무는 덜 주목받음
FDD	5단계 프로세스, 객체지향 컴포넌트 기반 개발, 2주 이내의 짧은 개발	방법 단순성, 특징에 의해 시스템 설계 및 구현, 객체 모델링	설계와 구현만 관심갖음. 다른 지원 접근법이 필요함.
OSS	지원자 기반, 분산 개발, 보통 문제 영역이 상업적인 일보다 더 도전적	라이센싱 실무:소스코드가 모든 부분에 자유롭게 이용가능	자체로는 방법이 아님:OSS 공동체 원칙을 상업 소프트웨어 개발에 변환하는 능력 있음
PP	실용주의, 프로그램 이론을 덜 중요시하고, 프로그램의 모든 측면에서 고수준 자동화 강조	구체적이고 경험적으로 타당한 팁과 힌트 이용. 소프트웨어 개발의 실증적 접근법	중요한 개별 실무에 초점 둠. 시스템 개발 전체에 사용되는 방법이 아님.
RUP	도구 지원을 포함한 완벽한 SW 개발 모델. 활동 기반 역할 할당	비즈니스 모델링, 도구 집합 지원	사용범위의 제약 없음. 테일러링, 요구 변화하는법 설명 부족.
Scrum	독립적,소규모,자발적조직 개발 팀,30일 배포 주기	"정의와 반복"에서 "Scrum 관점의 새로운 제품 개발"으로 패러다임 전환을 강조	30일 배포 주기를 관리하는 것은 자세하지만, 통합 및 인수 시험에 대한 설명 미비
제안 프로세스	소프트웨어 개발 활동마다 사용성 평가 수행후 개선, 반복 개발. 정보보호시스템 전문가 역할의 정의	스토리카드에 사용성 요구사항 정의, 인수시험, 통합시험 강조. 보호프로파일, 보안목표명세서, 평가기준 사용	다양한 적용 사례 필요

〈표 1〉 애자일 소프트웨어 개발 방법과 제안한 프로세스의 특징 비교

	프로세스 적용전	프로세스 적용후
패스워드 입력시간	6.326	4.918
패스워드 입력 정확도	초심자(63%) 숙련자(84%)	초심자(68%) 숙련자(89%)
패스워드 알아내는 확률	15%	5%

을 얼마나 향상시킬 수 있느냐가 된다. 제안한 프로세스에 따라 패스워드 입력 시간이 평균 6.326초 소요되었던 첫 릴리즈를, 평균 4.918초로 정제할 수 있었으며, 입력의 정확성이 평균 89%가 되었고, 패스워드 노출 확률은 5%가 되었다.

제안한 프로세스는 6단계, 15개 활동으로 구성되며, 제안한 프로세스는 사용성 요구분석, 계획수립, 통합시험, 인수시험 활동에 사용성 평가방법을 도입함으로서 사용성을 향상시킬 수 있었다. 사용자와의 인터페이스가 필요한 전자서명 소프트웨어도 사용성 향상을 위한 프로세스에 의해 사용성이 향상될 것으로 기대되며, 계속적인 연구를 통하여 구체적인 결과를 제시할 계획이다.

참 고 문 헌

[1] 김동현,이상준,서성채,김병기, "E-Business 영역의 소프트웨어 컴포넌트를 위한 참조 아키텍처", 하계종합학술대회 논문집, 대한전자공학회, 2000.

[2] 문서은,이상준,김병기, "기능성과 사용성 중심의 웹사이트 평가", 산학연 소프트웨어공학기술 학술대회, 2003.

[3] 박승배,박성배,강문설, "타인의 관찰에 의한 패스워드 노출로부터 안전한 패스워드 시스템", 정보처리학회논문지C, 제10권-C권, 제2호, 한국정보처리학회, 2003.

[4] 윤철호, 인간 컴퓨터 인터페이스, 대영사, 1996.

[5] 아라카와 히로키,히다카 쇼지, 손에 잡히는 유비쿼터스, 전자신문사, 2003.

[6] 이만영,원동호,이민섭,송주석,임종인,박춘식, 현대 암호학 및 응용, 생능출판사, 2002.

[7] 이상준, 소프트웨어 품질향상을 위한 객체지향 프로세스, 박사학위논문, 전남대학교, 1999.

[8] 정보보호기술 전망,http://www.

etnews.co.kr/news/detail.html?id=20030519 0008.

[9] Agile Alliance Web Site: Manifesto for Agile software Development. On-line at: http://agilemanifesto.org/.

[10]Agile Methodologies Survey Results, On-line at:http://www.shinetech. /agile_survey_results.jsp

[11]Anderson, J. and et al., Integrating Usability Techniques into Software Development, IEEE Software, Vol. 18, No. 1, Jan./Feb., 2001.

[12]Beck, K., Embracing Change With Extreme Programming, IEEE Computer, Vol. 32, No. 10, 1999.

[13]Beck, K., Extreme Programming Explained:Embrace Change, Addison-Wesley, 2000.

[14]Cockburn, A., Agile software Development, Addison-Wesley, 2002.

[15]Frank Stajano, Security for Ubiquitous Computing, John Wiley & Sons, 2002.

[16]Garfinkel, G., Schwartz, A. and Spafford, G. Practical Unix & Internet Security, 3rd Edition, O'Reilly & Associates, 2003.

[17]Giga Information GroupInc.http://www. computerworld.com/softwaretopics/software /appdev/story/0,10801,69182,00.html.

[18]ISO/IEC 9126, Information Technology-Software quality characteristics and metrics, 1998.

[19]Jacobson, I., Booch, G., Rumbaugh, J., The Unified Software Development Process, Addison-Wesley, 1999.

[20]Kieras D., A Guide to GOMS Model Usability Evaluation using NGOMSL, anonymous ftp ftp.eecs.umich.edu people/kieras , 1996.

[21]Microsoft.http://www.domainmart. com/news/NYT_symbols-as-passwods.htm.

[22]Nielsen, J., Usability Engineering, Morgan Kaufmann, 1993. see also http://www. useit.com/papers/heuristic/heuristic_evaluation.html

[23]Pressman, R. Software Engineering : A Practitioner's Approach(5th Edition), McGraw Hill, 2001.

[24]XP.org Extreme Programming:A gentle introduction. http://www.extremeprogramming.org/ Last modified January 26, 2003.

저 자 소 개

이상준 (E-mail : sjlee@seonam.ac.kr)
1991. 전남대학교 전산통계학과(이학사)
1993. 전남대학교 전산통계학과(이학석사)
1999. 전남대학교 전산통계학과(이학박사)
1995 ~ 현재 서남대학교 컴퓨터정보통신학과 조교수
관심 분야 : 소프트웨어공학, 컴퓨터보안, 컴퓨터교육

배석찬 (E-mail : scbae@kunsan.ac.kr)
1983. 전남대학교 계산통계학과(이학사)
1988. 전남대학교 전산통계학과(이학석사)
1995. 전남대학교 전산통계학과(이학박사)
1995 ~ 현재 현재 군산대학교 컴퓨터정보과학과 부교수
관심 분야 : 트랜잭션관리, 데이터베이스 보완