Journal of The Korea Society of Computer and Information
Vol. 19, No. 7, July 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.7.087

분석단계 보안에서 식별 및 인증의 보안 요건 정의에 대한 연구

신 성 윤*

A Study on Definitions of Security Requirements for Identification and Authentication on the Step of Analysis

Seong-Yoon Shin *

요 약

S/W 개발의 첫 번째 단계인 분석 단계에서는 식별 및 인증 요건 정의 원칙, 아이디 및 패스워드 관리 요건, 인증 프로세스 요건, 그리고 인증수단 요건 등에 관한 보안 요건들을 정의해야 한다. 식별은 어떤 시스템의 사용자나 시스템에서 실행 중인 애플리케이션을 특유하게 식별하는 기능을 말한다. 인증은 사용자나 애플리케이션이 진짜인지 가짜인지를 실제 예를 들어서 밝혀내는 기능을 말한다. 본 논문에서는 분석 단계의 이러한 식별 및 인증의 보안 요건을 제시한다. 첫째, 각자 가지고 있는 개별 ID는 유일하게 식별되어야 한다는 것이다. 둘째, 패스워드는 길이제한 및 표준 조합을 적용해야 하며, 주기적으로 변경해 줘야 한다는 것이다. 셋째, ID/PW 이외의 보다 강화된 인증 방식을 제공해야 하며, 인증 프로세스는 정의된 보안 요건을 만족해야 한다. 본 논문에서는 식별 및 인증단계의 보안 요건들을 실제 구현 방법을 들어 설명하고 있다.

▸ Keywords : 분석 단계, 식별, 인증, ID, 패스워드, 보안 요건

Abstract

TIn analysis as the first step of S/W development, security requirements of identification and authentication, ID and password management, authentication process, authentication method, ete. should be defined. Identification is to uniquely identify certain users and applications running on a certain system. Authentication means the function to determine true or false users and applications in some cases. This paper is to suggest the security requirements for identification and authentication in analysis step. Firstly, individual ID should be uniquely identified. The second element is to apply the length limitations, combination and periodic changes of passwords. The third should require the more reinforced authentication methods besides ID and passwords and

•제1저자 : 신성윤
•투고일 : 2014. 6. 26, 심사일 : 2014. 7. 3, 게재확정일 : 2014. 7. 30.
* 군산대학교 컴퓨터정보공학과(Dept. of Computer Information Engineering, Kunsan National University)

satisfy the defined security elements on authentication process. In this paper, the security requirements for the step of identification and authentication have been explained through several practical implementation methods.

▸ Keywords : Analysis Step, Identification, Authentication, ID, Password, Security Requirements

I. 서 론

컴퓨터 시스템에서 처리하는 정보보안은 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 정보보호는 정보를 제공하는 공급자 측면과 사용자 측면에서 논리적이고 물리적인 장치를 통해 정보의 훼손에서 유출까지를 미연에 방지를 하는 것에 목적을 두고 있다. 정보보안 기술은 정보보호의 기술, 암호화 기술, 해킹과 정보보호, 컴퓨터 바이러스, 시스템 보안, 네트워크 보안, 전자상거래 보안, 웹과 전자우편 보안 등 컴퓨터보안 전반에 걸쳐있다[1].

인터넷에서는 내가 어떤 상대와 통신하고 있는지 확인할 수가 없으므로 실제 내가 통신하고 있는 상대가 내가 원하는 상대가 맞는지 확인할 수 있게 해주는 기술을 사용자 인증, 개인 식별이라 한다[2].

모든 사용자는 개인적인 사용만을 위한 유일한 식별자(사용자 ID)를 가져야 하며 사용자의 신원을 확인하기 위해 적절한 인증 기법을 선택하여야 한다[3].

식별 및 인증은 생활에서 본인인지를 확인해야 하는 경우와 같이 컴퓨터 보안의 중요한 내용 중의 하나는 권한이 있는

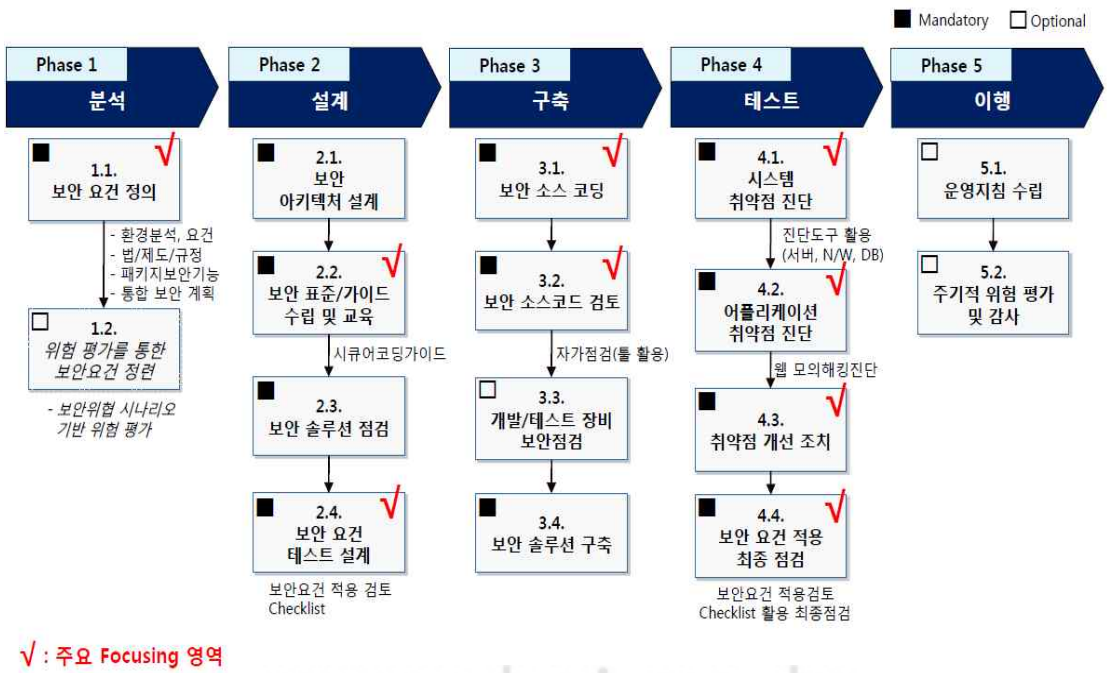

그림 1. 단계별 주요 보안 Activity
Fig. 1. Step-Wide Security Activity

사용자만이 시스템 내의 정보에 접근할 수 있도록 하는 것이다. 즉, 컴퓨터 시스템은 어떻게 여러 사용자들을 구별(식별)하고 인증처리를 할 수 있는지에 대한 사용자 식별과 인증의 문제이다[4].

가장 기본적인 식별 및 인증 방법은 컴퓨터와 그 사용자만이 알고 있는 정보인 지식을 확인 하는 방법이다. 첫 번째 예를 들면, 컴퓨터는 사용자가 알고 있는 개인 지식을 제시하게 하여 식별 및 인증하는 방식이 있는데 이 방법은 패스워드나 사용자 개개인의 신상에 관한 정보가 해당된다. 두 번째 예는 컴퓨터 시스템 사용자가 가지고 있는 물건을 제시하게 하여 식별 및 인증하는 방식인데 이 방법은 사용자의 카드 키, 스마트카드, 패스포트 등을 컴퓨터 시스템에 제시하는 방식이다. 세 번째 예는 컴퓨터 시스템 사용자가 자신의 육체의 일부를 제시하여 식별 및 인증하는 방식인데, 여기서 육체의 일부에 해당되는 것은 지문 인식, 홍채 인식, 음성 인식, 즉석 싸인 등이 해당된다.

II. 관련 연구

최근 들어 은행이나 기업의 기밀정보와 사용자들의 개인정보의 대량 유출 사고가 연속적으로 발생하였고, 이를 대처하기 위하여 내부 정보의 유출 방지를 위한 보안 인증 강화 및 접근통제에 관한 보안 기술들이 각광을 받고 있다.

[5]의 특허에서는 컴퓨팅 장치와 연관된 유효한 인증 데이터를 이용하여 자동으로 사용자 인증을 제공하기 위해 시스템이 제시되었다. [6]의 특허에서는 상품의 미세 화상의 물리적 unclonable 기능을 사용하는 위조에 대하여 각종 아이템을 보호하기 위한 방법 및 장치를 설명하였는데, 여기에서 보호는 휴대용 장치와 결합하여 제안 된 식별 및 인증 프로토콜을 기반으로 하는 것이다.

식별 및 인증 관련 논문으로는 [7]은 모바일 폰을 사용한 두 요소 인증을 보호하는 것에 관하여 이야기했다. 여기에서 우리는 OTP를 생성하는 휴대 전화를 사용하였고, 또한 두 요소 인증을 위하여 SMS 기반의 접근 방식을 적용하였으며 SMS 기반 OTP에 보안을 제공하였다. [8]에서는 사용자의 비밀번호를 그대로 사용하지만 비밀번호가 지속적으로 적합한 보안 강도를 가지도록 실제 비밀번호를 보완해 주는 기법을 제안한다. 그 외에도 다양한 식별 및 인증 기술들이 [9-11]에 자세히 나타나 있다.

다음 그림 1은 단계별 주요 보안 Activity를 나타내는데, V 표시된 영역은 주요 포커싱 영역이다[12]. 그림 1에서는 S/W의 각 단계별 보안 활동들이 자세히 표시되어 있다. 본 논문에서는 Phase 1 분석단계에서 보안요건의 정의 부분에

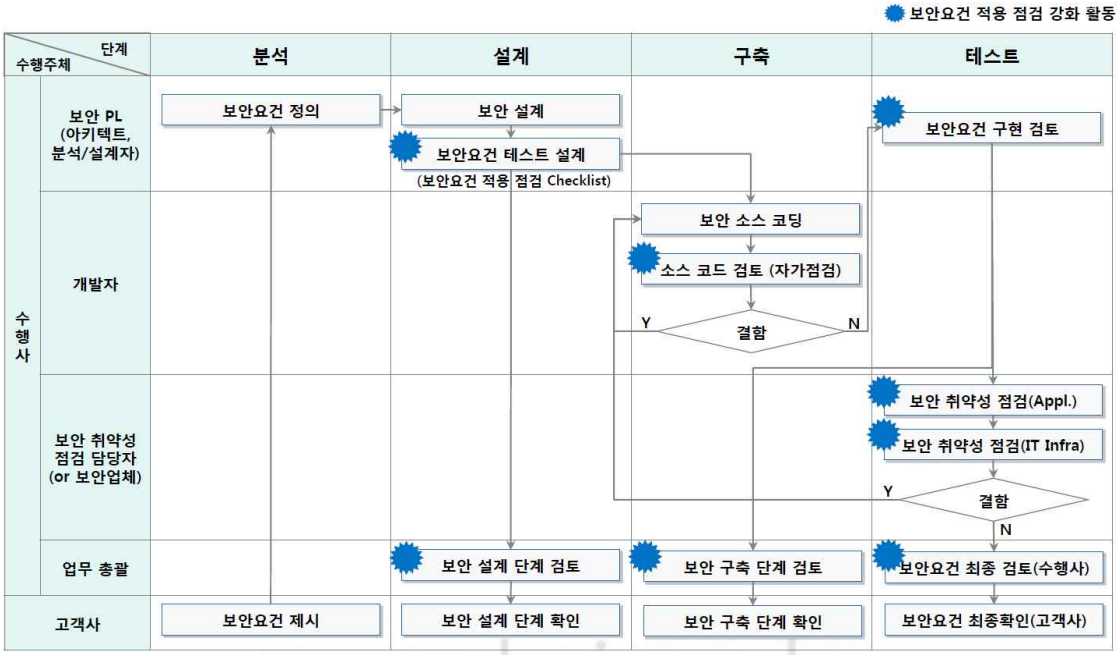

그림 2. 수행 주체별 보안성 점검 프로세스
Fig. 2. Process of Security Checking by Subject-classified Performance

서 식별 및 인증 단계를 다루도록 한다. 즉, 보안요건의 정의는 식별 및 인증, 접근통제, 암호화, 개발 보안, 로깅 및 감사, 그리고 취약점 관리로 나누어지는데, 여기서 식별 및 인증만 다루도록 한다.

다음 그림 2는 수행주체별 보안성 점검 프로세스 전체를 나타낸다. 그림 2의 분석단계에서 수행 주체는 보안 PL, 즉 아키텍트(보안 설계자)나 분석/설계자가 고객사가 제시한 보안요건을 바탕으로 식별 및 인증, 접근통제, 암호화, 개발 보안, 로깅 및 감사, 그리고 취약점 관리 등 보안 요건을 정의하는 것이다.

본 논문의 구성은 1장에서는 서론과 2장에서는 관련연구를 살펴보았으며, 3장에서는 식별 및 인증 요건 정의 원칙, 아이디 및 패스워드 관리 요건, 인증 프로세스 요건, 그리고 인증수단 요건 등, 식별 및 인증에 대하여 자세히 살펴보고, 4장에서는 구현단계로서 식별 및 인증 사례에 대해 살펴보고, 5장에서 결론을 맺도록 한다.

III. 식별 및 인증

1. 식별 및 인증요건 정의 원칙

식별 및 인증에 관한 세부 사항은 다음과 같이 분류하여 설명할 수 있다.

첫째. 식별에서 식별자는 각 개인의 신원을 나타내기 때문에 사용자의 책임 추적성 분석에 중요한 자료가 되며 반드시 유일해야 한다. 그리고 타인과 공유되어서는 되지 않으며, 중요한 의미를 갖는 식별자는 사용을 피해야 한하는 것이다. 즉, 식별은 계정이름 또는 ID에 의하여 사용자가 누구인지 인식하는 과정을 말하며 본인이 누구라는 것을 시스템을 밝히는 과정이라고 할 수 있다.

둘째, 인증은 어떠한 정보에 접근할 수 있는 능력이나 주체자의 자격을 검증하는 단계를 말하는데 이는 시스템의 사용자가 본인임을 주장하는데 그 사용자가 본인이 맞는다고 증명하는 과정을 말한다.

이러한 식별 및 인증요건 정의 원칙은 다음과 같이 말한 수 있다. 익명에게 공개를 목적으로 하는 프로그램을 제외한 모든 어플리케이션은 사용 전 반드시 인증과정을 거쳐야 하며 사용자 권한에 따른 통합 인증관리를 지원하도록 설계해야 한다.

2. 아이디 및 패스워드 관리 요건

아이디는 사용자를 구분하기 위한 공개된 식별자로서 대부분 본인이 쉽게 찾을 수 있다. 하지만 패스워드는 금방 잊어버리는 경우가 많으며 여러 개를 사용하므로 자주 혼돈하게 된다.

패스워드 만들기에 대해 살펴보면 다음과 같다.

첫째로, 대소문자 혼합 패스워드 방식으로, 짝수 번째 문자를 대문자로 혹은 2번째 문자를 소문자로 한다는 자신만의 규칙을 만들어 패스워드를 생성하는 것이다.

둘째, 문자와 숫자 혼합으로 생성하는 방법으로, 특히 자신의 개인정보가 들어간 숫자를 패스워드에 넣어 생성하는 사람들이 많다. 이때 숫자는 결코 유추 불가능한 숫자를 넣어서 사용하면 좋다.

셋째, 특수문자를 혼합하여 사용하는 방법으로, 숫자 대신 특수문자를 넣어 사용하면 매우 편리하고 다른 사용자와 구별이 확실히 된다.

넷째, 사이트마다 서로 다른 패스워드 적용하여 사용하면 편리하다는 것으로서 각 사이트의 특징을 기억하여 사용하면 편리하다.

본 논문에서는 이렇게 생성된 아이디 및 패스워드를 관리하기 위한 보안 요건에 대해 알아보도록 한다. 사용자의 계정(ID)의 발급, 운영, 변경, 폐기를 위한 시스템의 보안요건을 내부 어플리케이션, 외부 어플리케이션 및 IT 인프라로 나누어서 다음의 그림 3의 기준에 따라 정의한다.

계정 요건	내부 어플리케이션	대고객 어플리케이션	IT 인프라
개인용 ID발급	1 인 1 계정	1 인 1 계정	1 인 1 계정 (예외사항 정의 필요)
패스워드 조합기준	영자, 숫자 혼합	제한 없음	영,숫자,특수 중 2 개 이상 혼합
패스워드 최소길이	8	8	8
초기 패스워드 변경	강제	강제	강제
유효기간	10 일	3 개월(고객선택)	3 개월
재사용여부	불가	불가	불가

그림. 3 ID & PW 요건 정의(예)
Fig. 3. Requirement Definition of ID & PW(Example)

3. 인증 프로세스 요건

인증 프로세스란 사용자 로그인 정보를 확인하는 보안 절차이고, 허가된 사용자인지 확인하고 인정하는 과정이며, 사용자를 식별하여 특정 접근을 허용하는 일을 말한다.

본 논문에서는 시스템에 인증 시 보안수준 유지를 위한 인증 절차를 내부 어플리케이션, 대고객 어플리케이션 및 IT 인프라로 구분해서 세션 한도 시간, 인증 허용 회수 등의 기준을 정의하였다.

세션 한도 시간이란 서버와 클라이언트 간에 공유된 세션

키가 유지되는 시간 한도를 말하며, 인증 허용 회수는 인증 실패 횟수가 일정 회수에 도달하면 해당 관리자 계정을 일정 시간 동안 인증을 지연하는 것을 말한다. 이와 같은 인증 프로세스 요건 정의의 예시는 그림 4와 같다.

인증 프로세스 요건	내부 어플리케이션	대고객 어플리케이션	IT 인프라
인증 실패 허용횟수	6회	5회	3회
세션 한도시간 설정값	10, 20, 30분	10, 20, 30분	30분
세션 한도시간 설정	담당자 협의	담당자 협의	강제
인증 전 사용자 공지	없음	경고 베너	경고 베너
인증 후 사용자 공지	라스트 로그온 내역	라스트 로그온 내역	라스트 로그온 내역

그림 4. 인증 프로세스 요건의 정의(예)
Fig. 4. Requirement Definition of Authentication Process(Example)

4. 인증 수단 요건

인증 수단에는 공인인증서, OTP(One Time Password), 보안카드, HSM(Hardware Security Module), 2채널 인증, 휴대폰 SMS, 바이오 인증 등이 있다.

공인인증서는 신뢰된 공인인증기관이 발행하는 인증문서로서 일종의 전자금융거래용 인감증명서를 말한다. OTP(One Time Password) 발생기는 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 일회용 비밀번호를 말하며, 보안카드는 35개 이내의 난수가 적혀진 카드로서 전자금융거래를 수행할 때 이용한다. HSM(Hardware Security Module)이란 전자서명 생성키 등 비밀정보를 안전하게 저장·보관 및 키 생성, 전자서명 생성 등이 기기 내부에서 처리되도록 구현된 스마트 칩을 내장한 하드웨어 모듈을 말한다. 2채널 인증이란 전자금융거래 채널 이외에 거래승인을 위한 채널을 분리하여 이용하는 기술을 말한다. 휴대폰 SMS란 인터넷뱅킹, 텔레뱅킹 등의 전자금융 서비스를 이용한 자금이체 내역을 휴대폰으로 통지하는 서비스를 말한다. 바이오 인증이란 신체의 일부를 이용하여 접속 시 또는 자금 이체 시 신체정보를 이용하여 인증을 수행하며, 복제 및 해킹 위험이 거의 없다. 이 방법은 바이오 인식기기의 보급 및 사용자의 인식 등의 문제로 거의 사용되고 있지 않는 실정 이다.

본 논문에서는 인증 수단 요건으로, 다양한 사용자에 대한 식별 및 인증 방안을 설계해야 하며, 정보시스템의 성격에 따라 강화된 인증 방법을 적용할 수 있도록 설계하여야 한다. 그림 5는 인증 수단 요건 정의(예)이다.

인증 수단	아이디	패스워드	인증서	OTP	생체	IP식별
내부시스템	OK	OK	로긴, 주문 시	n/a	n/a	필요성 검토
IT 인프라(운영)	OK	OK	n/a	n/a	n/a	OK
IT 인프라(개발)	OK	OK	n/a	n/a	n/a	필요성 검토

그림 5. 인증 수단 요건 정의(예)
Fig. 5. Requirement Definition of Authentication Method(Example)

Ⅳ.제안하는 구현 방법

본 논문에서는 제안하는 구현의 방법으로서 △△△사의 분석 단계의 보안 요건 정의에서 식별 및 인증 구현 방법의 사례를 들었다. 그림 6은 식별 및 인증 단계의 보안 요건의 정의에서 ID 관리의 구현 방법이며 그림 7은 PW 정책의 구현 방법이다. 또한 그림 8은 인증 방식 정의의 구현 방법이고, 그림 9는 인증 프로세스의 구현 방법이며, 그림 10은 통합 인증 체계의 구현 방법이다.

요건ID	요건 명	Num	상세 요건
00-00-01	ID 관리	1	모든 어플리케이션에 대해 개별 사용자를 유일하게 식별해야 한다.
		2	어플리케이션 설계 시 모든 ID는 식별되고, 소속, 소유자 및 업무가 정의되어야 한다. (직원ID : 사번)
		3	어플리케이션 사용자 계정과 비밀번호를 개인별로 부여하고, 계정 등록, 변경, 폐기 등에 관해 체계적으로 관리 되도록 해야 함
		4	3개월 동안 로그인이 없는 사용자 ID는 비활성화 한다.
	로그		ID관리에 대한 로그 및 보고서를 생성한다 1. 로그생성 시기: 아이디의 생성 및 변경, 삭제 시 2. 로그포함 항목: 시간, 아이디, 작업유형(생성/변경/삭제 등) 3. 보관 주기 : 5년 4. ID 관리 내역 보고서

그림 6. ID 관리
Fig. 6. ID Management

00-00-02	패스워드 정책	1	최소한의 패스워드 요건과 같거나 그 이상의 강화된 표준을 적용한다. (직원 : 영문, 숫자 혼합 최소6자리)
		2	어플리케이션 사용자의 패스워드의 생성 기준 및 유효기간은 해당 응용시스템에서 강제화 하여 설정하는 것을 원칙으로 한다. - 직전 사용한 패스워드 사용금지, 사용자 ID와 패스워드는 서로 상이해야 한다. - 초기 부여된 패스워드는 반드시 사용자에 의해 변경토록 강제한다. - 주민번호, 동일숫자, 연속숫자 등 유추가 쉬운 비밀번호 등록을 제한한다.
		3	패스워드의 유효기간은 다음을 준수한다. (직원 : 최대 10일 단위로 변경토록 한다.)
		4	패스워드는 화면상에서 읽을수 없는 형태로 표시되어야 한다.
		5	업무 및 거래 시 사용되는 비밀번호의 자리수는 A5-I5체계를 수용하여 업무에 지장이 없도록 해야 한다. - 계좌 비밀번호 : 숫자 4자리, OTP : 숫자6자리, 보안카드 : 숫자 4자리 등
	로그 감사		패스워드 변경내역 로깅 및 보고서를 생성한다. 1. 로그생성 시기 : 패스워드 변경, 입력 오류 시 2. 로그포함 항목 : 시간, 아이디, 패스워드 변경여부, 입력오류횟수 3. 생성레포트 : 패스워드 변경 레포트 4. 보관주기 : 1년

그림 7. PW 관리
Fig. 7. PW Management

요건ID	요건 명	Num	상세 요건
00-00-03	인증 방식 정의	1	내부 직원의 어플리케이션 사용에 대한 인증은 기본적으로 통합인증을 적용 한다. - 통합인증의 인증방식은 ID/PW 또는 인증서 기반 인증을 적용한다.
		2	통합인증 예외 대상은 개별 시스템에서 인증을 처리한다. - 패스워드, IP(단말번호), 연변 등의 인증방식을 적용한다.
		3	어플리케이션 관리자는 제한된 단말에서만 접근이 가능하게 한다. - 인증방식에 단말 IP / MAC 주소 추가

그림 8. 인증 방식 정의
Fig. 8. Definition of Authentication Method

OO-OO-04	인증 프로세스	1	접속 시 마지막 접속정보를 표시한다. - 마지막 접속 IP, 접속시간(시작~종료)
		2	연속하여 일정횟수 이상 입력 오류 시 즉시 해당 비밀번호를 이용하는 계정을 잠금처리 한다. - 직원 : 5회 이상 입력 오류 시 계정잠금, Compliance 부에서 확인 후 해제 처리 등
		3	인증정보는 소스코드 내에 하드코딩 되지 않도록 설계한다.
		4	동일 계정의 멀티로그인을 제한한다.(직원)
		5	인증관련 로그를 생성한다. 로그 생성 시기 : 사용자 로그온 시 로그 포함 항목 : 사용자ID, 일시, 단말IP/ID, 접속성공/실패, 실패내역, 접속방법 등
		로그 감사	인증관련 감사보고서를 생성한다 접속내역 레포팅 - 일정시간 접속횟수/실패횟수가 5회 이상인 ID 리스트, 접속실패 내역 로그보관 주기 - 업무시스템 접속(가동) 기록 : 1년

그림 9. 인증 프로세스

Fig. 9. Authentication Process

요건ID	요건 명	Num	상세 요건
OO-OO-05	통합 인증 체계	1	통합인증체계는 SSO(Single Sign On)를 적용한 단일인증체계로 수립한다.
		2	SSO의 인증방식은 아래 인증 방식을 고려하여 적용한다. - ID/PW 방식의 인증
		3	클라이언트의 인증정보는(토큰정보) 반드시 암호화 되어 전달되도록 한다. - 토큰정보 암호화 - 국내 표준 암호알고리즘 및 국가 권고 기준 적용
		4	통합인증시스템은 인사시스템과 연동되어 인사변동사항을 지체 없이 반영한다.
		5	장애대비를 위한 이중화 및 개별 시스템에서 인증처리 하는 방식으로 전환 등의 대책이 강구되어야 한다.
		로그	로그생성 시기 : 사용자 접속 시 자동기록 로그포함 항목 : 시간, 아이디, 로그인 성공/실패, 실패 내역
		감사	접속내역 레포팅 - 일정시간 접속횟수/실패횟수가 5회 이상인 ID 리스트, 접속실패 내역 로그보관 주기 - 업무시스템 사용자 인증 접속(가동) 기록 : 1년

그림 10. 통합 인증 체계

Fig. 10. Integrated Authentication System

본 논문에서 제시하는 ID 관리, PW 관리, 인증 방식의 정의, 인증 프로세스의 정의, 그리고 통합 인증 체계를 인증 및 식별단계의 보안 요건으로 정의하고 한다. 이러한 보안 요건들은 일반으로 소기업, 중소기업, 대기업, 그리고 보안(생체) 회사로 구분하여 적용하여 평가 할 수 있다. 각각의 기업 5곳씩을 대상으로 인증 및 식별 현황을 조사하여 그 강도(보안의 정도) 평가를 그림 11과 같이 표시하였다.

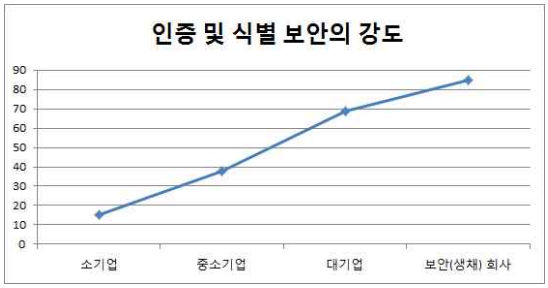

그림 11. 인증 및 식별에서 보안의 강도 평가

Fig. 11. Evaluation of Security Intensity in Identification and Authentication

일반적으로 소기업은 인증 및 식별에서 매우 낮은 보안의 강도를 갖고 있었다. 하지만, 대기업이라고 해서 70%가 넘는 높은 보안의 강도를 갖고 있지는 않았다. 국민은행이나 농협의 해킹 등도 이러한 이유 때문일 것이다. 보안(생체)회사의 보안의 강도는 80% 이상으로써 보안에 관해 어느 정도 철저하였으며 매우 높았다. 하지만 완벽한 보안을 추구할 뿐이지 완벽한 보안이란 없는 것 같다는 생각이 든다.

V. 결 론

S/W 개발의 첫 번째 단계인 분석 단계에서는 식별 및 인증 요건 정의 원칙, 아이디 및 패스워드 관리 요건, 인증 프로세스 요건, 그리고 인증수단 요건 등에 관한 보안 요건들을 정의해야 한다. 식별은 본인의 신원을 시스템에 밝히는 것(ID)으로서 시스템 사용자의 책임 추적성 분석이 가능하다. 이러한 ID는 고유한 값이어야 하여 공유되어서는 안 된다. 그리고 중요한 의미를 갖는 식별자는 사용을 금지하고 있다. 인증은 시스템에 접근자격을 검증하는 단계로서 패스워드를 말하며, 시스템이 자기 자신임을 장하는 사용자를 시스템이 자신으로 인정하는 절차로서 사용자를 증명하는 과정을 말한다.

본 논문에서는 분석 단계의 이러한 식별 및 인증의 보안요건을 제시하였다. 먼저, 개별적으로 가지고 있는 개별 ID는 유일하며 고유하게 다른 사람과 식별되어야 한다는 점이란 것을 강조했다. 그리고 인증에 사용되는 패스워드는 길이제한 및 표준 조합을 적용하여 만들어야 하며, 일정한 간격을 두고 되풀이하여 바꿔 주어야 한다는 점이다. 또한, ID/PW와 그 외의 공인인증서, OTP(On Time Password), 보안카드, HSM(Hardware Security Module), 2채널 인증, 휴대폰 SMS, 바이오 인증 등 보다 강력하고 강화된 인증 방식을 제공해야 하며, 인증 프로세스는 정의된 보안 요건을 만족하게 설정해야 한다. 본 연구에서는 이러한 초기 분석단계에서 식별 및 인증단계의 보안 요건들을 실제 제안하는 구현 방법을 들어 설명하여 전체적으로 필요한 보안 요건들을 한눈에 볼 수 있었다.

참고문헌

〔1〕 http://terms.naver.com/entry.nhn?docId=2073350&cid=208&categoryId=208#TABLE_OF_CONTENT1

〔2〕 http://northface32.blog.me/50120464405

〔3〕 http://cafe.naver.com/softwarequality/book1621832 /758

〔4〕 http://www.cyworld.com/B166er/6718585
〔5〕 Daniel D. Lam, "Automated user authentication identification for customized converged services," US Patent, US 8650628 B2, 2014
〔6〕 Sviatoslav Voloshynovskiy, Oleksiy Koval, Thierry Pun, "Secure item identification and authentication system and method based on unclonable features," US Patent, US 8705873 B2, 2014
〔7〕 Won-Hee Nam, Dea-Woo Park, "A Study on Cloud Network and Security System Analysis for Enhanced Security of Legislative Authority," The Journal of the Korean Institute of Information and Communication Engineering, Vol. 15, No. 6, pp. 1320-1326, 2011. 6
〔8〕 G. McGraw, "Software assurance for security," IEEE Computer, vol. 32, pp. 103-105, Apr. 1999.
〔9〕 Yoon Jae-Ho, "A Study on Identification & Authentication in Enrollment Systems," Thesis of Master of Engineering, Dept. of Graduate School of Sejong University, 2004
〔10〕 Yoon-Su Jeong, "Design of Patient Authentication Model in u-healthcare Environment using Coalition ID," Jouranl of Digital Convergence Vol. 11, No. 3, pp. 3-5-310, 2013. 2
〔11〕 Jonghoon Lee, Jungsoo Park, Seung Wook Jung, Souhwan Jung, "The Authentication and Key Management Method based on PUF for Secure USB," J-KICS, Vol. 38B, No. 12, pp. 944-953, 2013.12
〔12〕 Seong-Yoon Shin, Dai-Hyun Jang, Hyeong-Jin Kim, "A Study on Security Measure of Step-Wise Project," Journal of the Korea Institute of Information and Communication Engineering, Vol. 18, No. 4, pp. 771-778, Apr. 2012

저 자 소 개

신 성 윤
2003년 2월 : 군산대학교 컴퓨터과학과 이학박사
2006년~현재 : 군산대학교 컴퓨터정보공학과 교수
관심분야 : 영상처리, 컴퓨터비전, 가상현실, 멀티미디어
Email : s3397220@kunsan.ac.kr