S/W 개발 분석 단계에서 식별 및 인증

신성윤* · 진동수*** · 신광성* · 이현창** · 이양원*

*군산대학교 컴퓨터정보공학과

**원광대학교 정보전자상거래학부(융복합창의연구소)

***경인여자대학교 경영과

Legal System and Regulation Analysis by S/W Development Security

Seong-Yoon Shin* · Dong-Soo Jin*** · Kwong-Seong Shin* · Hyun-Chang Lee** · Yang-Won Lee*

*Dept. of Computer Information Engineering, Kunsan National University

**Div. Of Information and Electronic Commerce(Institute of Convergence and Creativity)
Wonkwang University

***Dept. of Business Administration, Kyung-In Woman's University

E-mail : {s397220, waver, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr, dsjin777@kiwu.ac.kr

Acknowledgement : "This research is partially supported by Institute of Information and Telecommunication Technology of KNU"

요 약

본 논문에서는 분석 단계의 이러한 식별 및 인증의 보안요건을 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.

ABSTRACT

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 satisfy the defined security elements on authentication process.

키워드

감사로그(Audit Log), 접속 로그(Access Log), 중요 정보(Major Information)

Ⅰ. 서 론

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].

II. 관련연구

[4]의 특허에서는 컴퓨팅 장치와 연관된 유효한 인증 데이터를 이용하여 자동으로 사용자 인증을 제공하기 위해 시스템이 제시되었다. [5]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.

III. 식별 및 인증

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.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.

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

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

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

IV. 구현 방법

본 논문에서는 제안하는 구현의 방법으로서 △△△사의 분석 단계의 보안 요건 정의에서 식별 및 인증 구현 방법의 사례를 들었다. 그림 1은 식별 및 인증 단계의 보안 요건의 정의에서 ID 관리의 구현 방법이며 그림 2는 PW 정책의 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 1. ID 관리

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 AS-IS체계를 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 2. PW 관리

V. 결 론

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.

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/book1621832/75 8

[4] Daniel D. Lam, “Automated user authentication identification for customized converged services,” US Patent, US 8650628 B2, 2014

[5] Sviatoslav Voloshynovskiy, Oleksiy Koval, Thierry Pun, “Secure item identification and authentication system and method based on unclonable features,” US Patent, US 8705873 B2, 2014