
식별 및 인증 단계 보안 요건의 정의

신성윤* · 김창호* · 장대현* · 이현창** · 이양원*

*군산대학교

**원광대학교

Definition of Security Requirement in Steps of Identification and Authentication

Seong-Yoon Shin* · Chang-Ho Kim* · Dai-Hyun Jang* · Hyun Chang Lee** · Yang-Won Rhee*

*Kunsan National University

**Wonkwang University

E-mail : {s3397220, over386, daihjang, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr

요 약

식별 및 인증은 어플리케이션 보안 요건의 한 영역이다. 개별 ID를 유일하게 식별해야 한다. 패스워드는 길이 제한 및 조합 표준을 적용해야 한다. 그리고 주기적으로 변경해야 한다. ID/PW 이외의 강화된 인증 방식을 제공해야 한다. 인증 프로세스는 정의된 보안 요건을 만족해야 한다.

ABSTRACT

Identification and authentication of the security requirements of the application area. Individual ID for uniquely be identified. Standard length of the password is limited and should be applied in combination. And must be changed periodically. ID/PW authentication scheme non-reinforced must be provided. The authentication process is defined in the security requirements should be satisfied

키워드

identification, authentication, security requirements

I. 서 론

현재 널리 사용되고 있는 웹 환경에서 사용자 식별 및 인증관련 보안서비스가 취약할 뿐만 아니라 이의 활용에 문제를 안고 있다. 이를 해결하기 위하여 웹 환경에서 자바 기술을 이용한 안전한 사용자 식별 및 인증 모델 설계[1] 기술이 발표 되었다.

모든 사용자는 개인적인 사용만을 위한 유일한 식별자(사용자 ID)를 가져야 하며 사용자의 신원을 확인하기 위해 적절한 인증 기법을 선택하여야 한다[2].

II. 식별 및 인증 요건의 정의 원칙

익명에게 공개를 목적으로 하는 프로그램을 제외한 모든 어플리케이션은 사용 전 반드시 인증 과정을 거쳐야 하며 사용자 권한에 따른 통합 인증 관리를 지원하도록 설계해야 한다.

III. 아이디 및 패스워드 관리 요건

사용자의 계정(ID)의 발급, 운영, 변경, 폐기를 위한 시스템의 보안 요건을 내부 어플리케이션, 외부 어플리케이션 및 IT 인프라로 나누어서 다

음의 기준에 따라 정의한다.

[아이디 및 패스워드 요건 정의 (예시)]

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

그림 1. 아이디 및 패스워드 요건

IV. 인증 프로세스 요건

시스템에 인증시 보안 수준 유지를 위한 인증 절차를 내부 어플리케이션, 대고객 어플리케이션 및 IT 인프라로 구분해서 세션 한도 시간, 인증 허용 회수 등의 기준을 정의한다.

V. 인증 수단 요건

다양한 사용자에게 대한 식별 및 인증 방안을 설계해야 하며, 정보 시스템의 성격에 따라 강화된 인증 방법을 적용할 수 있도록 설계하여야 한다.

VI. 결론

어플리케이션 보안 요건의 한 영역인 식별 및 인증을 다루었다. 사용자의 개별 ID는 유일하게 식별해야 한다. 그리고 사용자의 패스워드는 길이 제한 및 조합 표준을 적용하여 설정하고 일정한 주기를 갖고 바뀌어야 한다. 기본적인 ID/PW 이외의 보다 강화된 인증 방식을 설계해야 한다. 그리고 인증 프로세스는 정의된 보안 요건을 충족해야 한다.

참고문헌

- [1] 송기평, 손홍, 김선주, 조인준, “웹 환경에서 자바 기술을 이용한 안전한 사용자 식별 및 인증 모델 설계,” 한국해양정보통신학회종합 학술대회, Vol. 4, No. 2, pp.433-438, 2000
- [2] <http://cafe.naver.com/softwarequality/book1621832/758>