DOI: 10.3745/KIPSTC.2008.15-C.2.125

아이디/패스워드 통합 관리 제품의 취약성 분석 및 평가기준 제안

한 정 훈[†] · 이 병 희[††] · 홍 수 민[†] · 김 승 현[†††] · 원 동 호[††††] · 김 승 주[†††††]

요 약

인터넷 기술의 발달에 따라 온라인 서비스를 이용하기 위해 개인이 관리해야 할 아이디의 수가 증가하였고, 사용자의 아이디와 패스워드를 안전하고 편리하게 관리할 수 있는 아이디/패스워드 통합 관리 제품이 개발되어 사용되고 있다. 하지만 이러한 제품에서 관리자 패스워드가 노출되면 사용자의 모든 정보가 노출될 수 있는 위험이 있다. 따라서 현재 상용 제품의 취약성 분석을 통해 보안요구사항을 도출하고, 안전한 아이디/패스워드 통합 관리 제품 개발의 지침으로 사용될 평가기준이 필요하다. 본 논문에서는 도출된 보안요구사항을 바탕으로, 안전한 아이디/패스워드 통합 관리 제품을 위한 평가 기준을 제안한다.

키워드 : 아이디/패스워드 통합 관리 제품, 디지털 ID 관리 기술, 평가 기준

Analysis on Vulnerability of ID/PW Management Solution and Proposal of the Evaluation Criteria

Jeonghoon Han[†] · Byunghee Lee[††] · Sumin Hong[†] · Seunghyun Kim[†††]
Dongho Won[††††] · Seungjoo Kim[†††††]

ABSTRACT

As the development of Internet technology, the number of IDs managed by each individuals has been increased. And many software development institutes have developed ID/PW management solutions to facilitate secure and convenient management of ID/PW. However, these solutions also can be vulnerable in case of administrator's password exposure. Thus, we need to derive security requirements from the vulnerability analysis of these solutions, also we need evaluation criteria for secure ID/PW management solution development. In this paper, we analyze the vulnerability of ID/PW management solution and propose the evaluation criteria for secure ID/PW management solution.

Key Words : ID/PW Management Solution, Digital Identity Management, Evaluation Criteria

1. 서 론

인터넷 기술이 발달하고 이용인구가 증가함에 따라 인터넷에서 사용자가 관리해야 할 정보가 기하급수적으로 증가하고 있으며, 대부분의 사용자가 쉽고 간단한 아이디와 패스워드를 동일하게 사용하고 있기 때문에 해킹에 대한 위험이 높다[1]. 이러한 위험을 해결할 수 있는 방안으로 여러 웹사이트에 분산되어 있는 사용자의 아이디와 패스워드를 통합하여 안전하게 관리할 수 있는 아이디/패스워드 통합 관리 제품이 개발되어 사용되고 있다. 그리고 이러한 제품에 이동성을 지원하기 위해 기존의 PC에 설치하여 사용하는 제품과는 별도로 USB 메모리 장치에 설치가 가능한 제품도 함께 제공되고 있다. 그러나 이러한 제품은 사용자의 아이디/패스워드의 목록을 만들어 편리하고 안전하게 관리할 수 있는 이점도 있지만, 관리자 패스워드가 노출되면 저장되어 있는 사용자의 모든 정보가 노출될 수 있는 위험이 있다. 본 논문에서 분석한 아이디/패스워드 통합 관리 제품들은 사용자 개인정보 관리 기능의 안전성을 보장하기 위한 특별한 기준이 없이 개발되었기 때문에, 기존의 공개된 개인정보 해킹 방식에 취약하다. 따라서 안전한 아이디/패스워드 통합 관리 제품을 위한 평가기준이 필요하고, 이를 바탕으로 제품이 개발되어야 한다.

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술 개발사업의 일환으로 수행하였음. [IITA-2007-S-601-01, 자기통제 강화형 전자ID지갑 시스템 개발]
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 정 회 원 : 한국전자통신연구원 정보보호연구단 연구원
†††† 종신회원 : 성균관대학교 정보통신공학부 교수
††††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2007년 12월 7일, 심사완료 : 2008년 3월 3일

본 논문에서는 2장에서 아이디/패스워드 통합 관리 제품을 소개하고, 3장에서는 사용자 PC에서 패스워드가 노출될 수 있는 구간에 대해 키로그, PC 메모리 분석, USB 스니핑을 통해 취약성을 분석한다. 4장에서는 저장된 사용자의 개인정보 파일의 재사용 가능 여부와 삭제된 개인정보 파일의 복구 가능 여부에 대해 분석한다. 5장에서는 앞에서 분석된 결과를 바탕으로 안전한 아이디/패스워드 통합 관리 제품을 위한 평가 기준을 제안하고, 마지막으로 6장에서 결론을 맺는다.

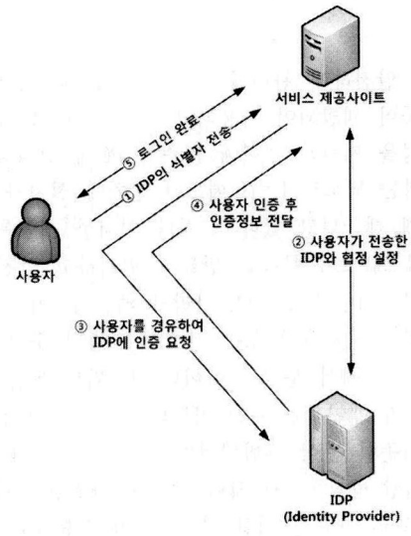
2. 아이디/패스워드 통합 관리 제품 소개

2.1 분석 대상 제품의 선정

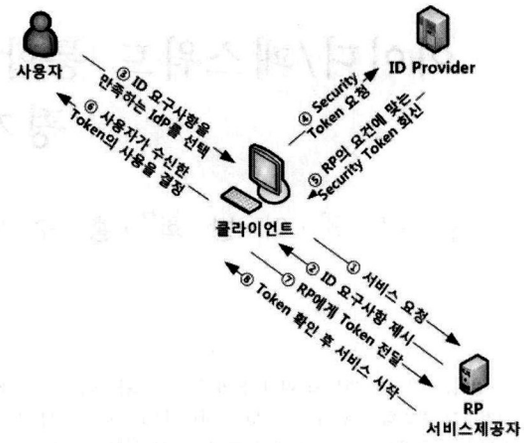
사용자의 분산된 아이디를 효율적으로 관리하기 위한 연구가 세계적으로 많이 이루어지고 있으며, 대표적인 인터넷 아이디 관리 기술로는 OpenID[2]와 Microsoft에서 개발 중인 CardSpace[3], OASIS의 SAML[4][5]이 있다. 국내에서는 한국전자통신연구원이 2004년부터 2007년까지 개발한 e-IDMS를 적용하여 대전광역시 통합ID관리시스템을 구축하였으며, 현재는 행정자치부의 통합ID관리 서비스로 활용되고 있다. OpenID는 (그림 1)에서와 같이 하나의 아이디로 OpenID를 지원하는 모든 서비스를 이용할 수 있는 기술이다[6].

CardSpace는 (그림 2)와 같이 아이디와 패스워드를 사용하지 않고, Security Token을 이용하여 모든 개인정보가 사용자에 의해 선택되어 관리되는 사용자 중심의 인터넷 아이디 관리 기술이다.

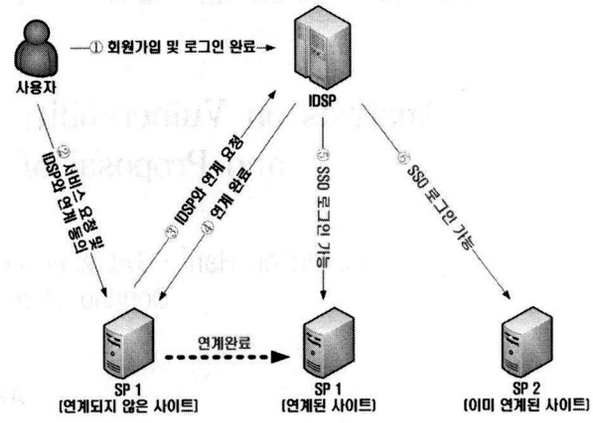
또한 한국전자통신연구원에서 개발한 e-IDMS가 채택한 SAML[7]은 (그림 3)과 같이 서비스를 제공하는 사이트(SP, Service Provider)에서 사용하는 아이디를 IDSP(IDentity Service Provider)에 연계하여 싱글사인온(SSO, Single-Sign-On)을 통해 분산되어 있는 사용자의 아이디를 통합하여 관리할 수 있는 인터넷 아이디 관리 기술이다.



(그림 1) OpenID의 동작방식



(그림 2) CardSpace의 동작방식



(그림 3) 아이디 연계를 통한 SAML의 동작방식

OpenID의 경우 현재 많은 사용자를 보유하고 있으며, 실제로 서비스되고 있는 기술이다. 하지만, 사용자가 이미 가입되어 있는 모든 인터넷 사이트가 OpenID를 지원해야 하기 때문에, 현재 분산되어 있는 아이디를 통합하는 방법이 아닌 대체하는 방식이다. 그리고 Microsoft의 CardSpace는 최근 해외에서 조금씩 증가하고 있는 추세이며, SAML은 이미 1억 개의 아이디가 만들어져 사용되고 있다[7]. 그 중 OpenID와 SAML의 경우, 사용자의 PC에 별도로 개인 정보를 저장하여 관리하는 기술을 사용하지 않는다. 본 논문에서는, 사용자 PC의 웹브라우저에 플러그인(Add-on) 형태로 설치되거나, 별도의 응용프로그램으로 설치되어 기존의 분산된 아이디/패스워드를 통합하여 저장 및 관리하는 제품을 대상으로 분석을 수행하였다. 본 논문에서 분석한 제품의 선정 기준은 다음과 같다.

1. 기존의 아이디/패스워드 관리 방식이 적용 가능한 제품
2. USB 메모리 장치에 설치가 가능한 이동성을 지원하는 제품
3. 현재 연구되는 대표적인 인터넷 관리기술인 OpenID와 CardSpace를 지원하는 제품

위 기준에 따라, OpenID를 지원하면서 기존의 아이디/패스워드를 통합하여 관리하는 제품으로는 Sxipper[8]를 선정하였고, 이는 Mozilla Firefox의 플러그인(Add-on) 형태로 설치되는 제품이다. 그리고 .NET 프레임워크 3.0에 포함되어 있으며, Windows Vista 운영체제에 정식으로 탑재되어 있는 인터넷 아이디 관리 기술인 CardSpace도 분석 대상으로 선정하였다. 또한, 웹브라우저에 플러그인(Add-on) 형태로 설치되며, 기존의 사용자 아이디/패스워드 목록을 저장하여 관리하는 제품인 RoboForm[9]도 분석 대상으로 선정하였다. 별도의 응용프로그램으로 설치되는 제품으로는, 국내 제품인 알패스[10], 국외 제품인 KeePass[11], Advanced Password Manager[12], Effective Password Manager[13], Password Keeper Expert[14], SecureWallet[15]을 분석 대상으로 선정하였고, 모두 기존의 사용자 아이디/패스워드 목록을 저장하여 관리하는 제품이다. 알패스, RoboForm, KeePass는 USB 메모리 장치에 설치가 가능한 제품도 함께 제공하고 있으며, 나머지 제품들은 알패스, RoboForm, KeePass와 유사한 기능을 가진 제품들 중에서 임의로 선택하였다.

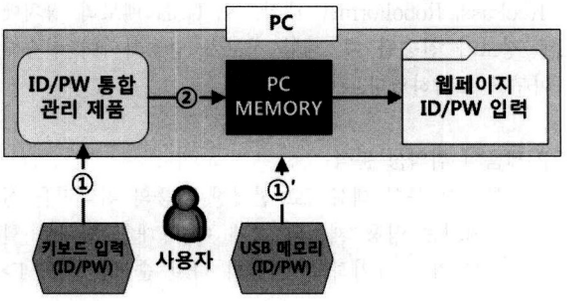
2.2 분석 대상 제품의 특징 및 분석 범위

분석 대상으로 선정한 제품의 특징은 <표 1>과 같으며, 이들 제품 중 USB 메모리 장치에 설치되는 별도의 프로그램을 제공하는 제품은 알패스, KeePass, RoboForm이 있다.

위 제품 중 CardSpace를 제외한 모든 제품은 (그림 4)와 같은 방식으로 동작하고 있으며, ①번 구간에서는 키로그 분석 툴을 이용하여 키보드를 통해 사용자가 입력하는 관리자 및 웹사이트의 아이디/패스워드 노출 여부를 조사하였고, ①'번 구간에서는 USB 메모리 장치의 스니핑을 통한 아이디/패스워드 노출 여부를 조사하였다. 또한 ②번 구간에서는 사용자로부터 입력된 아이디/패스워드와 제품에 등록되어 있는 웹사이트의 아이디/패스워드가 사용자의 PC 메모리에 암호화되지 않은 상태로 노출되는지 여부를 조사하였다.

〈표 1〉 제품의 설치 형태 및 이동성 지원 여부

제 품 명	설 치 형 태	이동성 지원
알패스	별도의 응용프로그램	○
Sxipper	플러그인(Add-on)	X
KeePass	별도의 응용프로그램	○
RoboForm	플러그인(Add-on)	○
Advanced Password Manager	별도의 응용프로그램	X
Effective Password Manager	별도의 응용프로그램	X
Password Keeper Expert	별도의 응용프로그램	X
SecureWallet	별도의 응용프로그램	X
CardSpace	운영체제에서 지원 / 플러그인(Add-on)	X



(그림 4) 아이디/패스워드 통합 관리 제품의 동작방식

3. 아이디/패스워드 통합 관리 제품의 취약성 분석

본 논문에서는 기존 연구 결과[16]에 4개의 제품과, 2개의 취약성 분석 항목을 추가하여 조사를 수행하였다. 그리고 아이디/패스워드 통합 관리 제품이 보안기능을 제공하고 있는지 분석하였기 때문에, 사용자 PC에 해킹 프로그램을 탐지할 수 있는 별도의 보안 솔루션이 설치되어 있지 않다는 가정 하에 조사를 수행하였다. 또한, 사용자의 PC에는 사용자 부주의 또는 공격자의 의도대로 해킹 프로그램이 설치되어 있다고 가정하였다.

3.1 취약성 분석 방법 및 도구 선정

3.1.1 키로그 분석 도구 및 방법

키로그 분석 도구로는 키보드와 마우스로부터 얻을 수 있는 일반적인 키로그 정보 외에 Static Text와 Edit Controls의 정보를 제공하는 SKIn2000을 사용하였다[17]. 아이디/패스워드 통합 관리 제품은 관리자의 패스워드가 노출되면 사용자가 등록한 모든 웹사이트 아이디/패스워드 목록이 노출될 수 있는 문제점이 있다. 따라서 제품을 처음 실행하였을 때, 관리자 패스워드를 입력하는 과정에서 해당 정보가 노출되는지 여부를 조사하였다.

3.1.2 메모리 분석 도구 및 방법

아이디/패스워드 통합 관리 제품이 사용하고 있는 메모리에 저장된 정보를 분석하기 위해 WinHex를 사용하였다[18]. 패스워드와 같은 비밀정보가 안전하게 관리되기 위해서는 해당 정보를 메모리에 암호화하여 저장하고, 복호화하여 사용한 후에는 복호화된 데이터가 메모리에서 삭제되어야 한다. 즉 복호화된 데이터가 메모리에 존재하는 시간이 가장 짧도록 제품이 구현되어야 한다. 따라서 제품이 실행되었을 때, 아이디/패스워드가 메모리에 암호화되어 저장되는지 여부와, 복호화하여 사용한 후 메모리에서 안전하게 삭제되는지 여부를 조사하였다.

3.1.3 USB 스니핑 도구 및 방법

USB 스니핑 도구로는 Bus Hound[19]를 사용하였고, USB 메모리 장치를 통해 이동성을 지원하는 제품인 알패

스, KeePass, RoboForm을 대상으로 USB 메모리 장치에서 PC로 정보가 전송될 때, 해당 정보가 암호화되어 전송되는지 여부를 조사하였다.

3.2 제품의 취약성 분석

본 논문에서 분석 대상으로 선정한 제품의 취약점을 설명하는 부분에서는 상용 제품의 실제 이름 대신 임의로 할당한 영문 대문자로 표기하고, 제품의 나열 순서는 <표 1>과 다르다.

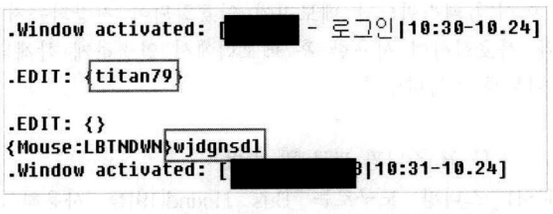
3.2.1 제품별 키로그를 통한 아이디/패스워드 노출

아이디/패스워드를 사용하지 않는 I 제품을 제외하고, 본 논문에서 분석 대상으로 선정한 제품들은 관리자 패스워드를 설정하는 기능을 모두 제공하고 있으며, 관리자 패스워드를 입력하여 인증을 거친 후에만 기존에 등록해놓은 웹사이트의 아이디/패스워드에 대한 접근이 가능하다. 키로그를 통한 정보의 노출 여부는 <표 2>와 같으며, 관리자 패스워드는 모든 제품에서 노출되었고, 웹사이트의 아이디/패스워드는 사용자가 키보드를 통해 직접 입력하는 정보가 아니기 때문에 노출되지 않았다. 그러나 공격자에게 관리자 패스워드가 노출되면 웹사이트 아이디/패스워드 목록에 대한 접근이 가능하게 되므로, 공격자는 모든 정보를 알 수 있게 된다.

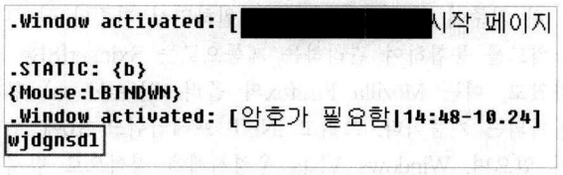
(그림 5)와 (그림 6)은 키로그를 통해 노출된 제품의 관리자 패스워드와 사용자가 등록해놓은 웹사이트의 아이디/패스워드 정보이다. 다른 제품들과는 달리 E 제품은 하나에 여러 사용자를 등록할 수 있도록 관리자 아이디를 등록하게 되어있으며, 관리자의 아이디도 키로그를 통해 노출되었다. 또한 G 제품의 경우 Secure Edit Controls[20] 기능을 제공하여, SKIn2000을 통한 Edit Control 정보는 노출되지 않았지만, 단순한 키로그 기능을 통해 관리자의 패스워드가 노출되었다.

〈표 2〉 키로그를 통한 아이디/패스워드 노출 여부

제 품 명	관리자 패스워드	등록된 웹사이트 아이디/패스워드
A 제품	○	X
B 제품	○	X
C 제품	○	X
D 제품	○	X
E 제품	○	X
F 제품	○	X
G 제품	○	X
H 제품	○	X



(그림 5) E 제품의 관리자 아이디/패스워드 노출



(그림 6) F 제품의 관리자 패스워드 노출

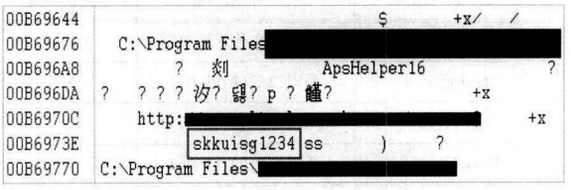
3.2.2 제품별 PC 메모리의 아이디/패스워드 노출

각 제품이 사용하는 PC의 메모리에서 정보의 노출 여부는 <표 3>과 같다. F, H, I 제품은 웹브라우저에 플러그인(Add-on) 형태로 설치되어 사용되기 때문에, 각 제품이 설치되는 웹브라우저인 Internet Explorer, Firefox가 사용하는 메모리를 분석하였다. I 제품은 아이디/패스워드를 사용하지 않아, 사용자가 추가한 개인카드의 정보가 노출되는지 여부를 조사하였으나, 노출되는 정보가 없었다.

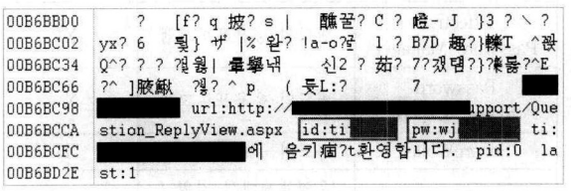
G 제품의 경우 제품에서 제공하는 Secure Edit Control 기능이 메모리에 관리자 패스워드가 노출되는 것을 방지하는 기능을 갖고 있지만, 관리자 패스워드를 입력하고 몇 초가 지나야 메모리에서 삭제되도록 구현되어 있어, 사용자가 패스워드를 입력한 초기에는 메모리에 암호화되지 않은 상태로 존재하고 있었다. 따라서 H 제품과 I 제품을 제외한 모든 제품에서 관리자 패스워드가 노출되었으며, 사용자가 등록한 웹사이트 아이디/패스워드는 D 제품과 I 제품을 제외한 모든 제품에서 노출되었다. (그림 7)과 (그림 8)은 사용자 PC의 메모리에 노출된 정보이다.

〈표 3〉 PC 메모리의 아이디/패스워드 노출 여부

제 품 명	관리자 패스워드	등록된 웹사이트 아이디/패스워드
A 제품	○	○
B 제품	○	○
C 제품	○	○
D 제품	○	X
E 제품	○	○
F 제품	○	○
G 제품	△	ID만 노출
H 제품	X	○



(그림 7) E 제품의 관리자 패스워드 노출



(그림 8) E 제품의 웹사이트 아이디/패스워드 노출

3.2.3 제품별 USB 스니핑을 통한 아이디/패스워드 노출

분석 대상 제품 중 USB 메모리 장치를 통해 이동성을 지원하는 제품인 E, G, H 제품을 조사한 결과, E 제품의 관리자 아이디만 노출되었으며, 노출된 정보는 (그림 9)와 같다.

```
5b 78 62 74  69 6f 6e 34  65 76 65 72  5d 0d 0a 50  [xbtion4ever]..P
6f 73 4c 65  66 74 3d 35  30 37 0d 0a  50 6f 73 54  osLeft=507..PosT
48 00 09 00  00 00 00 00  c0 c9 fa 85  20 00 00 00  BULK/INT XFER
c4 b9 33 86  00 00 00 00  00 02 00 00  00 00 00 00
86 00 24 01  74 49 2b f2  00 00 00 00  00 00 00 00
c8 9a 8e 85  c8 9a 8e 85  00 00 00 00  00 00 00 00
0f 00 00 e0  4c 94 fb 85  00 00 00 00  03 00 22 00  INTERNAL IOCTL
00 00 00 00  f0 67 24 86  00 00 00 00  74 88 bf f7
0d 00 00 00                                    13
```

(그림 9) E 제품 관리자 아이디 노출

4. 저장된 사용자의 개인정보 파일 분석

본 장에서는 각 제품의 관리자 패스워드와 웹사이트의 아이디/패스워드 목록을 저장하고 있는 파일의 재사용 가능 여부와 삭제된 개인정보 파일의 복구 가능성에 대해 분석하였다. 3장에서 관리자의 패스워드가 모두 노출되었기 때문에, 공격자가 관리자의 패스워드를 알고 있고 개인정보 파일의 재사용이 가능하다면, 사용자가 등록해놓은 웹사이트의 아이디/패스워드의 정보를 모두 알 수 있게 된다. 따라서 개인정보 파일은 재사용이 불가능해야 하고, 삭제된 개인정보 파일은 포렌식 툴에 의해서 복구가 불가능해야 한다. 이를 알아보기 위해, 먼저 저장된 개인정보 파일을 다른 PC에 복사한 후, 제품을 설치하여 복사된 파일의 정보를 재사용할 수 있는지 조사하였고, 현재 사용자의 정보를 삭제하는 기능을 포함하고 있는 E 제품을 대상으로 삭제된 개인정보 파일이 복구되는지 여부를 조사하였다. 또한 모든 제품을 대상으로 사용자의 PC에서 제품을 제거하는 경우, 함께 삭제된 개인정보 파일이 복구되는지 여부도 조사하였다.

4.1 개인정보 파일의 재사용

개인정보 파일을 재사용하기 위해서는 관리자의 패스워드를 알고 있어야 한다. 3장에서 키로그를 통해 모든 관리자의 패스워드가 노출되었기 때문에, 공격자는 관리자 패스워드를 알고 있다는 가정 하에 개인정보 파일의 재사용 가능 여부를 조사하였다. 또한 사용자의 PC에서 파일을 복사해올 수 있는 기능을 제공하는 해킹 프로그램을 사용할 경우, 공격자가 개인정보 파일이 저장되는 경로를 알고 있으면 해당 파일을 쉽게 획득할 수 있다[21]. 각 제품별 생성하여 저장하고 있는 개인정보 파일은 <표 4>와 같고, 해당 파일을 다른 PC에 복사한 후, 관리자 패스워드를 입력한 결과 I 제품을 제외한 모든 제품의 개인정보 파일이 재사용 가능하였다. I 제품은 운영체제에서 파일의 복사를 방지하고 있어, 개인정보 파일 복사를 통한 재사용 가능 여부 조사가 불가능하였다.

〈표 4〉 제품별 저장된 정보의 재사용 가능 여부

제 품 명	저장된 정보의 파일 이름	재사용 가능
A 제품	*.pswd	O
B 제품	*.apm	O
C 제품	*.dat, *.dat	O
D 제품	*.swdb	O
E 제품	*.apw	O
F 제품	*.txt, *.db, *.rdf	O
G 제품	*.kdb	O
H 제품	*.rfb, *.rfp	O
I 제품	*.db	X

4.2 삭제된 개인정보 파일의 복구

삭제된 개인정보 파일을 복구하기 위한 도구로는, 삭제되거나 손상된 파일을 복구하는 툴로 널리 알려져 있는 FinalData[22]를 사용하였다. 먼저 E 제품의 현재 사용자 삭제 기능을 통해 삭제된 개인정보 파일을 복구하는데 성공하였고, 사용자의 PC에서 다른 모든 제품을 제거한 후, 함께 삭제된 개인정보 파일의 복구도 가능하였다. 삭제된 개인정보 파일이 복구되는 경우, 4.1절에서와 같이 공격자가 사용자의 관리자 패스워드를 알고 있다면 사용자가 등록한 모든 웹사이트의 아이디/패스워드 목록이 노출된다고 할 수 있다. 또한 I 제품의 복구된 파일의 복사는 가능하였지만, 재사용을 시도할 경우 원래의 PC에서 뿐만 아니라, 다른 PC에서도 I 제품이 동작하지 않았다.

5. 안전한 아이디/패스워드 통합 관리 제품을 위한 평가기준 제안

5.1 안전하게 관리되어야 할 정보

아이디/패스워드 통합 관리 제품에서 노출되지 않아야 하는 가장 중요한 정보는 관리자 패스워드이다. 사용자의 개인정보 파일이 노출되더라도, 관리자 패스워드를 알지 못하면, 해당 파일에 포함된 정보를 알 수 없다. 또한, 사용자의 개인정보 파일도 안전하게 보호되어야 한다. 3장과 4장에서 분석한 결과와 같이, 관리자의 패스워드가 노출된 상태에서 개인정보 파일이 공격자에게 노출되면, 사용자가 등록한 모든 웹사이트의 아이디/패스워드가 노출될 수 있다. 그리고 관리자의 패스워드가 노출되지 않았다 하더라도, 공격자는 획득한 개인정보 파일을 이용하여 패스워드 추측 공격을 통해 관리자 패스워드를 알아낼 수 있다.

5.2 패스워드 및 저장정보의 안전한 관리를 위한 보안 요구사항

3장과 4장에서 취약성을 분석한 결과를 통해, 패스워드 및 저장정보의 안전한 관리를 위한 보안 요구사항을 도출하면 <표 5>와 같다. 보안 요구사항은 본 논문에서 분석한 취약성 분석 결과 외에도, 분석 대상 제품들이 제공하는 보안 기능을 바탕으로 도출하였다.

5.3 안전한 아이디/패스워드 통합 관리 제품을 위한 평가기준

5.2절에서 도출된 보안 요구사항을 바탕으로 한 안전한 아이디/패스워드 통합 관리 제품을 위한 평가기준은 <표 6>과 같다. '2.2. 복합 인증'은 제품이 포함해야 할 필수 보안기능이 아니고, 보다 안전한 사용자 인증을 위한 선택사항이다. 제안한 평가기준 중 기존의 제품들이 제공하지 않는, 새롭게 추가된 보안기능은 '1.1. 키보드 해킹방지', '1.3. 스니핑 방지', '3.5. 삭제된 저장정보의 복구 방지', '5.1. 감사 데이터의 생성', '5.2. 감사 데이터의 보호', '5.3. 감사 데이터의 분석, 검토'가 있다.

〈표 5〉 패스워드 및 저장정보의 안전한 관리를 위한 보안 요구사항

보 안 기 능	세 부 항 목	설 명
1. 도청방지	1.1. 키보드 해킹 방지	키보드 입력 정보의 기록, 외부로의 노출 방지
	1.2. 메모리 덤핑 공격 방지	개인정보의 메모리 노출 방지
	1.3. 스니핑 방지	외부에서 PC로, PC에서 외부로 전송되는 개인정보의 노출 방지
2. 사용자 인증	2.1. 관리자 인증	관리자 패스워드 설정을 통한 관리자 인증
	2.2. 복합 인증(선택사항)	관리자 패스워드와 함께 별도의 인증정보를 이용한 복합 인증 기능
	2.3. 재인증	관리자 패스워드 변경과 같은 개인정보 변경 작업에 대한 재인증 기능
3. 저장정보의 보호	3.1. 저장정보의 열람 방지	비인가된 사용자에 의한 개인정보 저장 파일의 열람 방지
	3.2. 저장정보의 복사 방지	비인가된 사용자에 의한 개인정보 저장 파일의 복사 방지
	3.3. 저장정보의 위·변조 방지	비인가된 사용자에 의한 개인정보 저장 파일의 위·변조 방지
	3.4. 저장정보의 삭제 방지	비인가된 사용자에 의한 개인정보 저장 파일의 삭제 방지
	3.5. 삭제된 저장정보의 복구 방지	삭제된 개인정보 저장 파일의 복구 방지
4. 암호 지원	4.1. 암호키 관리	개인정보를 암호화하여 저장하는데 사용되는 암호키의 안전한 관리
	4.2. 암호 알고리즘	개인정보를 암호화하여 저장하는데 사용되는 암호화 알고리즘의 안전성
5. 보안감사	5.1. 감사 데이터의 생성	제품이 제공하는 보안 기능 접근에 대한 감사 기록 생성
	5.2. 감사 데이터의 보호	비인가된 사용자에 의한 생성된 감사 기록의 열람, 위·변조, 복사, 삭제 방지
	5.3. 감사 데이터의 분석, 검토	관리자(인가된 사용자)에 의한 생성된 감사 기록의 분석 및 검토 기능 제공
6. 패스워드 생성	6.1. 안전한 패스워드 생성	숫자, 문자, 특수문자, 기호 등을 이용한 안전한 패스워드 생성 기능
7. 생명주기 지원	7.1. 결함 교정 및 버전 관리	제품에 결함이 발생하였을 경우, 개발자에 의한 결함 교정 및 그에 따른 제품의 업데이트와 버전 관리

〈표 6〉 안전한 아이디/패스워드 통합 관리 제품을 위한 평가 기준

보안 요구사항	세부 평가 기준
1.1. 키보드 해킹 방지	1.1.1. 키보드 입력 정보의 기록과 외부로의 노출을 방지하는 기능을 제공해야 한다
	1.1.2. 키보드 해킹 프로그램을 탐지하는 기능을 제품에 포함하거나, 포함하지 않을 때에는 해당 기능을 제공하는 보안 솔루션을 함께 제공해야 한다
1.2. 메모리 덤핑 공격 방지	1.2.1. 관리자 패스워드, 사용자 개인정보, 등록된 웹사이트의 아이디/패스워드가 암호화되지 않은 상태로 PC의 메모리에 노출되지 않아야 한다
	1.2.2. 메모리에 노출된 정보의 위·변조가 불가능해야 한다
1.3. 스니핑 방지	1.3.1. USB 메모리 장치에서 PC로, PC에서 USB 메모리 장치로 전송되는 개인정보가 암호화되지 않은 상태로 노출되지 않아야 한다
2.1. 관리자 인증	2.1.1. 제품을 설치하여 처음 실행 시, 관리자 패스워드 설정 기능을 제공해야 한다
2.2. 복합 인증(선택사항)	2.2.1. 관리자 패스워드, 별도의 인증정보(예: 인증키)를 함께 인증하여 두 가지 인증이 모두 성공하였을 경우에만 제품의 사용이 가능하도록 하는 기능을 제공해야 한다
2.3. 재인증	2.3.1. 사용자의 개인정보 변경, 관리자 패스워드 변경과 같은 주요 정보 변경 작업에 대해 재인증 기능을 제공해야 한다
3.1. 저장정보의 열람 방지	3.1.1. 비인가된 사용자에 의한 개인정보 저장 파일의 열람 방지 기능을 제공해야 한다
3.2. 저장정보의 복사 방지	3.2.1. 비인가된 사용자에 의한 개인정보 저장 파일의 복사 방지 기능을 제공해야 한다
3.3. 저장정보의 위·변조 방지	3.3.1. 비인가된 사용자에 의한 개인정보 저장 파일의 위·변조 방지 기능을 제공해야 한다
3.4. 저장정보의 삭제 방지	3.4.1. 비인가된 사용자에 의한 개인정보 저장 파일의 삭제 방지 기능을 제공해야 한다
	3.4.2. 제품의 재설치 및 제거 시, 기존에 보관되어 있던 개인정보 저장 파일의 삭제 의사를 확인하는 기능을 제공해야 한다
3.5. 삭제된 저장정보의 복구 방지	3.5.1. 제품의 현재 사용자 삭제 기능을 통해 삭제된 개인정보 저장 파일의 복구 방지 기능을 제공해야 한다
	3.5.2. 제품의 재설치 및 제거 시 삭제된 제품의 개인정보 파일 복구 방지 기능을 제공해야 한다
4.1. 암호키 관리	4.1.1. 개인정보를 암호화하여 저장하는데 사용되는 암호키의 생성, 분배, 파기 방식으로 해당 국가에서 인정한 기관으로부터 인증된 방식을 사용하여야 한다
4.2. 암호 알고리즘	4.2.1. 개인정보를 암호화하여 저장하는데 사용되는 암호화 알고리즘으로 해당 국가에서 인정한 기관으로부터 인증된 알고리즘을 사용하여야 한다
5.1. 감사 데이터의 생성	5.1.1. 제품이 제공하는 보안 기능 접근에 대한 감사 기록을 생성하는 기능을 제공해야 한다 (예: 인가된 또는 비인가된 사용자의 인증 시도, 패스워드 변경 등에 대한 로그 파일 생성)
5.2. 감사 데이터의 보호	5.2.1. 비인가된 사용자에 의한 생성된 감사 기록의 열람, 위·변조, 복사, 삭제 방지 기능을 제공해야 한다
5.3. 감사 데이터의 분석, 검토	5.3.1. 관리자(인가된 사용자)에 의한 생성된 감사 기록의 분석 및 검토 기능을 제공해야 한다
6.1. 안전한 패스워드 생성	6.1.1. 숫자, 문자, 특수문자, 기호 등을 이용한 안전한 패스워드 생성 기능을 제공해야 한다
7.1. 결함 교정 및 버전 관리	7.1.1. 제품에 결함이 발생하였을 경우, 개발자에 의한 결함 교정 및 그에 따른 제품의 업데이트와 버전 관리 기능을 제공해야 한다

〈표 7〉 제품별 평가기준 만족 여부

제품 / 기준	A 제품	B 제품	C 제품	D 제품	E 제품	F 제품	G 제품	H 제품	I 제품
1.1.1.	×	×	×	×	×	×	×	×	○
1.1.2.	×	×	×	×	×	×	×	×	○
1.2.1.	×	×	×	×	×	×	○	×	○
1.2.2.	-	-	-	-	×	-	○	○	○
1.3.1.	-	-	-	-	×	-	○	○	-
2.1.1.	○	○	○	○	○	○	○	○	×
2.2.1.	×	×	×	×	×	×	○	×	×
2.3.1.	○	○	×	×	○	×	×	○	×
3.1.1.	×	×	×	×	×	×	×	×	○
3.2.1.	×	×	×	×	×	×	×	×	○
3.3.1.	×	×	×	×	×	×	×	×	○
3.4.1.	×	×	×	×	×	×	×	×	○
3.4.2.	×	×	×	×	×	○	×	○	×
3.5.1.	-	-	-	-	×	-	-	-	-
3.5.2.	×	×	×	×	×	×	×	×	×
4.1.1.	-	-	-	-	-	-	-	-	-
4.2.1.	-	○	-	○	○	-	○	○	○
5.1.1.	×	×	×	×	×	×	×	×	×
5.2.1.	×	×	×	×	×	×	×	×	×
5.3.1.	×	×	×	×	×	×	×	×	×
6.1.1.	○	○	×	○	×	×	○	○	×
7.1.1.	○	○	○	○	○	○	○	○	○

(○ : 만족, × : 불만족, - : 해당사항 없음)

5.4 분석 대상 제품의 평가기준 만족 여부

분석한 제품이 제안한 평가기준의 각 항목을 만족하는지 여부는 <표 7>과 같고, 기준 '2.2.1.' 복합인증 관련 항목은 선택 사항이다. 또한 '4.1.1.' 암호키 관리 항목은 제품 개발 업체에서 보안상의 이유로 키 관리 방식을 공개하지 않아, 본 논문의 분석 결과만으로는 만족 여부를 판단할 수 없다. 그리고 '4.2.1.' 암호 알고리즘 항목은 업체에서 공개한 경우, 사용자의 개인정보 암호화 저장 방식으로 대부분 AES(Advanced Encryption Standard)를 사용하고 있다.

6. 결 론

사용자가 관리해야 하는 아이디/패스워드의 수가 증가함에 따라 보안상의 취약점이 발생하였으며, 이를 해결하기 위해 OpenID, CardSpace, SAML 등 다양한 인터넷 아이디 관리 기술이 개발되었다. 그러나 OpenID, CardSpace는 기존의 아이디/패스워드 관리 방식을 하나의 아이디 또는 개인 카드를 생성하여 대체하는 방식이기 때문에, 현재 사용하고 있는 인터넷 사이트에 모두 재가입을 해야만 하는 불편함이 있다. 또한 SAML의 경우에는 기존의 아이디/패스워드 관리 방식을 이용한 효율적인 관리 방법을 제공하고 있지만, 이를 지원하지 않는 사이트의 서비스에는 적용되지 않는다. 그러므로 현재의 상황에서 실제로 사용 가능한 제품은 기존의 분산된 아이디/패스워드를 통합하여 목록을 생성한 후, 안전하게 저장하여 관리하는 기능을 제공하는 제품들이다.

따라서 본 논문에서는 이러한 제품을 대상으로 기존의 공개된 해킹 방식을 이용하여 취약성을 분석하였고, 분석된 취약성과 각 제품이 제공하는 보안기능을 바탕으로 패스워드 및 저장정보의 안전한 관리를 위한 보안 요구사항을 도출하였다. 그리고 도출된 보안 요구사항을 바탕으로 안전한 아이디/패스워드 통합 관리 제품을 위한 평가기준을 제안하였다.

본 논문에서 분석한 취약성 결과와, 제안한 평가기준은 향후 안전한 아이디/패스워드 통합 관리 제품 개발에 유용하게 활용될 수 있을 것이며, 기존의 아이디/패스워드 관리 방식을 대체하게 될 CardSpace와 같은 새로운 인터넷 아이디 관리 기술의 안전한 사용자 저장정보 관리 방식 개발에 중요한 지침으로 활용될 수 있을 것이다.

참 고 문 헌

[1] 한국전자통신연구원 디지털ID보안연구팀, "Digital Identity 관리 기술 현황 및 전망", 전자통신동향분석 제 22권 제 1호, 2007.

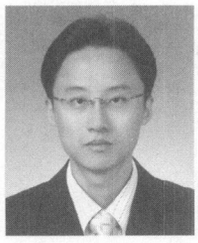
[2] 한국전자통신연구원 디지털ID보안연구팀, "인터넷 ID 관리 시스템 개요 및 비교", 전자통신동향분석 제 22권 제 3호, 2007.

[3] 한국정보보호진흥원, "웹 2.0과 ID관리기술 전망", 기술정책 07-06, 2007.

[4] OASIS SAML TC, "http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security"

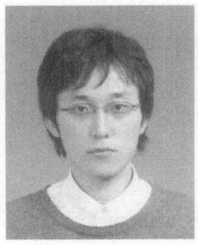
[5] Nick Ragouzis, John Hughes, Rob Philpott, and Eve Maler, "Security Assertion Markup Language(SAML)

V2.0 Technical Overview", OASIS SSTC Working Draft 10, 2006.10.9
[6] OpenID Foundation, "http://openid.net"
[7] SAML, "http://projectliberty.org/liberty/adoption"
[8] Sxipper, "http://www.sxipper.com"
[9] RoboForm, "http://www.roboform.com"
[10] 알패스, "http://www.altools.co.kr"
[11] KeePass, "http://keepass.info"
[12] Advanced Password Manager, "http://www.rayslab.com/password_manager/password_manager.html"
[13] Effective Password Manager, "http://www.intelore.com/password-manager.php"
[14] Password Keeper Expert, "http://www.softdemon.com/keeper/index.html"
[15] SecureWallet, "http://www.coolutils.com"
[16] 한정훈, 이병희, 원동호, 김승주, "아이디/패스워드 통합 관리 제품의 취약성 분석", 한국정보보호학회 동계학술대회, pp 418-421, 2007.
[17] SKIn2000, "http://www.keylogger.biz"
[18] WinHex, "http://www.x-ways.net/winhex/index-m.html"
[19] BusHound, "http://www.perisoft.net/bushound/index.htm"
[20] Secure Edit Contorls, "http://www.codeproject.com/editctrl/SecEditEx.asp"
[21] NetBus, "http://www.netbus.org/"
[22] FinalData, "http://www.finaldata.com"
[23] 한국전자통신연구원 디지털ID보안연구팀, "인터넷 ID 관리 서비스 2006년도 기술 백서", 2006.
[24] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, 2006.



한 정 훈

e-mail : jhhan@security.re.kr
2007년 성균관대학교 정보통신공학부 (학사)
2007년~현 재 성균관대학교 전자전기 컴퓨터공학과 석사과정
관심분야 : 정보보호, 네트워크 보안, 정보보호제품 보안성 평가 등

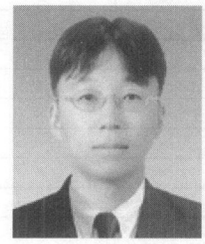


이 병 희

e-mail : bhlee@security.re.kr
2005년 성균관대학교 정보통신공학부 (학사)
2007년 성균관대학교 컴퓨터공학과 (석사)
2007년~현 재 성균관대학교 전자전기 컴퓨터공학과 박사과정
관심분야 : 정보보호제품 평가, 디지털 ID 관리, 패스워드 분석 등

홍 수 민

e-mail : smhong@security.re.kr
2005년 덕성여자대학교 수학과(학사)
2007년~현 재 성균관대학교 전자전기 컴퓨터공학과 석사과정
관심분야 : 정보보호, 생체인식, 금융보안, 암호이론, 암호 프로토콜



김 승 현

e-mail : ayo@etri.re.kr
2002년 금오공과 대학교 컴퓨터공학과(학사)
2004년 포스텍 대학원 컴퓨터공학과 공학석사
2004년~현 재 한국전자통신연구원 정보보호연구단 연구원
관심분야 : ID 관리, 웹 보안 등

원 동 호

e-mail : dhwon@security.re.kr
1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장
관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr
1994년~1999년 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년 한국정보보호진흥원 (KISA) 팀장
2004년~현 재 성균관대학교 정보통신공학부 교수
2001년 ~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET