정 보 보 호 학 회 지
제28권 제1호, 2018. 2

패스워드 매니저의 보안성 분석

김 수 린*, 김 형 식**

요 약

사용자는 비밀번호를 외워야하는 불편함을 줄이고 로그인 과정을 편리하게 이용하기 위해 패스워드 매니저를 사용한다. 패스워드 매니저는 크게 브라우저 기반의 패스워드 매니저와 웹 기반의 패스워드 매니저로 나눌 수 있다. 브라우저 기반의 패스워드 매니저의 경우 로컬에 사용자의 계정 정보와 암호화 키를 저장하기 때문에, 비밀번호 복구 프로그램을 사용하거나 간단한 코드를 이용하여 사용자의 계정 정보를 평문 형태로 추출할 수 있다. 로컬에 저장하는 브라우저 기반의 패스워드 매니저와 달리 웹 기반 패스워드 매니저는 웹을 기반으로 실행된다. 웹 기반 패스워드 매니저는 암호화 키를 웹 서버에 저장하기 때문에, 로컬 기반의 패스워드 매니저에 비해 키 노출 우려가 적다. 하지만 웹 기반이기 때문에 공격자가 웹 취약점을 이용하면 사용자의 정보가 누출될 위험성이 있다. 본 논문에서는 사용자의 편의성을 개선하고자 사용되는 패스워드 매니저를 브라우저에서 사용되는 브라우저 기반 패스워드 매니저와 웹에서 사용되는 웹 기반 패스워드 매니저로 분류하고 각 패스워드 매니저가 사용자의 계정 정보를 저장 및 관리하는 방법을 분석하고, 해당 패스워드 매니저들에서 발생 가능한 취약점에 대해 조사하였다.

Ⅰ. 서 론

최근 다양한 웹 서비스들이 제공됨에 따라 인터넷을 사용하는 사용자는 제공되는 서비스를 이용하기 위하여 아이디와 패스워드를 생성하여 회원가입을 하고, 로그인을 통해 자격 증명을 하며 해당 서비스를 이용한다. 기하급수적으로 늘어나는 서비스만큼 사용자가 외워야하는 계정 정보도 늘어난다. 그렇기 때문에, 비밀번호를 외우는 것은 사용자에게 어려운 과제이자 부담이다. 전문가들은 사용자의 정보를 보호하고자 여러 계정에서 비밀번호를 재사용하지 말 것을 권유하고, 보안상의 문제로 비밀번호를 어딘가에 적지 말 것을 권장한다. 사용자는 권장 사항을 지키기 위해서, 다양한 종류의 비밀번호를 외우고 있어야하며 원하는 서비스를 사용할 때 알맞게 사용해야하는 불편함을 가지고 있다. 심지어, 서비스마다 사용자는 주기적으로 특정 조건을 만족하게 비밀번호를 변경해야한다. 웹 서비스에서 새로운 계정을 생성할 때 사용자가 사전 공격에 취약한 비밀번호를 생성하는 것을 방지하기 위해 각 웹 서비스들은 특정 조건을 제시하여 대/소문자와 숫자, 특수기호를 섞도록 제안한다. 즉, 사용자는 많은 계정과 다양한 제약조건을 가진 비밀번호를 기억해야한다. 대부분의 사용자는 이전에 사용했던 비밀번호를 재사용하고 기록함으로써 새로운 비밀번호를 외워야하는 부담에 대처할 수 있지만, 사용자는 편리성과 보안성에 대한 문제점을 개선하고자 패스워드 매니저를 대안으로 선택하였다 [1].

패스워드 매니저란, 하나의 마스터 비밀번호로 각 사이트의 비밀번호를 비롯한 여러 개의 아이디와 도메인 주소와 같은 로그인 정보와 그 외의 카드 번호와 같은 사용자의 중요 정보들을 관리 및 보호하며 사용자가 웹 서비스를 편리하게 이용 할 수 있도록 도와주는 소프트웨어이다 [2].

패스워드 매니저가 사용자의 정보를 저장하는 방식에 따라 크게 두 가지 종류로 나눌 수 있다. 첫 번째는 브라우저 기반의 패스워드 매니저이다. 브라우저 기반의 패스워드 매니저는 브라우저에서 기본으로 제공하는 패스워드 매니저이다. 브라우저 기반 패스워드 매니저는 도메인 주소, 아이디, 비밀번호와 같은 사용자의 계정 정보를 사용자의 기기에 저장하는 패스워드 매니저로 사용자의 로그인과 관련된 정보들을 사용자의 컴퓨터의 특정 경로에 암호화하여 저장한다. 각 브라우저마다 암호화 키를 생성하는 방식은 다르지만, 브라우저 기

* 성균관대학교 전자전기컴퓨터공학과 (soolinkim@skku.edu, hyoung@skku.edu)
** 교신저자, 성균관대학교 전자전기컴퓨터공학과 (soolinkim@skku.edu, hyoung@skku.edu)

반 패스워드 매니저들은 암호화 키를 사용자의 기기에 저장한다. 이러한 브라우저 기반의 패스워드 매니저는 사용자의 계정 정보와 암호화 키가 사용자의 기기에 저장되기 때문에 비밀번호 복구 프로그램을 사용하거나 패스워드 매니저가 암호화에 사용한 로직 및 키를 알아낸다면 공격자는 사용자의 계정 정보를 추출할 수 있다. 다양한 브라우저 기반의 패스워드 매니저들이 사용자의 계정 정보를 사용자의 기기에 저장하기 때문에 브라우저 기반 패스워드 매니저에 저장되어있는 사용자의 계정 정보는 여러 가지 방법으로 공격이 가능하다 [1,7-9,19].

두 번째는 웹 기반 패스워드 매니저이다. 웹 기반 패스워드 매니저는 사용자의 아이디와 비밀번호를 서버로부터 얻은 키로 암호화하여 사용자의 계정 정보를 저장 및 관리한다. 사용자의 기기에 계정 정보와 암호화 키를 저장하는 브라우저 기반 패스워드 매니저와 달리 웹 기반 패스워드 매니저는 웹 기반으로 사용자의 계정을 관리하기 때문에 웹 기반의 패스워드 매니저는 공격자가 웹 취약점을 응용하여 공격한다면 사용자의 계정 정보가 노출될 수 있다. 공격자는 사이트 간 요청을 위조하는 공격인 CSRF을 활용하거나 사이트 간 스크립팅 공격인 XSS을 이용하여 패스워드 매니저가 다루는 사용자의 계정 데이터를 읽고 누출시킬 수 있다 [18]. 또한 패스워드 매니저들의 일부는 기존에 저장된 로그인 페이지 방식과 다른 상태(예: 로그인 필드의 액션이 변경됨)의 로그인 페이지가 감지됨에도 불구하고 자동으로 로그인 필드를 완성하는 문제점이 발견되었다. 이러한 자동 완성 방식의 문제점을 이용하여 원격의 공격자가 사용자와의 상호 작용 없이 사용자의 패스워드 매니저로부터 사용자의 여러 계정 정보를 추출 할 수 있는 공격에 대한 연구가 진행되었다 [20].

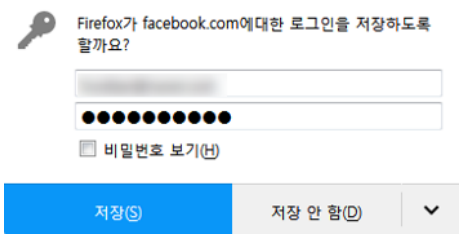
사용자의 사용성을 증진하기 위한 서비스인 패스워드 매니저들에 저장되어있는 사용자의 계정 정보를 노리는 다양한 공격들과 완화책이 연구되었다. 이러한 공격을 완화하기 위하여 패스워드 매니저를 위한 설계 지침을 제공하거나 새로운 패스워드 매니저를 설계하는 연구가 진행되었다 [18, 23].

본 논문에서는 사용자의 계정 정보와 암호화 키를 사용자의 기기에 저장하는 브라우저기반의 패스워드 매니저(예: Google Chrome)와 암호화 키를 서버로부터 받아 암호화하는 웹 기반 패스워드 매니저(예: LastPass, Roboform)로 분류하여 각각의 구조와 문제점을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 웹 브라우저 패스워드 매니저에 대해 분석한다. 웹을 기반으로 한 웹 기반 패스워드 매니저에 대한 분석은 3장에서 분석하며 각각의 패스워드 매니저에 대한 문제점은 4장과 5장에서 분석한다. 마지막으로, 6장에서는 본 논문에 대한 결론을 도출할 것이다.

Ⅱ. 브라우저 기반 패스워드 매니저

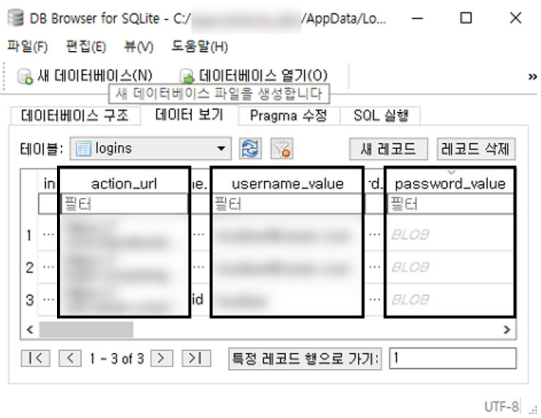
w3school이 제공한 통계를 바탕으로 사용자가 많이 사용하는 상위 3가지의 웹 브라우저인 Google Chrome, Mozilla Firefox, Internet Explorer를 선정하였다 [3]. Google Chrome, Mozilla Firefox, Internet Explorer는 로그인 정보를 저장하는 패스워드 매니저 기능을 제공하고 있다. 웹 서비스를 이용하기 위해 로그인 페이지에 사용자가 아이디와 비밀번호와 같은 사용자 계정 정보를 입력한 후 로그인하면 웹 브라우저는 [그림 1]과 같이 메시지를 통해 보여준다. [그림 1]의 메시지는 사용자의 계정 정보를 브라우저 기반 패스워드 매니저에 저장할 것인지 묻는 내용이다. 사용자가 패스워드 매니저를 사용하고자 저장 버튼을 누르면 사용자의 아이디와 비밀번호 등과 같은 사용자의 계정 정보를 브라우저마다 지정된 특정 경로에 암호화하여 저장한다. 사용자가 같은 웹 서비스를 사용하고자 같은 사이트에 접속하였을 경우, 브라우저 기반 패스워드 매니저는 컴퓨터 내부 특정 경로에 저장된 사용자 계정 정보를 복호화하여 웹 서비스 로그인 페이지에 사용자의 계정 정보 필드를 자동으로 완성해 주거나 저장된 정보를 이용하여 자동으로 로그인을 완료한다.



〔그림 1〕 Mozilla Firefox 패스워드 매니저 메시지 창

2.1. Google Chrome 패스워드 매니저

Google Chrome은 통계적으로 브라우저 전체 사용자 중 약 70% 정도가 사용하고 있는 웹 브라우저이다 [3]. Google Chrome의 패스워드 매니저는 사용자에게 자동 로그인 필드를 채워주기 위해 사용자의 아이디, 비밀번호 그리고 로그인 페이지의 URL 등과 같은 로그인에 사용되는 사용자의 계정 정보를 특정 경로[1]안에 부분적으로 암호화하여 저장한다. Login Data.sqlite 파일은 사용자 로그인 정보를 저장하고 있는 데이터베이스로써 사용자의 계정 정보와 도메인 정보를 포함하여 서버에서 제공하는 정보들을 저장하고 있다. Login Data.sqlite 파일을 DB Browser for SQLite 프로그램 [4]을 통해 열어보면 [그림 2]와 같이 구성되어있다. action_url 필드는 사용자의 계정 정보가 채워질 로그인 페이지의 URL 주소를 나타낸다. 그리고 username_value 필드는 사용자의 계정에 대한 아이디를 나타내며, password_value 필드는 사용자 계정에 대한 비밀번호를 나타낸다. [그림 2]와 같이 action_url과 username_value는 암호화되지 않은 평문 형태로 저장되는 것을 확인할 수 있다. 하지만 password_value는 [그림 2]와 같이 BLOB 형태로 암호화되어 저장되어있다.



〔그림 2〕 Login Data.sqlite에 저장된 사용자 로그인 정보

2.2. Mozilla Firefox 패스워드 매니저 분석

Mozilla Firefox에서 제공하는 패스워드 매니저가 사용자에게 계정 정보의 저장 여부를 묻고 사용자가 계정 정보의 저장을 승인할 경우 사용자의 아이디와 비밀번호, 로그인 페이지 URL과 같은 사용자의 계정 정보가 Google Chrome 패스워드 매니저와 유사하게 파일로 특정 경로[2]에 저장한다.

Mozilla Firefox 패스워드 매니저의 경우 버전에 따라 저장 방식이 상이하다. Firefox 3.5 이전의 패스워드 매니저는 key3.db 데이터베이스 파일에 마스터 비밀번호와 암호화 키를 보관하고 signons 파일에 암호화된 아이디와 비밀번호를 저장한다. 그러나 3.5 버전 이후로는 이전 버전과 마찬가지로 key3.db 데이터베이스 파일에 마스터비밀번호와 암호화 키를 보관하지만, signons 파일이 아닌 signons.sqlite 데이터베이스 파일에 암호화된 사용자의 아이디와 비밀번호를 저장한다. Firefox 32.0 버전의 패스워드 매니저는 기존 방식인 signons 형식으로 저장하는 대신에 logins.json 형식을 통하여 사용자의 계정 정보를 저장한다. Firefox 32.0 버전 이후의 패스워드 매니저는 logins.json 파일에 사용자 정보를 저장할 때 로그인 페이지에 대한 URL 주소는 암호화되지 않은 평문 형태로 저장했지만, 사용자의 아이디와 비밀번호는 암호화한 형태로 저장한다.

2.3. Internet Explorer 패스워드 매니저

Chrome과 Firefox 패스워드 매니저는 사용자의 계정 정보를 암호화한 형태로 파일에 저장하지만, Internet Explorer 패스워드 매니저는 사용자의 아이디와 비밀번호 등 로그인에 필요한 계정 정보들을 레지스트리에 저장한다. Internet Explorer 패스워드 매니저도 다른 패스워드 매니저들과 유사하게 사용자가 웹 서비스를 사용하기 위해 로그인을 할 경우, 사용자의 계정 정보의 저장 여부를 묻는다. 사용자가 자신의 계정 정보를 패스워드 매니저에 저장하고자 할 경우, Internet Explorer의 패스워드 매니저는 사용자 사용자의 컴퓨터 레지스트리에 사용자 계정 정보를 저장한다.

패스워드 매니저가 사용자의 계정 정보를 저장하는 레지스트리의 경로는 버전에 따라 저장되는 위치가 상이하다. Internet Explorer 4.0 ~ 6.0 버전은 사용자의 로그인 계정 정보를 Protected Storage System Provider 레지스트리[3]에 저장한다. 그러나Internet

1) %LOCALAPPDATA%\Google\Chrome\User Data\Default

2) %APPDATA%\Mozilla\Firefox\Profiles\[Profile Name]

3) HKEY_CURRENT_USER\Software\Microsoft\Protected Stora

Explorer 7.0 버전 이후부터는 사용자의 로그인 계정 정보를 이전 버전과 다른 레지스트리[4]에 저장한다.

Ⅲ. 웹 기반 패스워드 매니저

패스워드 매니저는 사용자의 비밀번호와 사용자의 아이디 그리고 해당 사이트 URL 주소를 데이터베이스로 저장 및 관리하며, 사용자는 마스터 아이디와 비밀번호를 통해 많은 사이트들의 로그인을 포함한 사용자의 계정 정보를 간편하게 관리한다. 이러한 패스워드 매니저의 장점을 다양한 매체(예: CNET [10], PC Magazine [11] 및 New Your Times [12])에서 설명하고 있다. 사용자가 웹 기반 패스워드 매니저를 사용하기 위해서는 확장 프로그램을 설치하거나 웹 사이트에 접속하여 해당 패스워드 매니저에 접속해야 한다. 사용자의 마스터 아이디와 비밀번호를 사용하여 패스워드 매니저에 로그인한 후 사용자는 이용하고자하는 서비스에 대한 로그인 계정 정보를 검색하고, 검색한 로그인 계정 정보를 사용하여 이용하고자하는 서비스에 로그인한다. 사용자가 이용하려는 서비스에 접속했을 때, 사용자의 마스터 아이디와 비밀번호를 입력하면 패스워드 매니저는 해당 서비스의 로그인 양식을 자동으로 채워준다.

3.1. LastPass

LastPass [16]는 북마크릿 기능, 웹 서비스 그리고 [그림 3]과 같이 확장프로그램으로 서비스를 제공한다. LastPass는 패스워드 매니저가 제공하는 대부분의 기능들을 가지고 있다. 또한 대부분의 브라우저들을 지원하며, 많은 이용자들이 사용하는 iOS와 안드로이드와 같은 모바일 운영체제와 윈도우즈, 맥과 같은 대부분의 데스크탑 운영체제를 지원하기 때문에 많은 사용자가 이용하고 있는 패스워드 매니저이다. 2013년 8월에는 백만 명이 넘는 사용자가 이용하고 있는 패스워드 매니저이다 [18].

〔그림 3〕 LastPass 패스워드 매니저〔16〕

ge System Provider

4) HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

3.2. RoboForm

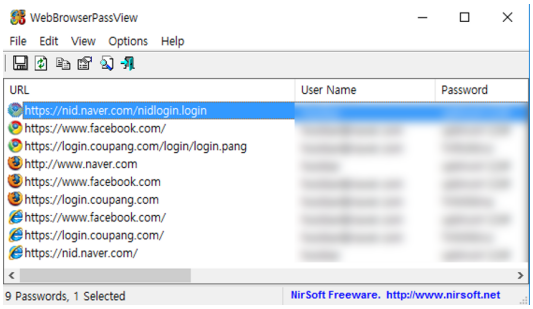
RoboForm [17]은 LastPass와 유사하게 북마크릿 기능, 확장프로그램과 같은 패스워드 매니저가 제공하는 대부분의 기능들을 가지고 있다. 특히RoboForm은 사용자의 로그인 계정 정보를 저장할 때 웹 애플리케이션의 이름이 붙여진 파일에 저장된다. 예를 들어, facebook.com에 대한 사용자의 계정 정보를 저장할 때 RoboForm 패스워드 매니저는 기본 파일 이름으로 "facebook"을 사용한다. 사용자의 계정 정보는 RoboForm 웹 사이트 또는 RoboForm 확장프로그램, 북마크릿 등의 기능을 통해 사용 및 관리가 가능하다 [18].

Ⅳ. 브라우저 기반 패스워드 매니저 문제점 분석

사용자가 아이디와 비밀번호를 입력해야 하는 번거로움을 덜어주기 위한 서비스인 자동 로그인 서비스 시스템은 로그인 필드를 자동으로 채워주기 때문에 사용자에게 편리함을 제공한다. 그러나 자동 로그인을 위해 사용되는 계정 정보와 암호화 키가 사용자 컴퓨터 내부에 저장된다는 점에서 공격자에게 사용자의 계정 정보가 유출될 위험이 있다 [19]. 악한 공격자가 [그림 4]과 같은 비밀번호 복구 프로그램 [5]을 사용하면 사용자의 비밀번호뿐만 아니라 사용자의 아이디와 로그인 페이지까지 복호화된 평문 상태로 획득할 수 있다. 암호화 방식에 대한 지식을 가진 공격자가 각 웹 브라우저에서 제공하는 패스워드 매니저의 사용자 계정 정보를 저장하는 경로와 계정 정보의 암호화 방법, 암호화 키를 알고 있다면 암호화되어 저장된 사용자의 모든 계정 정보들을 획득할 수 있다.

4.1. Google Chrome

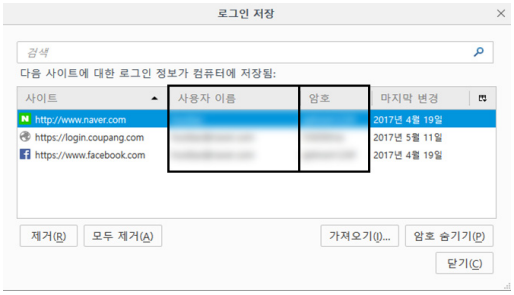
Google Chrome은 사용자의 계정 정보를 저장할 때 username_value 필드에 사용자의 아이디를 저장한다. 또한 action_url 필드에는 로그인하는 서비스의 URL 주소를 저장한다. username_value와 action_url의 경우 암호화되지 않은 평문 상태로 Login Data 파일에 저장한다. 그러나 비밀번호는 윈도우즈에서 제공하는 DPAPI (Data Protection API) 함수를 사용해 action_url 필드를 인자로 사용하여 암호화한 후 Login Data 파일에 저장한다. 따라서 공격자가 action_url 필드 정보를 안다면 윈도우즈에서 제공하는 CryptUnprotectData 함수를 사용하여 복호화할 수 있다 [1]. 또한, 윈도우즈 자격 증명에 사용되는 사용자 비밀번호가 있다면 브라우저에서 제공하는 설정 기능을 통해 직접 패스워드 매니저에 접속하여 사용자의 계정 정보를 획득할 수 있다. Google Chrome 패스워드 매니저에서는 윈도우즈 자격 증명에 이용되는 사용자 비밀번호를 해당 패스워드 매니저의 마스터 비밀번호로 활용하고 있다.



〔그림 4〕 Nirsoft사의 비밀번호 복구 프로그램〔5〕

4.2. Mozilla Firefox

Google Chrome과 Internet Explorer의 패스워드 매니저를 통해 사용자의 계정 정보에 접근하기 위해서는 윈도우즈 자격 증명에 사용되는 비밀번호를 입력하여 사용자의 인증을 요구한다. Firefox 패스워드 매니저는 저장된 사용자의 로그인 정보를 보호하기 위해 윈도우즈 자격 증명을 위한 비밀번호가 아닌 마스터 비밀번호 기능을 제공하지만, 기본 설정일 경우 마스터 비밀번호 기능은 사용되지 않는다. 따라서 [그림 5]와 같이



〔그림 5〕 Firefox 브라우저 패스워드 매니저

Mozilla Firefox의 패스워드 매니저는 웹 브라우저의 설정 옵션을 통해 '암호 보이기' 기능을 사용하여 사용자 인증 없이 아이디와 비밀번호 등 사용자의 계정 정보를 평문 상태로 보여준다 [19].

4.3. Internet Explorer

레지스트리에 저장하는 Internet Explorer 패스워드 매니저는 Internet Explorer 웹 브라우저에서 사용자의 계정 정보를 평문으로 확인하기 위해서 윈도우즈 자격 증명을 이용하여 사용자 인증을 요구한다. 따라서 윈도우즈의 자격 증명을 모르는 공격자들은 쉽게 사용자의 계정 정보를 확인할 수 없다. 그러나 레지스트리에 저장되어있는 비밀번호는 SHA-1 (Secure Hash Algorithm 1) 해시 함수를 사용하여 암호화 하는데, 이때 URL 주소를 해싱한 값을 키로 사용한다 [1]. Chrome 패스워드 매니저와 유사하게 Internet Explorer 패스워드 매니저는 윈도우즈에서 제공하는 DPAPI 함수로 이용하여 키를 생성한다. 이를 이용해 사용자의 비밀번호를 암호화한다. 그러나 사용자의 비밀번호를 암호화한 키가 사용자의 기기에 저장되어있기 때문에, 레지스트리에 저장된 레코드를 통해 복호화할 수 있다 [6,19].Ⅴ. 웹 기반 패스워드 매니저 문제점 분석

여러 사이트에서 반복되는 로그인 과정에 대한 부담을 줄이기 위해 브라우저 기반 패스워드 매니저뿐만 아니라 웹 기반으로 하는 패스워드 매니저는 사용자의 계정 정보가 한 번 저장된 후에 사용자가 해당 로그인 웹 페이지에 접근하면, 사용자의 마스터 아이디와 비밀번호를 이용하여 해당 로그인 필드를 자동으로 완성하는 기능을 제공한다. 또한, 웹 기반 패스워드 매니저는 웹을 통해 서비스를 제공하기 때문에 웹 기반 패스워드 매니저는 웹 취약점에 노출되어 있다.5.1. 자동 완성 기

능에 대한 문제점

David 등 [20]은 사용자의 계정 정보가 저장될 때의 로그인 페이지 상태와 다른 상태의 로그인 페이지 (예: HTTPS 인증서 오류 등)가 패스워드 매니저에 감지될 때 각각 패스워드 매니저들의 자동 완성 방식을 조사하였다. 패스워드 매니저들의 일부는 기존에 저장된 로그인 페이지 방식과 다른 상태의 로그인 페이지가 감지됨에도 불구하고 자동으로 로그인 필드를 완성하는 문제점이 발견되었다. 이러한 자동 완성 방식의 문제점을 이용하여 원격의 공격자가 사용자와의 상호 작용 없이 사용자의 패스워드 매니저로부터 사용자의 여러 계정 정보를 추출 할 수 있는 공격에 대한 연구가 진행되었다. 이를 방지하기 위해서 David 등 [20]은 HTTPS 인증서에 오류가 있는 특정 조건에서 패스워드 매니저가 로그인 필드에 자동 채우기를 수행하지 않기를 권장한다. 예를 들어, 간단한 클릭과 같은 사용자와의 상호 작용을 통해 자동으로 비밀번호를 채운다면 원격 공격을 방지할 수 있다.

사용자가 로그인 계정 정보를 저장했을 때의 로그인 버튼에 대한 액션과 사용자가 접근한 로그인 페이지의 로그인 버튼에 대한 액션이 다른 상태에서 패스워드 매니저들의 일부는 차이를 감지하지 못하고 자동 완성을 진행하였다. 이러한 차이를 감지하지 못하는 문제점을 통해 악의적인 JavaScript 코드를 실행하여 사용자의 정보를 탈취할 수 있다. David 등 [20]은 기존에 사용자가 계정 정보를 저장한 상태와 다른 상태의 로그인 페이지에서 악의적인 JavaScript 코드의 실행을 방지하기 위해 Google Chrome 등과 같이 신뢰할 수 있는 브라우저를 사용을 권장한다.

5.2. CSRF 및 XSS 공격에 대한 취약성

CSRF (Cross-site request forgery)는 사이트 간 요청을 위조하는 공격으로 웹 사이트를 공격할 수 있는 취약점 중 하나이다. 이 공격은 사용자의 의도와 상관없이 공격자가 원하는 행위를 특정 웹사이트에 요청하도록 하는 공격이다 [21].

XSS (Cross-site scripting)는 사이트 간 스크립팅 공격으로 웹 어플리케이션에서 많이 나타나는 취약점 중 하나이다. 웹 사이트 관리자가 아닌 공격자가 웹 페이지에 악의적인 스크립트를 삽입할 수 있는 취약점이다 [22].

공격자는 성공적인 사이트 간 요청을 위조하는 공격인 CSRF을 활용하거나 사이트 간 스크립팅 공격인 XSS을 이용하여 패스워드 매니저가 다루는 사용자의 계정 데이터를 읽고 누출시킬 수 있다 [18].

Ⅵ. 결 론

본 논문에서는 브라우저 기반의 패스워드 매니저와 웹 기반 패스워드 매니저가 사용자의 계정 정보를 저장 및 관리하는 방법을 분석하고, 해당 패스워드 매니저들에서 발생 가능한 취약점에 대해 조사하였다.

브라우저 기반의 패스워드 매니저는 사용자의 계정 정보와 암호화 키를 사용자의 컴퓨터 내부에 저장하는 패스워드 매니저이다. 브라우저 기반 패스워드 매니저는 사용자의 계정 정보들을 사용자의 컴퓨터의 특정 경로에 암호화하여 저장한다. 각 브라우저마다 암호화 키를 생성하는 방식은 다르지만 암호화 키와 사용자의 계정 정보가 사용자의 기기에 저장되어있기 때문에 공격자에 의해 사용자의 계정 정보가 평문 형태로 노출될 수 있다.

웹 기반 패스워드 매니저는 사용자의 아이디와 비밀번호를 서버로부터 얻은 암호화 키로 사용자의 계정 정보를 암호화하여 저장 및 관리한다. 웹 기반 패스워드 매니저는 웹 기반으로 사용자의 계정을 관리하기 때문에 공격자가 웹 취약점을 응용하여 공격한다면 사용자의 계정 정보가 노출될 수 있다.

향후 다양한 연구에서 얻어진 결과를 통해 보안 가이드라인을 만족하며 브라우저 기반 패스워드 매니저와 웹 기반 패스워드 매니저에 대한 취약점을 완화할 수 있는 패스워드 매니저 개발이 요구된다.

참 고 문 헌

[1] Gasti, Paolo, and Kasper B. Rasmussen. "On the security of password manager database formats." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 2012.

[2] Huth, Alexa, Michael Orlando, and Linda Pesante. "Password security, protection, and management." United States Computer Emergency Readiness Team (2012).

[3] w3schol Brwoser Statistic,“www.w3school.com/Brwoser/defualt.asp”.
[4] DB Browser for SQLite, SQLite Database Viewer Program, “http://sqlitebrowser.org/”.
[5] Nir soft사 비밀번호 복구 프로그램 WebBrowserPassView, “www.nirsoft.net”.
[6] Passcape, Recovering Internet Explorer Passwords : Theory and practice, “https://www.passcape.com/index.php?section=docsys&cmd=details&id=28#65”
[7] Zhao, Rui, and Chuan Yue. "All your browser-saved passwords could belong to us: A security analysis and a cloud-based new design." Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013.
[8] Gasti, Paolo, and Kasper B. Rasmussen. "On the security of password manager database formats." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2012.
[9] Boja, Catalin. "Security Survey of Internet Browsers Data Managers." arXiv preprint arXiv:1112.5760 (2011).
[10] CNET. Editor’s rating of password managers. http: //download.cnet.com/windows/password-managers/ ?&sort=editorsRating+asc.
[11] P. Magazine”. Editor’s rating of password managers. http:// www.pcmag.com/products/28042?sort=er+desc.
[12] D. Pogue. Remember all those passwords? no need. http: //nyti.ms/10ZhXgq, 2013.
[13] Content security policy: W3c editor’s draft, 2013. https://dvcs.w3.org/hg/content-security-policy/ raw-file/tip/csp-specification.dev.html.
[14] M.Rochkind. Security,forms,anderrorhandling. InExpertPHP and MySQL, pages 191–247. Springer, 2013.
[15] E. Grosse and M. Upadhyay. “Authentication at scale.” Security Privacy, IEEE, 11(1):15–22, Jan 2013.
[16] Lastpass. https://lastpass.com
[17] Roboform everywhere. http://www.roboform.com/ everywhere.
[18] Li, Zhiwei, et al. "The Emperor's New Password Manager: Security Analysis of Web-based Password Managers." USENIX Security Symposium. 2014.
[19] 김수린, and 김형식. "브라우저의 비밀번호 저장 기능에 대한 보안 분석." 한국정보과학회 학술발표논문집 (2017): 1024-1026.
[20] Silver, David, et al. "Password Managers: Attacks and Defenses." USENIX Security Symposium. 2014.
[21] https://en.wikipedia.org/wiki/Cross-site_request_forgery
[22] https://en.wikipedia.org/wiki/Cross-site_scripting
[23] Zhao, Rui, and Chuan Yue. "Toward a secure and usable cloud-based password manager for web browsers." Computers & Security 46 (2014): 32-47.

〈저자소개〉

김 수 린 (Soolin Kim)
학생회원
2017년 2월 : 상명대학교 컴퓨터과학과 졸업
2017년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 모바일 보안

김 형 식 (Hyoungshick Kim)
종신회원
1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터 과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월～현재 : 성균관대학교 전자전기컴퓨터공학과 조교수
관심분야 : 보안공학, 소셜 컴퓨팅