인터넷 개인 정보 유출과 전자 ID 지갑

최대선* 진승헌**

인터넷 상의 개인정보 유출은 DB 유출, 피싱, 스파이웨어, 스니핑, 패스워드 공격 등 다양한 경로를 통해 발생하며 그 피해 유형도 명의도용, 계정탈취, 보이스피싱, 스팸메일, 프라이버시 침해로 다양하다. 다양한 대응방안들이 제시되어 왔지만 사용자 편의성이 부족하고, 포괄적으로 문제를 해결하고 있지 못하다. ETRI에서 개발 중인 전자 ID 지갑은 인터넷에서 개인정보를 안전하고 편리하게 사용할 수 있도록 해주는 솔루션으로 사이트 가입, 주민등록번호 대체, 프로파일 제출, 사이트 로그인, 링크를 통한 개인정보 공유, 개인정보 동기화, 인터넷 지불, 개인정보 관리기능, 백업/휴대/로밍 기능 등을 제공하며, 모바일 버전도 제공된다. 전자 ID 지갑은 높은 사용자 편의성이 제공하며 인터넷 개인정보 유출 문제를 해결할 수 있다. 또한, 기존 대응 방안 중 하나인 주민등록번호 대체 서비스가 갖는 사용자 불편과 패스워드 보안성 문제 및 피싱 문제도 해결할 수 있다. ▧

목 차

* ETRI 디지털 ID 보안연구팀/선임연구원
** ETRI 디지털 ID 보안연구팀/팀장

Ⅰ. 서 론

최근 인터넷 상의 개인정보 유출 문제가 큰 이슈로 대두되고 있다. 인터넷 상의 개인정보는 다양한 피해 유형과 유출 경로가 존재하는 복잡한 문제이다. 현재까지 기술적 혹은 법제도 측면에서 다양한 대응 방안이 제시되어 왔지만, 여러 가지 사용자 불편을 초래하면서도 여전히 유출사고는 계속 발생하고 있다. 한편, 개인정보 중 주민등록번호 유출 및 도용 문제를 해결하기 위해 제시된 주민등록번호 대체 방안은 여러 가지 한계점을 갖고 있어, 광범위한 이용 시 또 다른 이슈를 야기할 가능성이 크다.

본 고에서는 인터넷 개인 정보 유출 현황과 기존 대응 방안 및 주민등록번호 대체 기술에 대해 살펴보고 이러한 문제를 해결하기 위해 한국전자통신연구원에서 개발 중인 전자 ID 지갑을 소개한다.

본 고는 다음과 같이 구성된다. Ⅱ 장에서는 인터넷 개인정보 유출 경로 및 피해유형에 대해 살펴보고 이에 대한 기존의 대응 방안을 설명한다. Ⅲ 장에서는 주민등록번호 대체 방안으로 제시된 i-PIN 과 G-PIN 에 대해 살펴보고, 이들이 내포한 한계점을 분석한다. Ⅳ 장에서는 인터넷 ID 관리 기술인 전자ID 지갑 기술을 살펴보고 전자ID 지갑을 이용해 앞서 제기된 개인정보 유출 문제와 주민등록번호 대체 방안의 문제를 어떻게 해결할 수 있는지 기술한다. Ⅴ 장에서 결론을 제시한다.

Ⅱ. 인터넷 개인 정보 유출

본 장에서는 인터넷에서 발생하는 개인정보 유출 시의 피해 유형과 유출경로를 설명한다. 그리고 기존의 대응방안을 기술한다.

1. 유출 피해 유형

인터넷 상에서 다루어지는 개인정보의 종류는 다음과 같다.

- ID, 패스워드: 웹 사이트에 가입할 때 등록하는 ID 와 패스워드로 이후 로그인 시에 사용된다.
- 개인 신상 정보: 이름, 주소, 전화번호, 이메일 주소, 나이, 학력, 출신지역 등이 개인 신상 정보를 구성한다.
- 주민등록번호: 웹사이트 가입시 제출된 주민등록 번호로 실명확인, 중복가입 방지에 이용된다.
- 비즈니스 개인정보: 취급기관에 따라 다양한 종류의 개인정보가 있다. 공공기관의 개인행정정보, 의료기관에서의 개인의료기록, 금융기관의 자산보유 및 거래기록, 쇼핑몰에서의 구매기록 등 매우 다양하며 중요도가 높은 정보들이다.
- 기타 개인정보: 사진, 동영상, 주고 받은 이메일 등도 개인정보에 포함 될 수 있다.

개인정보 유출에 따른 피해 유형은 다음과 같다.

- 명의 도용: 이름과 주민등록번호를 이용하여 타 사이트에 도용된 명의로 가입하거나, 글쓰기 등을 수행할 수 있다. 오프라인 상에서도 타인의 명의를 도용할 수 있다.
- 계정 탈취: 유출된 ID, 패스워드를 이용하여 대부분의 계정에 로그인하는 것으로 로그인 후 해당 사이트에서 보관하고 있는 모든 개인정보 유출이 가능하며, 로그인 후 수행할 있는 모든 서비스의 도용이 가능하다(예: ID 도용한 글쓰기, 게임사이트 아이템 훔치기, 행정처리). 또한 패스워드를 변경하여 원래 사용자가 사용할 수 없도록 할 수도 있다. 통상 사

용자들은 여러 사이트에서 동일한 ID, 패스워드를 사용하므로 한 사이트의 ID, 패스워드 유출만으로도 피해 범위가 커질 수 있다.

- 보이스 피싱: 유출된 전화번호로 보이스 피싱(전화사기)을 통한 2 차 범죄가 가능하다.
- 스팸메일: 유출된 이메일로 스팸메일이 발송될 수 있다.
- 프라이버시 침해: 개인의료기록, 구매기록, 사진, 동영상, 이메일 등 민감한 사생활이 노출될 수 있다.
- 기타 범죄: 개인행정기록, 금융거래 기록 등 중요 정보를 이용한 다양한 2 차 범죄가 가능하다.

모든 유형의 개인정보 유출이 문제지만 명의도용, 계정탈취 및 2 차 범죄는 매우 심각한 재산상, 사회적 피해를 초래할 수 있다.

2. 개인정보 유출 유형

인터넷 상에서 개인정보가 유출되는 유형은 크게 다음과 같이 분류할 수 있다.

가. 웹사이트의 사용자 DB 유출

- 유출 경로
  * 내부자가 사용자 DB 를 악의나 실수로 외부로 유출시키는 경우이다.
  * 외부의 해커가 웹사이트 서버에 침입하여 사용자 DB 를 절취할 수 있다.
- 대표 사례: 옥션, LGT 등 최근 크게 문제가 되고 있는 개인정보 유출 유형이다.
  * 한꺼번에 대량의 개인정보가 유출될 수 있기 때문에, 가장 심각한 문제를 야기하는 유형이다.

나. 피싱

- 유출 경로
  * 사용자를 실제 사이트와 유사한 피싱 사이트로 유도 후 ID, 패스워드, 기타 개인정보를 입력하게 하여 이를 절취하는 방법이다.
- 대표 사례
  * 이베이 피싱, 웹사이트에서 문제가 생겼거나, 금전적 이익을 준다고 유혹하여 피싱 사이트로 유도한다.

다. 스파이웨어/네트웍스니핑

- 유출 경로
  * 사용자 PC 에 설치된 스파이웨어를 통해 사용자가 키보드로 입력하는 ID, 패스워드를 절취하거나 혹은 파일에 저장된 정보 탈취가 가능하다.
  * 네트워크로 전송되는 ID, 패스워드, 개인정보를 도청한다. 최근에는 도청이 쉬운 무선랜 환경에서 더 큰 문제가 되고 있다.

라. 패스워드 공격

- 유출 경로
  * 특정 사이트에서의 특정 사용자 ID 의 패스워드를 획득하기 위해 패스워드 추측이나 사전 공격(dictionary attack), 모든 문자열 조합 시도(brute-force attack)를 시도한다.
- 대표 사례
  * 게임사이트에 대한 패스워드 공격이 많다. 일단 ID, 패스워드를 획득하고 나면 얻을 수 있는 이익(게임 아이템 등)이 존재하기 때문이다.

3. 기존의 대응방안

2 절에서 기술된 개인정보 유출 유형에 대응하기 위해 법/제도/정책적인 대응방안과 관련 기술들이 많이 제시되고 있다. 법/제도/정책적인 대응방안으로는 다음과 같은 것들이 있다.

- 개인 정보 유출에 대한 처벌 강화: 웹사이트 운영자에게 웹사이트의 해킹이나 내부자 유출에 대한 처벌을 강화하여 관리를 강화하도록 하는 조치로 기술적인 보안 대책의 강화를 위한 모티브를 제공한다.
- 개인 정보 악용에 대한 처벌 강화: 다양한 경로로 유출된 개인정보를 악용하는 사례에 대한 처벌 강화로 명의도용, 개인정보 거래, 계정탈취 등의 행위를 억지한다.
- 특정 개인정보 수집 금지: 중요한 개인정보에 대한 수집을 금지하여, 이의 유출 및 악용을 예방하는 차원으로 현재는 주민등록번호에 대한 수집 금지가 진행되고 있다. 그 대안으로 i-PIN, G-PIN 같은 기술적인 주민등록번호 대체방안이 제시되고 있다.
- 대면등록: 명의 도용을 방지하기 위해 중요한 웹사이트나 서비스의 경우 가입단계에서 직접 대면 확인을 요구하는 정책이다.
- 패스워드 관리: 패스워드의 보안성을 높여 쉽게 공격 당하지 않도록 사용자에게 길이가 길고 다양한 문자열을 포함한 패스워드를 사용하도록 요구한다. 또한 모든 사이트의 패스워

드를 다르게 사용하고, 주기적으로 패스워드를 갱신하도록 요구하는 방법으로 매운 큰 사용자 불편을 초래한다.

개인 정보 유출에 대한 기술적 대응 방안은 다음과 같은 것이 있다.

- 명의 도용 방지 서비스: 주민등록번호와 이름이 유출되어 타인에 의해 웹사이트 가입이나 오프라인 상에서 사용되었을 때 이를 사용자에게 통보해 주거나, 해당 주민등록번호와 이름을 통한 명의 확인 자체를 차단하는 서비스이다. 차단한 경우에는 사용자가 필요할 때만 차단을 해제하고 사용할 수 있다. 현재 인터넷 웹사이트에 가입시 이름과 주민등록번호를 입력하면 웹사이트는 이를 신용평가기관에 전송하여, 이름과 주민등록번호 간의 일치성을 확인하게 되는데, 이 과정에 개입하여 이를 차단하거나 사용자에게 통보해 주는 서비스이다[1],[2].
- 주민등록번호 대체 수단: Ⅲ장에서 설명한다.
- 강화 인증: 유출된 ID, 패스워드를 이용해 타인의 계정에 로그인하는 것을 막기 위해 로그인 시에 패스워드 이외의 추가적인 강화된 인증 수단을 적용한다. 또는 로그인 단계에서는 ID와 패스워드만을 확인하고, 계좌 이체나 지불 등 심각한 금전적 손실이 발생할 수 있는 기능을 이용시에 추가적인 강화된 인증을 요구할 수 있다. 강화된 인증수단은 패스워드보다 보안성이 높아 쉽게 도용할 수 없다. 강화된 인증 수단으로는 공인인증서, 보안카드, 하드웨어 토큰, OTP, 생체인증 등이 있다[3],[4].
- 피싱 방지: 피싱 자체를 두 가지 유형으로 나눌 수 있다.
  * 가입 단계에서의 피싱: 사용자에게 사이트 가입을 유도한 후 사용자가 입력한 개인정보를 절취하는 경우이다.
  * 로그인 단계에서의 피싱: 사용자에게 사이트 로그인을 유도한 후 사용자가 입력한 ID와 패스워드를 절취하는 방식으로, 이후 계정탈취를 목적으로 하는 경우이다.

피싱을 방지하는 기술은 다음과 같다.

- 네거티브 리스트 방식: 피싱 사이트로 알려진 사이트 목록을 관리하여 해당 사이트 접근시 사용자에게 경고한다. 가입 및 로그인 단계의 피싱에 모두 적용될 수 있다. 그러나 모든 피싱 사이트 목록을 100% 파악할 수 없고 신규 피싱 사이트를 막을 수 없다는 단점이 있다[5].
- 포지티브 리스트 방식: SSL, EV 인증서 등 서버를 인증할 수 있는 별도의 수단을 두고, 이러한 인증을 통과하였는지를 사용자에게 알린다. 가입 및 로그인 단계의 피싱에 모두 적용

될 수 있다. 그러나 이러한 인증서를 제공하지 않는 사이트가 훨씬 다수이므로 사용자는 포지티브 표시가 출력되지 않아도 별로 경각심을 갖지 않게 된다[6].

- 상호인증(Mutual Authentication): 로그인 단계에서의 피싱을 막기 위한 수단으로 사전에 확인된 실제 사이트를 기록해 두고, 추후 방문시 이것이 전에 방문한 실제 사이트인지 확인하는 방법이다.
- 안티 스파이웨어: 컴퓨터 바이러스 백신과 유사한 프로그램으로 컴퓨터에 설치된 스파이웨어를 탐지하고 제거한다.
- 키보드 해킹 방지 프로그램: 키보드 입력을 도청하는 것을 방지하는 키보드해킹 방지 프로그램이다[7].
- 암호화: 통신 상에 전송되는 개인정보를 암호화하여 도청하더라도 이용할 수 없도록 하는 기술이다. SSL 이 대표적 암호화 기술이다[8].

III. 주민등록번호 대체 방안

1. 개요

현재 웹사이트 가입시 제출되는 주민등록번호는 실명확인(실제 존재하는 사람의 주민등록번호인지 확인), 중복가입 방지에 이용된다. 그런데 현재의 주민등록번호 사용 방식은 다음과 같은 문제를 갖는다.

첫째, 타인의 주민등록번호를 도용해 사용하는 경우는 본인여부를 확인할 수 없다. 따라서 주민번호와 이름이 유출되면 명의 도용이 가능하다. 둘째, 주민등록번호 자체에 출생지, 성별 등 개인정보를 포함하고 있으므로 주민등록번호 유출시, 프라이버시 침해가 발생할 수 있다.

주민등록번호 대체방안은 주민등록번호가 유출되었을 때 번호에 포함된 개인정보 유출과 명의도용 문제를 해소하기 위해 주민등록번호 대신 대체정보를 사용할 수 있도록 해주는 방법이다. 주민등록번호 대체방안은 실명확인과 중복가입방지 및 본인확인 기능도 제공한다.

2. i-PIN

i-PIN 서비스는 민간 웹사이트에서의 주민등록번호 대체를 위해 제공되는 서비스로 5 개 본인확인기관을 통해 제공된다. i-PIN 이용 방식은 다음과 같다.

- 본인확인 기관에서 대면등록, 공인인증서, 휴대폰 SMS, 신용카드 번호 등으로 본인확인을

거친다.

- 본인확인 기관 사이트에 가입하여 ID, 패스워드를 발급받는다. 이메일 주소와 패스워드, 혹인 공인인증서를 인증수단으로 사용하는 경우도 있다.
- 웹사이트 가입시 i-PIN 을 통한 주민등록번호 대체 이용을 선택하면, 먼저 5 개 본인확인 기관 중 자신이 가입한 기관을 선택한다.
- 선택한 자신의 본인확인기관 사이트로 자동이동 후 등록한 ID, 패스워드 등 인증수단을 이용하여 로그인 한다.
- i-PIN 발급을 선택하면, 주민등록번호 대체 정보가 발급되어 가입하려고 하는 웹사이트로 전송된다.
- 최초 웹사이트로 자동으로 돌아가 이후 과정을 진행한다.

최근 인터넷 개인정보 유출 문제가 부각되어 그 대책의 일환으로 주민등록번호 대체 서비스의 적용이 확대될 전망이다.

3. G-PIN

G-PIN 서비스는 전자정부 사이트에서의 주민등록번호 대체를 위해 제공되는 서비스로 행정안전부 G-PIN 사이트를 통해 제공된다. G-PIN 이용 방식은 다음과 같다.

- 공인인증서 또는 행정기관 방문 대면등록으로 본인확인을 거친다.
- G-PIN 사이트에 가입하여 ID, 패스워드를 발급받는다.
- 웹사이트 가입시 주민등록번호 대체 이용을 선택하면 G-PIN 사이트로 자동 이동된다.
- G-PIN 사이트에 등록한 ID, 패스워드를 이용하여 로그인 한다.
- 주민등록번호 대체 정보가 발급되어 가입하려고 하는 웹사이트로 전송된다.
- 최초 웹사이트로 이동되어 이후 과정을 진행한다.

i-PIN 과 G-PIN 서비스 간의 연계가 2008 년 7 월부터 제공된다. 연계가 되면 i-PIN 가입자가 전자정부 사이트를 이용할 때도 i-PIN 을 통한 본인확인을 할 수 있고, G-PIN 가입자가 민간 웹사이트 이용 시에도 G-PIN 기관을 통해 본인확인을 할 수 있게 된다. 이용 방식 측면에서는 웹사이트(전자정부&민간)에서 주민등록번호 대체를 선택하면, i-PIN 5 개 기관과 G-PIN 기관, 총 6 개 기관 중 자신이 가입한 기관을 선택하고 해당 사이트로 이동되어 ID, 패스워드를 입력, 로그인하는 방식으로 구성된다.

4. i-PIN, G-PIN 의 한계점

i-PIN 과 G-PIN 서비스는 주민등록번호 대체 수단 제공 기능은 달성했지만, 폭넓게 보급되어 사용되게 되면 사용자 편의성과 보안 문제 등이 부각될 수 있다. 사용자 편의성 문제는 6 개의 본인확인 기관이 존재함에 따라 대체 서비스 이용시 자신이 어느 기관에 가입했는지 기억하지 못하는 경우가 많이 발생할 수 있다.

보안 문제로는 패스워드로 사용자를 인증하는 주민등록번호 대체 서비스의 계정이 유출되는 계정탈취 문제가 있다. 주민등록번호 대체 서비스의 계정탈취는 일반 웹사이트의 그것보다 훨씬 치명적인 결과를 초래한다. 주민등록번호 대체 서비스를 통해 모든 웹사이트에서 본인확인을 수행하게 되므로 주민등록번호 대체 서비스의 계정이 탈취되면 해당 명의 도용 및 타 웹사이트 계정탈취가 추가적으로 발생할 가능성이 매우 높다. 또한 기존 주민등록번호 입력 방식에서는 주민등록번호가 본인확인을 제공하지 못하므로(도용된 번호일 가능성이 있으므로) 주민등록번호를 입력해서 가입했다 하더라도 본인임을 확인할 필요가 있는 경우, 별도의 본인확인을 수행하는 것이 일반적이었다. 주민등록번호 대체 서비스는 본인확인을 제공하므로, 대체 서비스를 이용해 가입한 사용자 계정에 대해서는 별도의 본인확인 절차를 수행하지 않게 될 가능성이 높다. 이러한 상태에서 주민등록번호 대체 서비스의 계정탈취는 큰 피해를 초래할 수 있는 것이다. 다른 말로 주민등록번호 대체 서비스 계정탈취가 집중적으로 시도될 가능성이 높다고 할 수 있다.

주민등록번호 대체 서비스 계정탈취는 피싱, 스파이웨어/스니핑 또는 패스워드 공격에 의해 이루어질 수 있다. i-PIN, G-PIN 서비스를 모방한 피싱 사이트가 창궐할 가능성이 높으며, 패스워드 공격도 집중적으로 이루어질 것으로 예상된다. 현재의 i-PIN, G-PIN 는 패스워드 공격 가능성과 피싱 사이트 발생 가능성에 대응하지 못하고 있다. 특히 피싱 사이트의 경우는 i-PIN, G-PIN 자체의 문제가 아니며 주민등록번호 대체 서비스 차원에서 대응할 수 있는 수단이 현재로는 없다.

IV. 전자 ID 지갑

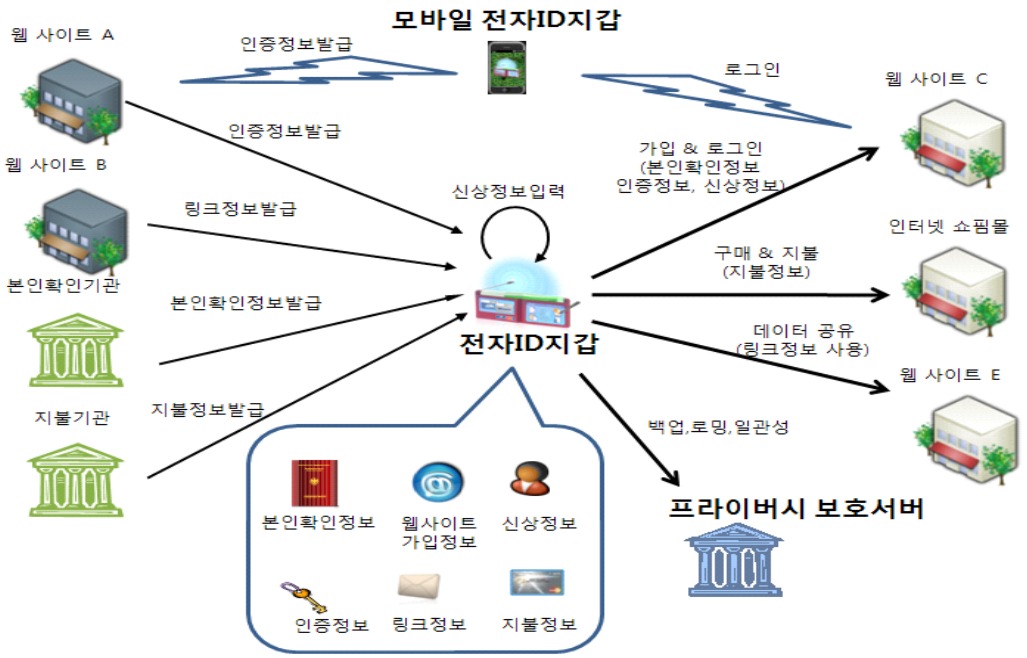
ETRI 에서 개발 중인 전자 ID 지갑 기술은 인터넷 상의 개인 정보를 안전하게 관리하고 편리하게 사용할 수 있도록 해주는 기술이다. 본 장에서는 전자 ID 지갑 기술의 기본 개념 및 주요 기능을 살펴보고 전자 ID 지갑을 통해 인터넷 개인 정보 유출 문제를 어떻게 해결할 수 있는지 기술한다.

1. 기본 개념

전자 ID 지갑은 사용자의 PC 나 모바일 단말에 설치되어 동작하는 소프트웨어로서 사용자의 ID 정보, 즉 개인정보를 직접 저장하거나 개인정보가 저장된 위치를 가리키는 링크 정보를 저장/관리하고 있다. 전자 ID 지갑에 저장되어 있는 개인정보는 사용자의 직접 관리 및 통제 하에 편리하고 안전하게 사용될 수 있다. (그림 1)은 전자 ID 지갑의 기본 개념을 보여준다.

전자 ID 지갑에 저장되는 개인정보는 웹사이트를 이용하며 생성되거나 사용자가 직접 입력한다. 전자 ID 지갑에 저장되는 개인정보는 다음과 같다.

- 본인확인 정보: i-PIN 기관이나 G-PIN 기관 같은 본인확인기관에서 발급받은 주민등록번호 대체 본인확인 정보로 웹사이트 가입시 제출한다.
- 웹사이트 가입 정보: 사용자가 가입한 웹사이트와 가입시 사용한 ID 등의 정보로 웹사이트 가입시 생성되고 추후 이 사이트를 로그인할 때 사용자 ID 입력대신 제출된다.
- 신상정보: Ⅱ 장 1 절에서 설명된 사용자 개인신상 정보로 사용자가 직접 입력하면 웹사이트 가입시 제출된다.
- 인증정보: 공인인증서 등 사용자 인증 수단으로, 강화된 인증을 수행할 때 사용한다.



(그림 1) 전자 ID 지갑 개념도

- 링크정보: Ⅱ장 1 절에서 설명된 비즈니스 개인정보, 즉 웹사이트가 보유한 사용자 정보에 대한 링크를 의미한다. 링크를 통해 사용자 정보에 대한 관리를 할 수 있고, 링크를 통해 실제 데이터를 획득할 수 있다.
- 지불정보: 신용카드, 계좌이체, 휴대폰 SMS 등 현존하는 인터넷 지불 수단을 사용하기 위한 정보로 신용카드 번호, 계좌번호 등을 지불기관을 통해 발급받거나 사용자가 직접 입력을 통해 전자ID 지갑에 저장되며, 인터넷 지불 수단 사용시 지불기관에 제출된다.

2. 주요 기능

전자ID 지갑은 다음과 같은 기능을 제공한다.

- 사이트 가입: 전자ID 지갑을 통해 웹사이트에 가입할 때 사용자 ID 만을 입력하면, 사용자 인증을 위한 비밀키가 자동 생성되며, 해당 사이트 가입을 표시하는 사이트카드를 발급해 준다. 발급된 사이트카드는 전자ID 지갑에 저장, 추후 사이트 로그인시 해당 카드를 클릭하는 것만으로 로그인이 되며, 사이트카드 관리를 통해 자신이 가입한 웹사이트 목록과 주고받은 정보 내용을 관리할 수 있다.
- 주민등록번호 대체 본인확인: 전자 ID 지갑을 통해 본인확인기관에서 주민등록번호 대체 정보인 i-PIN 이나 G-PIN 을 발급받는다. PIN 은 카드 형태로 발급되어 전자ID 지갑에 저장된다. 추후 웹사이트 가입시 PIN 카드를 클릭하기만 하면 본인확인 절차가 완료된다.
- 프로파일 제출: 웹 사이트 가입을 위해 사용자가 자신의 신상정보를 매번 직접 입력하지 않고, 전자ID 지갑에 저장되어 있던 프로파일 카드를 클릭하는 것만으로 신상정보 제출이 가능하다.
- 사이트 로그인: 웹사이트에 로그인하기 위해 ID, 패스워드를 입력하는 대신, 해당 사이트 가입시 발급받은 사이트 카드를 클릭하는 것만으로 로그인이 완료된다.
- 링크를 통한 개인정보 공유: 웹사이트에서 저장하고 있는 비즈니스 개인정보에 대한 링크를 전자ID 지갑에 저장한다. 링크는 데이터카드 형태로 저장되며, 개인 정보에 대한 사용 계약을 담고 있다. 링크는 전자ID 지갑과 정보를 소비하는 웹사이트 간에도 형성될 수 있다. 웹사이트 이용시 특정 비즈니스 개인정보를 소비 웹사이트에 제공하는 방법은 소비 웹사이트에 해당 데이터카드를 제출(클릭)하는 형태로 이루어진다. 소비 웹사이트와 링크가 형성되며, 소비 웹사이트는 이 링크를 통해 제공 웹사이트에서 실제 데이터를 가져올 수 있다. 이때 데이터 흐름은 전자ID 지갑을 경유하여 이루어 진다.

- 개인정보 동기화: 한번 제출된 개인정보(신상정보, 비즈니스 개인정보)의 내용이 변경되었을 때 전자 ID 지갑을 통해 이를 동기화할 수 있다. 프로파일 제출 기능을 통해 제출된 개인 신상정보는 전자 ID 지갑에서 정보를 수정한 뒤 동기화 기능을 호출하면, 이 정보가 제출된 웹사이트로 변경된 신상정보가 전송된다.
- 인터넷 지불: 인터넷 쇼핑몰 등에서 구매 후 결제단계에서 신용카드 번호나 계좌번호를 직접 입력하는 대신, 전자 ID 지갑에 저장되어있는 지불카드(신용카드 혹은 계좌번호, SMS 등)을 선택(클릭)하는 것으로 지불이 이루어진다.
- 개인정보 관리 기능: 인터넷을 이용하며 가입한 웹사이트나 제출했던 개인정보, 혹은 웹사이트에 분산되어 있는 자신의 비즈니스 개인정보를 전자 ID 지갑을 통해 편리하게 관리할 수 있다.
- 전자 ID 지갑 백업, 휴대, 로밍 기능: 전자 ID 지갑 데이터 저장장치 변경을 통한 휴대 기능 및 백업이 제공되며, 온라인 서버를 통한 자동 백업과 별도의 저장매체 휴대없이 이동하여 사용할 수 있는 로밍 기능이 제공된다.
- 모바일 전자 ID 지갑: 휴대폰을 통해 무선인터넷 이용시, ID, 패스워드 입력 불편이나, 개인정보 입력 불편을 해소할 수 있도록 전자 ID 지갑 기능을 수행하는 휴대폰 버전의 전자 ID 지갑이 제공된다. 또한 PC 방 등에서 강화인증 수단으로 휴대폰을 사용할 수 있는 기능도 제공된다.

3. 개인정보 유출 방지

Ⅱ장 2 절에서 설명된 인터넷 개인 정보 유출 유형들에 대해 전자 ID 지갑이 제시하고 있는 대응책과 기존 대응 방안과의 차별성은 다음과 같다.

가. 웹사이트의 사용자 DB 유출

- 전자 ID 지갑을 사용하면 모든 개인 정보를 웹사이트에 보관하지 않고, 전자 ID 지갑 또는 개인정보 생성 웹사이트로부터 필요 시에 필요한 정보만을 인출해 사용할 수 있으므로 웹사이트에 보관되는 개인정보 자체를 줄일 수 있다.
- 또한 제공되는 개인정보에 대한 사용조건(사용목적, 보관기간, 활용 범위)에 대한 명확한 양방 간의 계약이 형성되므로, 문제 발생시 책임 범위를 명확히 할 수 있다.
- 패스워드에 해당되는 전자 ID 지갑 로그인용 비밀키가 유출되더라도, 각 사이트마다 서로 다른 비밀키를 사용하므로, 유출한 비밀키로 계정탈취를 할 수 없다.

- 기존 대응은 사용자 DB 유출을 차단하거나 사후 악영향을 최소화하기 위한 수단이나 전자ID 지갑은 웹사이트에 보관되는 사용자 개인정보 범위 자체를 축소할 수 있다.

나. 피싱

- 가입 단계에서의 피싱은 서버 인증서의 url 확인을 전자 ID 지갑이 직접 수행하고 사용자에게 안전한 웹사이트임을 표시한다.
- 로그인 단계에서 전자ID 지갑을 통해 로그인하게 되면 전자ID 지갑이 직접 상호인증을 수행하므로 피싱 사이트는 이를 통과할 수 없다.
- 기존의 방법은 리스트를 이용해 관리하거나 사용자의 판단에 의존하였는데, 리스트는 불충분하기 쉽고 사용자의 판단에 의존하는 경우 번거로움 때문에 사용자가 오류를 유발하기 쉬웠다. 이에 반해 전자ID 지갑은 이를 자동으로 처리해 주므로 거의 완벽한 피싱 방지가 가능하다.

다. 스파이웨어/네트웍스니핑

- 전자ID 지갑을 통해 로그인하게 되면 ID 패스워드를 키보드를 통해 입력하지 않기 때문에 키보드 해킹의 소지가 없어진다.
- 개인정보는 안전하게 암호화되어 저장되므로 스파이웨어에 의한 유출을 방지할 수 있다.
- 네트워크로 ID 및 개인정보 전송시 항상 암호화를 해서 통신하므로 네트워크 스니핑도 방지할 수 있다.
- 기존의 키보드 해킹 방지 툴은 100% 완전하지 못하지만 전자ID 지갑은 원천적으로 그런 가능성을 배제할 수 있다.
- 네트워크 암호화를 위해서는 인증서 설정 등 사용자에게 어려움을 주는 요소가 있었지만 전자ID 지갑에서는 그런 요소를 배제하였다.

라. 패스워드 공격

- 사용자가 선택한 패스워드 대신, 전자 ID 지갑이 생성한 보안성 높은 로그인용 비밀키를 사용하므로 패스워드 공격에 대해 안전하다.
- 로그인용 비밀키는 정기적으로 갱신될 수 있는데, 이때 사용자의 개입이 필요하지 않아 편리하다.
- 기존에 사용자가 선택하는 패스워드는 사용자가 기억하고 입력해야 하기 때문에 길이나 복잡도를 높이는데 한계가 있다. 따라서 높은 보안성을 갖는 패스워드를 사용하도록 하기

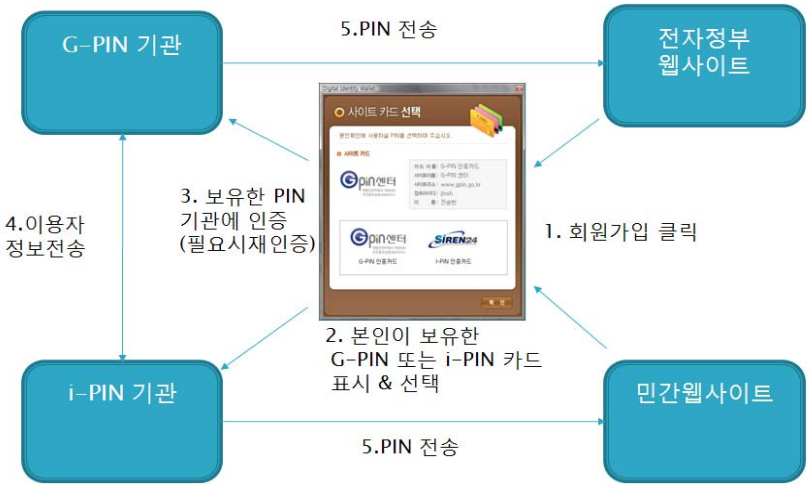
가 어려웠다. 또한 패스워드의 주기적 갱신도 사용자 불편을 초래하는 면이 존재하였다.

4. i-PIN/G-PIN 한계점 개선

전자 ID 지갑을 통해 III 장 4 절에서 제기했던 i-PIN, G-PIN 의 한계점을 개선할 수 있다. (그림 2)는 전자 ID 지갑을 적용한 i-PIN, G-PIN 서비스 방식을 보여준다. 전자 ID 지갑을 통해 i-PIN, G-PIN 사이트에 가입하고, 추후 i-PIN, G-PIN 사용시 전자 ID 지갑에서 자신이 발급받은 PIN 카드를 선택하는 것으로 모든 절차가 완료된다.

전자 ID 지갑의 적용을 통해 i-PIN, G-PIN 의 한계점을 다음과 같이 개선할 수 있다.

- PIN 기관 선택에 따른 사용자 불편: 전자 ID 지갑에서 자신이 가입한 PIN 기관에서 발급받는 PIN 카드를 보여주고 여기서 선택(클릭)만 하면 되기 때문에 기억 및 선택의 불편함을 해소하였다.
- 패스워드 보안성 문제: 보안성 높은 비밀키를 사용하므로 패스워드에 대한 관리 불편이 없고 패스워드 공격으로부터 안전성을 높였다.
- 피싱 방지 문제: PIN 기관 피싱 문제는 로그인 단계에서만 발생되는 것만 의미가 있다. 전자 ID 지갑은 PIN 기관의 사이트와 상호인증을 수행하므로 로그인 단계의 피싱을 막을 수 있다.



(그림 2) 전자 ID 지갑을 적용한 i-PIN, G-PIN 서비스

V. 결 론

본 고에서는 최근 이슈가 되고 있는 인터넷 개인 정보 유출 문제에 대해 분석하고, 이에 대한 대응 방안을 살펴보았다. 명의도용, 계정탈취, 보이스피싱, 스팸메일, 프라이버시 침해 등 피해 유형도 다양하고 유출경로도 DB 유출, 피싱, 스파이웨어, 스니핑, 패스워드 공격 등 다양하다. 이러한 문제를 해결하기 위해 다양한 대응 방안이 제시되었지만, 사용자 편의성과 포괄성 면에서 많은 개선이 필요하다. 특히 주민등록번호 대체 서비스는 원래 목적을 달성하였지만 사용자 불편과 보안성 문제, 특히 피싱 문제에 많이 노출될 수 있는 한계점을 갖고 있다. ETRI 에서 개발 중인 전자 ID 지갑은 인터넷 상에서 개인정보를 안전하고 편리하게 사용할 수 있도록 해주는 솔루션으로 사이트 가입, 주민등록번호 대체, 프로파일 제출, 사이트 로그인, 링크를 통한 개인정보 공유, 개인정보 동기화, 인터넷 지불, 개인정보 관리기능, 백업/휴대/로밍 기능을 제공하며, 이의 모바일 버전도 제공된다. 전자 ID 지갑은 사용자 편의성과 높은 보안성을 유지하며 제시된 인터넷 개인정보 유출 문제를 해결할 수 있음을 보여준다. 한편, i-PIN, G-PIN 의 주민등록번호 대체 서비스의 문제인 사용자 불편과 패스워드 보안성을 해결하고 피싱 문제를 전자 ID 지갑은 효과적으로 해결할 수 있다. 전자 ID 지갑은 2008 년 9 월에 상용화될 예정이다.

<참 고 문 헌>

[1] Siren24 명의도용방지 서비스, http://www.siren24.com/v2alimi/index.jsp

[2] IDChecker 솔루션, http://IDchecker.co.kr

[3] 한국정보인증 공인인증서비스, http://www.signgate.com/

[4] 금융보안연구원 OTP 인증센터, http://www.fsa.or.kr/business_3.htm

[5] IE 피싱방지기능, http://www.microsoft.com/korea/athome/security/online/ie7.mspx

[6] Verisign EV Certificate, http://www.verisign.com/ssl/ssl-information-center/extended-valIDation-ssl-certificates/index.html

[7] nProtect 키보드해킹 방지 프로그램, http://www.nprotect.co.kr/

[8] SSL, wikipedia, http://en.wikipedia.org/wiki/Ssl

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.