情報保護學會論文誌
第17卷 第2號, 2007. 4

주민등록번호 대체수단에 대한 구현 취약점 분석*

최 윤 성, 이 윤 호, 김 승 주, 원 동 호†
성균관대학교 정보통신공학부 정보보호연구소

Security Analysis on the Implementation Vulnerabilities of I-PIN

Younsung Choi, Yunho Lee, Seungjoo Kim, Dongho Won†
Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University

요 약

주민등록번호는 공공기관뿐만 아니라 민간분야에서도 개인의 신원확인을 위해 사용되고 있다. 뿐만 아니라 주민등록번호는 인터넷 웹사이트에 회원가입을 할 때 필수적으로 요구되는 사항이다. 인터넷상에 개인의 주민등록번호와 이름이 유포돼 오남용 문제가 심각해짐에 따라, 정보통신부의 계획에 의거 현재 5개의 주민등록번호 대체수단을 통합한 I-PIN (Internet Personal Identification Number) 서비스를 시행 중이다. 이에 본 논문에서는 현재 운영 중인 5개의 I-PIN 서비스를 분석하여 이들 각각의 구현 취약점에 대해 알아본다. 그리고 실제로 회원 가입 시 I-PIN 서비스를 이용하는 17개의 홈페이지를 분석한 후, I-PIN 서비스의 전체적인 문제점을 파악하고 그에 대한 대책을 제시한다.

ABSTRACT

A resident registration number is used to confirm and prove his/her identity in a government/non-governmental agency. It is a essential requirement to become the registered member on internet website in Korea. It is serious problem that the resident registration number and name are outflowed in internet and misused by others. So the MIC(Ministry of Information and Communication) in Korea plans and operates the identification system using I-PIN that integrate 5 alternative methods of resident registration number. In this paper, we analyze the problem about the method of 5 I-PIN services and show the security analysis on the implementation vulnerabilities of I-PIN services. we also analyze 17 websites that provides identification system using I-PIN. Finally, we analyze the overall problem of I-PIN service and propose the countermeasure about the problem.

Keywords : *I-PIN, Security Analysis, Network Security*

I. 서 론

주민등록번호는 주민등록 과정에서 국가에서 국민에게 부여하는 고유 번호로서, 공공기관뿐만 아니라 민간분야에서도 광범위하게 사용되고 있다. 특히 주민등록번호에는 개인정보가 포함되어 있을 뿐만 아니라 영구적으로 변하지 않기 때문에, 분산되어 구축된 데이터베

접수일: 2007년 1월 10일; 채택일: 2007년 3월 13일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (IITA-2006-C1090-0603-0028)
† 교신저자, dhwon@security.re.kr

이스에서 개인정보를 검색하고 처리할 때 효율적이다. 그래서 인터넷 홈페이지에서도 이런 주민등록번호의 장점을 이용하기 위하여, 사용자가 홈페이지에 회원가입을 요청하면, 홈페이지에서는 사용자의 주민등록번호를 필수적으로 입력하도록 요구하고 있다. 하지만 사용자의 주민등록번호가 여러 홈페이지의 데이터베이스에서 관리됨에 따라, 주민등록번호가 유출되거나 불법적으로 사용되는 등의 다양한 문제가 발생하고 있는 실정이다[1].

I-PIN 서비스는 인터넷상에 개인의 주민등록번호와 이름이 유포돼 오남용 문제가 심각해짐에 따라, 가상의 주민등록번호와 같은 대체수단을 통해 인터넷을 이용할 수 있게 하여 개인정보를 보호하려는 취지로 현재 정보통신부의 계획에 따라 시행되고 있다. 주민등록번호가 개인을 식별할 수 있도록 영구적으로 지정된 고유 식별번호인 반면, I-PIN은 일시적으로 개인을 식별하기 위해 제 3의 신뢰기관이 부여하는 사용자 식별번호이다. 현재 시행되고 있는 5가지 I-PIN 서비스는 동작원리는 비슷하지만 안전성과 편리성 등에서 차이가 있으며, 각각 동작과정에서 몇 가지 보안상의 문제가 발생한다.

뿐만 아니라, 회원가입 시 I-PIN 서비스를 제공하는 홈페이지는 총 17개인데, 각 홈페이지에서 I-PIN을 이용하여 회원가입을 하는 과정에서 다양한 문제가 발생하고 있다. 그 중 하나는 I-PIN 서비스에서 사용되는 ID, 비밀번호, I-PIN 번호 등이 아무런 보안과정을 거치지 않고 평문으로 노출된다는 것이다. 또한, I-PIN 서비스를 이용한 회원가입 과정에서 I-PIN 팝업창들이 제대로 구현되지 않아서 I-PIN 서비스를 사용하지 못하는 홈페이지도 존재한다. 그리고 5개의 I-PIN 서비스간의 가입정보가 연동이 되지 않아서 한명의 사용자가 하나의 홈페이지에 중복가입 할 수 있다.

본 논문에서는 먼저 2장에서 인터넷상의 주민등록번호 사용으로 발생하는 개인정보 노출의 심각성을 알아보고 주민등록번호를 이용한 사용자 신원확인 체계를 살펴본다. 그리고 3장에서는 5개의 I-PIN 서비스의 동작원리와 문제점에 대해서 분석한다. 그리고 I-PIN 서비스의 식별자 할당 방식에 대해서도 살펴본다. 4장에서는 현재 회원가입 시 I-PIN 서비스를 이용하는 17개의 홈페이지에서 I-PIN 서비스가 어떻게 구현되었는지 분석하고 노출되는 정보를 알아본다. 5장에서는 분석한 자료를 바탕으로 I-PIN 서비스의 종합적인 문제와 그에 대한 대책에 대하여 알아보며, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 주민등록번호를 이용한 사용자 신원확인 체계

2.1 주민등록번호의 개인정보

주민등록번호는 그 자체에 개인정보를 포함하고 있다. 그래서 다른 장비를 사용하지 않고도 주민등록번호 소지자의 기본적인 개인정보를 알 수 있다는 점에서, 필수적인 개인정보가 거의 무방비상태로 노출된다고 할 수 있으며, 이로 인해 사생활의 비밀을 침해당할 수 있다. 주민등록번호가 영구적으로 변하지 않기 때문에 사용이 편리하다는 것은 사실이나, 대부분의 일상생활에서 신원확인수단으로 사용되고 있기 때문에 주민등록번호가 한번 노출되면 주민등록번호에 포함된 개인정보뿐만 아니라, 일상생활과 관련된 개인 프라이버시를 침해하는 문제도 발생할 수 있다. 특히 주민등록번호는 공공기관뿐만 아니라 민간기업에서도 널리 사용되고 있어서, 인터넷 홈페이지를 통해 회원제 사이트를 운영하고 있는 대부분의 업체들이 회원가입을 위한 등록사항에 주민등록번호를 필수항목으로 기재토록 하고 있다. 문제는 회원가입을 하는 사용자들이 주민등록번호를 통한 개인정보유출의 가능성이나 주민등록번호의 유출로 인한 프라이버시 침해를 심각하게 인식하지 못하고 있다는 점이다[2].

위에서 말한 주민등록번호에 담긴 기본적인 개인정보는 다음과 같다. 주민등록번호의 앞 6자리는 사용자의 생년월일을 나타내고 있다. 예를 들어 주민등록번호가 820605이면, 사용자의 태어난 날짜가 1982년 6월 5일이다. 주민등록번호의 뒤 7자리는 사용자의 태어난 세기, 성별, 외국인 여부, 출생신고 지역, 출생신고 순서, 주민등록번호의 진위여부를 나타내고 있다. 예를 들어 주민등록번호의 뒤 자리가 2134239일 때, 순서대로 2, 1342, 3, 9로 나누어 볼 수 있다. 첫 번째 2는 사용자가 20세기(1900년~1999년)에 태어난 여성인 것을 말해주고 있다. 첫 번째 숫자가 1이면 사용자가 20세기에 태어난 남성인 것을 알 수 있고, 2이면 20세기에 태어난 여성, 9이면 19세기에 태어난 남성, 0이면 19세기에 태어난 여성, 3이면 21세기에 태어난 남성이며, 4이면 21세기에 태어난 여성이다. 지금까지 살펴본 숫자는 모두 국적이 한국인 사람을 대상으로 한 것이며, 국적이 한국이 아닌 외국인이 20세기에 태어난 남성이면 5, 20세기에 태어난 여성이면 6, 21세기에 태어난 남성이면 7, 21세기에 태어난 여성이면 8이다. 이렇게 첫 번째 자

〔표 1〕 주민등록번호에 포함된 개인정보

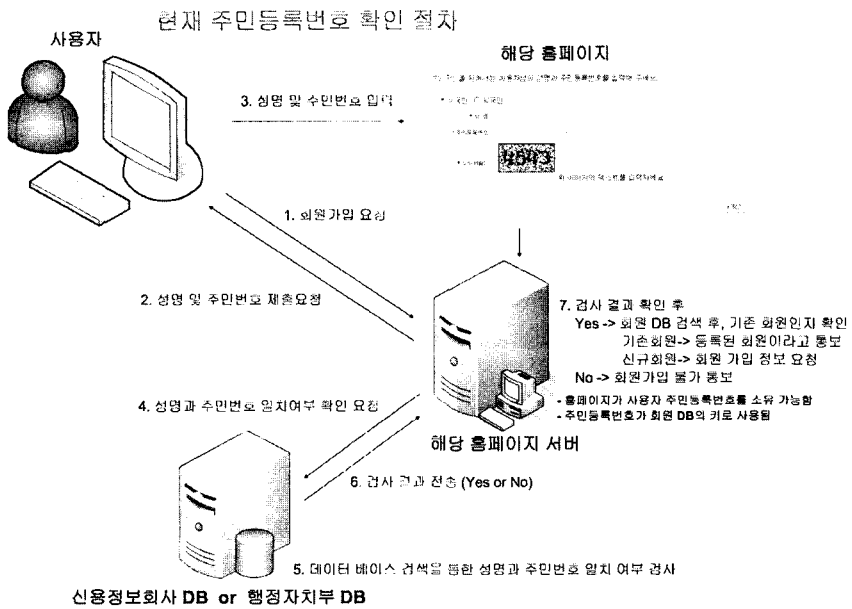
주민등록번호 숫자 순서	주민등록번호에 포함된 개인정보
1~2번째 숫자	- 태어난 연도 뒷자리 수
3~4번째 숫자	- 태어난 월
5~6번째 숫자	- 태어난 날
7번째 숫자	- 남/여 여부와 태어난 세기, 외국인 여부
8~11번째 숫자	- 출생신고를 한 읍,면,동사무소의 유일한 지역코드
12번째 숫자	- 지역코드가 같은 곳에서 생일, 성별이 같은 사람이 신고한 순서
13번째 숫자	- 주민등록번호 검증코드

리는 사용자의 태어난 세기와 성별을 뜻한다. 2~5번째 자리인 1342는 사용자가 출생신고를 한 읍, 면, 동사무소의 유일한 지역코드이다. 그리고 6번째 자리인 3은 출생신고를 한 읍, 면, 동사무소에서 생일, 성별이 같은 사람이 신고한 순서를 뜻한다. 즉 여기서 3은 1342라는 지역코드를 가지는 해당 읍, 면, 동사무소에서 1982년 6월 5일에 태어난 여자아이가 출생신고를 하는 것이 3번째라는 뜻이다. 그리고 마지막으로 숫자인 9는 해당 주민등록번호의 진위여부를 체크하는 검증코드이다. 이 검증코드를 이용해서 사용자가 임의로 생성한 잘못된 주민등록번호를 밝혀낼 수 있다. 주민등록번호는 위에서 설명한 것과 같은 방식으로 생성되므로, 주민등록번호에는 개인정보가 포함되어 있다. 〔표 1〕은 주민등록번호에 포함된 개인정보를 정리하고 있다.

2.2 주민등록번호를 이용한 사용자 신원확인 절차

일반적으로 사용자가 I-PIN 서비스 도입 사이트에 회원가입을 하기 위해서는 〔그림 1〕과 같이 자신의 성명과 주민등록번호를 입력하여야 한다. 이때 프로그램을 이용한 자동 회원가입을 막기 위해 이미지를 이용한 보안문자를 사용하기도 한다. 사용자가 입력한 성명과 주민등록번호는 행정자치부나 신용정보회사의 데이터베이스에 전달되어 그곳에 저장된 정보의 검색을 통해 일치 여부를 확인받게 된다. 인터넷사이트는 검사 결과와 중복가입여부를 토대로 사용자의 홈페이지 회원가입 허가여부를 결정하게 된다.

이때 인터넷사이트가 사용자의 주민등록번호를 소유하게 되고, 그 주민등록번호가 각 사용자를 위한 데이터베이스 관리 및 사용자 속성 관리에서 키로 사용됨으로써 문제가 되고 있다. 즉 한 사용자의 주민등록번호가 한 홈페이지 데이터베이스에만 저장되어 있는 것이 아



〔그림 1〕 주민등록번호를 이용해서 인터넷 사이트에 가입하는 과정

니라, 매우 많은 홈페이지의 데이터베이스 상에 존재하게 되어 유출될 가능성이 높다. 하나의 인터넷 페이지 데이터베이스의 유출은 다른 홈페이지 데이터베이스에도 영향을 미치게 된다. 즉 다른 사용자가 유출된 주민등록번호를 이용하여 특정 홈페이지에 가입하게 되면 실제 사용자가 해당 페이지에 가입을 못하게 되는 것이다.

이것은 현재 주민등록번호가 개개인에게 할당된 고유한 식별로 평생 동안 변경되지 않기 때문이다. 그리고 2.1절에서 살펴본 것과 같이 주민등록번호에는 사용자의 일반적인 개인정보가 포함되어 있기 때문에 노출되었을 때 많은 문제가 발생한다. 이러한 문제를 해결하기 위해서 정보통신부에서는 'I-PIN'이라고 통칭되는 주민등록번호 대체수단 서비스를 시행하게 되었다. 그리고 I-PIN에는 사용자의 개인정보가 포함되어 있지 않기 때문에 주민등록번호 체계에서 발생하는 여려가지 문제를 해결할 수 있게 된다.

Ⅲ. I-PIN 서비스의 종류와 특징

주민등록번호 대체수단이란 사용자가 자신의 신원정보를 신뢰할 수 있는 기관(본인확인기관)에게 제공하여 본인임을 확인받은 뒤 한국정보보호진흥원이 인정한 기술이나 방식을 이용하여 본인확인정보를 발급받아 인터넷 사이트 회원가입이나 성인인증 등을 위해 주민등록번호 대신 사용하는 것이라고 정의되며 I-PIN이라고 통칭되고 있다[3].

현재 시행되고 있는 I-PIN 서비스의 종류는 해당 I-PIN 서비스를 제공하는 기관에 따라서, 한국신용정보

[표 2] 각 I-PIN 서비스에 따른 특징

구분	나이스아이핀 (한국신용정보)	가상주민번호 (한국신용평가정보)	Siren24아이핀 (서울신용평가정보)	OnePass (한국정보인증)	그린버튼 (한국전자인증)
I-PIN 번호(식별자) 구성 및 명칭	13자리 난수로 구성된 나이스아이핀 [2615118028014]	13자리 난수로 구성된 가상주민번호 [5216414811635]	13자리 난수로 구성된 가상식별코드 [3313060444105]	13자리 난수로 구성된 식별번호 [3517368115561]	13자리 난수로 구성된 본인확인정보 [7814065387899]
	- I-PIN 번호는 사업자 DB에 사용자 주민등록번호 대신 들어가는 정보이다. - I-PIN 번호 중 2자리(셋째, 넷째자리)는 각 본인확인기관에 할당된 번호이다.				
사용자에게 I-PIN 번호 재공 여부	알려줌	알려줌	알려주지 않음	알려주지 않음	그린버튼 홈페이지에서 조회 가능
I-PIN 번호 발급 전 추가적 본인확인 방법	범용 공인인증서 신용카드정보 휴대폰 인증정보 대면확인	범용 공인인증서 신용카드정보 휴대폰 인증정보 대면확인	범용 공인인증서 신용카드정보 휴대폰 인증정보 보호자 인증 대면확인	범용 공인인증서	범용 공인인증서 신용카드정보
I-PIN 정보를 발급/검증을 하는 팝업창의 형태	가입하고자 하는 인터넷사이트에서 본인확인기관으로이동 하지 않고 팝업창을 통해 I-PIN 정보의 발급 및 검증을 요청함	- 팝업창 방식 - 다른 I-PIN 서비스의 방식과 동일 - 직접입력방식 - 이용자가 인터넷 사이트에 직접 입력한 가상주민번호를 해당 사이트가 본인확인기관에 전송하여 검증	가입하고자 하는 인터넷사이트에서 본인확인기관으로이동 하지 않고 팝업창을 통해 I-PIN 정보의 발급 및 검증을 요청함	가입하고자 하는 인터넷사이트에서 본인확인기관으로이동 하지 않고 팝업창을 통해 I-PIN 정보의 발급 및 검증을 요청함	가입하고자 하는 인터넷사이트에서 본인확인기관으로이동 하지 않고 팝업창을 통해 I-PIN 정보의 발급 및 검증을 요청함
회원가입 시 필요한 사용자 입력정보	나이스아이핀 (I-PIN 번호)에 접근할 수 있는 식별 ID 및 비밀번호 * 식별 ID 및 비밀번호는 사용자가 직접 설정	* I-PIN 번호와 동일한 가상주민번호를 입력 * 식별 ID 및 비밀번호는 사용자가 직접 설정	개인 ID 및 비밀번호 * 개인 ID 및 비밀번호는 사용자가 직접 설정	범용 공인인증서에 접근할 수 있는 비밀번호 * 비밀번호는 사용자가 직접 설정	실명인증서 에 접근할 수 있는 E-mail 주소와 비밀번호 * E-mail와 비밀번호는 사용자가 직접 설정

의 "나이스아이핀", 한국신용평가정보의 "가상주민번호서비스", 서울신용평가정보의 "Siren24아이핀", 한국정보인증의 "OnePass", 한국전자인증의 "그린버튼" 이렇게 5가지로 나눌 수 있다. 5가지의 I-PIN 서비스는 I-PIN 번호(식별자)의 구성, 발급 시 본인확인 방법 등에서 서로 다른 특징이 있는데, [표 2]는 각 I-PIN 서비스에 따른 특징을 정리하고 있다. 이제부터 분석하는 I-PIN 서비스 관련 내용은 2006년 12월 21일부터 2007년 1월 10일까지의 수집된 데이터를 정리한 것이다.

본인확인기관은 사용자로부터 개인정보를 입력받은 후, 사용자의 주민등록번호를 대신할 식별자(I-PIN 번호)를 생성한다. 사용자가 인터넷 사이트에 회원으로 가입을 하고자 할 때, 본인확인기관은 사용자의 요청에 따라 해당 사이트에 주민등록번호를 대신할 I-PIN 번호를 제공한다. 이 I-PIN 번호는 13자리로 구성되어 있으며 본인확인기관에 따라 서로 다른 번호를 생성한다. I-PIN 번호의 3,4번째 숫자는 본인확인기관에 따라 고정된 값으로써, 15는 한국신용정보, 16은 한국신용평가정보, 13은 서울신용평가정보, 17은 한국정보인증, 14는 한국전자인증을 의미한다. 본인확인기관에서 사용자에게 I-PIN 번호를 할당되는 방식은 "사용자별 I-PIN 할당 방식"과 "(사용자+서비스)별 I-PIN 할당 방식"으로 나눌 수 있다. [표 3]은 두 가지 방식에 대해서 설명하고 있다.

I-PIN 서비스를 이용한 회원가입 방식은 일반적인 사용자, I-PIN 서비스 도입 사이트, 본인확인기관으로 구성된다. 여기서 I-PIN 정보는 사용자가 I-PIN 서비스를 통해 I-PIN 서비스 도입 사이트에 회원가입을 하기 위해 각 I-PIN 서비스 별로 필요한 정보(가상주민번호, 식별 ID/비밀번호 등)를 의미한다. I-PIN 서비스에서는 I-PIN 번호가 수시로 변경이 가능하거나 사이트 별로 다르게 설정되기 때문에, 주민등록번호가 회원 DB의 키로 사용되는 문제를 보완할 수 있다. 사용자가 I-PIN 서비스 도입 사이트에서 실행되는 I-PIN 팝업창에 자신의 I-PIN 정보를 입력하면, 사용자 I-PIN 정보는 I-PIN 서비스 도입 사이트를 거치지 않고 직접 본인확인기관으로 전달된다. 본인확인기관에서는 사용자의 I-PIN 정보의 유효성 검증 결과와 사용자의 주민등록번호 대신 사용될 I-PIN 번호를 포함한 본인확인정보를 I-PIN 서비스 도입 사이트로 전달한다. 그러므로 사용자의 주민등록번호는 I-PIN 서비스 도입 사이트의 회원 DB에 저장되지 않는다. [그림 2]는 사용자가 I-PIN 서비스를

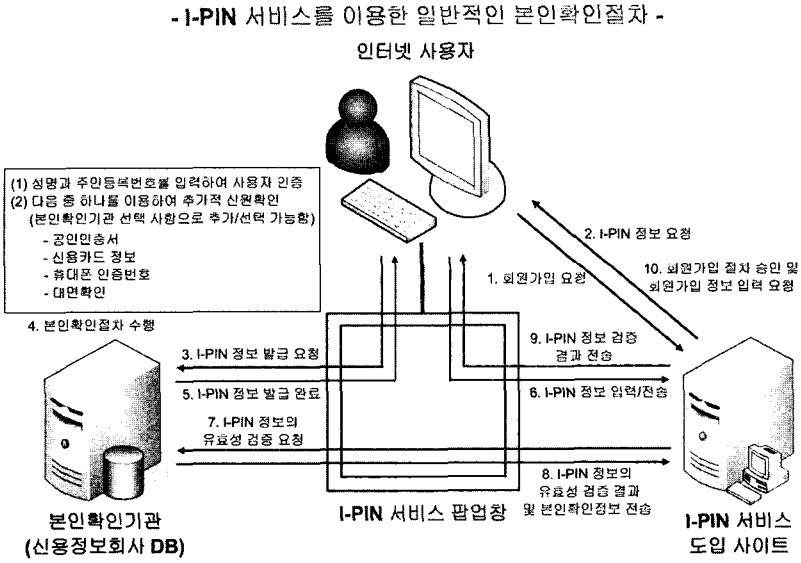
[표 3] 사용자별 I-PIN 할당 방식, (사용자+서비스)별 I-PIN 할당 방식의 비교

구분	사용자별 I-PIN 할당 방식	(사용자+서비스)별 I-PIN 할당 방식
발급 방식	-발급/폐지/재발급의 개념이 존재 -사용자가 I-PIN 번호를 재발급 받기 전에는 언제나 동일한 I-PIN을 사용하는 방식	-재발급의 개념이 없고 I-PIN의 발급/폐지의 개념만 존재 -각 사용자에 대해 각 홈페이지에 할당된 I-PIN 번호가 언제나 동일함 -서로 다른 사용자에 대한 각 홈페이지의 I-PIN 번호가 서로 다름
장점	-자신의 I-PIN 번호가 노출되었을 때, 새로운 I-PIN 번호를 재발급 가능	-I-PIN 서비스 도입 사이트 마다 각각의 사용자에게 서로 다른 I-PIN 번호를 부여하게 되므로 주민등록번호와 같은 회원 DB의 키로 사용될 수 없음
단점	-재발급 받지 않고 하나의 I-PIN 번호가 오랜 기간 사용될 경우, 주민등록번호와 마찬가지로 I-PIN 번호가 회원 DB을 연결하는 키로 사용될 수 있음	-I-PIN 번호의 유효기간이 없음
예시	-나이스아이핀 방식을 제외한 4개 방식	-나이스아이핀 방식 [한국신용정보]

이용하여 I-PIN 서비스 도입 사이트에 회원가입을 하기 위한 절차를 보여준다. 이때 사용자의 컴퓨터에 클라이언트가 설치되는 방식은 OnePass와 그린버튼이며, 나이스아이핀, Siren24아이핀, 가상주민번호 방식은 클라이언트가 설치되는 것이 아니라 팝업창을 통해서 본인확인기관과 보안 통신(https)을 하도록 되어 있다. 현재는 I-PIN 팝업창을 5개 I-PIN 서비스에서 공통으로 적용하고 있어 모두 연결되고 있으며, 공인인증서를 이용한 본인확인을 위해서 공인인증서 용 본인확인 툴킷이 설치되는 형태이다. 그리고 팝업창을 통해 이루어지는 I-PIN 서비스를 위한 통신은 모두 사용자를 거쳐서 전달되고 있다.

[일반적인 I-PIN 서비스의 동작방식]

① 사용자는 I-PIN 서비스 도입 사이트에 회원가입을 요청한다.



〔그림 2〕 I-PIN 서비스를 이용한 일반적인 본인확인절차

② I-PIN 서비스 도입 사이트에서는 사용자에게 5개 I-PIN 서비스 중 하나의 I-PIN 정보를 입력할 것을 요청한다.

③ I-PIN 정보가 없는 사용자는 I-PIN 정보의 발급을 요청하기 위해서 본인확인기관에 접속한다. 이때 I-PIN 서비스 도입 사이트와 연동되어 I-PIN 서비스 도입 사이트에서 실행되는 I-PIN 팝업창에서 바로 I-PIN의 발급되는 경우도 있다.

④ 본인확인기관은 사용자에게 성명과 주민등록번호 그리고 추가적인 본인확인정보를 요청함으로써 사용자의 본인을 확인한다. 이때 추가적인 정보를 획득하는 방식으로 범용공인인증서, 신용카드 정보, 휴대폰 인증정보, 대면확인 등을 이용한다.

⑤ 본인확인 기관에서는 사용자에게 직접 I-PIN 번호를 발급하거나 I-PIN 번호에 접근할 수 있는 방법을 제공함으로써 I-PIN 정보의 발급을 완료한다.

⑥ 사용자는 팝업창 형태의 I-PIN 팝업창에 발급받은 I-PIN 정보를 입력하고 본인확인기관으로 전송한다. 이때 홈페이지에서 직접 I-PIN 정보를 입력받아 본인확인기관으로 전송하는 경우도 있다.

⑦ I-PIN 서비스 도입 사이트는 인터넷 사용자에게 입력 받은 I-PIN 정보를 본인확인기관으로 전송하고 유효성 검사를 요청한다. 본인확인기관과 I-PIN 서비스 도입 사이트 간의 통신도 I-PIN 팝업창을 통해서만 가능하다.

⑧ 본인확인기관은 전달받은 사용자의 I-PIN 정보의 유효성을 검사한 후, 유효성 검증 결과와 사용자의 본인확인정보(주민등록번호 제외)를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 본인확인기관으로부터 사용자의 I-PIN 정보가 유효하다는 결과가 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

⑩ I-PIN 서비스 도입 사이트에서는 사용자에게 주민등록번호의 입력을 제외한 추가적인 회원가입 절차를 진행하는 것을 허용한다.

이제부터 5가지의 I-PIN 서비스의 동작 방식과 취약점에 대해서 자세히 살펴본다.

3.1 한국신용정보의 나이스아이핀

한국신용정보에서 제공하는 나이스아이핀에서는 사용자가 정당한 식별 ID와 비밀번호를 입력하면, 한국신용정보에서 사용자의 I-PIN 번호를 I-PIN 서비스 도입 사이트로 전송한다. 즉, I-PIN 번호(나이스아이핀) 13자리를 본인이 외워서 입력할 필요 없이, 사용자가 식별 ID와 비밀번호를 관리하는 것만으로 나이스아이핀을 제공하는 모든 사이트를 통제할 수 있다. 식별 ID와 비밀번호는 I-PIN 번호에 접근할 수 있는 수단이다. 그리

고 사용자는 본인확인기관 홈페이지로 이동할 필요 없이, I-PIN 서비스 도입 사이트에서 I-PIN 팝업창을 통하여 식별 ID와 비밀번호 및 I-PIN 번호의 발급이 가능하다. 그리고 나이스아이핀에는 I-PIN 번호를 발급할 때, (사용자+서비스)별 I-PIN 할당 방식을 따른다. 즉 사용자에게 각 홈페이지마다 서로 다른 I-PIN 번호가 할당되어 회원가입을 하게 된다. 하지만 한번 홈페이지에 할당된 I-PIN 번호는 변경되지 않는다. 즉 사용자가 한번 가입한 홈페이지에서 탈퇴한 후 다시 가입할 때, 이전에 할당되었던 I-PIN 번호를 그대로 사용하게 되는 것이다. 그리고 한국신용정보에서 I-PIN 서비스 도입 사이트로 전송되기 전에, 사용자에게 I-PIN 번호의 전송을 허가받는 팝업창이 생성된다. 한국신용정보에서 제공하는 나이스아이핀의 동작방식은 아래의 〔그림 3〕과 같다.

[나이스아이핀 동작방식]

① 인터넷 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트는 인터넷 사용자에게 나이스아이핀 용 식별 ID와 비밀번호를 입력할 것을 요청한다.

③ 사용자는 한국신용정보에 접속하여 식별 ID와 비밀번호 발급을 요청한다. 이때 I-PIN 서비스 도입 사이트에서 팝업창 형태의 I-PIN 팝업창을 통해서 식별 ID와 비밀번호 발급요청을 할 수도 있다.

④ 한국신용정보는 사용자에게 성명과 주민등록번호를 요청하고, 범용공인인증서, 신용카드 정보, 휴대폰 인증정보 또는 대면확인 등을 이용하여 본인확인절차를 수행한다. 그리고 사용자는 나이스아이핀에 필요한 식별 ID와 비밀번호를 설정한다. 이 후 한국신용정보에서는 사용자가 홈페이지에 회원가입을 할 때 마다, I-PIN 서비스 도입 사이트 별로 다른 I-PIN 번호를 생성하여 발급한다.

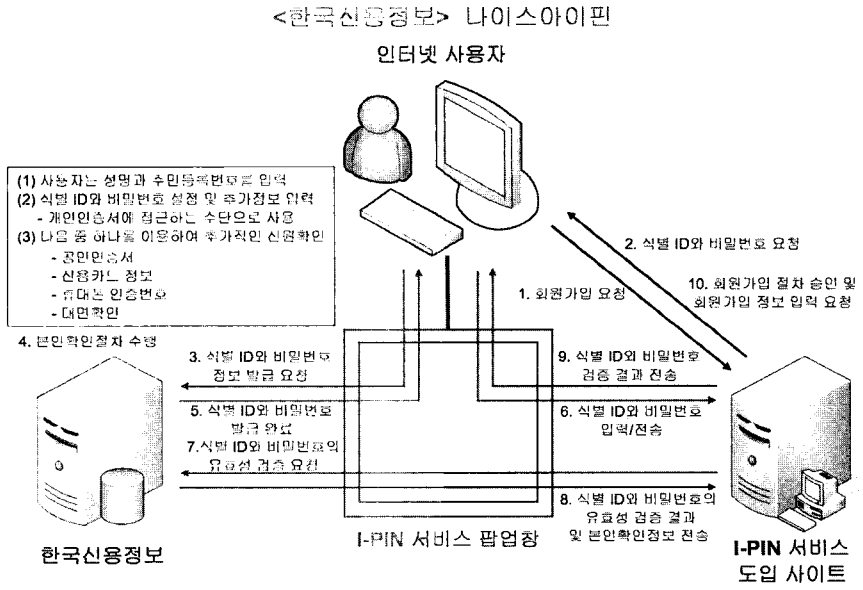
⑤ 한국신용정보에서는 사용자가 설정한 식별 ID와 비밀번호의 사용을 허가하여 사용자가 개인 인증키 서비스를 이용할 수 있도록 한다.

⑥ 사용자는 I-PIN 서비스 도입 사이트에서 동작하는 I-PIN 팝업창에 식별 ID와 비밀번호를 입력하여 한국신용정보로 전송한다.

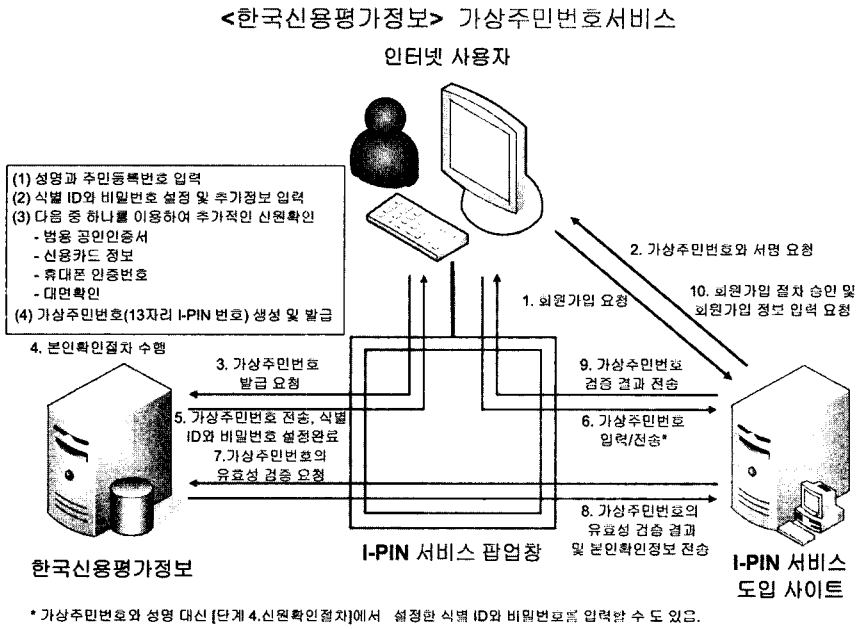
⑦ I-PIN 서비스 도입 사이트에서는 팝업창을 통해 전달받은 사용자의 식별 ID와 비밀번호를 한국신용정보에 전송하고 유효성 검증을 요청한다.

⑧ 한국신용정보에서는 전달받은 사용자의 식별 ID와 비밀번호를 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 한국신용정보로부터 사용자의 식별 ID와 비밀번



〔그림 3〕 나이스아이핀의 동작방식



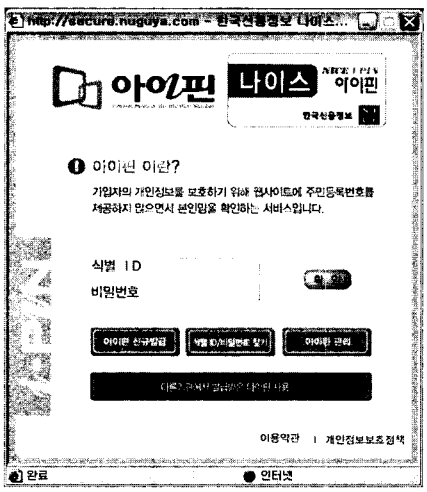
〔그림 6〕 가상주민번호의 동작방식 (I-PIN 팝업창)

호가 유효하다는 결과가 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

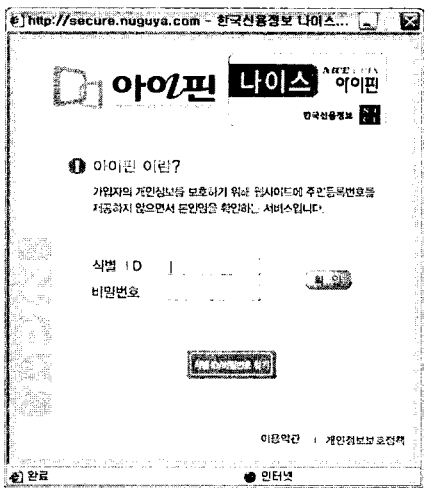
⑩ I-PIN 서비스 도입 사이트에서는 사용자에게 주민등록번호의 입력을 제외한 추가적인 회원가입 절차를 진행하는 것을 허용한다.

[나이스아이핀 팝업창]

나이스아이핀에 사용되는 I-PIN 팝업창은 다음 〔그림 4〕와 〔그림 5〕와 같이 2가지로 분류할 수 있다. 〔그림 4〕는 5가지의 I-PIN 서비스 중에서, 나이스아이핀을 기본적으로 이용하여 사용자 회원가입을 제공하는 인터넷 사이트에서 실행되는 I-PIN 팝업창이다. 〔그림 5〕는 타 I-PIN 서비스를 기본적으로 사용하는 홈페이지에서 실행되는 I-PIN 팝업창에서 추가로 나이스아이핀을 이용할 수 있도록 전환되었을 때 실행되는 I-PIN 팝업창이다.



〔그림 4〕 〔타입 1〕 나이스아이핀 팝업창



〔그림 5〕 〔타입 2〕 나이스아이핀 팝업창

3.2 한국신용평가정보의 가상주민번호

가상주민번호는 인터넷 상에서 회원가입, 미성년자 확인 등을 위한 본인 인증 시 사용자의 주민등록번호 대신 가상번호를 사용함으로써 고유한 개인정보의 노출을 방지 할 수 있는 개인정보보호 기술이다[3]. 가상주민번호는 기존의 실명확인 서비스 방식과 유사한 방식이기 때문에, 개인사용자와 인터넷 업체들의 불편을 최소화할 수 있는 장점이 있다. 한국신용평가정보에서 제공하는 이 가상주민번호는 사용자가 자신의 I-PIN 정보를 입력하는 방식에 따라서 2 가지로 분류할 수 있다. 첫 번째로, 사용자가 자신의 성명과 가상주민번호(I-PIN 번호)를 I-PIN 서비스 도입 사이트에서 실행되는 I-PIN 팝업창에 입력하여 한국신용평가정보로 전송하는 방식이 있다. 이 방식에서는 사용자가 자신의 가상주민번호를 잊어버렸을 때, 가상주민번호를 입력하는 대신 사용자가 가상주민번호를 신청할 때 설정한 식별 ID와 비밀번호를 I-PIN 팝업창에 입력함으로써 본인확인을 받을 수 도 있다. 두 번째로, 사용자가 회원가입을 요청하는 I-PIN 서비스 도입 사이트에 직접 자신의 성명과 가상주민번호를 입력하는 방식이 있다. 이 방식에서는 첫 번째 방식과 달리 식별 ID와 비밀번호만으로는 본인확인을 받을 수 없다. 하지만 식별 ID와 비밀번호를 이용하여 자신의 가상주민번호 번호의 조회하는 팝업창을 제공한다. 한국신용평가정보에서 제공하는 가상주민번호서비스의 동작방식 중 I-PIN 팝업창을 이용하는 방식은 다음 〔그림 6〕에서 설명하고 있다.

[가상주민번호 동작방식 - I-PIN 팝업창을 이용하는 방식]

① 인터넷 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트에서는 사용자에게 가상주민번호와 성명를 입력할 것을 요청한다.

③ 사용자가 한국신용평가정보에 접속하여 가상주민번호 발급요청을 한다.

④ 한국신용평가정보에서는 사용자에게 성명과 주민등록번호를 요청하고, 범용공인인증서, 신용카드 정보, 휴대폰 인증정보, 대면확인을 이용한 본인확인과정 과정을 수행한다. 본인확인과정이 끝나면, 한국신용평가정보에서는 가상주민번호를 생성한다. 그리고 사용자는 식별 ID와 비밀번호를 설정한다. 이 식별 ID는 가상주민번호를 확인하거나 재발급 받을 때 사용한다.

⑤ 한국신용평가정보에서는 생성한 가상주민번호를 전송하고, 식별 ID와 비밀번호 설정을 완료한다.

⑥ 사용자는 가상주민번호와 성명을 I-PIN 팝업창에서 입력한다. 이때 가상주민번호와 성명 대신에, ④에서 설정한 식별 ID와 비밀번호를 입력함으로써 본인확인을 받을 수도 있다.

⑦ I-PIN 서비스 도입 사이트에서는 팝업창을 통해 사용자가 입력한 가상주민번호를 한국신용평가정보에 전송하여 사용자 가상주민번호의 유효성 검증 요청을 한다.

⑧ 한국신용평가정보에서는 전달받은 사용자의 가상주민번호와 성명을 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 한국신용평가정보로부터 사용자 가상주민번호와 성명의 유효성 검증 결과를 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

⑩ I-PIN 서비스 도입 사이트에서는 사용자에게 주민등록번호의 입력을 제외한 다른 회원가입 절차를 진행하는 것을 허용한다.

다음 〔그림 7〕은 한국신용평가정보에서 제공하는 가상주민번호서비스의 동작방식 중 사용자가 자신의 성명과 가상주민번호를 I-PIN 서비스 도입 사이트에 직접 입력하는 방식을 설명하고 있다.

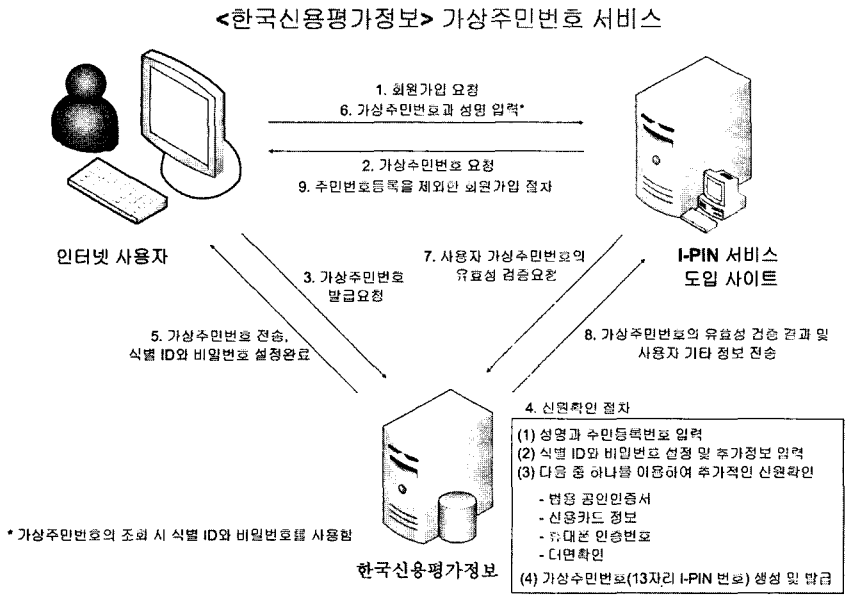
[가상주민번호 동작방식 - 가상주민번호를 I-PIN 서비스 도입 사이트에 직접 입력하는 방식]

① 인터넷 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트에서는 사용자에게 가상주민번호를 입력할 것을 요청한다.

③ 인터넷 사용자가 한국신용평가정보에 접속하여 가상주민번호의 발급을 요청한다.

④ 한국신용평가정보에서는 사용자에게 성명과 주민등록번호를 요청하고, 범용공인인증서, 신용카드 정보, 휴대폰 인증정보, 대면확인을 이용한 추가적인 본인확인 과정을 수행한다. 본인확인과정이 끝나면, 한국신용평가정보에서는 가상주민번호를 생성한다. 그리고 사용자는 식별 ID와 비밀번호



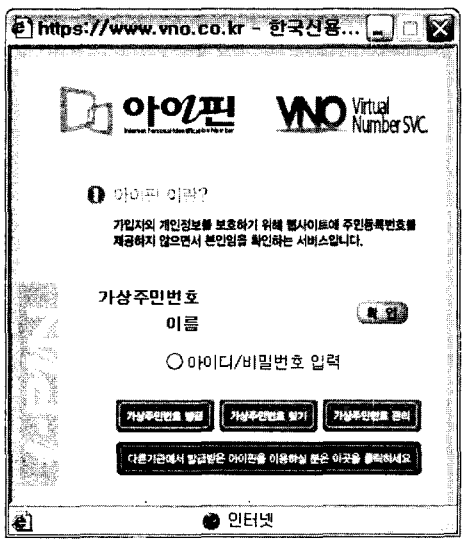
〔그림 7〕 가상주민번호의 동작방식 (가상주민번호를 I-PIN 서비스 도입 사이트에 직접 입력)

를 설정한다. 이 식별 ID는 가상주민번호를 확인하거나 재발급 받을 때 사용한다.

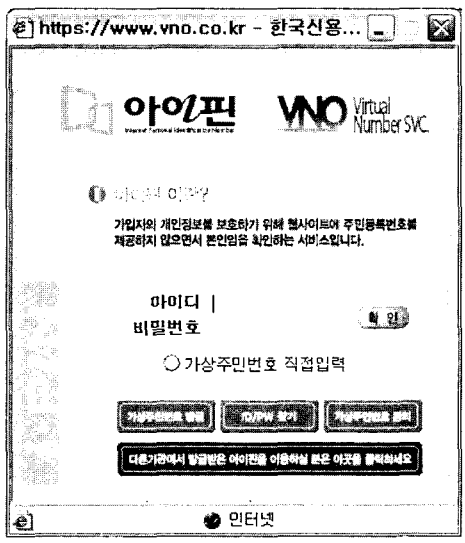
⑤ 한국신용평가정보에서는 생성한 가상주민번호를 전송하고, 식별 ID와 비밀번호 설정을 완료한다.

⑥ 사용자는 가상주민번호를 I-PIN 서비스 도입 사이트에 입력한다. 사용자가 자신의 가상주민번호를 잊어버렸을 경우, 한국신용평가정보의 가상주민번호 관련 홈페이지인 www.vno.co.kr에 접속하여 자신의 식별 ID와 비밀번호를 입력하고 가상주민번호를 확인하거나, I-PIN 서비스 도입 사이트에서 실행되는 가상주민번호를 조회할 팝업창에 자신의 식별 ID와 비밀번호를 입력함으로써 자신의 가상주민번호를 조회할 수 있다.

⑦ I-PIN 서비스 도입 사이트에서는 사용자가 입력한 가상주민번호를 한국신용평가정보에 전송하여 사용자 가상주민번호의 유효성 검증 요청을 한다.



〔그림 8〕 〔타입 1〕 가상주민번호 팝업창



〔그림 9〕 〔타입 2〕 가상주민번호 팝업창

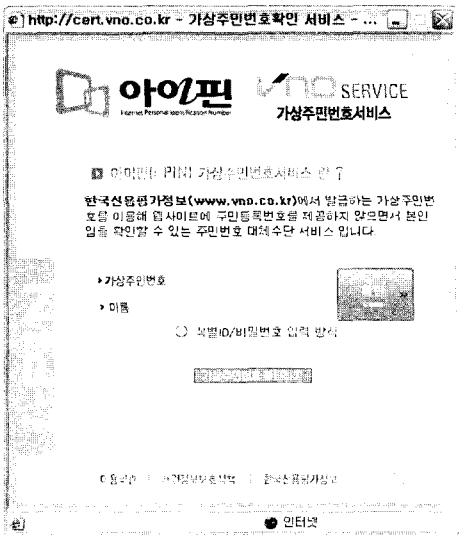
⑧ 한국신용평가정보에서는 전달받은 사용자의 가상주민번호를 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 사용자 가상주민번호의 유효성 검증 결과에 따라서, I-PIN 서비스 도입 사이트에서는 사용자에게 주민등록번호를 입력을 제외한 추가적 회원가입 절차를 진행하는 것을 허용한다.

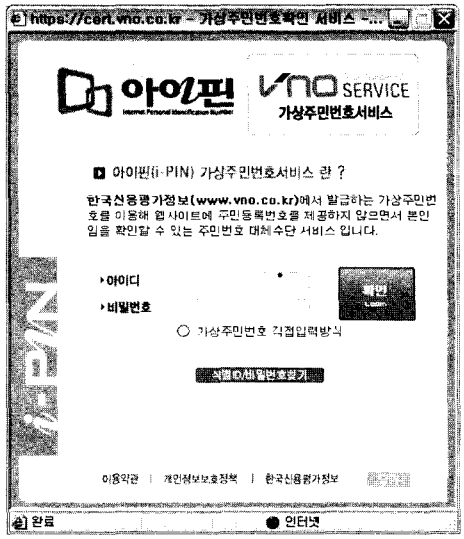
[가상주민번호 팝업창]

가상주민번호에 사용되는 I-PIN 팝업창은 I-PIN 서비스 도입 사이트가 제공하는 기본적인 I-PIN 서비스에 따라서 4가지로 분류할 수 있다. 〔그림 8〕은 5가지의 I-PIN 서비스 중에서, 기본적으로 가상주민번호를 이용하여 회원가입을 제공하는 홈페이지에서 실행되는 I-PIN 팝업창이다. 〔그림 9〕는 사용자가 자신의 가상주민번호를 잊어버렸을 경우, 〔그림 8〕에서 가상주민번호와 사용자 이름을 입력하는 방식 대신 식별 ID와 비밀번호를 입력하는 방식으로 전환하였을 때 실행되는 I-PIN 팝업창이다.

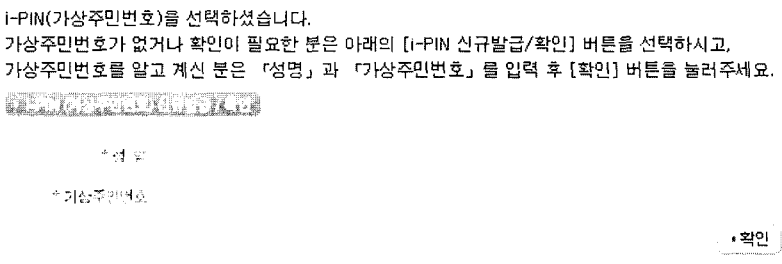
〔그림 10〕은 타 I-PIN 서비스를 기본적으로 사용하는 홈페이지의 I-PIN 팝업창에 추가로 설치되어 있는 가상주민번호 버튼을 눌렀을 때 실행되는 I-PIN 팝업창이다. 〔그림 11〕은 〔그림 10〕에서 가상주민번호와 사용자 이름을 입력하는 방식 대신 식별 ID와 비밀번호를 입력하는 방식으로 전환하였을 때 실행되는 I-PIN 팝업창이다.



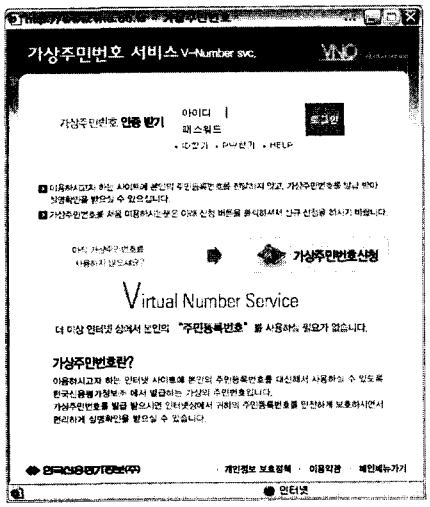
〔그림 10〕 〔타입 3〕 가상주민번호 팝업창



〔그림 11〕 〔타입 4〕 가상주민번호 팝업창



〔그림 12〕 〔타입 5〕 I-PIN 서비스 도입 사이트 직접 입력 방식



〔그림 13〕 〔타입 5〕에서의 가상주민번호 조회

[홈페이지 상에서 가상주민번호 입력방식]

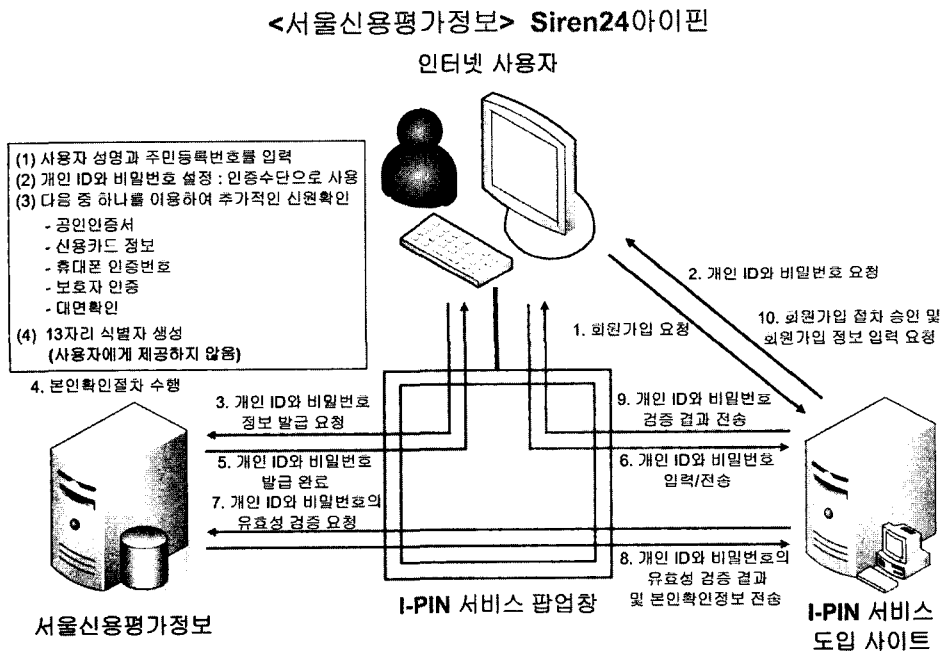
가상주민번호에는 홈페이지 회원가입 과정에서 사용자가 주민등록번호를 대신하여, 홈페이지 상의 입력란에 직접 가상주민번호를 입력하는 방식이 있다. 〔그림 12〕는 사용자가 I-PIN 서비스 도입 사이트에서 회원가입을 하기 위해서 가상주민번호를 직접 입력하는 홈페이지 화면이다.

[가상주민번호의 조회]

홈페이지 상에서 가상주민번호를 입력하는 방식에서 사용자가 자신의 가상주민번호를 잊어버린 경우에, 사용자는 가상주민번호 발급 시 설정한 식별 ID와 비밀번호를 이용하여 자신의 가상주민번호를 조회할 수 있다. 이것은 사용자가 회원가입을 요청하는 홈페이지에 가상주민번호 조회 또는 확인 버튼을 눌렀을 때 실행된다. 〔그림 13〕은 〔그림 10〕의 홈페이지에 가상주민번호를 입력하기 전에 식별 ID와 비밀번호를 입력하여 가상주민번호를 조회할 수 있는 창의 모습이다.

3.3 서울신용평가정보의 Siren24아이핀

서울신용평가정보에서 제공하는 Siren24아이핀은 사용자가 정당한 개인 ID와 비밀번호를 입력하면, 서울신용평가정보에서 사용자의 I-PIN 번호를 I-PIN 서비스 도입 사이트로 전송한다. 이 방식은 한국신용정보의 나이스아이핀과 유사하게 개인별 ID/ PW 발급 및 이용을 기본으로 한다. 그리고 사용자는 본인확인기관 홈페이지로 이동할 필요 없이, I-PIN 서비스 도



〔그림 14〕 Siren24아이핀의 동작방식

입 사이트에서 I-PIN 팝업창을 통하여 개인 ID와 비밀번호 및 I-PIN 번호를 발급하는 것이 가능하다. 한국신용정보의 나이스아이핀과 달리 사용자별 I-PIN 할당 방식을 사용하기 때문에, 사용자가 I-PIN을 재발급받기 전에는 I-PIN 서비스 도입 사이트에 회원가입을 할 때 마다 언제나 동일한 I-PIN을 사용한다. 이때 사용자가 입력하는 개인 ID와 비밀번호는 TrustSSL 방식으로 본인확인기관으로 전송된다. 서울신용평가정보에서 제공하는 Siren24아이핀의 동작방식은 다음 〔그림 14〕와 같다.

[Siren24아이핀 동작방식]

① 인터넷 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트에서는 사용자에게 Siren24아이핀 용 개인 ID와 비밀번호를 입력할 것을 요청한다.

③ 인터넷 사용자가 서울신용평가정보에 접속하여 개인 ID와 비밀번호 발급을 요청한다.

④ 서울신용평가정보는 사용자에게 성명과 주민등록번호을 요청하고 범용공인인증서, 신용카드 정보 , 휴대폰 인증정보, 대면확인를 이용한 본인확인과정 과정을 수행한다. 그리고 사용자는 개인 ID와 비밀번호를 설정하게 하게 되는데, 이 모든 과정은 TrustSSL 통신방식을 이용하여 수행된다. 그리고 서울신용평가정보에서 생성한 I-PIN(13자리 식별자)은 사용자에게는 지급되지 않고, 사용자가가 홈페이지에 회원가입을 요청할 때 마다, 서울신용평가정보가 I-PIN 서비스 도입 사이트에 직접 사용자의 I-PIN을 전송한다.

⑤ 서울신용평가정보에서는 사용자가 설정한 개인 ID와 비밀번호의 사용을 허가하여 사용자가 개인 ID 서비스를 이용할 수 있도록 허용한다.

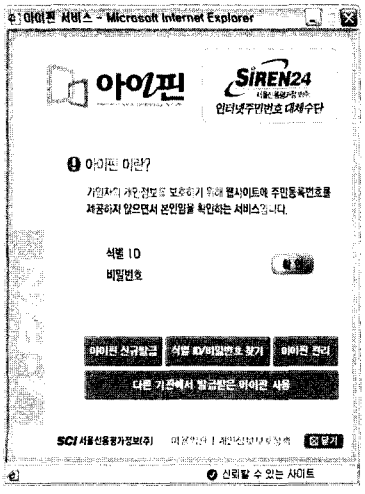
⑥ 사용자는 I-PIN 서비스 도입 사이트에서 동작하는 I-PIN 팝업창에 개인 ID와 비밀번호를 입력하여 서울신용평가정보로 전송한다.

⑦ I-PIN 서비스 도입 사이트에서는 팝업창을 통해 사용자가 입력한 개인 ID와 비밀번호를 서울신용평가정보에 전송하여 사용자 개인 ID와 비밀번호의 유효성 검증 요청을 한다.

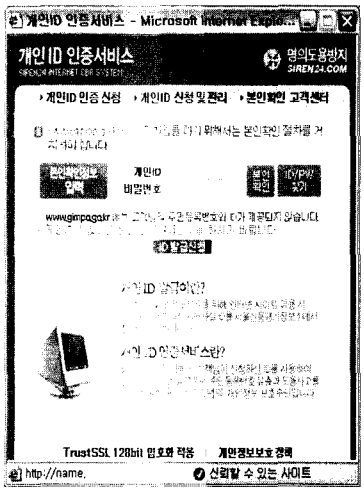
⑧ 서울신용평가정보에서는 전달받은 사용자의 개인 ID와 비밀번호를 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 서울신용평가정보로부터 사용자 개인 ID와 비밀번호의 유효성 검증 결과를 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

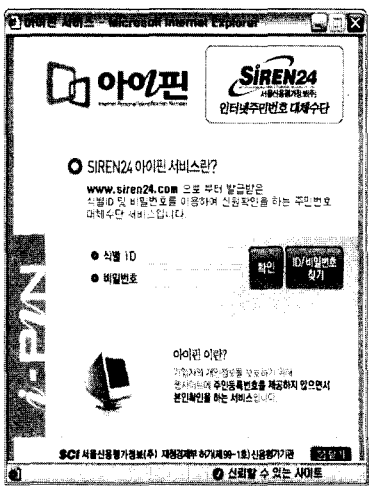
⑩ I-PIN 서비스 도입 사이트에서는 사용자에게 주민등록번호의 입력을 제외한 추가적인 회원가입 절차를 진행하는 것을 허용한다.



〔그림 15〕 〔타입 1〕 Siren24아이핀 팝업창



〔그림 16〕 〔타입 2〕 Siren24아이핀 팝업창



〔그림 17〕 〔타입 3〕 Siren24아이핀 팝업창

[Siren24아이핀 팝업창]

Siren24아이핀에 사용되는 I-PIN 팝업창은 다음 [그림 15], [그림 16] 그리고 [그림 17]에서 보는 것과 같이 3 가지로 분류할 수 있다. [그림 15]와 [그림 16]은 5가지의 I-PIN 서비스 중에서, 기본적으로 Siren24아이핀을 이용하여 회원가입을 제공하는 홈페이지에서 실행되는 I-PIN 팝업창들이다. 즉, 기본적으로 Siren24 아이핀을 이용하여 회원가입을 제공하는 홈페이지들은 [그림 15]의 팝업창이나 [그림 16]의 팝업창을 사용한다. [그림 17]은 타 I-PIN 서비스를 기본적으로 사용하는 홈페이지의 I-PIN 팝업창에 추가로 설치되어 있는 Siren24 아이핀 버튼을 클릭하였을 때 실행되는 I-PIN 팝업창이다.

3.4 한국정보인증의 OnePass

한국정보인증에서 제공하는 OnePass는 사용자의 주민등록번호 대신에 범용 공인인증서를 이용하여 본인을 확인하는 방식이다. 사용자가 OnePass로 I-PIN 서비스 도입 사이트에 회원가입을 하기 위해서는 자신의 범용 공인인증서를 소유하고, 해당 공인인증서 비밀번호만 알고 있으면 된다. 이런 방식을 한국정보인증에서는 "Onepass(One's Personal Authenticated Safety Signature)"라고 한다. 사용자가 Onepass 서비스를 이용할 때 I-PIN 팝업창에 입력하는 공인인증서 비밀번호는 자체적인 보안방식으로 전송된다. 만약 자신의 범용 공인인증서가 없는 사용자라면, 한국정보인증과 같은 공인인증기관에서 범용 공인인증서를 발급 받아야한다. 한국정보인증의 경우 범용 공인인증서 발급과정을 인터넷을 통한 온라인과정뿐만 아니라 사용자가 직접 한국정보인증을 방문하는 오프라인과정을 거쳐야 한다. OnePass에서는 범용 공인인증서(신용카드 및 핸드폰을 통한 본인확인 방식 불가)로만 추가적인 사용자 본인확인을 제공한다. 한국정보인증에서 제공하는 OnePass의 동작방식은 다음 [그림 18]과 같다.

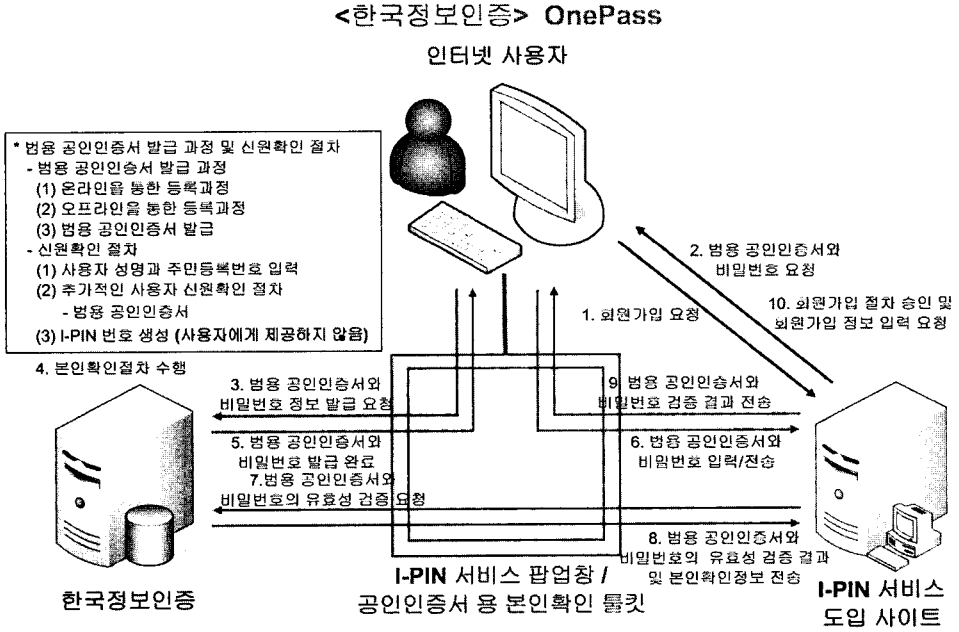
[OnePass 동작방식]

① 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트에서 사용자에게 범용 공인인증서와 해당 공인인증서의 비밀번호를 입력할 것을 요청한다.

③ 사용자가 한국정보인증 등과 같은 범용 공인인증서 발급기관에 접속하고 방문하여 OnePass의 이용을 요청한다.

④ 한국정보인증의 경우, 범용 공인인증서 발급과정



[그림 18] OnePass의 동작방식

중 온라인상에서 사용자에게 성명과 주민등록번호를 요청한다. 그리고 사용자가 직접 한국정보인증을 방문하여야 범용공인인증서를 발급 받을 수 있다. 범용 공인인증서가 있는 사용자만을 대상으로, OnePass를 이용하기 위한 본인확인과정을 거치고 사용자는 범용 공인인증서 비밀번호를 설정하게 된다. 이때 한국정보인증에서 생성한 I-PIN (13자리 식별자)은 사용자에게는 지급되지 않고, 사용자가가 홈페이지에 회원가입을 요청할 때 마다, 한국정보인증이 I-PIN 서비스 도입 사이트에 직접 사용자의 I-PIN 번호를 전송한다.

⑤ 한국정보인증에서는 범용 공인인증서를 사용자에게 발급하고 사용자가 OnePass를 이용하는 것을 허가한다.

⑥ 사용자는 I-PIN 서비스 도입 사이트에서 동작하는 I-PIN 팝업창에서 범용공인인증서를 선택하면, 공인인증서 용 본인확인 툴킷이 실행된다. 사용자는 툴킷에서 범용 공인인증서를 선택하고 비밀번호를 입력한다.

⑦ I-PIN 서비스 도입 사이트에서는 팝업창을 통해 사용자가 선택한 공인인증서와 비밀번호를 입력받아 한국정보인증에 전송하여 사용자 입력 값의 유효성 검증 요청을 한다.

⑧ 한국정보인증에서는 전달받은 사용자의 개인 ID와 비밀번호를 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 한국정보인증로부터 사용자 공인인증서와 비밀번호의 유효성 검증 결과를 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

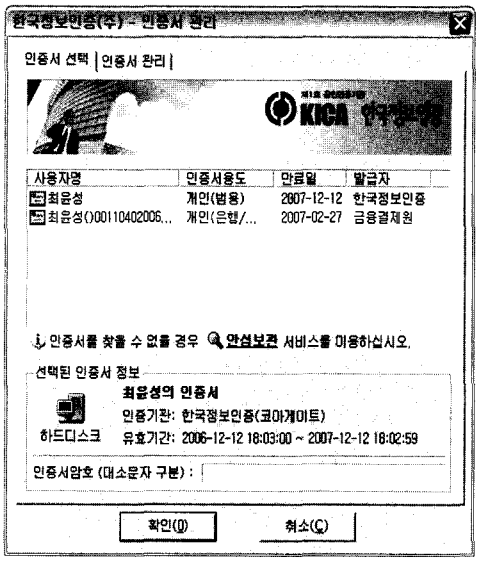
⑩ I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 주민등록번호의 입력을 제외한 추가적인 회원가입 절차를 진행하는 것을 허용한다.

[OnePass 팝업창]

OnePass에 사용되는 I-PIN 팝업창은 다음 〔그림 19〕와 같다.

3.5 한국전자인증의 그린버튼

한국전자인증에서 제공하는 그린버튼은 사용자가 정



〔그림 19〕 〔타입 1〕 OnePass 팝업창

당한 E-mail 주소와 비밀번호를 입력하면, 한국전자인증에서 사용자의 I-PIN 번호를 포함한 본인확인서(실명확인서)를 I-PIN 서비스 도입 사이트로 전송한다. 이 본인확인서는 사용자에게 전송되는 것이 아니라, 한국전자인증에서 생성하고 소유하고 있다. 이 본인확인서에는 사용자의 I-PIN, 이름, 연령대 코드 등이 포함되어 있다. 따라서 사용자가 자신의 I-PIN 번호를 확인하기 위해서는 그린버튼 홈페이지 (www.greenbutton.co.kr)에 접속하여야 한다. 한국전자인증에서 제공하는 그린버튼서비스의 동작방식은 다음 〔그림 20〕과 같다.

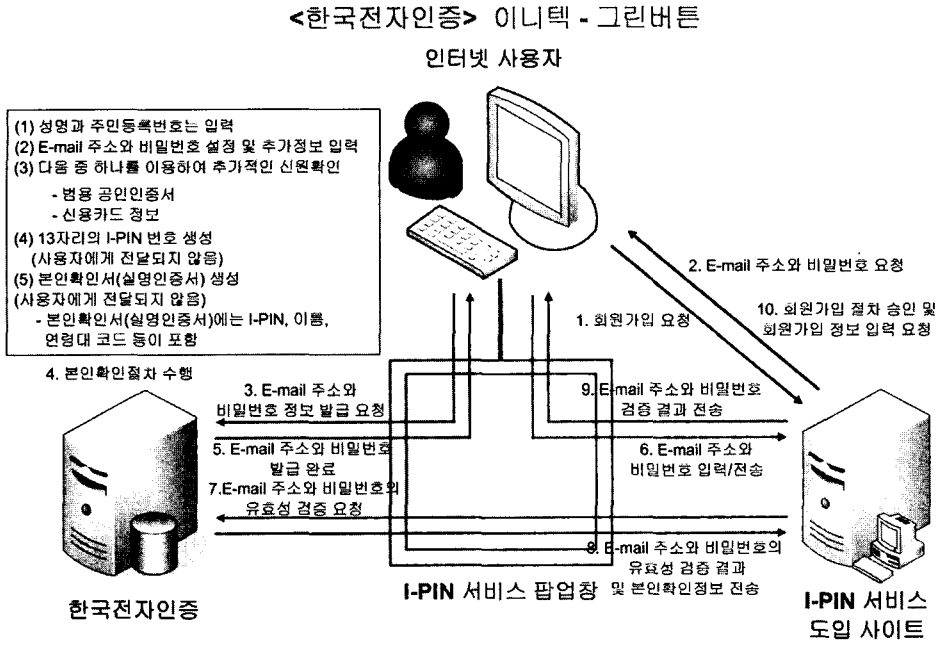
[그린버튼 동작방식]

① 사용자는 I-PIN 서비스 도입 사이트에서 회원가입을 요청한다.

② I-PIN 서비스 도입 사이트에서 사용자에게 그린버튼 용 E-mail 주소와 비밀번호를 입력할 것을 요청한다.

③ 사용자는 한국전자인증에 접속하여 그린버튼의 이용을 요청한다. 본인확인서(실명인증서)의 발급을 요청한다. 이때 본인확인서는 그린버튼 서버에 저장되며 사용자에게는 전송되지 않는다.

④ 한국전자인증은 사용자에게 성명과 주민등록번호를 요청하고 범용 공인인증서와 신용카드 정보를 이용하여 본인확인과정 과정을 수행한다. 그리고 사용자는 그린버튼에서 사용할 E-mail 주소와 비밀



〔그림 20〕 그린버튼의 동작방식

번호를 설정한다. 이때 한국전자인증에서 생성한 I-PIN(13자리 식별자)은 사용자에게는 지급되지 않으며, 사용자의 I-PIN, 이름, 연령대 코드 등이 포함된 본인확인서를 발급한다. 본인확인서는 그린버튼 서버에 저장되며 사용자에게는 전송되지 않는다.

⑤ 한국전자인증에서는 사용자가 설정한 E-mail 주소와 비밀번호의 사용을 허가하여 사용자가 그린버튼을 이용할 수 있도록 한다.

⑥ 사용자는 I-PIN 서비스 도입 사이트에서 동작하는 I-PIN 팝업창에서 그린버튼에서 사용하기로 설정한 E-mail 주소와 비밀번호를 입력하여 한국전자인증으로 전송한다.

⑦ I-PIN 서비스 도입 사이트에서는 팝업창을 통해 E-mail 주소와 비밀번호를 입력받아 한국전자인증에 사용자 입력값의 유효성 검증 요청을 한다.

⑧ 한국전자인증에서는 전달받은 사용자의 E-mail 주소와 비밀번호를 검사한 후, 유효성 검증 결과와 사용자의 기타정보를 I-PIN 서비스 도입 사이트에 전송한다.

⑨ 한국전자인증으로부터 사용자 E-mail 주소와 비밀번호의 유효성 검증 결과를 전송받은 I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 I-PIN 정보의 유효성 검증 결과를 전송한다.

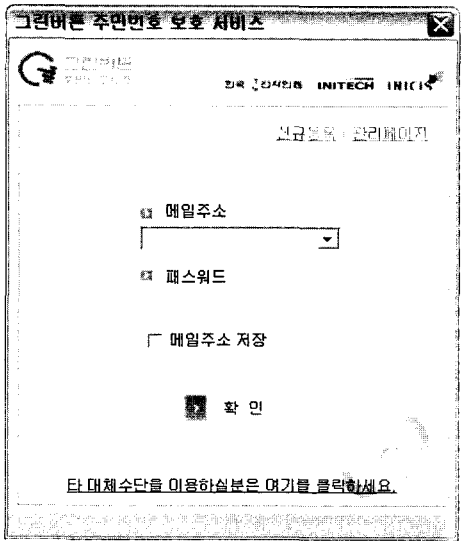
⑩ I-PIN 서비스 도입 사이트에서는 인터넷 사용자에게 주민등록번호의 입력을 제외한 추가적인 회원가입 절차를 진행하는 것을 허용한다.

[그린버튼 팝업창]

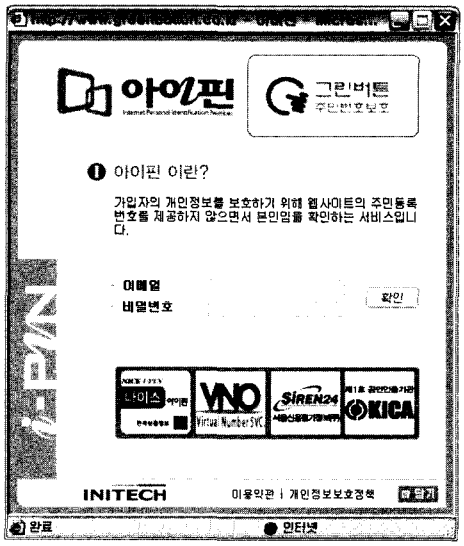
그린버튼에 사용되는 I-PIN 팝업창은 다음 〔그림 21〕과 〔그림 22〕와 같이 2가지로 분류할 수 있다. 〔그림 21〕은 5가지의 I-PIN 서비스 중에서, 기본적으로 그린버튼을 이용하여 회원가입을 제공하는 홈페이지에서 실행되는 I-PIN 팝업창이다. 〔그림 22〕는 타 I-PIN 서비스를 기본적으로 사용하는 홈페이지에서 실행되는 I-PIN 팝업창에 추가로 설치되어 있는 그린버튼 버튼을 눌렀을 때 실행되는 I-PIN 팝업창이다.

Ⅳ. I-PIN 서비스를 제공하는 홈페이지의 분석

정보통신부가 발표한 자료에 따르면 현재 I-PIN 서비스를 이용한 회원가입이나 Q/A 작성에 대한 권한을 제공하는 홈페이지는 총 17곳이다. 17개의 홈페이지가 제공하는 I-PIN 서비스는 홈페이지마다 차이가 있다. I-PIN 서비스가 잘 작동하여 사용에 불편함이 없는 홈페이지가 있는 반면에, I-PIN 서비스가 제대로 동작하지 않아서 사용자로 하여금 회원가입에 불편함을 느끼



〔그림 21〕 〔타입 1〕 그린버튼 팝업창

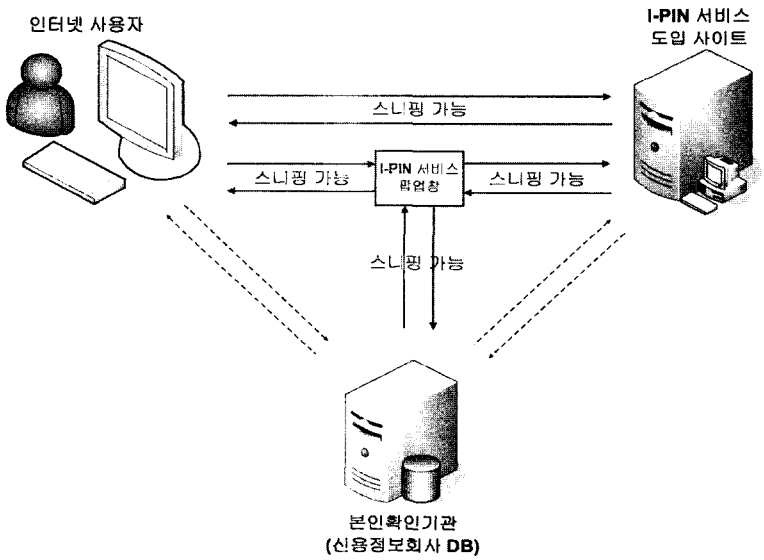


〔그림 22〕 〔타입 2〕 그린버튼 팝업창

게 하는 홈페이지도 있다. 그리고 17개의 홈페이지 중에서 현재 I-PIN 서비스를 이용한 회원가입을 제공하지 않는 곳도 있다. 우선 〔표 4〕에서는 I-PIN 서비스를 제공하는 홈페이지를 분석한 자료와 특징을 정리하였다.

〔표 4〕에서 설명하는 것과 같이, 정보통신부 홈페이지의 경우에는 사용자가 성명과 가상주민번호를 입력할 때, 정보통신부 홈페이지에서 지원하는 보안접속(SSL)을 선택하더라도 사용자의 가상주민번호가 노출된다. 그리고 KMPS 인트라넷 홈페이지 경우에는 I-PIN 서비스를 이용하고자 할 때, KMPS의 사내 ID와 비밀번호가 필요하여 구체한 분석이 어려워서 아래 인터넷 사이트별 분석자료에서 생략하였다. 그리고 영등포구청 홈페이지에서 제공하는 I-PIN 서비스에서는 별다른 취약점이 발견되지 않아 아래 인터넷 사이트 별 분석자료에서 생략하였다.

I-PIN 서비스를 이용한 17개 홈페이지의 분석과정에



〔그림 23〕 I-PIN 서비스 팝업창을 이용한 사용자 I-PIN 정보 입력방식에서의 스니핑

〔표 4〕 현재 I-PIN 서비스를 이용한 회원가입이나 Q/A 작성에 대한 권한을 제공하는 홈페이지 분석

사이트 종류	No	사이트 명	도입 목적	기본적인 I-PIN 서비스	서비스 개시일	타 I-PIN 서비스 지원여부	비고
공공기관	[01]	정보통신부[09] (http://www.mic.go.kr)	회원가입	가상주민번호	05.09.13	X	-
				OnePass	05.10.24	X	-
	[02]	정보보호기술 훈련장[10] (http://www.sis.or.kr)	회원가입	OnePass	06.03.02	○	-
				가상주민번호	06.07.14	X	-
	[03]	인터넷침해사고 대응지원센터[11] (http://www.krcert.or.kr)	회원가입	나이스아이핀	05.10.26	○	-
				OnePass	06.04.12	○	-
	[04]	김포시청[12] (http://www.gimpo.go.kr)	회원가입	Siren24아이핀	06.05.01	X	-
	[05]	영등포구청[13] (http://www.ydp.go.kr)	회원가입 및 Q&A 작성	Siren24아이핀	06.05.08	X	-
	[06]	한국정보문화진흥원[14] (http://www.kado.or.kr)	회원가입	나이스아이핀	06.06.23	○	-
	[07]	한국소프트웨어진흥원[15] (http://www.software.or.kr)	회원가입	가상주민번호	06.06.30	X	-
				OnePass	?	X	-
	[08]	정보통신연구진흥원[16] (http://www.iita.re.kr)	회원가입	가상주민번호	06.07.05	X	I-PIN 서비스를 이용할 때 주민등록번호를 추가로 입력해야 함
	[09]	충북도청[17] (http://www.cb21.net)	회원가입	Siren24아이핀	06.08.08	○	1월9일 현재 I-PIN 서비스를 이용한 회원가입 불가
	[10]	IT수출정보데이터베이스[18] (http://www.itx.or.kr)	회원가입	Siren24아이핀	06.08.24	○	-
본인확인기관	[11]	한국신용정보[19] (http://www.nice.co.kr)	Q&A (게시물 게재)	나이스아이핀	05.08.30	○	-
	[12]	서울신용평가정보[20] (http://www.sci.co.kr)	Q&A (게시물 게재)	Siren24아이핀	06.01.31	○	-
민간업체	[13]	라이크호스트[21] (http://www.likehost.com)	회원가입	OnePass	05.04.20	○	-
	[14]	쎌덤[22] (http://www.celldom.co.kr)	회원가입	가상주민번호	05.08.01	X	1월9일 현재 I-PIN 서비스를 이용한 회원가입 불가
	[15]	칠리칠리닷컴[23] (http://www.chili72.com)	회원가입	가상주민번호	06.07.25	○	-
	[16]	테크노비전[24] (http://www.technovision.co.kr)	A/S 신청을 위한 회원가입	그린버튼	05.08.09	○	-
	[17]	KMPS 인트라넷[25] (https://pay.kmps.co.kr)	사내 인트라넷 회원가입	그린버튼	06.02.07	X	KMPS의 사내 ID 및 비밀번호 필요

대해서 자세히 살펴보면 다음과 같다. 17개의 홈페이지에 대한 분석실험에는 네트워크 트래픽 모니터링/분석 도구인 Ethereal v0.99.0을 사용하였다. 우선 5가지 I-PIN 서비스에 등록하고 각각의 홈페이지에서 회원가입을 요청한 후, 홈페이지에서 제공하는 모든 I-PIN 서비스를 이용하여 회원가입을 시도하였다. 이 과정에서 정당한 사용자만 알고 있어야 하는 I-PIN 관련 중요정보 및 개인정보가 노출되지는 않는지 분석하였다. 2장에서 살펴본 바와 같이 사용자가 I-PIN 서비스를 제공받기 위해서 자신의 I-PIN 정보를 전송하는 과정은 크게 I-PIN 팝업창을 이용하는 방식과 I-PIN 서비스 도입 사이트에 I-PIN 정보를 직접 입력하는 방식이 있다. 이 두 가지 방식에 따라 분석할 수 있는 범위는 차이가 있다. 〔그림 23〕은 I-PIN 팝업창을 이용한 I-PIN 입력방식에서 본 실험과정과 관련이 있으면서 스니핑(Sniffing)이 가능한 통신과정 및 통신내용을 붉은 실선으로 나타내고 있다.

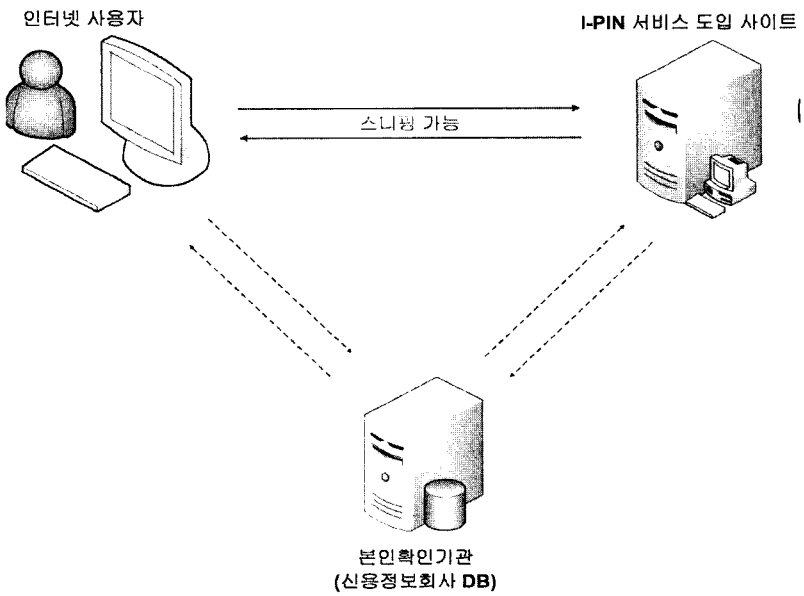
〔그림 23〕에서처럼 사용자가 I-PIN 팝업창을 이용해 I-PIN 정보를 입력할 때에는 인터넷 사용자와 I-PIN 서비스 도입 사이트와 본인확인기관 간의 통신이 모두 인터넷 사용자를 통해서 전달된다. 그것은 I-PIN 관련 통신은 모두 I-PIN 팝업창을 통한 HTTP 나 HTTPS 방식으로 이루어지기 때문이다. 그러므로 사용자 PC나 사용자와 연결되어 있는 허브에서는 사용자와 I-PIN 서비스 도입 사이트 간의 통신내용, 사용자와 I-PIN 팝업창 간의 통신내용이 모두 스니핑이 가능하다.

하지만 I-PIN 팝업창을 통하지 않는 I-PIN 서비스 도입 사이트와 본인확인기관과의 통신내용은 본 논문의 실험과정에서는 스니핑을 할 수 없다. 그리고 I-PIN 팝업창을 통하지 않는 인터넷 사용자와 본인확인기관 간의 통신은 인터넷 사용자가 본인확인기관 홈페이지에 접속하여 자료를 검색하거나 회원가입을 하는 것과 같은 내용으로 이루어진다. 이것은 본 실험과정과는 무관하므로 통신을 스니핑하는 대상에서 배제한다.

〔그림 24〕는 I-PIN 서비스 도입 사이트에서 사용자의 I-PIN 정보를 입력받을 때, 스니핑이 가능한 통신과정 및 통신내용을 붉은 실선으로 나타내고 있다.

〔그림 23〕과 마찬가지로, 〔그림 24〕에서도 I-PIN 팝업창을 통하지 않는 I-PIN 서비스 도입 사이트와 본인확인기관과의 통신내용은 본 논문의 실험과정에서는 스니핑을 할 수 없다. 그리고 I-PIN 팝업창을 통하지 않는 인터넷 사용자와 본인확인기관 간의 통신은 인터넷 사용자가 본인확인기관 홈페이지에 접속하여 자료를 검색하거나 회원가입을 하는 것과 같은 내용으로 이루어진다. 이것은 본 실험과정과는 무관하므로 통신을 스니핑하는 대상에서 배제한다. 그러므로 사용자와 I-PIN 서비스 도입 사이트간의 통신내용만 스니핑이 가능하다.

지금부터 현재 I-PIN 서비스를 이용한 회원가입을 제공하는 17개 홈페이지에 대해서 수행한 I-PIN 관련 정



〔그림 24〕 I-PIN 서비스 도입 사이트에서의 사용자 I-PIN 정보 입력방식에서의 스니핑

〔표 5〕 정보통신부 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설명
가상주민번호 (가상주민번호를 I-PIN 서비스 도입 사이트에 직접입력)	타입 5	단계 6	그림 25	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 가상주민번호를 이용하여 정보통신부에 회원가입을 하기 위해서, 홈페이지 상에 입력한 가상주민등록번호[5216414811635]가 평문으로 노출되었다. - 노출된 가상주민번호를 이용하면, 해당 가상주민번호의 사용자로 위장하여 가상주민번호를 지원하는 홈페이지에 회원가입이 가능하다.
	가상주민번호 조회 과정	단계 6	그림 26	- [2007년 1월 8일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 가상주민번호를 조회하는 과정에서는 식별 ID[oneoneeyes]와 비밀번호[cys420]를 사용한다. 이 과정에서 입력되지 않은 사용자의 가상주민등록번호[5216414811635]와 주민등록번호[82042010****2]가 평문으로 노출되었다. 이 현상은 사용자가 입력한 식별 ID와 비밀번호를 한국신용평가정보로 전송한 후, 한국신용평가정보의 가상주민번호 조회 결과에 사용자의 주민등록번호가 포함되어 있기 때문이다. - 노출된 가상주민번호를 이용하면, 해당 가상주민번호의 사용자로 위장하여 가상주민번호를 지원하는 홈페이지에 회원가입이 가능하다.
중복가입 가능 여부				- 한 사용자는 정보통신부 홈페이지에서 2개의 서로 다른 ID를 생성할 수 있다.
오류 발생 여부				- 해당 사항 없음

보 노출 실험결과에 대해서 알아보겠다. 본 실험은 2006년 12월에서 2007년 1월 사이에 수행되었으며, 실험기간 중 취약성이 확인된 최신 데이터를 이용하여 분석하였다. 4장의 1절~15절에서는 각 홈페이지에 대한 정보노출에 대한 실험분석 결과에 대해서 살펴본다. 위에서 설명하였듯이, KMPS 인트라넷 홈페이지와 영등포구청 홈페이지에 관한 분석한 결과는 취약성을 확인할 수 없는 관계로 본 아래 분석 자료에서는 생략하였다.

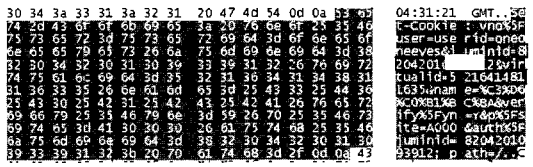
본 실험의 분석에 사용된 데이터들은 I-PIN 서비스를 이용하고 있는 사용자 PC에서 네트워크 트래픽 모니터링/분석 도구인 Ethereal v0.99.0을 이용하여 수집된 것이다. 각 홈페이지 분석 결과 중 설명에 명시된 날짜는 해당 그림에서 보이는 데이터가 수집된 시간을 보여주고 있다.

이제부터는 I-PIN 서비스를 이용한 회원가입을 제공하는 공공기관 사이트들에 대해서 알아본다.

1. [01] 정보통신부 홈페이지 분석

정보통신부 홈페이지에서는 가상주민번호와 OnePass를 기본적으로 제공한다. 다른 I-PIN 서비스는 지원하지 않는다. 사용자가 정보통신부 홈페이지에서 가상주민번호를 이용하기 위해서 자신의 가상주민번호를 홈페이지 상에 입력하는 과정이 보안접속임에도 불구하고, 입력하는 가상주민등록번호가 평문으로 노출된다.

〔그림 25〕 〔가상주민번호〕 I-PIN 번호의 노출



〔그림 26〕 〔가상주민번호〕
I-PIN 번호와 주민등록번호 번호의 노출

2. [02] 정보보호기술 훈련장 분석

정보보호기술 훈련장은 가상주민번호와 OnePass를 기본적으로 제공한다. 다른 I-PIN 서비스를 통한 회원가입은 제공하는데, 이때 그린버튼의 I-PIN 번호와 Siren24아이핀의 개인 ID와 비밀번호가 평문으로 노출

〔표 6〕 정보보호기술 훈련장 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설명
그린버튼	타입 1	단계 9	그림 27	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 정보보호기술 훈련장 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
Siren24 아이핀	타입 3	단계 6	그림 28	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀 팝업창[타입 3]에 입력한 개인 ID[gosky37]와 비밀번호[cys420]가 평문으로 서울신용평가정보로 전송된다. - 노출된 개인 ID와 비밀번호를 이용하면, 해당 개인 ID의 사용자로 위장하여 Siren24 아이핀을 지원하는 다른 홈페이지에 회원가입이 가능하다.
중복가입 가능 여부				- 한 사용자는 정보보호기술 훈련장 홈페이지에 4개의 서로 다른 ID를 생성할 수 있다.
오류 발생 여부				- 나이스아이핀은 본인확인 과정에서 오류가 발생한다.

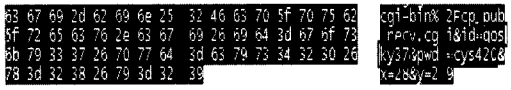
되므로 획득 가능하다. 그리고 나이스아이핀을 이용 시 오류가 발생한다.

〔그림 27〕 〔그린버튼〕 I-PIN 번호의 노출

〔그림 28〕 〔Siren24아이핀〕 개인 ID와 비밀번호 노출

3. [03] 인터넷침해사고 대응지원센터 분석

인터넷침해사고 대응지원센터 홈페이지에서는 나이스아이핀과 OnePass를 기본적으로 제공한다. 기본적으로 제공되는 2개의 I-PIN 서비스에서 각각 연결되는 다른 4개의 I-PIN 서비스를 이용한 회원가입을 지원하고 있다. 인터넷침해사고 대응지원센터 홈페이지에서는 I-PIN 서비스를 이용한 본인확인 과정에서 오류가 많이 발생하는데, 〔표 7〕에서 인터넷침해사고 대응지원센터 홈페이지에서 발생하는 I-PIN 서비스 관련 오류사항을 정리하였다. 또한 나이스아이핀을 회원가입을 할 때 사용자의 식별자가 평문으로 노출된다. 그리고 그린버튼은 회원가입 시 오류가 발생하더라도 I-PIN 번호가 평문으로 노출된다. Siren24 아이핀에서는 개인 ID와 비밀번호가 평문으로 노출된다.



〔그림 29〕 〔Siren24아이핀〕 개인 ID와 비밀번호의 노출

〔그림 30〕 〔그린버튼〕 I-PIN 번호의 노출

〔표 7〕 인터넷침해사고 대응지원센터 홈페이지의 I-PIN 서비스 오류 현황

기본적인 대체수단명	인터넷침해사고 대응지원센터의 I-PIN 서비스 오류 현황				
	나이스아이핀	가상주민번호	Siren24아이핀	OnePass	그린버튼
나이스아이핀	오류	오류	오류	오류	오류
OnePass	오류	오류	정상적으로 동작	정상적으로 동작	정상적으로 동작

〔표 8〕 인터넷침해사고 대응지원센터 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
Siren24 아이핀	타입 3	단계 6	그림 29	- [2007년 1월 8일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀 팝업창[타입 3]에 입력한 개인 ID[gosky37]와 비밀번호[cys420]가 평문으로 서울신용평가정보로 전송된다. - 노출된 개인 ID와 비밀번호를 이용하면, 해당 개인 ID의 사용자로 위장하여 Siren24 아이핀을 지원하는 다른 홈페이지에 회원가입이 가능하다.
그린버튼	타입 1	단계 9	그림 30	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 인터넷침해사고 대응지원센터 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 인터넷침해사고 대응지원센터 홈페이지에 3개의 서로 다른 ID를 생성할 수 있다.
오류 발생 여부				- 나이스아이핀 팝업창이 기본적으로 실행되었을 때는 나이스아이핀 뿐만 아니라, 가상주민번호, Siren24아이핀, 범용 공인인증서, 그린버튼 모두 오류가 발생한다. - OnePass가 기본적으로 실행되었을 때는 나이스아이핀 뿐만 아니라, 가상주민번호도 오류가 발생한다.

4. [04] 김포시청 분석

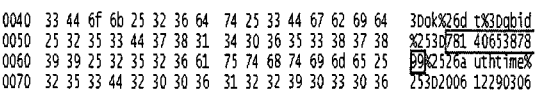
김포시청 홈페이지에서는 Siren24아이핀을 이용한 회원가입만을 지원한다. 이때 Siren24아이핀의 I-PIN 번호가 평문을 전송되어 노출되므로 획득 가능하다.

〔그림 31〕 〔Siren24아이핀〕 I-PIN 번호의 노출

5. [06] 한국정보문화진흥원 홈페이지 분석

한국정보문화진흥원 홈페이지에서는 기본적으로 나이스아이핀을 제공하며, 다른 4개의 I-PIN 서비스도 이용가능하다. 하지만 나이스아이핀과 OnePass 그리고 그린버튼에서를 이용한 본인확인 과정에서 사용자에게 할당된 I-PIN 번호가 평문으로 노출된다. 그리고 가상주민번호와 Siren24아이핀은 오류가 발생한다.

〔그림 32〕 〔나이스아이핀〕 I-PIN 번호의 노출



〔그림 33〕 〔그린버튼〕 I-PIN 번호의 노출

〔표 9〕 김포시청 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
Siren24 아이핀	타입 2	단계 6	그림 31	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 김포시청 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- Siren24아이핀만을 지원한다.
오류 발생 여부				- I-PIN 서비스 관련 오류가 발생하지 않는다.

〔표 10〕 한국정보문화진흥원 홈페이지 분석 결과

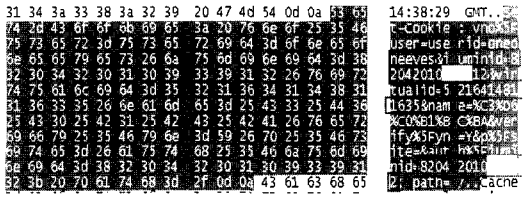
서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
나이스 아이핀	타입 1	단계 9	그림 32	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - 나이스아이핀을 이용한 본인확인 절차가 완료된 뒤, 한국신용정보에서 한국정보문화진흥원 홈페이지로 전송된 사용자의 I-PIN 번호[4915581064325]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 하지만 나이스아이핀은 사용자에게 홈페이지 마다 다른 I-PIN 번호를 할당하기 때문에 다른 I-PIN 서비스에서 I-PIN 번호가 노출되는 경우와 달리, 해당 I-PIN 번호의 사용자가 나이스아이핀을 이용하여 가입하는 홈페이지를 알아낼 수는 없다
그린버튼	타입 1	단계 9	그림 33	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 한국정보문화진흥원 홈페이지로 전송된 사용자의 I-PIN 번호[78140653878 99]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
OnePass	타입 1	단계 9	그림 34	- [2007년 1월 9일에 수집된 네트워크 패킷을 이용한 실험결과] - OnePass를 이용한 본인확인 절차가 완료된 뒤, 한국정보인증에서 한국정보문화진흥원 홈페이지로 전송된 사용자의 I-PIN 번호[3517368115561]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 한국정보문화진흥원 홈페이지에 3개의 서로 다른 ID를 생성할 수 있다.
오류 발생 여부				- 가상주민번호는 본인확인 과정에서 오류가 발생한다. - Siren24아이핀은 본인확인 과정에서 오류가 발생한다.

그림 34. (OnePass) I-PIN 번호의 노출

〔그림 36〕 〔가상주민번호〕 식별 ID와 비밀번호의 노출

6. [07] 한국소프트웨어진흥원 홈페이지 분석

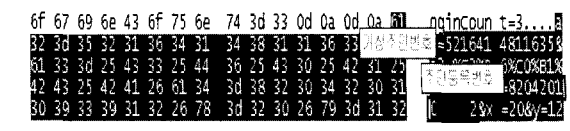
한국소프트웨어진흥원 홈페이지에서는 가상주민번호와 OnePass를 기본적으로 제공한다. OnePass를 이용하여 회원가입을 하고자 할 때 오류가 발생하여 정상적으로 회원에 가입할 수 없다



〔그림 35〕 〔가상주민번호〕 I-PIN 번호 및 주민등록번호 노출

7. [08] 정보통신연구진흥원 홈페이지 분석

정보통신연구진흥원 홈페이지에서는 가상주민번호만을 제공하며, 다른 I-PIN 서비스는 지원하지 않는다. 사용자가 가상주민번호를 입력하는 과정에서 사용자의 I-PIN 번호가 노출된다. 뿐만 아니라, 가상주민번호를 이용하는데 반드시 사용자의 주민등록번호를 입력하여야 하는 문제가 있다.



〔그림 37〕 〔가상주민번호〕 I-PIN 번호와 주민등록번호의 노출

〔표 11〕 한국소프트웨어진흥원 홈페이지 분석 결과

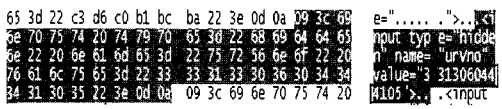
서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
가상주민번호 (가상주민번호를 I-PIN 서비스 도입 사이트에 직접입력)	가상주민번호 조회 과정	단계 6	그림 35	- [2007년 1월 7일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 가상주민번호를 조회하는 과정에서는 식별 ID[oneoneeyes]와 비밀번호 [cys420]을 사용한다. 이 과정에서 입력되지 않은 사용자의 가상주민등록번호 [5216414811635]와 주민등록번호[82042010****2]가 평문으로 노출되었다. 이 현상은 사용자가 입력한 식별 ID와 비밀번호를 한국신용평가정보로 전송한 후, 한국신용평가정보의 가상주민번호 조회 결과에 사용자의 주민등록번호가 포함되어 있기 때문이다. - 노출된 가상주민번호를 이용하면, 해당 가상주민번호의 사용자로 위장하여 가상주민번호를 지원하는 홈페이지에 회원가입이 가능하다.
			그림 36	- [2007년 1월 7일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 가상주민번호를 조회하는 과정에서 식별 ID[oneoneeyes]와 비밀번호 [cys420]가 평문으로 노출된다. 노출된 식별 ID와 비밀번호를 이용하면, 해당 사용자의 I-PIN 번호를 알아 낼 수 있다. - 알아낸 I-PIN 번호로 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
중복가입 가능 여부				- 지원하는 2가지의 I-PIN 서비스 중 1가지 I-PIN 서비스에서 오류가 발생하여 중복 가입이 되지 않는다.
오류 발생 여부				- OnePass는 본인확인 과정에서 오류가 발생한다.
특이 사항				- 사용자가 입력하지 않은 주민등록번호도 노출된다.

〔표 12〕 정보통신연구진흥원 홈페이지 분석 결과

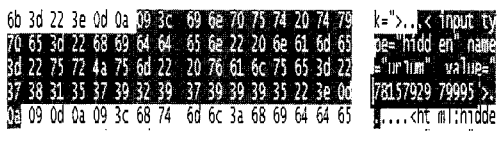
서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설명
가상주민번호 (가상주민번호를 I-PIN 서비스 도입 사이트에 직접입력)	타입 5	단계 6	그림 37	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - 정보통신연구진흥원 홈페이지에 회원가입을 하기 위해서는 가상주민번호뿐만 아니라 반드시 사용자의 주민등록번호를 입력하여야 하는 문제가 있다. 그리고 이 과정에서 입력한 가상주민등록번호와 주민등록번호[82042010****2]가 평문으로 노출된다. - 노출된 가상주민번호를 이용하면, 해당 가상주민번호의 사용자로 위장하여 가상주민번호를 지원하는 타 홈페이지에 회원가입 가능하다.
중복가입 가능 여부				- 가상주민번호만을 지원하여 중복가입이 되지 않는다.
특이 사항				- I-PIN 서비스를 사용하는데 반드시 사용자의 주민등록번호를 입력해야 한다.

8. [09] 충북도청 홈페이지 분석

충북도청 홈페이지에서는 기본적으로 Siren24 아이핀을 제공하며, 다른 4개의 I-PIN 서비스를 이용한 회원가입도 제공한다. 다른 4개의 I-PIN 서비스를 이용해서 회원가입을 할 때 오류가 발생하여 정상적인 회원가입이 되지 않는다. 뿐만 아니라, 5개의 I-PIN 서비스에서 모두 사용자의 I-PIN 번호가 노출된다. 충북도청은 2007년 1월 2일부터 I-PIN을 이용한 회원가입을 제공하지 않는다. 본 실험결과는 2006년 12월에 수행한 실험에서 나온 결과이다.



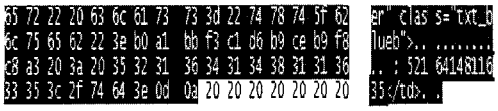
〔그림 38〕 〔Siren24아이핀〕 I-PIN 번호의 노출



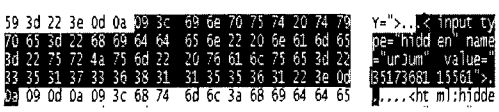
〔그림 39〕 〔나이스아이핀〕 I-PIN 번호의 노출

〔표 13〕 충북도청 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설명
Siren24 아이핀	타입 1	단계 8	그림 38	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
나이스아이핀	타입 2	단계 8	그림 39	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - 나이스아이핀을 이용한 본인확인 절차가 완료된 뒤, 한국신용정보에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[7815792979995]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 하지만 나이스아이핀은 사용자에게 홈페이지 마다 다른 I-PIN 번호를 할당하기 때문에, 다른 I-PIN 서비스에서 I-PIN 번호가 노출되는 경우와 달리, 해당 I-PIN 번호의 사용자가 나이스아이핀을 이용하여 가입하는 홈페이지를 알아낼 수는 없다
가상주민번호 (I-PIN 팝업창 사용방식)	타입 3	단계 8	그림 40	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - 가상주민번호를 이용한 본인확인 절차가 완료된 뒤, 한국신용평가정보 중에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[5216414811635]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 가상주민번호를 이용하면 해당 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
OnePass	타입 1	단계 8	그림 41	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - OnePass를 이용한 본인확인 절차가 완료된 뒤, 한국정보인증에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[3517368115561]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 OnePass를 이용하여 가입하는 홈페이지를 알아낼 수 있다.
그린버튼	타입 1	단계 8	그림 42	- [2006년 12월 22일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 한국정보문화진흥원 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 5가지의 I-PIN 서비스 중 4가지 I-PIN 서비스에서 오류가 발생하여 중복 가입이 되지 않는다.
오류 발생 여부				- 나이스아이핀은 본인확인 과정에서 오류가 발생한다. - 가상주민번호는 본인확인 과정에서 오류 발생한다. - OnePass는 본인확인 과정에서 오류가 발생한다. - 그린버튼은 본인확인 과정에서 오류가 발생한다.
특이 사항				- 1월 2일부터 I-PIN 서비스를 이용한 회원가입을 제공하지 않는다.



〔그림 40〕〔가상주민번호〕 I-PIN 번호의 노출

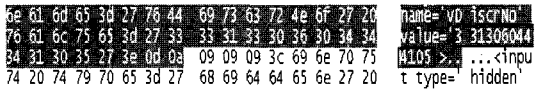


〔그림 41〕〔OnePass〕 I-PIN 번호의 노출

〔그림 42〕〔그린버튼〕 I-PIN 번호의 노출

9. [10] IT수출정보데이터베이스 홈페이지 분석

IT수출정보데이터베이스 홈페이지에서는 기본적으로 Siren24 아이핀을 제공하며, 다른 4개의 I-PIN 서비스를 이용한 회원가입도 제공한다. 다른 4개의 I-PIN 서비스를 이용해서 회원가입을 할 때는 오류가 발생하여 정상적인 회원가입이 되지 않는다. 뿐만 아니라, Siren24아이핀과 그린버튼을 이용할 때 사용자의 I-PIN 번호가 노출되는 문제가 있다.



〔그림 43〕〔Siren24아이핀〕 I-PIN 번호의 노출

〔그림 44〕〔그린버튼〕 I-PIN 번호의 노출

지금까지는 I-PIN 서비스를 이용한 회원가입을 제공하는 공공기관 홈페이지에 대한 I-PIN 관련 실험 결과를 알아보았다. 이제부터는 I-PIN 서비스를 이용한 회원가입을 제공하는 본인확인기관 홈페이지에 대한 I-PIN 관련 실험 결과를 알아본다. 본인확인기관은 사용자에게 I-PIN 서비스를 제공하는 기관이다.

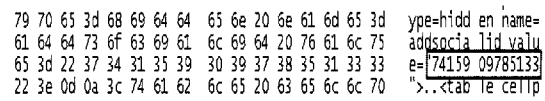
10. [11] 한국신용정보 홈페이지 분석

한국신용정보 홈페이지에서는 I-PIN 서비스 도입 사이트의 게시판에 글을 쓰는 권한을 I-PIN 서비스를 통하여 로그인을 한 사용자에게 제공한다. 기본적으로는 나이스아이핀을 제공하며, 다른 4개의 I-PIN 서비스도 이용이 가능하다. 5가지의 I-PIN 서비스 회원가입을 하

〔표 14〕 IT 수출정보데이터베이스 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설명
Siren24 아이핀	타입 1	단계 9	그림 43	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지 간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
그린버튼	타입 2	단계 9	그림 44	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 한국정보문화진흥원 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 5가지의 I-PIN 서비스 중 4가지 I-PIN 서비스에서 오류가 발생하여 중복 가입이 되지 않는다.
오류 발생 여부				- 나이스아이핀은 본인확인 과정에서 오류가 발생한다. - 가상주민번호는 본인확인 과정에서 오류가 발생한다. - OnePass는 본인확인 과정에서 오류가 발생한다. - 그린버튼은 본인확인 과정에서 오류가 발생한다.

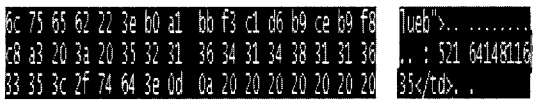
는 과정에서 사용자의 I-PIN 번호가 평문으로 노출된다. 그리고 Siren24아이핀에서는 사용자의 개인 ID가 노출된다.



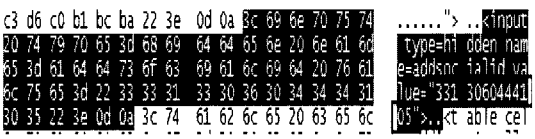
〔그림 45〕〔나이스아이핀〕 I-PIN 번호의 노출

〔표 15〕 한국신용정보 홈페이지 분석 결과

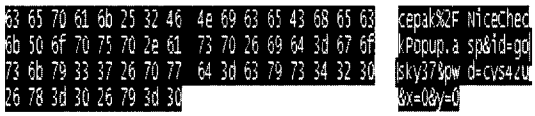
서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
나이스 아이핀	타입 1	단계 9	그림 45	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 나이스아이핀을 이용한 본인확인 절차가 완료된 뒤, 한국신용정보에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[7415909785133]가 사용자와 홈페이지 간의 통신에서 평문으로 노출된다. - 하지만 나이스아이핀은 사용자에게 홈페이지 마다 다른 I-PIN 번호를 할당하기 때문에, 다른 I-PIN 서비스에서 I-PIN 번호가 노출되는 경우와 달리, 해당 I-PIN 번호의 사용자가 나이스아이핀을 이용하여 가입하는 홈페이지를 알아낼 수는 없다.
가상 주민번호 (I-PIN 팝업창 사용방식)	타입 3	단계 9	그림 46	- [2007년 1월 4일에 수집된 네트워크 패킷을 이용한 실험결과] - 가상주민번호를 이용한 본인확인 절차가 완료된 뒤, 한국신용평가정보 증에서 충북도청 홈페이지로 전송된 사용자의 I-PIN 번호[5216414811635]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 가상주민번호를 이용하면 해당 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
Siren24 아이핀	타입 3	단계 9	그림 47	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 한국신용정보 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
		단계 6	그림 48	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀 팝업창[타입 3]에 입력한 개인 ID[gosky37]와 비밀번호[cys420]가 평문으로 서울신용평가정보로 전송된다. - 노출된 개인 ID와 비밀번호를 이용하면, 해당 개인 ID의 사용자로 위장하여 Siren24 아이핀을 지원하는 다른 홈페이지에 회원가입이 가능하다.
그린버튼	타입 1	단계 9	그림 49	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 한국신용정보 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
OnePass	타입 1	단계 9	그림 50	- [2007년 1월 9일에 수집된 네트워크 패킷을 이용한 실험결과] - OnePass를 이용한 본인확인 절차가 완료된 뒤, 한국정보인증에서 한국신용정보 홈페이지로 전송된 사용자의 I-PIN 번호[3517368115561]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 OnePass를 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 한국신용정보 홈페이지에 5명의 서로 다른 신분으로 게시판에 글을 적을 수 있다.
오류 발생 여부				- 해당 사항 없음



〔그림 46〕〔가상주민번호〕 I-PIN 번호의 노출



〔그림 47〕〔Siren24아이핀〕 I-PIN 번호의 노출



〔그림 48〕〔Siren24아이핀〕 개인 ID/PW의 노출

〔그림 49〕〔그린버튼〕 I-PIN 번호의 노출

〔그림 50〕〔OnePass〕 I-PIN 번호의 노출

11. [12] 서울신용평가정보 분석

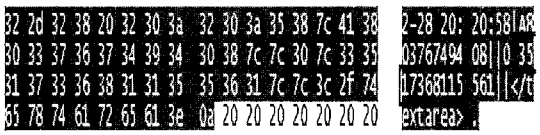
서울신용평가정보 홈페이지에서는 사용자가 게시판에 글을 작성하기 위해서 I-PIN 서비스를 통해서 로그인하여야 한다. 기본적으로 Siren24아이핀을 제공하며, 다른 4개의 I-PIN 서비스도 사용 가능하다. 하지만 그린버튼의 I-PIN 번호가 평문으로 노출된다.

〔그림 51〕〔그린버튼〕 I-PIN 번호의 노출

지금까지는 I-PIN 서비스를 이용한 회원가입을 제공하는 본인확인기관의 홈페이지에 대한 I-PIN 관련 실험 결과를 알아보았다. 이제부터는 민간업체의 홈페이지에 대한 I-PIN 실험 결과를 알아본다.

12. [13] 라이크호스트 홈페이지 분석

라이크호스트 홈페이지는 17개의 홈페이지 중에서 I-PIN 서비스를 가장 먼저 도입하였다. 라이크호스트는 OnePass를 기본적으로 제공하며 타 I-PIN을 이용한 회원가입도 가능하다. 하지만 5개의 I-PIN 서비스 모두, 회원가입 과정에서 I-PIN 번호가 노출되는 문제점이 있다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. 뿐만 아니라, Siren24아이핀에서는 사용자의 개인 ID와 비밀번호가 획득 가능하다



〔그림 52〕〔OnePass〕 I-PIN 번호의 노출

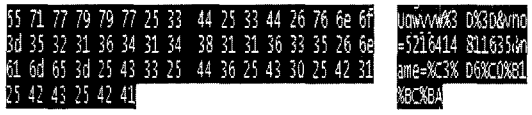
〔표 16〕 서울신용평가정보 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
그린버튼	타입 1	단계 9	그림 51	- 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 서울신용평가정보 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지 간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 서울신용평가정보 홈페이지에 5개의 서로 다른 ID를 생성할 수 있음
오류 발생 여부				- 해당 사항 없음

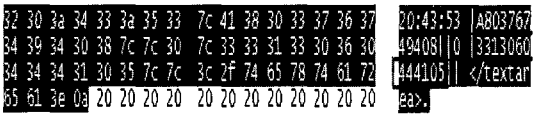
〔표 17〕 라이크호스트 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
OnePass	타입 1	단계 9	그림 52	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - OnePass를 이용한 본인확인 절차가 완료된 뒤, 한국정보인증에서 라이크호스트 홈페이지로 전송된 사용자의 I-PIN 번호[3517368115561]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 OnePass를 이용하여 가입하는 홈페이지를 알아낼 수 있다.
나이스 아이핀	타입 2	단계 9	그림 53	- [2006년 12월 21일에 수집된 네트워크 패킷을 이용한 실험결과] - 나이스아이핀을 이용한 본인확인 절차가 완료된 뒤, 한국신용정보에서 라이크 호스트 홈페이지로 전송된 사용자의 I-PIN 번호 [5315717299686]가 사용자와 홈페이지 간의 통신에서 평문으로 노출된다. - 하지만 나이스아이핀은 사용자에게 홈페이지 마다 다른 I-PIN 번호를 할당하기 때문에, 다른 I-PIN 서비스에서 I-PIN 번호가 노출되는 경우와 달리, 해당 I-PIN 번호의 사용자가 나이스아이핀을 이용하여 가입하는 홈페이지를 알아낼 수는 없다.
가상 주민번호 (I-PIN 팝업창 사용방식)	타입 3	단계 9	그림 54	- [2007년 1월 4일에 수집된 네트워크 패킷을 이용한 실험결과] - 가상주민번호를 이용한 본인확인 절차가 완료된 뒤, 한국신용평가정보 중에서 라이크호스트 홈페이지로 전송된 사용자의 I-PIN 번호[5216414811635]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 가상주민번호를 이용하면 해당 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
Siren24 아이핀	타입 3	단계 9	그림 55	- [2006년 12월 21일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 한국신용정보 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
		단계 6	그림 56	- [2006년 12월 21일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀 팝업창[타입 3]에 입력한 개인 ID[gosky37]와 비밀번호[cys420]가 평문으로 서울신용평가정보로 전송된다. 노출된 개인 ID와 비밀번호를 이용하면, 해당 개인 ID의 사용자로 위장하여 Siren24 아이핀을 지원하는 다른 홈페이지에 회원가입이 가능하다.
그린버튼	타입 3	단계 9	그림 57	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 라이크호스트 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 라이크호스트 홈페이지에 5개의 서로 다른 ID를 생성 가능하다
오류 발생 여부				- 해당 사항 없음

〔그림 53〕 〔나이스아이핀〕 I-PIN 번호의 노출



〔그림 54〕 〔가상주민번호〕 식별 ID 및 비밀번호



〔그림 55〕 〔Siren24아이핀〕 I-PIN 번호의 노출

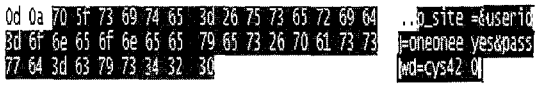
〔그림 56〕 〔Siren24아이핀〕 개인 ID 및 비밀번호의 노출

〔그림 57〕 〔그린버튼〕 I-PIN 번호의 노출

13. [14] 쎌덤 홈페이지 분석

쎌덤 홈페이지에서는 가상주민번호를 통한 회원가입만이 가능하며 타 I-PIN 서비스는 지원하지 않는다. 하지만 가상주민번호의 식별 ID와 비밀번호, 그리고 식별자가 평문으로 노출되어 획득이 가능하다. 현재(2007년 1월 9일) 쎌덤 홈페이지에서는 I-PIN을 이용한 회원가입이 제공되지 않고 있다. 아래의 분석자료는 2006년 12월에 실시된 실험의 데이터를 이용하여 만들어졌다.

〔그림 58〕 〔가상주민번호〕 I-PIN 번호의 노출



〔그림 59〕 〔가상주민번호〕 식별 ID와 비밀번호의 노출

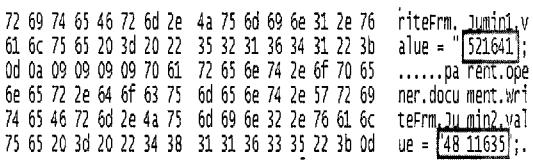
14. [15] 칠리칠리닷컴 홈페이지 분석

칠리칠리닷컴 홈페이지에서는 기본적으로 제공되는 가상주민번호를 제공한다. 사용자가 가상주민번호를 입력하는 과정에서 사용자의 식별자가 노출된다. 다른 4개의 I-PIN 서비스는 지원하지만, 나이스아이핀과 OnePass는 본인확인 중에 오류가 발생한다. 오류가 발

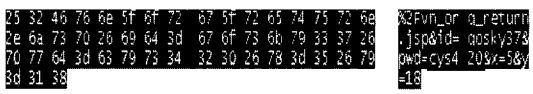
〔표 18〕 쎌덤 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	구 분 설 명
가상 주민번호 (가상주민번호를 I-PIN 서비스 도입 사이트에 직접입력)	타입 5	단계 6	그림 58	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 자신의 가상주민번호[예 : 5216414811635]를 홈페이지 상에 직접 입력하는 과정에서 가상주민번호[I-PIN 번호]가 평문으로 노출된다. - 노출된 가상주민번호를 이용하면 해당 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
	가상 주민번호 조회 과정	단계 6	그림 59	- [2006년 12월 28일에 수집된 네트워크 패킷을 이용한 실험결과] - 사용자가 가상주민번호를 조회하는 과정에서 식별 ID[oneoneeyes]와 비밀번호 [cys420]가 평문으로 노출된다. - 노출된 식별 ID와 비밀번호를 이용하면, 해당 사용자의 I-PIN 번호를 알아 낼 수 있다., 알아낸 I-PIN 번호로 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
중복가입 가능 여부				- 가상주민번호만을 제공하므로 중복가입이 되지 않는다.
오류 발생 여부				- 해당 사항 없음

생하지 않은 가상주민번호와 Siren24아이핀과 그린버튼에서는 본인확인 과정이 완료된 후 I-PIN 번호가 노출되었다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. 뿐만 아니라, Siren24아이핀에서는 사용자의 개인 ID와 비밀번호가 획득 가능하다.

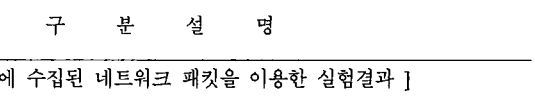


〔그림 60〕 〔가상주민번호〕 I-PIN 번호의 노출



〔그림 61〕 〔Siren24아이핀〕 개인 ID와 비밀번호 노출

〔그림 62〕 〔Siren24아이핀〕 I-PIN 번호의 노출



〔그림 63〕 〔그린버튼〕 I-PIN 번호의 노출

〔표 19〕 칠리칠리닷컴 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	구 분 설 명
가상주민번호 (I-PIN 팝업창 사용방식)	타입 1	단계 9	그림 60	- [2006년 12월 29일에 수집된 네트워크 패킷을 이용한 실험결과] - 가상주민번호를 이용한 본인확인 절차가 완료된 뒤, 한국신용평가정보 증에서 칠리칠리닷컴 홈페이지로 전송된 사용자의 I-PIN 번호[5216414811635]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 가상주민번호를 이용하면 해당 I-PIN 번호의 사용자로 위장하여 가상주민번호를 지원하는 다른 홈페이지에 회원가입이 가능하다.
Siren24 아이핀	타입 3	단계 9	그림 61	- [2007년 1월 8일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀을 이용한 본인확인 절차가 완료된 뒤, 서울신용평가정보에서 칠리칠리닷컴 홈페이지로 전송된 사용자의 I-PIN 번호[3313060444105]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 Siren24아이핀을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
		단계 6	그림 62	- [2007년 1월 8일에 수집된 네트워크 패킷을 이용한 실험결과] - Siren24아이핀 팝업창[타입 3]에 입력한 개인 ID[gosky37]와 비밀번호[cys420]가 평문으로 서울신용평가정보로 전송된다. 노출된 개인 ID와 비밀번호를 이용하면, 해당 개인 ID의 사용자로 위장하여 Siren24 아이핀을 지원하는 다른 홈페이지에 회원가입이 가능하다.
그린버튼	타입 1	단계 9	그림 63	- [2007년 1월 9일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 칠리칠리닷컴 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. 이는 I-PIN 서비스를 이용한 본인확인 절차 이후에 수행되는 회원가입과정에서 사용자의 I-PIN 번호가 노출되기 때문이다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
중복가입 가능 여부				- 한 사용자는 서울신용평가정보 홈페이지에 3개의 서로 다른 ID를 생성할 수 있다.
오류 발생 여부				- 나이스아이핀은 본인확인 과정에서 오류가 발생한다. - OnePass는 본인확인 과정에서 오류가 발생한다.

15. [16] 테크노비젼 홈페이지 분석

테크노비젼 홈페이지에서는 그린버튼을 기본적으로 제공하며 타 I-PIN을 이용한 회원가입도 가능하다. 하지만 그린버튼 팝업창(타입 2)를 사용하기 때문에, 그린버튼을 이용할 때 입력하는 E-mail 주소와 비밀번호, 그리고 식별자가 평문으로 노출되어 획득이 가능하다. 또한 다른 4개의 I-PIN 서비스는 회원가입을 하고자 할 때, 실행과정에서 오류가 발생하여 회원가입이 제대로 실행되지 않는다. 하지만 가상주민번호는 회원가입 시 오류가 발생하더라도 식별자와 식별 ID와 비밀번호가 평문으로 노출되어 획득이 가능하다. 테크노비젼 홈페이지에서 기본적으로 그린버튼을 이용하므로, 가상주민번호 팝업창의 타입은 원래는 가상주민번호와 성명을 입력하는 경우에는 타입 3, 식별 ID와 비밀번호를 입력하는 경우에는 타입 4가 되어야 한다. 하지만 I-PIN 팝업창 간 링크 시 발생하는 오류 때문인지, 가상주민번호와 성명을 입력하는 경우에는 타입 1, 식별 ID와 비밀번호를 입력하는 경우에는 타입 2가 사용된다.

〔그림 64〕 〔그린버튼〕 I-PIN 번호의 노출

〔그림 65〕 〔그린버튼〕 E-mail 주소와 비밀번호의 노출

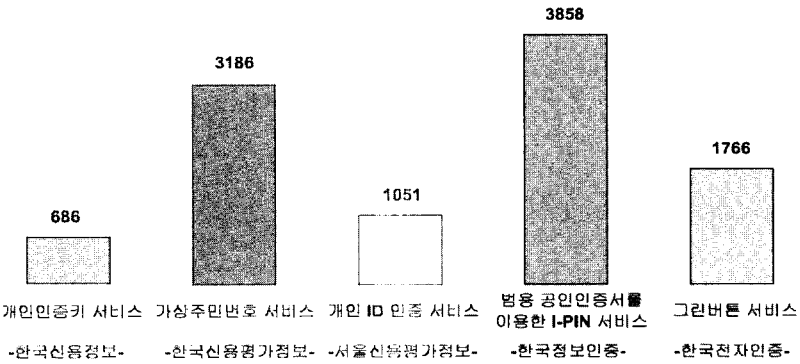
V. I-PIN 서비스의 취약점 분석과 그에 대한 대책

현재 I-PIN 서비스를 통해서 회원가입 및 I-PIN 서비스 도입 사이트의 게시판에 글을 작성할 수 있는 작업 등을 할 수 있는 홈페이지는 17 개로, 지금은 한정된 홈페이지에서만 사용 가능하지만 앞으로 I-PIN의 사용이 확산될 전망이다. 정보통신부에서는 본격적으로 I-PIN 서비스를 시행하기 전에 시범기간을 운영하여 I-PIN 서비스 별 발급현황을 조사하였다. 그 결과는 아래의 그림 66와 같다. 사용자들은 5가지의 I-PIN 서비스 중 비교적 사용이 간단하고 널리 알려진 가상주민번호와 OnePass를 많이 사용하는 것으로 나타났다. 17개의 홈페이지 중 인지도가 높은 정보통신부에서 가상주민번호와 OnePass만을 제공하는 것도 또 하나의 이유라고 판단된다.

현재 홈페이지에 I-PIN 서비스의 도입하는 것은 사용을 권장하는 가이드라인 수준이어서 법적인 구속력은 없다. 또 하나의 문제는 I-PIN 서비스가 활성화되었을

〔표 20〕 테크노비젼 홈페이지 분석 결과

서비스 종류	I-PIN 팝업창 타입	동작 단계	그림 번호	설 명
그린버튼	타입 2	단계 9	그림 64	- [2006년 12월 21일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼을 이용한 본인확인 절차가 완료된 뒤, 한국전자인증에서 테크노비젼 홈페이지로 전송된 사용자의 I-PIN 번호[7814065387899]가 사용자와 홈페이지간의 통신에서 평문으로 노출된다. - 노출된 I-PIN 번호를 이용하면, 해당 I-PIN 번호의 사용자가 그린버튼을 이용하여 가입하는 홈페이지를 알아낼 수 있다.
		단계 6	그림 65	- [2006년 12월 21일에 수집된 네트워크 패킷을 이용한 실험결과] - 그린버튼 팝업창[타입 2]에 입력한 E-mail 주소[yschoi@security.re.kr]와 비밀번호[THSRLARH]가 평문으로 한국전자인증으로 전송된다. - 노출된 E-MAIL 주소와 비밀번호를 이용하면, 해당 개인 E-mail 주소의 사용자로 위장하여 그린버튼을 지원하는 다른 홈페이지에 회원가입이 가능하다.
중복가입 가능 여부				- 그린버튼을 제외한 타 서비스들의 오류로 중복가입이 안된다.
오류 발생 여부				- 나이스아이핀은 본인확인 과정에서 오류가 발생한다. - 가상주민번호는 본인확인 과정에서 오류가 발생한다. - Siren24아이핀은 본인확인 과정에서 오류가 발생한다. - OnePass는 본인확인 과정에서 오류가 발생한다.



〔그림 66〕 I-PIN 서비스 별 발급 현황

〔표 21〕 I-PIN을 제공하는 홈페이지 별 취약점 분석

사이트 종류	No	사이트 명	다른 홈페이지에 회원가입이 가능한 사용자 정보의 노출	해당 I-PIN 번호 사용자의 다른 홈페이지 가입여부가 확인 가능한 정보의 노출	본인확인 과정에서의 오류 발생 여부	중복 가입 가능 여부
공공기관	[01]	정보통신부 (http://www.mic.go.kr)	○	○	X	○
	[02]	정보보호기술 훈련장 (http://www.sis.or.kr)	X	○	○	○
	[03]	인터넷침해사고 대응지원센터 (http://www.krcert.or.kr)	○	○	○	○
	[04]	김포시청 (http://www.gimpo.go.kr)	X	○	X	X
	[05]	영등포구청 (http://www.ydp.go.kr)	X	X	X	X
	[06]	한국정보문화진흥원 (http://www.kado.or.kr)	X	○	○	○
	[07]	한국소프트웨어진흥원 (http://www.software.or.kr)	○	○	○	I-PIN 팝업창의 오류발생으로 중복가입이 불가능
	[08]	정보통신연구진흥원 (http://www.iita.re.kr)	○	○	X	X
	[09]	충북도청 (http://www.cb21.net)	○	○	○	I-PIN 팝업창의 오류발생으로 중복가입이 불가능
	[10]	IT수출정보데이터베이스 (http://www.itx.or.kr)	X	○	○	I-PIN 팝업창의 오류발생으로 중복가입이 불가능
본인확인 기관	[11]	한국신용정보 (http://www.nice.co.kr)	○	○	X	○
	[12]	서울신용평가정보 (http://www.sci.co.kr)	X	○	X	○
민간업체	[13]	라이크호스트 (http://www.likehost.com)	○	○	X	○
	[14]	쎌덤 (http://www.celldom.co.kr)	○	○	X	X
	[15]	칠리칠리닷컴 (http://www.chili72.com)	○	○	X	○
	[16]	테크노비젼 (http://www.technovision.co.kr)	○	○	○	I-PIN 팝업창의 오류발생으로 중복가입이 불가능
	[17]	KMPS 인트라넷 (https://pay.kmps.co.kr)	I-PIN 서비스를 받기 위해서는 KMPS의 사내 ID와 비밀번호가 필요하여 일반적인 사용자는 I-PIN 서비스를 이용하지 못함			

때 사용자의 주민등록번호, 성명, E-mail 주소, 휴대폰 번호 등의 개인 정보가 집중화될 본인확인업체 5곳 모두가 공인된 공공기관이 아닌 민간 업체라는 점이다. 앞으로 많은 사용자 정보가 민간 업체 5곳에 모두 집중되는 만큼, 정보 유출 사고가 날 경우를 대비하여 기술적, 제도적 신뢰성을 갖추도록 하는 법제도가 마련되어야 하지만 아직은 준비가 되지 않은 상태이다[1].

그리고 아직 I-PIN 서비스의 운영상태도 완전하지 못하다. I-PIN 서비스를 지원하는 총 17개의 홈페이지 중 5개의 홈페이지에서 I-PIN 서비스 관련 오류가 발생한다. 대부분 I-PIN 서비스간의 연동 문제이지만, 17개의 홈페이지 중에서 7개의 홈페이지에서 오류가 발생한 것은 심각한 문제다. 이 문제를 제외하더라도 현재 I-PIN 서비스에는 I-PIN 서비스의 이용 시 입력하는 정보(ID/PW 등)의 노출, I-PIN 번호의 노출, 중복가입 가능 등의 문제점이 있다. 물론 본인확인기관에서는 이용자

[표 22] I-PIN 서비스 별 사용자 정보의 노출

사이트 종류	No	사이트 명	나이스아이핀	가상주민번호	Siren24아이핀	OnePass	그린버튼
공공기관	[01]	정보통신부 (http://www.mic.go.kr)	-	I-PIN 번호 노출 식별 ID와 비밀번호 노출	-	-	-
	[02]	정보보호기술 훈련장 (http://www.sis.or.kr)	-	-	개인 ID와 비밀번호 노출	-	I-PIN 번호 노출
	[03]	인터넷침해사고 대응지원센터 (http://www.krcert.or.kr)	-	-	개인 ID와 비밀번호 노출	-	I-PIN 번호 노출
	[04]	김포시청 (http://www.gimpo.go.kr)	-	-	I-PIN 번호 노출	-	-
	[05]	영등포구청 (http://www.ydp.go.kr)	-	-	-	-	-
	[06]	한국정보문화진흥원 (http://www.kado.or.kr)	I-PIN 번호 노출	-	-	I-PIN 번호 노출	I-PIN 번호 노출
	[07]	한국소프트웨어진흥원 (http://www.software.or.kr)	-	I-PIN 번호 노출 식별 ID와 비밀번호 노출 주민등록번호 노출	-	-	-
	[08]	정보통신연구진흥원 (http://www.iita.re.kr)	-	I-PIN 번호 노출 주민등록번호 노출	-	-	-
	[09]	충북도청 (http://www.cb21.net)	I-PIN 번호 노출	I-PIN 번호 노출	I-PIN 번호 노출	I-PIN 번호 노출	I-PIN 번호 노출
	[10]	IT수출정보데이터베이스 (http://www.itx.or.kr)	-	-	I-PIN 번호 노출	-	I-PIN 번호 노출
본인확인기관	[11]	한국신용정보 (http://www.nice.co.kr)	I-PIN 번호 노출	I-PIN 번호 노출	I-PIN 번호 노출 개인 ID와 비밀번호 노출	I-PIN 번호 노출	I-PIN 번호 노출
	[12]	서울신용평가정보 (http://www.sci.co.kr)	-	-	-	-	I-PIN 번호 노출
민간업체	[13]	라이크호스트 (http://www.likehost.com)	I-PIN 번호 노출	I-PIN 번호 노출	I-PIN 번호 노출 개인 ID와 비밀번호 노출	I-PIN 번호 노출	I-PIN 번호 노출
	[14]	쎌덤 (http://www.celldom.co.kr)	-	I-PIN 번호 노출 식별 ID와 비밀번호 노출	-	-	-
	[15]	칠리칠리닷컴 (http://www.chili72.com)	-	I-PIN 번호 노출	I-PIN 번호 노출 개인 ID와 비밀번호 노출	-	I-PIN 번호 노출
	[16]	테크노비젼 (http://www.technovision.co.kr)	-	-	-	-	I-PIN 번호 노출 E-mail 주소와 비밀번호 노출
	[17]	KMPS 인트라넷 (https://pay.kmps.co.kr)	-	-	-	-	-

가 중복으로 가입되어 있는지 확인하는 중복가입확인정보를 전달하고 있으나, 해당 정보의 이용여부는 웹사이트 운영정책에 따라 결정되는 사항이므로 중복가입이 가능하는 것을 문제점으로 보기에는 부족할 수 있다. 하지만 중복가입을 허용하는 특별한 이유가 없는 상황에서 중복가입이 가능하게 하면, I-PIN 웹사이트나 I-PIN 서비스의 이용횟수만 늘리는 역할을 할 뿐이다. 특별한 이유가 없을 때는 중복가입이 불가능하게 설정되어야 한다.

이번 장에서는 본 논문에서 분석한 자료를 바탕으로 I-PIN을 이용한 본인확인 시스템에 대한 취약점에 대해 자세히 알아보고 그에 대한 대책을 알아본다.

현재 I-PIN 서비스를 제공하는 인터넷 사이트에서는 대부분 I-PIN 팝업창이 동작하고 있는데, 이 I-PIN 팝업창은 사용자의 I-PIN 정보를 입력 받아서 해당 본인확인기관으로 전송한다. 본인확인기관에서는 I-PIN 팝업창을 통하여 전달받은 사용자의 I-PIN 정보의 유효성을 검사하여 정당한 사용자임이 확인되면, 해당 인터넷 사이트로 주민등록번호를 제외한 사용자 정보(I-PIN 번호, 성별, 연령대 코드 등)를 전송하게 된다. 이렇듯 I-PIN 서비스에서 I-PIN 팝업창의 역할은 중요하며, I-PIN 팝업창에서 입력되는 정보로 I-PIN 서비스를 이용하는 사용자의 신분확인을 하게 되므로 I-PIN 팝업창에서 본인확인기관까지 안전하게 전송되어야 한다.

아래의 표들은 지금까지 분석한 I-PIN 관련 자료들을 분석한 표이다. 〔표 21〕에서는 현재 I-PIN 서비스 제공하는 홈페이지 별로 발생하는 취약점을 정리하였다. 표 22에서는 각 홈페이지에 대한 I-PIN 서비스 별 사용자 정보의 노출에 대해서 정리하였다.

〔표 21〕과 〔표 22〕에서 알 수 있듯이, 5개의 I-PIN 서비스가 동작하는 과정에서 발생하는 I-PIN 관련 정보의 노출과 인터넷 홈페이지에서 I-PIN 서비스를 이용한 회원가입 과정에서 발생하는 I-PIN 관련 정보의 노출이 발생하고 있다. 특히 [07] 한국소프트웨어진흥원 홈페이지와 [08] 한국정보통신연구원 홈페이지는 I-PIN 팝업창에서 입력하지도 않은 사용자의 주민등록번호가 평문으로 노출되었다.

〔표 23〕에서는 각 I-PIN 서비스 별 팝업창의 현황에 대해서 정리하였다. 〔표 24〕에서는 〔표 24〕 I-PIN 서비스 별 홈페이지 분석자료를 종합하였다.

지금까지 5가지 종류의 I-PIN 서비스의 특징 및 동작원리와 I-PIN 서비스를 제공하는 17개의 홈페이지에 대해서 분석하였다. 이를 바탕으로 I-PIN 서비스의 취약점을 분석하여 그에 따른 해결책을 알아본다.

○ I-PIN 서비스를 이용한 회원가입을 제공하는 인터넷 사이트의 취약점

I-PIN 서비스를 이용한 회원가입을 제공하는 인터넷 사이트에서 나타날 수 있는 I-PIN 서비스 관련 취약점은 사용자와 인터넷 사이트 간의 통신 중에 사용자의 중요한 입력정보가 평문으로 노출되는 현상, 본인확인기관에서 제공하는 I-PIN 서비스를 잘못 구현하여 사용

〔표 23〕 각 I-PIN 서비스 별 사용자의 I-PIN 정보 입력 방식

구분	나이스아이핀	가상주민번호	Siren24아이핀	OnePass	그린버튼
보안통신 I-PIN 팝업창 지원 (사용자 입력정보가 노출되지 않음)	타입 1 타입 2	타입 1 타입 2 타입 3 타입 4	타입 1 타입 2	타입 1	타입 1
일반적인 I-PIN 팝업창 지원 (사용자 입력정보가 노출됨)	-	*	타입 3	-	타입 2
I-PIN 서비스 도입 사이트에서 직접 입력 지원 (사용자 입력정보가 노출되지 않음)	-	타입 5	-	-	-
I-PIN 서비스 도입 사이트에서 직접 입력 지원 (사용자 입력정보가 노출)	-	타입 5	-	-	-

* 가상주민번호를 조회할 때, 사용자 정보가 노출된다.

자 정보가 노출되는 현상, 인터넷 사이트에서 실행되는 I-PIN 팝업창에 오류가 발생하는 현상 등이 있다.

사용자와 인터넷 사이트 간의 통신 중에 사용자의 중요한 입력정보가 평문으로 노출되는 현상은 가상주민번호 동작과정 중 사용자의 가상주민번호를 I-PIN 서비스 도입 사이트에서 직접 입력할 때 사용자의 가상주민번호가 평문으로 노출되는 경우에 발생한다. 이러한 현상이 발생하는 인터넷 사이트로는 [01] 정보통신부, [08] 정보통신연구진흥원, 그리고 [14] 쎌덤이 있다.

본인확인기관에서 제공하는 I-PIN 서비스를 잘못 구현하여 사용자 정보가 노출되는 현상으로는 I-PIN 번호가 인터넷 사이트의 회원가입 과정에서 보안과정을 거치지 않고 표시되거나, I-PIN 번호가 회원가입 과정에서 표시는 되지 않으나 회원가입 과정에 사용되며 그 내용이 노출되어 사용되는 경우가 있다. 이런 현상이 발생하는 인터넷 사이트로는 [06] 한국정보문화진흥원, [09] 충북도청, [12] 한국신용정보, [13] 라이크호스트 그리고 [15] 칠리칠리닷컴이 있다.

인터넷 사이트에서 실행되는 I-PIN 팝업창에 오류가 발생하는 현상으로는 인터넷 사이트에서 사용되는 특정 I-PIN 팝업창이 계속 오류가 발생하거나 특정 I-PIN 팝업창에서 타 I-PIN 팝업창으로 이동할 때 오류가 발생하는 경우가 있다. 이러한 현상이 발생하는 인터넷 사이트로는 [02] 정보보호기술 훈련장, [03] 인터넷침해사고대응지원센터, [06] 한국정보문화진흥원, [07] 한국소프트웨어진흥원, [09] 충북도청, [10] IT수출정보데이터베이스, [15] 칠리칠리닷컴, [16] 테크노비젼이 있다.

○ I-PIN 서비스를 제공하는 본인확인기관의 취약점

I-PIN 서비스를 제공하는 본인확인기관에서 나타날 수 있는 I-PIN 서비스 관련 취약점으로는 I-PIN 팝업창의 입력값이 평문으로 전송되는 현상과 I-PIN 서비스 팝업창이 사용자에게 I-PIN 번호가 전송할 때 평문으로 전송하는 현상이 있다.

I-PIN 팝업창의 입력값이 평문으로 전송되는 현상은 특정 I-PIN 서비스가 보안통신을 하는 보안 팝업창만 지원하는 것이 아니라, 입력값이 평문으로 전송되는 일반 팝업창도 지원하거나 일반 팝업창만 지원할 때 발생한다. I-PIN 팝업창에 입력하는 정보가 평문으로 본인확인기관에 전송되는 I-PIN 팝업창이 존재하는 I-PIN 서비스는 Siren24아이핀[팝업창 타입 3], 그린버튼[팝업창 타입 2]가 있다. Siren24아이핀[팝업창 타입 3]이 사용되는 홈페이지에는 [02] 정보보호기술 훈련장, [03] 인터넷침해사고 대응지원센터, [11] 한국신용정보, [13] 라이크호스트, [15] 칠리칠리닷컴이 있다. 그린버튼[팝업창 타입 2]가 사용되는 홈페이지에는 [16] 테크노비젼이 있다. 2006년 12월에는 가상주민번호의 팝업창[타입 1~4]에서도 팝업창 내 입력값이 본인확인기관으로 평문으로 전송되었었다. 하지만 본 실험이 진행되는 동안 취약점이 보완되어서, 현재는 가상주민번호의 [팝

〔표 24〕 I-PIN 서비스 별 홈페이지 분석자료 종합

구분	나이스아이핀	가상주민번호	Siren24아이핀	OnePass	그린버튼
해당 I-PIN 서비스를 제공하는 홈페이지의 수	10	11	11	11	10
해당 I-PIN 서비스의 이용이 가능한 홈페이지의 수	4	6	9	7	8
해당 I-PIN 서비스 과정에서 오류가 발생하여, 해당 I-PIN 서비스로는 회원가입이 홈페이지의 수	6	5	2	4	2
해당 I-PIN 번호 사용자가 다른 홈페이지에 회원가입을 하는지 확인할 수 있는 정보의가 노출되는 홈페이지 수	4	8	5	4	10
해당 I-PIN 서비스 과정에서 다른 홈페이지에 회원가입이 가능한 사용자 정보의 노출되는 홈페이지 수	-	8	4	-	1

업창 타입 1~4]에 입력하는 값은 본인확인기관으로 보안처리를 거쳐서 전송된다. 그러나 식별 ID와 비밀번호를 이용해서 가상주민번호를 조회할 때에는 여전히 식별 ID, 비밀번호, 가상주민번호 그리고 주민등록번호까지 노출되는 문제가 발생하고 있다.

I-PIN 서비스 팝업창이 사용자에게 I-PIN 번호가 전송할 때 평문으로 전송하는 현상은 본인확인기관에서 사용자의 I-PIN 번호를 해당 인터넷 사이트로 전송하기 전에 사용자에게 전송을 확인 받는 과정에서 발생하거나. 전송된 I-PIN 번호가 사용자와 인터넷 사이트 사이의 통신에 노출될 때 발생한다. 이러한 현상이 발생하는 I-PIN 서비스로는 나이스아이핀[팝업창 타입 1,2]와 그린버튼[팝업창 타입 1,2]가 있다.

지금부터 본 논문에서 분석한 I-PIN 서비스를 이용한 회원가입을 제공하는 인터넷 사이트의 취약점과 I-PIN 서비스를 제공하는 본인확인기관의 취약점과 이외의 문제점을 전체적으로 포괄하여 I-PIN 서비스의 취약점과 그에 따른 대책에 대해서 논의한다.

1. 다른 홈페이지에 회원가입이 가능한 사용자 정보 (ID, PW, 가상주민등록번호 등)의 노출 취약점 및 대책

현재 I-PIN 서비스를 이용한 회원가입을 제공하는 17개의 홈페이지에 중 다른 사람이 사용자의 이름으로 회원가입이 가능한 사용자 정보가 노출되는 곳은 10개의 홈페이지였다. 사용자가 입력하는 값이 노출되면, 다른 사용자가 아무런 어려움 없이 사용자의 이름으로 I-PIN 서비스 도입 사이트에 가입할 수 있다. I-PIN 서비스에서 발생하는 해당 문제는, 주민등록번호의 입력을 통한 회원등록과정에서의 주민등록번호와 이름의 유출되었을 때와 유사하다.

이를 방지하기 위해서는 사용자가 입력하는 정보가 SSL 통신방식이나 안전성이 증명된 통신방식을 통하여 암호화되어 전송되어야 한다. 그리고 본인확인기관에서 I-PIN 서비스 도입 사이트로 전송하는 I-PIN 번호가 사용자의 웹브라우저에 표시되면, 사용자의 I-PIN 번호가 유출될 가능성이 높다. 사용자에게 I-PIN을 전송할 필요가 없을 경우에는, 본인확인기관과 I-PIN 서비스 도입 사이트 사이에서 비밀통신을 통해 안전하게 전송되어야 한다.

2. I-PIN 번호의 노출 문제 및 대책

현재 I-PIN 서비스를 이용한 회원가입을 제공하는 17개의 홈페이지 중 15개 홈페이지에서 I-PIN 번호가 평문으로 노출되고 있다. 특히 사용자별 I-PIN 할당 방식(가상주민번호, Siren24아이핀, OnePass, 그린버튼)에서 I-PIN 번호가 노출되면, 사용자가 식별자를 변경하거나 유효기간이 지나기 전까지는 주민등록번호와 같이 고정된 본인정보가 되므로 문제가 된다. 그 중 가상주민번호에서의 I-PIN 번호는 주민등록번호와 같은 역할을 하는데, 17개의 홈페이지 중 8개의 홈페이지에서 평문으로 노출되었다.

이를 방지하기 위해서는 사용자에게 I-PIN 번호를 전달할 필요가 없는 경우, 본인확인기관과 사용자와의 통신이나 홈페이지와 사용자간의 통신에서 I-PIN 번호가 보여주지 않도록 하여야 한다. 그리고 I-PIN 번호가 전송될 때는 통신내용이 SSL 통신방식이나 안전성이 증명된 통신방식을 통하여 암호화되어 전송되어야 한다.

3. I-PIN 서비스 이용 시 오류발생 취약점 및 대책

현재 I-PIN 서비스를 통한 회원가입을 제공하는 17개의 홈페이지 중 8개의 홈페이지에서 I-PIN 관련 오류가 발생하고 있다. 대부분 사용자가 I-PIN 서비스 도입 사이트에서 기본적으로 제공하는 I-PIN 서비스 이외의 타 I-PIN 서비스를 사용하고자 때, I-PIN 서비스 간의 호환이 잘 안되어 본인확인이 되지 않는 현상이다.

5개의 본인확인기관의 I-PIN 서비스 방식이 완벽히 통합된 I-PIN 서비스 팝업창을 개발하여야 한다. 지금도 5가지의 I-PIN 서비스를 통합한 I-PIN 서비스 팝업창이 사용 중 이지만, 오류가 많이 발생하고 I-PIN 서비스 도입 사이트마다 각자 다르게 구현하여 사용 중 이라서 취약점이 많이 발생한다. 공인된 기관에서 5가지의 I-PIN 서비스를 통합하여 안정성과 효율성을 만족하는 I-PIN 서비스 팝업창이 필요하다.

4. 중복가입 여부 확인 불가 취약점 및 대책

현재 5개의 I-PIN 서비스는 특정 사용자의 중복가입을 확인할 수 가 없는 상황이다. 즉 Siren24아이핀을 통해 회원에 가입한 홈페이지에는 같은 사용자가 그린버튼을 이용해서 회원가입을 할 수 있다는 뜻이다. 현재

17개의 홈페이지 중 8개의 홈페이지에서 중복가입이 가능하다. 하지만 4개의 홈페이지를 제외하고, 4개의 홈페이지에서 I-PIN 서비스의 오류로 기본적으로 제공하는 I-PIN 서비스 이외의 타 I-PIN 서비스를 제공하지 못하는 문제만 해결하면 17개 중 12개의 홈페이지에서 중복가입이 가능해진다. 정보통신부에서 제공하는 인터넷상의 주민번호 대체수단 가이드라인에는, 본인확인기관에서 인터넷 사업자에게 서비스 간의 중복가입여부를 확인하는 중복가입확인정보를 제공해야한다고 명시되어있다.

〔표 25〕 I-PIN 서비스 관련 취약점에 대한 해결방안 및 대책 수립과정

일 시	진 행 사 항
2007년 1월 11일	▪ 성균관대학교 정보보호연구소에서는 본 논문에서 지적한 주민등록번호 대체수단에 대한 구현 취약점을 한국정보보호진흥원에 공식 통보
2007년 1월 12일	▪ 한국정보보호진흥원은 긴급대책회의를 개최하고, 관련기관들에게 취약점을 통보
2007년 1월 15일 - 2007년 2월 28일	▪ 성균관대 정보보호연구소에서는 한국정보보호진흥원으로 위촉연구원을 파견하여 I-PIN 관련 취약점에 대한 대책 마련을 위한 연구 수행
2007년 1월 16일	▪ 한국정보보호진흥원은 I-PIN 관련 취약점에 대한 대책을 마련하고자 외부전문가, 본인확인기관 담당자와 함께 I-PIN 서비스의 안전성 강화방안 회의 개최
- 2007년 2월 28일	▪ I-PIN 관련 취약점에 대한 원인분석 및 수정보완

〔표 26〕 I-PIN 서비스 별 취약점 조치현황

본인확인기관명 (서비스명)	취 약 점	조 치 방 법	조치현황
한국신용정보 (나이스아이핀)	아이핀 번호, 성명, 성별, 연령대, 중복가입확인정보 등 개인정보 노출	웹사이트에 정보 전달 이후 이용자에게 보여지는 페이지 상에서 해당 정보를 보내지 않도록 웹사이트 소스코드 수정 요청	2007년 1월 조치완료
	서비스 연동 오류	인증 결과 값 전달을 위한 페이지 주소(URL) 오류 정정	2007년 1월 조치완료
한국신용평가정보 (가상주민번호)	식별ID, 비밀번호 노출	이용자와 본인확인기관간 보안 통신을 하도록 변경	2007년 1월 조치완료
	주민번호 노출	이용자와 본인확인기관간 보안 통신을 하도록 변경	2007년 1월 조치완료
	아이핀 번호, 성명, 성별, 연령대, 중복가입확인정보 등 개인정보 노출	웹사이트에 정보 전달 이후 이용자에게 보여지는 페이지 상에서 해당 정보를 보내지 않도록 웹사이트 소스코드 수정 요청	2007년 1월 조치완료
	서비스 연동 오류	인증 결과 값 전달을 위한 페이지 주소(URL) 오류 정정	2007년 1월 조치완료
서울신용평가정보 (Siren24아이핀)	식별ID, 비밀번호 노출	이용자와 본인확인기관간 보안 통신을 하도록 변경	2007년 1월 조치완료
	아이핀 번호, 성명, 성별, 연령대, 중복가입확인정보 등 개인정보 노출	웹사이트에 정보 전달 이후 이용자에게 보여지는 페이지 상에서 해당 정보를 보내지 않도록 웹사이트 소스코드 수정 요청	2007년 1월 조치완료
	서비스 연동 오류	인증 결과 값 전달을 위한 페이지 주소(URL) 오류 정정	2007년 1월 조치완료
한국정보인증 (OnePass)	아이핀 번호, 성명, 성별, 연령대, 중복가입확인정보 등 개인정보 노출	웹사이트에 정보 전달 이후 이용자에게 보여지는 페이지 상에서 해당 정보를 보내지 않도록 웹사이트 소스코드 수정 요청	2007년 1월 조치완료
	서비스 연동 오류	인증 결과 값 전달을 위한 페이지 주소(URL) 오류 정정	2007년 1월 조치완료
한국전자인증 (그린버튼)	식별ID, 비밀번호 노출	이용자와 본인확인기관간 보안 통신을 하도록 변경	2007년 1월 조치완료
	아이핀 번호, 성명, 성별, 연령대, 중복가입확인정보 등 개인정보 노출	웹사이트에 정보 전달 이후 이용자에게 보여지는 페이지 상에서 해당 정보를 보내지 않도록 웹사이트 소스코드 수정 요청	2007년 1월 조치완료
	서비스 연동 오류	인증 결과 값 전달을 위한 페이지 주소(URL) 오류 정정	2007년 1월 조치완료

Ⅵ. 결 론

본 논문에서는 인터넷 상에서 I-PIN 서비스가 안전하게 사용되기 위한 대책을 마련하기 위해서 먼저 인터넷 상의 주민등록번호 사용으로 발생하는 개인정보가 심각하게 노출되는 문제점과 주민등록번호를 이용한 사용자 신원확인 체계를 살펴본 후, I-PIN의 종합적인 문제점에 대해서 알아보았다. 그러기 위해서 5개의 I-PIN 서비스의 동작원리와 문제점에 대해서 분석하고 I-PIN 서비스의 식별자 할당 방식에 대해서도 살펴보았다. 그리고 I-PIN 서비스를 이용한 회원가입을 제공하는 17개의 홈페이지에서의 구현 취약점에 대해서 설명하였다.

〔표 27〕 I-PIN 도입 사이트 별 조치현황

사이트 종류	No	사이트 명	취약점	조치방법	조치현황
공공기관	[01]	정보통신부 (http://www.mic.go.kr)	I-PIN 번호 입력시 노출 / I-PIN 서비스 ID와 비밀번호의 노출	보안접속 / 추가회원가입란 HTTPS 통신	2007년 2월 조치완료
	[02]	정보보호기술 훈련장 (http://www.sis.or.kr)	I-PIN 번호 입력시 노출 / I-PIN 서비스 ID와 비밀번호의 노출	보안접속 / 추가회원가입란 HTTPS 통신	2007년 1월 조치완료
	[03]	인터넷침해사고 대응지원센터 (http://www.krcert.or.kr)	I-PIN 번호 입력시 노출 / I-PIN 서비스 ID와 비밀번호의 노출	보안접속 / 추가회원가입란 HTTPS 통신	2007년 1월 조치완료
	[04]	김포시청 (http://www.gimpo.go.kr)	I-PIN 번호 노출	-	I-PIN 번호는 노출되지 않으나 예전버전의 I-PIN 팝업창을 사용
	[05]	영등포구청 (http://www.ydp.go.kr)	-	-	I-PIN 번호는 노출되지 않으나 예전버전의 I-PIN 팝업창을 사용
	[06]	한국정보문화진흥원 (http://www.kado.or.kr)	I-PIN 번호 노출	I-PIN 번호 등 개인정보 보여주기 제외 또는 HTTPS 통신 필요	2007년 1월 조치완료
	[07]	한국소프트웨어진흥원 (http://www.software.or.kr)	가상주민번호 노출 / I-PIN 서비스 ID와 비밀번호의 노출 / 주민번호 노출	보안접속 / 추가회원가입란 HTTPS 통신 / 주민등록번호 입력 제한	2007년 1월 조치완료
	[08]	정보통신연구진흥원 (http://www.iita.re.kr)	가상주민번호 노출 / 주민번호 노출	보안접속 / 주민등록번호 입력 제한	2007년 1월 조치완료
	[09]	충북도청 (http://www.cb21.net)	I-PIN 번호 노출	i-PIN 등 개인정보 보여주기 제외 또는 HTTPS 통신 필요	2007년 1월 조치완료
	[10]	IT수출정보데이터베이스 (http://www.itx.or.kr)	I-PIN 번호 노출	i-PIN 등 개인정보 보여주기 제외 또는 HTTPS 통신 필요	2007년 1월 조치완료
본인확인기관	[11]	한국신용정보 (http://www.nice.co.kr)	I-PIN 번호 앞자리 6개 노출	I-PIN 출력창 없애기	2007년 1월 조치완료
	[12]	서울신용평가정보 (http://www.sci.co.kr)	I-PIN 번호 노출	I-PIN 번호 등 개인정보 보여주기 제외 또는 HTTPS 통신 필요	2007년 1월 조치완료
민간업체	[13]	라이크호스트 (http://www.likehost.com)	회원가입 란에 I-PIN 번호 노출	I-PIN 번호 등 개인정보 보여주기 제외 또는 HTTPS 통신 필요	2007년 1월 조치완료
	[14]	쎌덤 (http://www.celldom.co.kr)	현재 회원가입이 안됨	-	다른 인터넷 사이트와 통합 중
	[15]	칠리칠리닷컴 (http://www.chili72.com)	회원가입 란에 I-PIN 번호 노출	회원가입란에 I-PIN 번호란 없애기 / 회원가입란 이상 수정 필요	2007년 1월 조치완료
	[16]	테크노비젼 (http://www.technovision.co.kr)	I-PIN 번호 노출 / I-PIN 서비스 ID와 비밀번호의 노출	보안접속 / 추가회원가입란 HTTPS 통신	2007년 1월 조치완료
	[17]	KMPS 인트라넷 (https://pay.kmps.co.kr)	-	-	내부망으로 운영

본 논문의 논문심사기간 동안(투고일 : 2007년 1월 10일), 한국정보보호진흥원에서는 성균관대학교 정보보호연구소를 주축으로 본 논문에서 지적한 I-PIN의 구현 취약점에 대한 해결방안을 연구하고 대책을 마련하였다. 그 결과, 2007년 2월말까지 본 논문에서 지적한 I-PIN 구현 취약점은 대부분 수정되었다. 위 〔표 25〕에서는 I-PIN 서비스 구현 취약점에 대한 해결방안 및 대책을 수립했던 과정을 설명한다.

본 논문에서 지적한 취약점에 대한 현재까지의 보안 조치사항을 I-PIN 서비스(본인확인기관)와 I-PIN 도입 사이트 별로 표로 정리하면 다음과 같다.

○ I-PIN 서비스(본인확인기관) 별 조치현황

I-PIN 서비스를 제공하는 본인확인기관에서는 각 구현 취약점에 대한 조치하였다. 〔표 26〕는 I-PIN 서비스 별 취약점 조치현황을 보여주고 있다.

○ I-PIN 도입 웹사이트 조치현황

I-PIN 서비스를 도입한 인터넷 사이트에서는 아래와 같이 취약점을 보안하도록 조치하였다. 〔표 27〕은 I-PIN 도입 사이트 별 조치현황을 보여주고 있다.

앞으로 I-PIN 서비스가 지속적인 발전하기 위해서는 본 논문에서 분석한 구현 취약점뿐만 아니라 또 다른 취약점을 찾아내고 해당 취약점에 대한 보안조치가 신속히 이루어져야 한다. 본 논문을 시작으로 I-PIN 서비스의 종합적인 문제와 그에 대한 해결책을 마련하기 위한 연구가 심도 있게 이루어져서, 주민등록번호 대체수단으로써 I-PIN 서비스가 효과적으로 사용될 수 있도록 하여야 하겠다.

참고문헌

〔1〕 염흥열, 이석래 저, 〔특집〕 인터넷 상에서 주민등록번호 대체수단 발전방향, 대한전자공학회, 전자공학회지 제32권 11호, 2005. 11, pp. 61~73.

〔2〕 이민영, 주민등록번호 남용억제에 관한 법제적 고찰, 정보통신정책, 제16권 8호 통권346호 pp. 1~17, 2004

〔3〕 인터넷상의 주민번호 대체수단 가이드라인, 정보통신부, 2006.10

〔4〕 주민번호 대체수단 소개 및 진행현황, 한국정보보호진흥원, 2006

〔5〕 주민번호대체수단-본격도입, 정보통신부 보도자료, 2006.10

〔6〕 전성배, 인터넷상의 주민번호 대체수단 가이드라인 및 향후 추진 로드맵, 2005.10 공청회 발표자료

〔7〕 염흥열, 주민등록번호 보호 수단, 2005.6.9, 디지털타임즈 전망대

〔8〕 이석래, 주민번호대체수단으로 공인인증서 활용방안, 2005.8.31. PKI-KR2005

〔9〕 정보통신부 홈페이지 (http://www.mic.go.kr)

〔10〕 정보보호기술 훈련장 (http://www.sis.or.kr)

〔11〕 인터넷침해사고 대응지원센터 (http://www.krcert.or.kr)

〔12〕 김포시청 (http://www.gimpo.go.kr)

〔13〕 영등포구청 (http://www.ydp.go.kr)

〔14〕 한국정보문화진흥원 홈페이지 (http://www.kado.or.kr)

〔15〕 한국소프트웨어진흥원 홈페이지 (http://www.software.or.kr)

〔16〕 정보통신연구진흥원 홈페이지 (http://www.iita.re.kr)

〔17〕 충북도청 홈페이지 (http://www.cb21.net)

〔18〕 IT수출정보데이터베이스 홈페이지 (http://www.itx.or.kr)

〔19〕 한국신용정보 홈페이지 (http://www.nice.co.kr)

〔20〕 서울신용평가정보 (http://www.sci.co.kr)

〔21〕 라이크호스트 홈페이지 (http://www.likehost.com)

〔22〕 쎌덤 홈페이지 (http://www.celldom.co.kr)

〔23〕 칠리칠리닷컴 홈페이지 (http://www.chili72.com)

〔24〕 테크노비젼 홈페이지 (http://www.technovision.co.kr)

〔25〕 17-KMPS 인트라넷 (https://pay.kmps.co.kr)

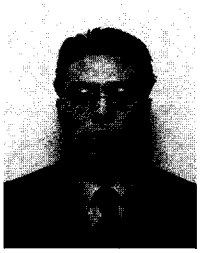
〈著者紹介〉

최 윤 성 (Younsung Choi) 학생회원

2006년 2월: 성균관대학교 정보통신공학부(공학사)
2006년~현재: 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 디지털 포렌식, 정보보호 응용, PKI, 보안성 평가

이 윤 호 (Yunho Lee) 학생회원

1991년 2월: 성균관대학교 정보공학과(공학사)
1993년 2월: 성균관대학교 대학원 정보공학과(공학석사)
1993년 3월~2000년 4월: 한국통신 연구개발본부 전임연구원
2000년 5월~2005년 1월: KBS인터넷㈜ 기술지원팀장
2005년 3월~현재: 성균관대학교 컴퓨터공학과 박사과정 재학 중
2006년 6월~현재: ㈜애니온소프트 기술이사
<관심분야> 암호이론, 정보보호 응용, 전자투표, 워터마킹



김 승 주 (Seungjoo Kim) 종신회원

1994년 2월~1999년 2월: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재: 성균관대학교 정보통신공학부 교수
2001년 1월~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월~현재: 교육인적자원부 유해정보차단 자문위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won) 종신회원

1976년~1988년: 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호 인증기술연구센터 센터장
<관심분야> 암호이론, 정보이론, 정보보호