제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

개인정보 노출의 예방 방법에 관한 연구

이기성*, 안효범*
*공주대학교 정보통신공학부
e-mail:hbahn@kongju.ac.kr

A Study on a Prevention Method for Personal Information Exposure

Ki-Sung Lee*, Hyo-Beom Ahn*
*Division of Information and Communication Engineering,
Kongju National University.

요 약

정보통신망의 발전과 함께 인터넷 사용 인구와 다양한 개방적 구조의 서비스 이용률이 지속적으로 증가하고 있다. 하지만 서비스 이용자들의 보안의식은 크게 달라지지 않아 서비스 이용자들의 직접적인 입력으로 인터넷상에 노출되는 개인정보가 늘어나고 있는 실정이며 이로 인한 이차적인 침해로 인하여 개인에게 정신적인 피해와 금전적 손괴 심지어는 신체적인 위험을 주는 각종범죄가 행해지고 있다. 본 논문에서는 이와 같은 개인정보의 노출을 예방하기 위해 서비스 이용자가 게시물을 등록하는 과정에서 개인정보의 노출을 예방 할 수 있는 게시물의 등록 방법을 제시한다. 이 방법은 게시물 등록 시 게시물에서 검출된 개인정보의 목록과 위험의 정도 그리고 개인정보 노출로 인한 이차적 침해유형을 서비스 이용자에게 명시하고 해당 개인정보에 대한 처리를 서비스 이용자에게 결정하도록 하는 방법으로서 서비스 이용자의 개인 정보보호 의식 수준을 끌어올려 개인정보 노출과 이차적인 침해사고를 일차적으로 예방할 수 있다.

1. 서론

정보통신망의 지속적인 발전과 스마트 모바일 기기의 보급으로 개인의 인터넷 이용률이 지속적으로 증가하고 있다[1]. 더불어 인터넷을 통한 비즈니스의 일환으로 다양한 콘텐츠를 제공하는 사이트들이 급속히 증가하고 있으며 이와 같은 대부분의 사이트들은 서비스 이용자들의 사용 편의와 참여를 위하여 게시물 등록 기능을 제공하고 있다. 특히 최근에는 블로그, 소셜 네트워크, 콘텐츠 커뮤니티 등 국내외의 소셜 미디어 서비스 이용자와 게시물이 폭발적으로 증가하고 있는 추세이다.

하지만 인터넷 이용률의 지속적인 증가에 비해 서비스 이용자들의 보안 의식수준은 제자리걸음을 하고 있으며 이에 따른 역기능 또한 증가하고 있는 실정이다. 보안 의식이 부족한 연령층의 서비스 이용자들이 점점 늘어남에 따라 서비스 이용자들의 직접적인 입력으로 인터넷상에 노출 되어지는 개인정보가 늘어나고 있으며 이로 인하여 노출된 개인정보를 이용한 명의도용 및 계정탈취, 피싱, 스팸 메시지, 프라이버시 침해, 유괴 등 개인에게 정신적인 피해와 금전적 손괴 심지어는 신체적인 위험을 주는 각종 범죄가 행해지고 있다[2,3,4].

이러한 개인정보의 이차적인 침해를 방지하기 위해서는 개인정보 노출을 사전에 예방하는 방법이 필요하다. 개인에 의하여 이루어지는 개인정보 노출은 보안의식의 부족으로 일어나는 경우가 대부분이기 때문에 본 논문에서는 서비스 이용자가 개인정보보호의 중요성을 효과적으로 인지하도록 하는 게시물 등록방법의 개선안을 제시한다.

본 논문의 2장에서는 개인정보 노출 문제에 대한 기존 연구에 대하여 살펴보며, 3장은 개인정보 노출을 예방할 수 있는 게시물 등록의 방법과 예시를 제시하며, 4장에서는 본 방법의 특징과 기대효과를 설명하고, 5장에서는 결론을 설명한다.

2. 개인정보 노출 문제에 대한 기존 연구

2.1 개인정보 노출 문제에 대한 연구

한국 인터넷 진흥원은 개인정보 노출을 최소화하기 위해 예방・대응・사후관리를 목적으로 “개인정보 노출대응체계(Privacy Incident Response System)"를 지난 2009년 11월에 구축하여 개인정보를 신속히 검색하여 삭제 및 대응할 수 있는 체계를 마련하였다[5]. 하지만 이 시스템은 외부 검색엔진에 이미 노출된 개인정보를 대상으로 하는 사후 조치이기 때문에 개인정보의 노출을 사전에 예방할 수 없다.

2.2 개인정보 노출 예방에 대한 연구

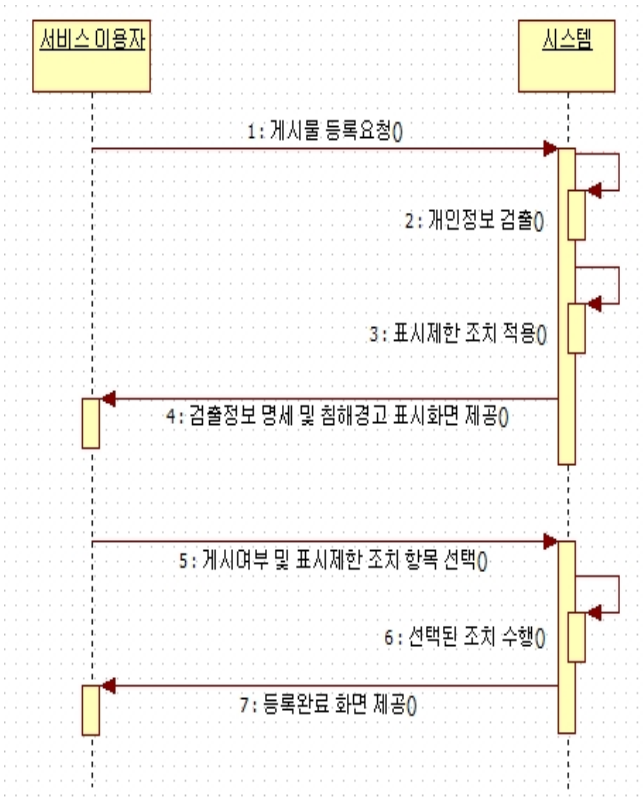
기업들은 서비스 이용자의 직접적인 입력으로 인터넷에 노출되는 개인정보를 사전에 예방하는 방법에 대한 다수의 특허를 출원하였다[6,7,8]. 하지만 해당 특허와 시중의 제품들은 공통적으로 게시물에서 개인정보나 악성코드를 검출하여 정책에 따라 마스킹하거나 삭제하는 방식이고 내부정보의 노출 방지를 위한 것이기 때문에 관리자에게처럼 서비스를 이용하는 개인에게 게시물내의 개인정보에 대한 명세를 제공하지 않는다. 따라서 서비스 이용자의 보안의식을 개선시키는데 어려움이 있다.

3. 개인정보 노출예방 게시물 등록 방법

본 장에서는 개인의 보안의식 고취를 통하여 개인정보 노출을 예방하기 위한 개인정보 노출예방 게시물 등록 방법의 개선안을 제시하려 한다. 제시하려는 방법은 서비스 이용자가 게시물을 등록하는 과정에서 적용되며 개인정보 검출과 침해 경고 및 선별적 개인정보 표시제한 보호조치를 수행하여 개인정보의 노출을 예방한다.

3.1 개인정보 노출예방 게시물 등록의 절차

본 논문에서 제시하는 방법은 다음과 같은 과정을 거쳐 게시물 등록을 수행한다.



(그림 1) 개인정보 노출예방 게시물 등록의 절차

① 서비스 이용자는 게시물을 작성 후 등록을 요청한다.
② 시스템은 게시물에서 개인정보의 유형에 따라 개인정보일 가능성이 높은 항목을 탐색하여 추출한다.
③ 시스템은 탐색된 개인정보 항목을 복사하고 복사한 개인정보에 대해 표시제한 보호조치를 적용한다.
④ 시스템은 추출된 개인정보와 표시제한 보호조치를 취한 해당 개인정보 그리고 노출로 발생할 수 있는 피해사항을 서비스 이용자에게 화면으로 제공한다.
⑤ 서비스 이용자는 게시물내의 개인정보 및 노출로 발생할 수 있는 피해사항을 확인하고 개인정보 표시제한 조치 여부를 선택하여 등록을 요청하거나 등록을 취소한다.
⑥ 시스템은 서비스 이용자가 표시제한 보호조치를 선택한 항목을 표시제한 보호조치를 적용한 결과로 게시물을 등록한다.
⑦ 시스템은 서비스 이용자에게 등록완료 화면을 제공한다.

3.2 유형별 개인정보의 검출

개인정보는 대부분 유형별로 일정한 패턴을 가지고 있다. 서비스 이용자가 개인정보가 포함된 게시물 작성 후 등록을 요청하면 게시물에서 개인정보의 유형별로 추정되는 패턴을 인식하여 해당 개인정보를 추출한다.

<표 1> 개인정보의 유형과 종류[9]

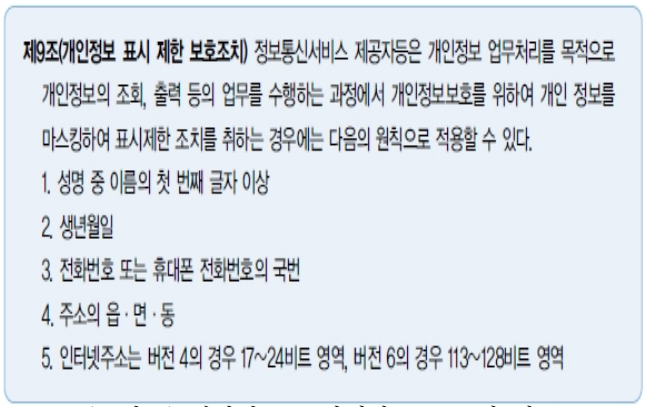
구 분	개인정보유형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타수익정보	보험(건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수,임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과, 직무태도
법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일(log file), 쿠키(cookies)
위치정보	GPS나 휴대폰에의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

게시물에서 개인정보로 추정되는 패턴을 인식하는 방법으로 정규 표현 식을 이용할 수 있다. 정규표현식이란 특정한 규칙을 가진 문자열의 집합을 표현하는 데 사용하는 형식 언어이다. 주로 텍스트 탐색과 문자열 조작에 쓰이며 하나의 문자와 일치하거나, 혹은 문자열의 일부분이나 전체 문자열인 문자 집합들과 일치하게 된다[10]. 정규표현식의 패턴은 (그림 2)와 같이 나타낼 수 있다.

(그림 2) 정규 표현 식의 패턴 예시

3.3 개인정보 표시제한 보호조치

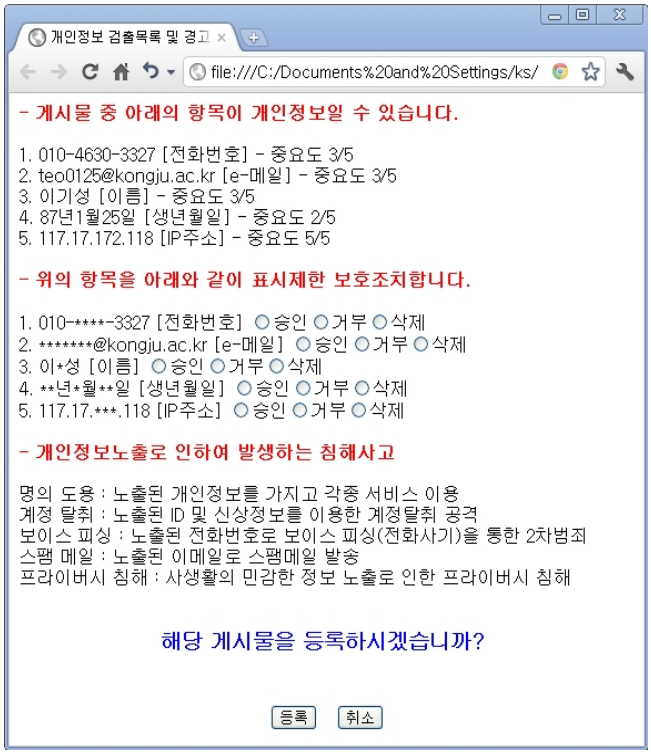
개인정보가 검출된 이후에는 해당 개인정보를 복사하고 복사한 개인정보에 표시제한 보호조치를 수행한다. 표시제한 보호조치는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 제9조 개인정보 표시 제한 보호조치를 참고하여 정책을 설정한다[12].



(그림 3) 개인정보 표시제한 보호조치 기준

3.4 개인정보 노출경고 화면 제공

개인정보 노출로 인하여 개인은 정신적 피해뿐만 아니라 명의도용, 보이스 피싱에 의한 금전적 손괴, 유괴 등 2차 침해사고에 노출된다[4]. 사용자들에게 개인정보 침해에 경각심을 일깨우기 위하여 검출된 개인정보와 함께 해당 개인정보의 노출로 발생할 수 있는 침해 유형과 발생할 수 있는 피해를 게시물 등록 화면에 표시하여 경고함으로서 서비스 이용자는 해당 내용을 인지하고 본인의 판단에 따라 게시물을 등록하거나 취소할 수 있다.



(그림 4) 개인정보 노출예방 게시물 등록방법의 예시

제공된 화면에서 서비스 이용자가 모든 항목의 표시제한 보호조치 여부를 결정하고 등록을 선택하면 시스템은 서비스 이용자가 표시제한 보호조치 거부를 선택한 최소한의 개인정보만 공개하여 게시물을 등록한다.

4. 분석 및 기대효과

본 논문에서 제시한 방법의 특성에 따라 얻을 수 있는 기대효과는 다음과 같다.

4.1 개인의 정보보호 의식 고취

이 방법은 게시물 등록 시 개인정보로 추정되는 항목과 개인정보 노출에 따르는 위험사항을 명시하기 때문에 서비스 이용자들에게 개인정보에 대한 명세를 제공하고 개인정보 노출에 대한 경각심을 일깨워 개인정보 노출을 일차적으로 예방할 수 있다.

4.2 양 방향적인 보안조치

이 방법은 기본적으로 게시물에서 검출된 개인정보에 표시제한 보호조치를 수행하며 서비스 이용자가 개인정보 표시제한 보호조치 거부를 선택한 최소한의 개인정보만 공개하여 게시물을 등록한다. 이는 서비스 이용자에게 개인정보에 대한 결정권을 주는 것으로 기존의 일 방향적인 보안 조치에서 벗어나 서비스 이용자에게 편의를 제공하고 공개한 개인정보에 대해서 책임을 가지도록 만든다.

4.3 이차적인 침해사고 예방

서비스 이용자의 보안인식 제고로 인터넷상에 노출되는 개인정보가 줄어들면 자연히 이차적인 개인정보 침해사고도 줄어들게 된다. 따라서 개인정보 노출 및 침해사고의 대응 비용을 절감할 수 있을 것으로 기대된다.

5. 결론

본 논문에서 제시한 방법은 텍스트만이 아닌 음성, 영상 등 다양한 형식에 포함된 개인정보에 대해서 확장할 수 있으며 악성코드의 필터링 기능을 추가하여 보안성을 강화시킬 수 있다. 또한 개별 개인정보의 위험도를 산정하도록 하여 서비스 이용자에게 검출된 개인정보의 위험 수준을 보다 분명하게 명시할 수 있으며 게시물 등록 시 뿐만 아니라 게시물 작성 시에 동작하도록 설계하여 개인정보보호 수준을 향상시킬 수 있다.

본 논문에서 제시한 개인정보 노출예방 게시물 등록 방법은 최근 스마트 모바일 환경과 개방적 구조의 웹 2.0 환경에서 서비스 이용자의 정보보호 의식수준 개선을 통하여 효과적으로 개인정보 노출을 예방할 수 있으며 서비스 이용자에게 검출된 개인정보에 대한 결정권을 부여함으로서 기존의 일 방향적인 보안조치에서 벗어나 서비스 이용자가 정보보호를 인식하고 함께 참여하는 양 방향적인 보안 문화를 만들어 나갈 수 있도록 도와준다. 이에 따라 이차적인 침해사고가 감소되고 개인의 안전한 서비스 이용이 가능할 것으로 기대된다.

참고문헌

[1] 한국인터넷진흥원 ISIS “개인 인터넷이용 통계” http://isis.kisa.or.kr/sub02/?pageId=020200, 2010
[2] 한국인터넷진흥원 ISIS “개인 정보보호 실태” http://isis.kisa.or.kr/sub07/?pageId=070100, 2010
[3] Pew Internet & American Life Project, "Older Adults and Social Media", Aug 27, 2010
[4] 개인정보보호종합지원시스템 “개인정보침해사례” http://www.privacy.go.kr/nns/ntc/pex/personalExam.do
[5] 최진영, 하태균, 이강신, 원유재 “개인정보 노출대응 체계”, KISTI, 2009
[6] 트리니티소프트, KR-A-2008-0000086, 2010
[7] 소만사, KR-A-2010-0034330, 2010
[8] 어울림엘시스, KR-A-2011-0055921, 2011
[9] 한국인터넷진흥원 보호나라 "개인정보의 유형과 종류" http://www.boho.or.kr/private/priv_01.jsp?page_id=1
[10] 행정안전부 개인정보보호과 “공공기관 홈페이지 개인정보 노출방지 가이드라인”, pp. 40-42, 2011
[11] 행정안전부·한국인터넷진흥원 “공공기관 개인정보 영향평가 수행 안내서”, pp. 31, 2011
[12] 방송통신위원회·한국인터넷진흥원 "개인정보의 기술적·관리적 보호조치 기준 해설서", pp. 76-77, 2010