M2M 환경에서의 SNS 개인정보 유출 위험 및 대응방안

고준영, 이근호

백석대학교 정보통신학부

SNS disclosure of personal information in M2M environment threats and countermeasures

Jun-Young Go, Keun-Ho Lee

Dept. of Information and Communication, Baekseok University

요약 IT기술의 발전과 더불어 온라인상에서 인적 네트워크 형성을 도와주는 소셜네트워크 서비스가 등장한다. 소셜네트워크의 등장은 전 세계인과 기업 환경에도 많은 변화를 가져오고 있다. 수많은 기업과 많은 사람들이 사용하고 있는 소셜 네트워크 서비스는 급격한 발전을 하고 있지만 보안위협 요소에 대해서는 대수롭지 않게 생각을 하고 있다. 또한 M2M의 발전으로 여러 휴대용 기계로부터의 접속이 많아지고 있지만, 그 취약성에 대한 인식을 하지 않고 있는 것이 사실이다. 본 논문에서는 개인정보에 대해 살펴본 후 소셜 네트워크 상에 있는 보안위협 요소와 M2M상에서의 SNS접속에 대한 취약성과 대응방안에 대하여 살펴본다.

• **주제어** : 사물통신, 소셜네트워크서비스, 개인정보, 보안

Abstract It appeared with the development of IT skills to help the social network SNS(Social Network Service) on the online form. Many people around the world and in the business environment changes is the emergence of social networks are bringing. And the rapid development of the idea, but are insignificant for the security threats that are used by many people in many companies, and social network services. In addition, although it is true that this connection is increased from the number of mobile machines to the development of M2M, that is not recognized for that vulnerability. To evaluate and identify vulnerabilities against security threats and countermeasures for the SNS access the social network on the M2M After looking for privacy and in the present.

• **Keyword** : M2M, SNS, Personal Information, Security

1. 서론

최근 스마트폰의 발전과 더불어 시간과 장소에 구애 받지 않는 네트워크망의 연결로 인하여 쉽게 인터넷을 접할 수 있는 요즘, 온라인상에서 이용자들이 인맥을 새롭게 쌓거나 기존 인맥과의 관계를 강화하고, 자신의 일상생활에 대한 표현과 다른 주요 정보들을 얻을 수 있는 SNS(Social Networking Service)를 남녀노소 가리지 않고 수많은 사람들이 이용을 하고 있다. 그러나 SNS상에

서 개인정보 침해 및 오남용 문제가 날로 늘어나고 심각해지고 있다.

IT 강국이라고 자부하는 우리나라에서는 IT분야의 외면적 발전과는 달리 이에 대한 적절한 대비책 마련은 소홀히 하고 있는 것이 사실이다. 2000년 이래 세계의 주요 학술대회나 보고서의 주요 이슈는 개인 정보보호에 대한 것이었다. 이러한 개인정보보호문제에 대해서 관심이 높은 이유는 우리의 일상생활에서 정보통신 기술의

*교신저자 : 이근호(root1004@bu.ac.kr)

접수일 : 2014년 2월 5일, 수정일 2014년 3월 21일, 게재확정일 : 2014년 3월 25일

급속한 발전이 있었기 때문이다. 이러한 발전에 따라 SNS를 쉽게 접하는 요즘 많은 이용자들이 무관심하게 사용하여온 개인정보보호에 대한 문제점을 분석하여 그 대응책을 마련하고자 한다.

2. 관련연구

2.1 프라이버시

프라이버시(Privacy)의 사전적 의미는 ① 다른 사람들의 주목이나 모임으로부터 떨어져 있는 상태, ② 다른 사람들의 주시 또는 모임을 피해온둔하고 있는 장소, ③ 무슨 말을 했는지 또는 어떠한 행동을 하였는지를 드러내지 않는 것, ④ 사적인 일 또는 비밀을 뜻한다.

프라이버시는 '혼자 있을 권리'에서 출발한다. 이것은 소극적 측면 이며 '내가 지금 혼자 있고 싶고, 누구한테 방해받고 싶지 않다'는 의사가 권리로서 존중되어야 한다는 것이다. 결국 사생활의 비밀을 침해받지 않은 권리라는 얘기다. 적극적 측면 은 자신이 결정한 대로 그 생활을 영위한다는 점이다. 단순히 외부로부터 간섭을 받지 않을 소극적 권리로서의 의미와 함께 외부로부터 간섭받지 않은 상태에서 자신의 사생활을 영위하고 발전시켜나갈 적극적 권리라는 뜻이 있다[1].

2.2 SNS 특징 및 현황

SNS는 기존의 인간관계 강화를 위한 새로운 네트워크 구축 수단으로, 사회적 관계를 통해서 SNS 사용자들이 생성한 콘텐츠에 대한 접근 및 사회적 관계를 형성을 지원하며, 이름, 성별, 주소, 이메일, 취미, 연령 등 개인의 신상정보를 공유하고 인터넷 안에서만 아닌 오프라인 사교모임과 취미활동, 토론, 여론 형성 등 개인적, 사회적 상호작용을 지원한다. 또한 개인과 기업에 대한 여론형성과 교류와 같은 온라인 협업, 경험공유, 교육, 사회적 신뢰, 정보제공을 한다.

SNS에 대한 이용자들의 관심이 증대하며 이를 통한 콘텐츠의 공유와 이용이 활성화됨에 따라, 관련 산업 진흥 및 서비스 수준도 향상되었다. SNS의 방문자 수 및 가입자 수에 따라 해당 사업의 성공 여부가 결정되고 최근 SNS는 메신저와 모바일 등의 서비스와 연동되어 이를 이용한 새로운 비즈니스 모델 개발 등을 통해 새로운 부가가치를 창출한다.

대표적인 SNS 사이트로 FaceBook, MySpace, SecondLife, 싸이월드, 카카오톡 등이 있으며 지속적으로 성장하고, 국내·외 주요 SNS 서비스 사이트들은 최근 큰 폭의 트래픽 증가를 보이는 등 인터넷 이용자들의 관심과 이용이 집중되고 있다. Table 1은 한국, 미국, 영국의 주요 SNS 서비스 개시일과 가입자 수를 나타낸 것이다[2].

[Table 1] SNS Registration State

	SNS	Start	Restriation
Domestic	Cyworld	1999.8.	25,000,000
	Daum	1999.5.	31,000,000
	Naver	2003.10	27,000,000
US	FaceBook	2003.1.	123,000,000
	MySpace	2004.	280,000,000
	SecondLife	2003.6.	224,000
UK	Bebo	2005.1.	1,900,000

또한 시장조사기관 이마케터(eMarketer)가 발표한 자료에 따르면 한 달에 한 번 이상 SNS를 이용하는 이용자는 12억 명에 이르렀으며, 2014년 현재까지 계속 증가하고 있다. 이는 전 세계 70억 인구 중 31.4%에 해당하는 22억 명이 인터넷을 이용하며, 그 중 54.5%인 12억 명이 SNS를 이용한다는 것을 의미한다[3,4].

2.3 M2M에서의 SNS에 대한 위협 요소

M2M 기기의 네트워크 접속 시의 보안 위협에는 네트워크에서 발생하는 보안 위협이 포함되며, 개인 프라이버시와 가로채기, 방해, 기밀누설 변조, 불법도용 비인가 접근, 비인가 무단 변조의 위험이 있다[9].

M2M 환경에서의 SNS 접속 시 M2M Device간에 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있고, M2M 네트워크의 불법 도용 및 접근을 통한 권한 위배와, 중간자에 의한 공격의 위협 요소가 있다[5].

3. M2M환경에서 SNS 개인정보 유출 위협

M2M Device로의 네트워크 접속이 많아지며, 이러한 M2M Device로 SNS에 대한 접속이 많아지고 이용이 증대되면서 이에 따른 보안 위협도 크게 증가하고 있다. M2M의 보안에는 디바이스 보안, 게이트웨이 보안, 네트워크보안이 있으며 데이터의 기밀성, 무결성, 게이트웨이

및 프라이버시보호 등의 보안 조건을 만족해야 한다[6].

- 패스워드 스니핑

중간자 공격을 통한 데이터의 불법 스니핑을 이용하여 사용자가 SNS에 로그인을 함과 동시에 계정 탈취가 가능함에 따라 M2M 기기의 네트워크상의 데이터 암호화가 필요하다.

- M2M Device 의 불법 도용

M2M Device 는 휴대가 편리함에 따라 상대적으로 물리적 보안이 허술하다. 이를 이용한 장치로의 악성소프트웨어 삽입 또는 장치 변경으로 인해 악성 디바이스로 이용될 가능성이 있어 M2M 장치의 물리적 보안이 필요하다.

다음에 보여질 표3은 현재 SNS 상에서의 보안 위협과 그에 해당하는 세부 내용 이다[7].

[Tabel 2] Security Threats in SNS

Threats	Contents
Privacy	· Personal profile collection
	· 2th data collection
	· Face
	· contents based image search
	· difficult of prefect ID delection
Network	· SN spam
	· XSS, worm, virus
	· phising using SNS
ID	· information ouput using network
	· deny profile using ID
	· cyber stalking
Scocial	· cyber bullying
	· industrial spy

3.1 프라이버시 위협

SNS상에 저장되어 있는 개인의 프로파일은 이용자와 제3자에 의해 수집되어 사적인 용도로 데이터화 되어 사용이 가능하다. 이는 네트워크 기술의 발전과 디스크 저장장치의 발전 등에 따른 프로파일 수집과 저장 능력의 향상에 기인한 것이며, 최근 정보검색 기술의 발전 또한 웹상에서 SNS이용자의 변경된 정보를 쉽게 추적 및 저장할 수 있으며, 원하는 조건에 해당하는 상세검색을 통해 그 조건에 맞는 사람만 간추려 낼 수 있다.

이후 데이터 수집으로 개인의 프로파일에 나타난 정보 외에도 SNS 이용시간, 방문기록, IP주소 등의 부가적

인 2차 정보 취득이 가능하며 이러한 2차 정보를 통해서 스팸과 불법광고 등의 수단으로 악용될 가능성이 있다.

또한 얼굴인식은 SNS의 개인 프로파일에 기록이 되어 있을 사용자의 이미지를 식별하여 최근 컴퓨팅 기술의 발전과 보다 빠르고 효율적인 얼굴 인식 알고리즘에 의해 특정 인물을 쉽게 추적하여 사생활 침해 가능성이 있다.

얼굴인식 기술을 활용한 콘텐츠 기반 이미지 검색(Content-Based Image Retrieval, CBIR)은 수사를 위한 목적으로 개발이 되었지만, 이를 통해 해당 이미지와 유사한 다른 이미지들을 인터넷 상에서 검색하여 추적함으로써 사용자의 위치정보를 획득할 수 있다.

마지막으로, SNS 상에서 사용자 계정을 삭제하였음에도 불구하고 콘텐츠나 댓글 등의 2차 정보에 잔존할 수 있다. 이러한 2차 정보를 완전히 삭제하는 것은 수동으로 해당정보를 제거를 해야 가능하여 많은 작업 단계가 요구된다. 이렇게 잔존하는 2차 정보를 통해서 계정을 삭제한 이용자에 대한 개인정보수집이 가능하다.

3.2 기존 네트워크상에서의 보안 위협

소셜 네트워크 스팸(SN Spam)은 SNS 사용자의 명단을 추출하는 자동화된 검색도구를 이용하여 이들에게 스팸 메일을 발송하고 특정 이미지나 문구를 이용하여 초대 메시지와 메신저 대화를 통해서 피싱 목적의 위조된 외부 사이트로 이동하도록 링크가 가능하도록 한 기법이다.

XSS, 웹·바이러스 는 SNS 사이트의 글에 첨부되는 첨부파일과 게시되는 동영상 등의 콘텐츠에 악성코드나 웜을 삽입하여 해당 SNS사이트의 방문자를 통해 유포한다. 이렇게 유포된 악성코드나 웜을 통해서 사용자의 계정이 손상되고 피싱 및 트래픽 과부하가 걸리는 등 개인정보 유출 등을 초래하게 하는 심각한 상황을 야기시키고 있다.

3.3 ID 관련 위협

SNS를 이용한 피싱으로 SNS상에서 개인의 프로파일과 게시판 등의 특정 웹 페이지에 악성코드를 심어놓음으로써 이를 사용하는 사용자를 특정 피싱 사이트로 유도한다. 사용자 간의 신뢰관계 및 다수의 사용자가 이용하는 SNS의 특성 상 피싱으로 인한 피해는 점차 확산될 것으로 예상된다[5].

또한 네트워크 침입을 통한 정보유출로 SNS 상에서

프라이버시 보호를 위한 가장 기본적인 수단으로 각 회원 간 ‘친구 맺기’를 통한 특정인의 정보에 대한 접근 통제 방법이다. 하지만 특정인을 사칭하여 ‘친구 맺기’를 시도한 후 개인정보를 획득하는 경우가 발생한다. 이와 비슷한 ID 도용에 의한 프로파일 위조 및 명예훼손으로 연예인이나 유명인사 또는 유명 상표에 대한 명예훼손을 목적으로 비슷한 가짜 프로파일 생성이 가능한 방법을 이용해 특정인을 명예훼손 하는 사건이 점차 증가하고 있다.

3.4 사회적 위험

사이버 스토킹(Cyber Stalking)은 SNS상의 게시물과 메신저, 이메일 등을 이용하여 피해자와 반복적인 접촉을 가능하게 함으로써 기존의 오프라인 스토킹보다 시간, 장소에 구애받지 않으며, 불특정 다수로 하여금 쉽게 상대방을 위협하고 괴롭힐수가 있다[7].

이와 반대로 사이버 괴롭힘(Cyber Bullying)은 인터넷과 이동전화를 통해 진행되는 방법으로 사이버 폭력이라고도 지칭하며, SNS의용이성, 익명성 등과 같은 특성으로 인해 사이버 괴롭힘에 취약하다.

또한 사회공학 기법을 이용한 공격이 점차 증가하는 추세로서, 이는 SNS 상에서 사생활 보호 설정이 미흡한 경우 주로 발생할 수 있다. 사용자는 이러한 정보를 이용하여 특정 기업의 정보를 탈취가 가능한 점을 이용해 산업스파이가 기승을 부리고 있다.

4. 대응 방안

4.1 스팸을 방지한 자동 필터링

필터링 기술을 피싱, 바이러스, 스팸 등 불법 유입 방지에 이용한다. 필터링 기술은 유행과 해당 문화를 반영하지 못하여 인적 개입을 통한 유해 콘텐츠 식별 및 분류를 완전히 대체하지는 못하지만 자동·반복적으로 생성하고 유포하는 콘텐츠를 효과적으로 방어 가능하다. 이러한 필터링에 적합한 알고리즘으로 네이브 베이지언(Naive Bayesian)을 들 수 있다.

가설H와 데이터 D, H의 사전확률P(H), D를 보게 됨으로써 가지는 H가 ‘참’이 되는 조건부 확률P(D|H), D의 경계 확률P(D), P(H|D)는 사후확률이다. 이 확률은 주어진 데이터와 가설에 대한 사전 믿음이 주어진 상태에서 가설이 참일 때의 확률이다.

$$P(H|D) = \frac{P(D|H)P(H)}{P(D)}$$

다른 말로 하면, 먼저 어떤 문서 d가 있고, 이것을 특정 카테고리 c에 속할 확률은 P(c|d)라고 할 수 있고, 구하고자 하는 P(c|d)는 베이즈 정리에 따라 $P(c|d) = \frac{P(c)P(d|c)}{P(d)}$ 가 된다. 여기에 분모 p(d)는 항상 같기 때문에 분자 P(c)P(d|c)에 대해서만 계산한다. 문서 d를 구성하고 있는 i번째 단어를 X_i 라고 하고 각 단어들은 서로간에 연관성없이 독립적으로 출현한다고 가정하면, 이제P(d|c)는 $\prod_i P(x_i|c)$ 로 계산될 수 있다. 결국 어떤 문서 d가 특정 카테고리 c에 속할 확률은 그 카테고리 c에 속한 문서들 사이에 출현한 단어 x_i 확률의 곱으로 계산될 수 있다.

위의 수식을 활용하여 특정 텍스트에서 개별단어의 출현빈도를 모두 기록하고 비슷한 분류의 텍스트를 계속 추가시켜 단어들의 연관을 추적하면 임의의 텍스트가 해당분류에 포함되는지 구분을 할 수 있다. 다음은 네이브 베이지언 알고리즘을 사용한 스팸 필터링 방법이다[7].

네이브 베이지언 알고리즘을 사용한 스팸 필터링 방법은 스팸으로 판단된 문서들에서 자주 출현한 단어를 많이 포함한 문서는 스팸일 가능성이 높다는 가정을 주어 스팸지수를 계산한다.

- 1) 사전에 스팸으로 판단된 문서 - 사용자들이 사전에 스팸으로 등록한 모든 데이터셋을 말한다.
- 2) 자주 출현한 단어 - 전체 데이터셋에서 각 단어의 빈도수를 계산한 후 스팸의 특성으로 예상되는 단어를 말한다.
- 3) 스팸 가능성 - 대상이 되는 문서로부터 추출된 스팸의 특성 단어의 가중치를 계산한 지수가 높을수록 스팸일 가능성이 높다.

위와 같은 기존의 방법을 이용하여 자동 필터링을 이용하고, 여기에 빅데이터의 기법을 이용하여 자도 사용되는 스팸의 내용을 자동으로 필터링을 하도록 하는 방법도 하나의 대응방법이다.

SNS서버에서 SPAM에 대한 검색 기능을 강화하여 사전에 차단할 수 있는 방법과 DB화를 패턴의 분석을 통하여 차단할 수 있다.

[Fig. 1] SPAM Result Process

4.2 Spidering 제한

Spidering이라 함은 검색엔진의 색인에 들어갈 내용을 만들기 위해 웹사이트들을 방문하여 웹 페이지 및 기타 여러 가지 정보를 읽어오는 것을 말하며, indexing 이라고도 불린다. 이를 SNS 운영자가 본래의 용도 외에 이용하는 것을 제한하여 불법적인 개인정보 수집 활동을 방지할 필요가 있다.

5. 결론

본 논문에서는 인터넷의 발전과 더불어 사이버공간에서의 가상공간에 집결하는 것이 가능하게 되어 온라인상에서 인적 네트워크 형성을 도와주는 SNS의 이용에 대한 사용자들의 보안 위협에 관하여 알아보았다. 하루가 다르게 발전하는 인터넷 기술과 내 손안의 컴퓨터라 불리는 스마트폰으로 인하여 SNS는 더욱 많은 사람들이 이용하고 있지만, 자신도 모르는 사이 자신의 정보들이 노출되고, 악용되는 문제점을 가져왔다. 더욱 발전된 기술로 인해 인터넷과 SNS이용자가 많아질 것으로 예상되기 때문에 이에 따른 개인정보보호에 대한 보안요소가 강화되어 이용자들의 개인정보가 쉽게 노출이 되는 일 없이 안전하게 사용할 수 있길 기대한다. 또한 SNS의 역기능에 대한 이용자의 인식 제고 및 홍보, 교육과 현행 규제정책의 재해석 및 재정비, 데이터 처리 과정의 투명성, 사이버 윤리 교육 강화가 이뤄지길 기대한다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2013R1A1A1A05012348)

REFERENCES

- [1] 「Information and Communication Network Utilization and Information Protection Act」 Amendment, Information and Communication, 2006.
- [2] Dong-Hee Kim, Eun-Jae Yu, Gyeong-Sik Min "Online social network environment, security threats and implications", Information Security Issue Report, 2008.
- [3] Gyu-Won Jang, Hyeon-Seok Yun. "Privacy in cyberspace". Information Society Policy Research Forum Article 22, Issue 3 Forum. 2011.
- [4] Hee-Yeon Kim, Ju-Hyeon Oh. "Status and social implications of domestic SNS". Information and Communications Policy Studies No. 12, No. 24, 2012.
- [5] Keun-Ho Lee, "M2M (Machine to Machine) communication of threat analysis" Korea Academic Society 2010 Spring Conference eye Writings Part 1.
- [6] Seun-Gi Mun 3others "M2M communication for building secure mutual authentication and key exchange protocol", Journal of Cryptology, Volume 20, No. 1, pp. 73-83, 2010.
- [7] Min-Yeong Ju, "The Twitter account hacking, spamming hundreds of diet", Blotter, 2010.
- [8] Cyber Police, <http://www.police.go.kr>.

저자소개

고 준 영(Jun-Young Go)

[학생회원]

· 2009년 3월 : 백석대학교 정보통신학부 재학생

<관심분야> : M2M 보안, 지능형자동차 보안 등

이 근 호(Keun-Ho Lee)

[종신회원]

- 2006년 8월 : 고려대학교 컴퓨터
학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성
전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교
정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개
인정보보호