ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

국방정보보호를 위한 軍 SNS 보호프로파일(PP) 개발에 관한 연구☆

Research on Military SNS Protection Profile for National defense

유 덕 훈[1] 김 승 주[1*]
DeokHoon Yu SeungJoo Kim

요 약

새로운 커뮤니케이션 플랫폼인 소셜네트워크 서비스(이하 SNS : Social Network Service)는 다양한 정보의 빠른 전달과 함께 상호신뢰를 바탕으로 의사소통을 강화하고 친밀감을 형성해 조직 활성화에 기여하였다. SNS의 사회적 중요성이 높아짐에 따라 군에서도 SNS를 통해 자발적 참여와 신뢰관계 구축을 바탕으로 군내 · 외 유대감 강화에 활용하고 있다. 그러나 국방 SNS 도입시 개인정보의 노출이나 프라이버시 침해, 군사자료의 유출 등과 같은 역기능은 군에 치명적인 요인이 될 수 있어 이에 대한 보안대책이 필요하다. 본 논문에서는 국방 SNS 도입을 위해 SNS 기능별 유형을 분류하고, 유형별 구조를 분석하여 국방 SNS에 필요한 보안기능요구사항을 제시하고자 한다.

☞ 주제어 : 국방정보보호, 보호프로파일, 소셜네트워크 서비스

ABSTRACT

Social Network Service(SNS) have become very popular during the past few years. Also SNS, an current communication platform, greatly contributes to transmit the information rapidly and strengthen a sense of community and fellowship in military service. however it has vulnerable factors. For example, invasion of privacy, exposure of personal information and military data. In this particular case, it is a deathblow to the military service. Military Social Network Service require to protect the military security threats and disclosure of defense secrets. For such reasons we need the secure SNS that protects from any attacks or vulnerable factors. We present classification of functional type and analysis the SNS architecture. The goal of this work is propose military SNS security functional requirements for practical use safely.

☞ keyword : Military Security, Protection Profile, Social Network Service

1. 서 론

소셜네트워크 서비스(이하 SNS라 한다)의 등장은 사회구성원들간에 다양한 정보를 개방·공유 하는 등 쌍방향 의사소통을 가능하게 만들었다.

SNS의 중요성이 사회적으로 높아지면서 군에서도 '군장병 SNS 가이드라인'을 제작하는 등 SNS 활용과 보안에 대해 관심을 보이고 있다. SNS는 유형별로 기능이 매우 전문화 되어 있고 종류도 다양해 군사용으로 도입시 매우 폭넓게 활용될 수 있을 것으로 기대된다.

그러나 상용 어플리케이션이나 시스템을 도입하기 위해서는 군내 보안위협에 대비할 수 있는 보안기능들이 필수적으로 포함되어야 한다. 특히 SNS는 개인정보의 노출 위험이 높고 허위정보의 전파나 정보탈취 등 위협요소가 많아 군내 사용시 각별한 주의가 요구된다.

본 논문에서는 상용 SNS에 대한 연구를 위해 기능별로 유형을 분류하고 유형별 대표적인 SNS 구조를 분석하여 SNS의 통합모델을 제시하였다. 그리고 SNS 위협으로부터 취약점을 도출하여 상용 SNS를 군에 적용할 수 있는지 판단하였으며, 군내 보안환경을 고려한 추가적인 위협 도출과 이에 대한 보안기능요구사항을 제시하였다.

논문 구성은 2장에서 SNS 정의와 공통평가기준에 대해 소개 하였으며 3장은 SNS의 기능별 유형 분류와 통합모델을 제시하고 상용 SNS에서의 보안위협을 설명하였다. 4장에서는 군 SNS 도입을 위한 보호프로파일을 작성

1 Center for Information Security Technologies(CIST), Korea University
* Corresponding author (skim71@korea.ac.kr)
[Received 30 October 2012, Reviewed 1 November 2012, Accepted 10 December 2012]
☆ "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(NIPA-2012-H301-12-4008)

하고 5장에서 결론을 맺었다.

2. 관련연구

2.1 소셜네트워크 서비스

SNS란 사용자 간의 자유로운 의사 소통과 정보 공유, 그리고 인맥 확대 등을 통해 사회적 관계를 형성하고 강화시켜주는 온라인 플랫폼이라고 정의하고 있다[1]. Social Network Service란 말을 직역하면 사회적 인맥 서비스라고 할 수 있는데 넓은 의미로는 인맥에 관련된 모든 종류의 서비스들을 SNS라고 할 수도 있다[2].

미국 UC 버클리대 교수와 미시간 주립대 교수는 SNS에 대해 사용자들로 하여금 제한된 시스템내에서 공개적이거나 반공개적으로 자신의 프로필을 구성하고, 인적 연결을 공유하는 타 이용자들의 목록을 보여주며, 자신의 연계목록 및 다른 사용자들에 의해 생성된 목록을 열람하거나 관계를 맺을 수 있도록 하는 웹 기반 서비스라고 정의하였다[3].

국방에서 SNS를 안전하게 활용하기 위해서는 먼저 SNS에 대한 기본적인 구조와 보안기능을 분석하여 근본적인 개념부터 새롭게 정의할 필요가 있는데, 국방 SNS에 대한 정의는 4장에서 설명한다.

2.2 공통평가기준(CC:Common Criteria)

국제공통평가기준(이하 CC)은 국가마다 다른 정보보호시스템 평가기준을 연계시키고 평가결과를 상호인증하기 위해 제정된 평가기준으로, IT제품의 보안기능성과 평가 과정에서 그 제품에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써 독립적으로 수행한 보안성 평가 결과들간에 상호비교를 가능하게 한다. CC는 세 부분으로 구성되어 있는데, 제1부는 소개 및 일반모델로 CC에서 사용되는 용어의 정의와 개념에 대해 자세히 설명한다. 제2부 보안기능요구사항(SFR : Security Functional Requirement)은 보안활동에 대한 정의 및 해석에 대해 서술하며 제3부 보증요구사항(SAR : Security Assurance Requirement)은 정보보호시스템이 제공해야 하는 기능 및 보증요구사항을 기술하고 있다[4].

정보보호시스템 평가의 핵심인 보호프로파일은 평가대상(TOE)을 설정하고 TOE의 보안문제에 대응하기 위한 보안요구사항을 기술한 문서이다.

본 논문에서는 공통평가기준 3.1(R3)을 바탕으로 국방 SNS 보안기능요구사항을 제시하고자 한다.

3. SNS 유형과 위협분석

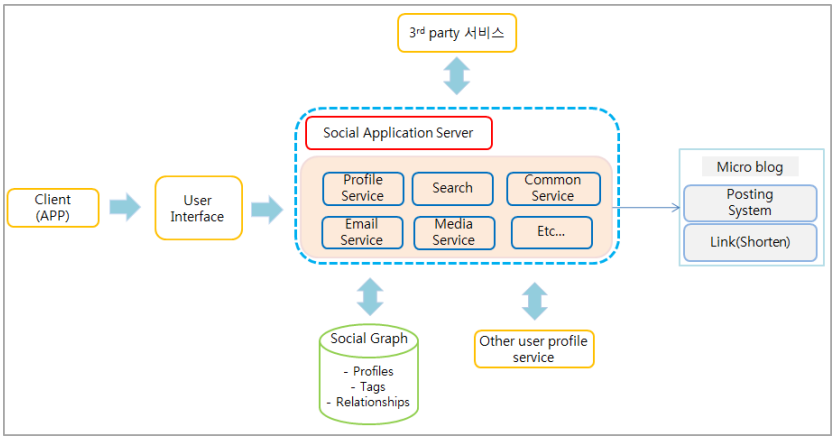
3.1 SNS 유형분류

SNS에 대한 기능별 유형을 분류하고, 유형별 구조를 분석하여 국방에서 요구하는 보안기능을 도출하여야 한다.

본 논문에서는 기존의 연구에서 제시했던 SNS 유형에서 자신과 친구의 위치를 알려주는 위치기반 SNS와 사이버 공간에서 다수의 사람들과 커뮤니케이션 할 수 있는 가상환경 SNS를 새롭게 추가하여 표 1과 같이 10개의 유형으로 분류하였다. 대부분의 SNS는 기능에 따라 제시

(표 1) SNS의 기능별 유형분류
(Table 1) Functional Classification of the SNS

구 분	내 용	서비스
프로필 기반	특정 사용자나 분야의 제한 없이 누구나 참여 가능한 서비스	페이스북, 마이스페이스
비즈니스 기반	업무나 사업관계를 목적으로 하는 전문적인 비즈니스 중심의 서비스	링크드인, 비즈니스 페이스
블로그 기반	개인 미디어인 블로그를 중심으로 소셜네트워크 기능이 결합된 서비스	네이버통, 윈도우라이브스페이스
버티컬	사진, 동영상, 리뷰 등 특정 분야의 버티컬 UCC 중심의 서비스	유투브, 아프리카, 다음팟
협업기반	공동 창작, 협업 기반의 서비스	위키피디아
커뮤니케이션 중심	채팅, 메일, 동영상, 컨퍼러싱 등 사용자간 연결 커뮤니케이션 중심의 서비스	세이클럽, 네이트온, 미보
관심주제 기반	분야별로 관심 주제에 따라 특화된 네트워크 서비스	도그스터, 트렌드밀
마이크로블로깅	짧은 단문형 서비스로 대형 소셜네트워킹 서비스 시장의 틈새를 공략하는 서비스	트위터, 텀블러, 미투데이
가상환경 기반 (추가)	사이버 공간을 통한 가상세계에서 아바타 등을 통해 자신을 표현하고 커뮤니케이션 하는 서비스	세컨드 라이프
위치기반(추가)	다른 SNS와 결합하여 친구위치나 자신의 위치를 알려주는 서비스	포스퀘어, 씨온



(그림 1) SNS 구조 통합모델
(Figure 1) SNS Total Model

된 10개의 유형으로 분류할 수 있다[5].

3.2 SNS 구조

SNS의 구조를 살펴보면 SNS는 사람들이 수행할 수 있는 다음과 같은 특정 구성요소를 포함한다[6].

- SNS의 특징은 사용자들의 온라인 프로필을 정의한다.
- 친구나 동료들과 사회적 관계를 형성한다.
- 그 연결된 활동의 알림을 통보 받는다.
- 본인이 소속된 지역사회 활동에 참여하고 서비스의 제어권한 설정이나 개인정보보호 설정을 할 수 있다. 그리고 응용 프로그램이나 협업 서비스 기관의 공개 인터페이스와 상호 작용하는 서비스를 제휴할 수 있다.

SNS의 공통된 구조는 클라이언트로부터 유입되는 정보를 식별 및 인증하는 기능에서부터 필요한 정보를 찾기위한 검색 기능이나 메일, 미디어 서비스 등 유형별로 특성화된 다양한 기능이 지원된다. 사용자의 정보는 데이터베이스에 저장되고 데이터베이스에는 사용자와 연결된 인적구성도와 관계도, 프로필 등 중요한 정보를 저장한다[7].

대부분의 SNS가 이러한 구조를 구성하고 있으나 트위터와 같은 단문 형식의 마이크로 블로깅 시스템에서는 포스팅 시스템이나 긴 문자열을 짧게 해주는 Shorten 기능이 요구된다. 마이크로 블로깅은 기본적으로 불특정 다수를 대상으로 하는 커뮤니케이션이기 때문에 메시지가 급격하게 전파되며 형식이 복잡하지 않아 제약을 받지 않는다[8]. 따라서 국방 SNS에서 마이크로 블로깅 서비스를 이용하기 위해서는 외부에 배포되는 글을 선택하거나 키워드를 설정하여 필터링 하는 등 선별적 배포를 위한 정책이 동반되어야 한다.

유형별로 대표적인 SNS 구조를 분석하여 그림 1과 같이 SNS 구조의 통합모델을 제시하였으며, 이를 바탕으로 4.3.장에서 SNS PP의 TOE를 정의하였다.

3.3 SNS 보안위협

위협은 현재까지 알려진 위협과 발생가능한 위협으로 구분할 수 있는데, 현재까지 알려진 위협은 취약점 데이터베이스를 통해 확인할 수 있다. 미국국립표준기술원(NIST)의 취약점 데이터베이스(National Vulnerability Database)에서는 공통취약점 목록표 CWE(The Common Weakness Enumeration)를 제시하고 있다[9]. CWE는 대표적인 단일 취약점 유형 뿐만 아니라 관련된 세부 취약점 항목을 추가로 확인할 수 있으므로 이 목록표를 통해 현재까지 알려진 위협에 대한 취약점을 확인할 수 있다. 그러나 CWE에서 제시하는 취약점은 보안에 대한 전반적인 범위를 포괄하고 있기 때문에 SNS에 특화된 보안위협을 도출하기 위해서는 어떤 위협이 어떻게 발생하는지 분석할 필요가 있다.

SNS에서 발생 가능한 보안위협은 유럽정보보호전문기관(ENISA)에서 제시한 15가지 위협과 시만텍의 위험 보고서를 통해 SNS 위협과 가능한 공격 시나리오를 작

성하였다[10,11].

- SNS 스팸 : 무작위 인원들을 대상으로 친구요청을 신청 후 수락이 되면 스팸메일을 발송하거나 사용자의 정보를 수집하여 취미나 관심사항에 맞는 스팸메시지를 발송하는 맞춤형 스팸
- SNS 사기 : SNS는 개인의 관심사항이 노출되기 때문에 이를 악용하여 대상자에게 접근후 호의를 제공하고 이를 빌미로 금전 등을 요구한다.
- 악성코드 : 어플리케이션이나 게시판 등에 악성스크립트 코드를 삽입후 사용자가 감염된 사이트에 접근하면 그 사용자의 정보를 획득한다.
- 패스워드(개인정보) 공격 : 보안질문을 통해 패스워드에 대한 힌트나 답을 추측해 낼 수 있는 서비스를 제공하는데, 질문에 대한 답을 쉽게 추측하거나 맞출 수 있기 때문에 공격자는 사용자의 계정정보를 획득할 수 있고 다시 계정을 셋팅 후 다른 사람들의 정보를 수집하거나 스팸을 보낼 수 있다.
- 어플리케이션 접근 공격 : 어플리케이션 설치 승인 시 사용자의 이름과 사진, 아이디, 친구목록 등 기본적인 정보를 모두 공개하도록 요구하며, 설문조사를 유도하는 등 어플리케이션의 주된 목적이 제공되는 컨텐츠 서비스에 가입하도록 사용자를 속인다.
- 검색엔진 공격 : 키워드 및 유도하고자 하는 링크를 검색결과 처음에 등장시키거나 높은 순위에 랭크시킴으로써 사용자들의 접근을 유도, 공격자는 트위터를 통해 최신 키워드나 트랜드를 확인하고 이 메시지가 포함된 정상적인 트위터 사이트를 악성사이트의 Short URL로 교체하여 리트윗 한다.
- 유명인 및 친구명의 사칭 : 유명인의 사진과 가짜 프로필을 등록하여 잘못된 정보를 전파하거나 사람들이 팔로우를 신청하도록 유도하여 이를 이용해 광고나 스팸메시지에 악용한다.
- XSS : 악성스크립트를 포함한 URL을 피해자에게 노출시켜 원하는 행위를 할 수 있다.
- CSRF : XSS와 유사하나 Web에서 사용되는 신뢰된 사용자의 권한을 이용할 수 있다.
- 피싱 : 계정과 패스워드를 알아내기 위해 원래사이트의 복사본을 만들어 접속하는 사용자의 계정과 패스워드를 획득한다.
- 기업정보 유출 및 평판위험 : SNS 서비스를 통해 기업의 민감한 내용을 유출시키거나 조직에서 사용된 보안소프트웨어의 취약점을 게시함으로써 공격자에게 정보를 노출시킬 수 있다.

(표 2) 국방 SNS 자산
(Table 2) Military SNS Assets

비밀자료	1급	국가 안전보장 및 국가 이익에 치명적 위험을 초래
	2급	국가 안전보장 및 국가 이익에 현저한 위험을 초래(암호자재)
	3급	국가 안전보장 및 국가 이익에 상당한 위험을 초래(음어자재)
	대외비	비밀은 아니지만 대외 유출시 군에 유해하거나 지장을 초래하는 자료
중요자료	전투근무지원을 위한 민감한 평문정보로써 제대규모, 전투편성표 등의 자료와 군수물자 및 전투장비 현황, 부대위치 등의 내용	
일반자료	문헌관리나 지식자료 등 일반적인 평문정보로 인터넷에서 공유할 수 있는 자료	

4. 국방 SNS 보호프로파일

4.1 국방 SNS 정의

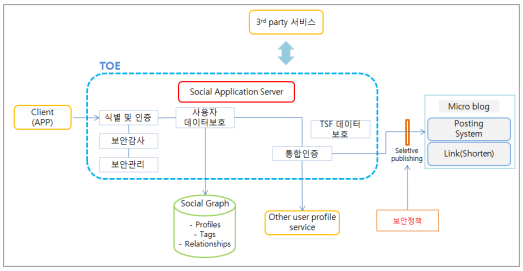
국방 SNS란 사용자 역할에 대한 접근권한을 통제하며 연결된 사람들의 정보를 포함하는 ID 관리 도구이다. 군은 폐쇄적인 조직이지만 SNS를 통해 연결된 모든 사람들의 정보를 프로파일 검색이나 통합인증을 통해 다른 사이트에서도 확인할 수 있으며, 한 사람의 ID가 도용되거나 유출되었을 경우 연결된 사람들의 정보뿐만 아니라 SNS를 통해 각종 군사정보가 노출될 수 있기 때문이다.

4.2 국방 SNS 자산

국방 SNS에서 자산은 국방정보시스템에서 생산, 처리, 저장, 유통되는 정보의 기밀성 수준으로 구분된다[12]. 비밀자료는 대외비를 포함한 3급 이상의 군사기밀로 누설될 경우 국가이익에 위협을 초래할 것으로 인정되는 가치를 지닌 정보이다[13]. 그러나 현재 군에서 SNS를 통해 군사기밀이 직접 유출된 사례나 위협은 발생하지 않았지만, 비밀 유출의 경로가 다양해지고 있으며 비밀이 아니더라도 외부 노출시 군사보안이 위협 받을 수 있는 민감한 평문 정보들은 군에 위협을 초래할 수 있다.

4.3 TOE(Target of Evaluation) 개요 및 범위

국방 SNS의 TOE는 사용자에게 소셜 서비스를 제공하는 웹 서버로써 공용망을 통해 통신이 이루어지며, TOE



(그림 2) TOE 범위
(Figure 2) TOE Range

는 서비스를 제공하기 위한 사용자 식별 및 인증 모듈과 중요 데이터의 안전한 관리를 위한 보안관리 모듈, 사건 발생시 조사를 위한 보안감사 모듈, 사용자 데이터 보호와 TSF 데이터 보호 모듈로 구성된다. 그림 2는 TOE 범위를 설명한다.

- 식별 및 인증 : 관리자와 사용자의 식별 및 인증기능을 수행한다. TOE에 인가된 관리자만 접근할 수 있으며 인증 실패시 적절한 대응행동을 제공한다.
- 보안관리 : TSF(TOE Security Functionality) 데이터, 보안역할 등과 관련된 사항을 효율적으로 관리하기 위한 수단을 제공한다.
- 보안감사 : 보안관련 사건들의 감사 레코드를 생성하고 기록한다. 필요시 기록된 내용을 통해 어떤 보안관련 행동이 발생했는지 알 수 있고 책임을 물을 수 있는 자료로도 활용될 수 있다.
- 사용자 데이터 보호 : 접근통제 및 정보흐름 통제를 수행하여 침입을 탐지하고 차단할 수 있다.
- TSF 데이터 보호 : TOE의 TSF를 보호하기 위해 데이터의 가용성, 무결성, 비밀성 보호와 TOE 자체 상태 확인을 수행한다.

4.4 보안문제 정의

TOE 보안문제는 TOE 보안 환경에 미치는 위협, 조직의 보안정책, 그리고 지원되어야 할 가정사항으로 구분된다.

4.4.1 위협

민간영역에서의 SNS 위협은 대부분 개인정보 수집이나 계정획득과 관련되어 있기 때문에 상용 SNS는 위협으로부터 개인정보보호와 사용자의 계정관리에 집중된 보안기능을 지원하고 있다[14]. 반면에 군 정보통신망에서의 보안위협은 올해 초부터 4월까지 인터넷망을 통해 악성 바이러스들이 군 전장망에 312건, 국방망은 5,901건이나 침투하는 등 외부 공격 위협에 항상 노출되어 있다[15]. 따라서 군에서 도입한 SNS가 보안기능이 취약하면 오히려 군내 또다른 보안문제를 발생시킬 수 있는데, 군은 민간에 비해 위협원과 공격 대상, 공격자가 군 정보통신망에 접근하는 목적 자체가 달라 상용 SNS의 보안기능만으로는 군에서 발생할 수 있는 위협에 충분히 대비할 수 없다.

결국 국방정보보호를 위해서는 군내 발생 가능한 모든 위협에 대한 보안기능이 필요하다. 국방 SNS에 대한 위협은 취약점 데이터베이스와 각종 위협 보고서, 논문 등을 통해 다음과 같이 도출하였다. 표 3은 국방 SNS의 위협을 도출한 근거를 나타낸다.

① SQL 취약점 : 공격자가 임의의 SQL 명령을 통해 인증을 우회하여 내부 자료에 접근할 수 있다[9].
② 인증 취약점 : 인증을 우회하고 사용자 및 쿠키의 임의의 값을 통해 관리자 권한을 얻을 수 있다[9].
③ 코드주입 : 공격자가 URL을 통해 임의의 PHP 코드를 실행할 수 있어 정보 변조나 유출이 가능하다[9].
④ XSS : 원격 공격자가 임의의 웹 스크립트나 HTML을 삽입할 수 있다[9].
⑤ CSRF : 관리자 작업을 통해 관리자 계정을 추가 요청해 관리자의 인증을 하이재킹 할 수 있다[9].
⑥ 버퍼오버플로우 : 원격 공격자가 응용 프로그램의 제한을 초과하도록 하여 중요한 정보를 얻을 수 있다[9].
⑦ 개인정보 공개설정 : 노출된 개인정보를 통해 특정 사용자를 위장하거나 훼손, 정보조작 등이 가능하다[10].
⑧ 완전한 정보삭제 어려움 : 링크 및 가공된 정보들의 증가로 원하지 않는 정보의 완전한 삭제가 어렵다[10].
⑨ 불법 AP를 통한 네트워크 침입 : 불법 설치된 Rogue AP를 통해 내부 네트워크의 모든 자원에 접속할 수 있다[16].
⑩ 시스템 및 OS패치 취약 : 공격자는 특정서버를 대상으로 다수의 traffic을 발생시켜 악의적인 목적으로 시스템의 동작을 마비시킬 수 있다[16].
⑪ 전송데이터 암호 취약점 : 공격자는 전송 데이터를 도청하여 암호를 해독한 후 데이터를 다시 전송하여 획득하고자 하는 값을 유추하거나 수집할 수

있다[16].

⑫ Shorten URL : URL Shortening 서비스를 통해 바이러스 및 악성코드에 감염시킬 수 있다[11].

⑬ 어플리케이션 설치 : 게임이나 퀴즈 등의 타사 응용 프로그램을 추가할 수 있는데 이러한 응용 프로그램을 통해 악성코드 등에 감염될 수 있다[17].

⑭ 검색엔진 조작 : 검색엔진을 통해 검색한 결과를 조작하여 높은 순위에 랭크시킴으로써 사용자들을 유도할 수 있다[11].

⑮ 취약한 패스워드 설정 : 힌트를 제공하는 보안질문 서비스를 통해 사용자의 패스워드를 유추할 수 있다[11].

⑯ 명의사칭 : SNS에서 유명인이나 친구의 정보를 이용하여 허위계정을 만들어 접근할 수 있다[11].

⑰ 평판조작 : 특정 조직이나 기업에 소속된 사용자들이 의도적으로 평판을 조작할 수 있다[18].

⑱ 서버정보 제공 : 에러페이지를 통해 웹서버에서 해당 비정상 요청에 대해 알려주는 페이지를 이용해 서버 정보가 노출될 수 있다[19].

⑲ 사용자 인증체계 취약 : 공격자는 전송되는 URL 또는 URL의 파라미터를 조작하여 전송함으로써 사용자로 인증을 시도할 수 있다[19].

⑳ 관리자 페이지 권한 미설정 : 사용자 인증 후 접속되는 페이지의 URL을 주소창에 직접 입력하거나 쿠키를 조작하여 인증을 시도할 수 있다[19].

㉑ 첨부파일 다운로드 : 상대경로 표시 문자열을 통해 허가되지 않은 상위경로로 이동하여 시스템 주요 파일, 소스코드 등 중요자료의 열람이 가능하다[19].

㉒ 첨부파일 업로드 : 파일 첨부를 할 수 있는 게시판에 허용된 파일 이외에 악의적인 스크립트가 포함된 소스파일을 첨부할 수 있다[19].

4.4.2 조직의 보안정책

조직의 보안정책은 TOE를 운영하는 조직 내부의 보

(표 3) 위협과 취약점 대응

(Table 3) Correspond to Threats and Vulnerabilities

위협 / 취약점	T. 스팸메일유입	T. 기록실패	T. 연속인증·우회	T. 재사용공격	T. 피싱	T. 위장	T. 저장데이터훼손	T. 전송데이터훼손	T. 서비스거부공격	T. 잔여정보	T. 정보누출	T. 암호해독공격	T. 바이러스·웜침해	T. 웹콘텐츠변조	T. 허위정보유포
①			O				O								
②			O												
③							O						O		
④							O						O	O	
⑤			O	O									O		
⑥		O							O						
⑦	O					O				O	O				
⑧	O					O				O	O				
⑨							O	O							
⑩		O							O						
⑪								O				O			
⑫					O								O		
⑬	O				O								O		
⑭					O								O		O
⑮						O				O					
⑯	O					O									O
⑰															O
⑱				O					O						
⑲			O					O							
⑳			O	O				O							
㉑							O								
㉒							O							O	

(표 4) 보안문제 정의
(Table 4) Definition of Security Problem

보안문제		내 용
위협	T.스팸 메일유입	메일서버로 사용자들이 원하지 않는 광고성 이메일이나 악성 메일을 일방적으로 보낼 수 있다.
	T.기록 실패	위협원은 저장용량을 소진시켜 보안관련 사건이 기록되지 않도록 할 수 있다.
	T.연속 인증시도/우회	내부에 접근하기 위해 연속적으로 인증을 시도하거나 우회하여 인가된 관리자 권한을 획득할 수 있다.
	T.재사용 공격	위협원은 관리자 인증 데이터를 재사용하여 TOE에 접근할 수 있다.
	T.피싱	원래 사이트의 복사본을 만들어 접속하는 사용자의 계정을 획득할 수 있다.
	T.위장	위협원은 사용자 개인정보를 이용하여 정당한 사용자로 위장할 수 있다.
	T.저장데이터훼손	위협원 또는 인가된 사용자는 시스템에 저장된 데이터를 변경, 삭제할 수 있다.
	T.전송데이터훼손	위협원은 서버의 전송 정보를 변경하여 사용자의 정보를 훼손할 수 있다.
	T.서비스 거부공격	위협원은 웹 서버의 오작동을 유발시켜 조직의 정상적인 웹 서비스 제공을 방해할 수 있다.
	T.잔여 정보	사용자의 잔여정보를 적절하게 제거하지 못해 위협원이 정보에 접근할 수 있다.
	T.정보 누출	위협원은 TOE로부터 누출된 정보를 악용할 수 있다.
	T.암호 해독공격	암호해독 공격을 사용하여 인가되지 않은 전송 데이터에 접근할 수 있다.
	T.바이러스 · 웜 침해	위협원은 네트워크, 이동식 저장매체 등을 통해 바이러스를 유입시켜 PC 또는 서버자원을 손상시킬 수 있다.
	T.웹 콘텐츠 변조	위협원은 악의적인 목적으로 웹 콘텐츠를 변조할 수 있다.
	T.허위 정보유포	위협원은 정보를 조작하거나 허위 사실을 유포할 수 있다.
조직의 보안 정책	P.보안 감사	보안관련 행동에 관한 사건탐지, 감사데이터 생성 및 대응한다.
	P.운영 환경분리	군 SNS는 인터넷망과 군 정보통신망을 물리적으로 분리하여 운영한다.
	P.안전한 관리	인가된 관리자는 정기적인 교육을 통해 시스템을 안전하게 관리하고, 그에따라 시스템을 운영한다.
가정 사항	A.물리적 보안	TOE는 군 정보통신망과 물리적으로 분리된 안전한 환경에 위치한다.
	A.운영체제보강	운영체제상의 취약점을 제거하여 운영체제에 대한 신뢰성과 안정성을 보장한다.
	A.신뢰된 관리자	TOE의 인가된 관리자는 악의가 없으며 TOE에 대해 적절히 교육 받았고 정확하게 임무를 수행한다.

안정책을 의미한다. 국방에서 민간과 구분되는 가장 큰 특징은 인터넷망과 국방 정보통신망을 물리적으로 분리하여 운영한다는 점이다[13].

4.4.3 가정사항

가정사항은 TOE의 운영환경에서 시행되거나 유지되어야 하는 가정사항을 보여준다. TOE가 가정사항을 만족시키지 못하는 운영환경에 설치될 경우, TOE는 모든 보안 기능성을 제공하지 못할 것이다.

위협과 조직의 보안정책, 가정사항을 종합하여 표 4와 같이 보안문제 정의를 서술하였다.

4.5 보안목적

본 논문에서 제안하는 보안목적은 TOE에 대한 보안목적과 운영환경에 대한 보안목적으로 분류하여 정의한다. TOE 보안목적은 TOE에서 직접 다루어지는 보안목적이고 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확하게 제공할 수 있도록 운영환경에서 지원하는 비기술적/절차적 수단에 의해 이루어지는 보안영역으로 표 5는 보안목적을 설명한다.

4.5.1 보안목적의 이론적 근거

보안목적의 이론적 근거는 명세한 보안목적이 적합하고 보안문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증하는 것이다. 보안목적의 이론적 근거는 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해서 다루어지며, 각 보안목적은 표 6과 같이 대응된다.

(표 5) 보안목적
(Table 5) Security Goal

보안목적		내용
TOE에 대한 보안목적	O.감사	TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 관리자가 적절하게 검토할 수 있는 수단을 제공해야 한다.
	O.관리	TOE는 TOE의 인가된 사용자가 TOE를 효율적으로 관리할 수 있는 관리수단을 안전한 방법으로 제공해야 한다.
	O.식별 및 인증	TOE는 사용자를 유일하게 식별해야 하며, TOE의 관리 및 객체에 대한 접근을 허용하기 전에 사용자의 신원을 인증해야 한다. 또한, 악의적인 연속인증 시도에 대응 수단을 갖추어야 한다.
	O.정보흐름 통제	클라이언트와 서버 간 통신의 전송 정보, 즉 사용자 데이터 및 TSF 데이터를 인가되지 않은 정보의 유·출입으로부터 통제해야 한다.
	O.정보누출대응	TOE는 정상적으로 사용되는 정보가 악용되지 못하도록 대응수단을 마련해야 한다.
	O.바이러스 차단	TOE는 네트워크, 저장매체 등에서 유입되는 바이러스나 웜, 악성코드 등을 탐지하고 이에대한 수단을 제공해야 한다.
	O.잔여정보 제거	TOE는 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.
	O.TSF데이터보호	TOE에 저장된 TSF 데이터 혹은 신뢰할 수 있는 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
	O.안전한 암호기능	TOE는 비인가된 사용자가 통신내용 도청 및 내부 기록 변조를 방지하기 위해 암호기능을 사용해야 한다.
	O.침해사고 식별/대응	TOE에서 발생하는 침해사고 등에 관한 이벤트 관리, 분석 및 대응을 위해 보안 관리를 제공해야 한다.
운영 환경에 대한 보안목적	OE.물리적 보안	TOE는 인가된 관리자만 접근 가능하며 군 정보통신망과 물리적으로 분리된 안전한 환경에 위치해야 한다.
	OE.운영체제보강	TOE 및 운영환경의 관리자는 운영체제의 취약점에 대한 보강작업을 수행하여 TOE와 다른 응용 프로그램간의 간섭이 없음을 보장해야 한다.
	OE.신뢰된 관리자	TOE의 인가된 관리자는 악의가 없으며 TOE 관리기능에 대해 적절히 교육 받았고 지침에 따라 정확하게 의무를 수행해야 한다.

(표 6) 보안목적의 이론적 근거
(Table 6) Theory base of Security Goal

보안문제 정의 \ 보안목적	O.감사	O.관리	O.식별및인증	O.정보흐름통제	O.정보누출대응	O.바이러스차단	O.잔여정보제거	O.TSF데이터보호	O.안전한암호기능	O.침해사고식별/대응	OE.물리적 보안	OE.운영체제보강	OE.신뢰된관리자
T.스팸메일 유입						√							
T.기록실패	√												
T.연속인증 시도 및 인증우회	√		√										
T.재사용 공격			√							√			
T.피싱						√				√			
T.위장	√		√							√			
T.저장데이터 훼손								√					
T.전송데이터 훼손				√									
T.서비스 거부공격	√									√			
T.잔여정보							√						
T.정보누출					√		√						

(표 6) 보안목적의 이론적 근거(다시)
(Table 6) Theory base of Security Goal

보안문제 정의 \ 보안목적	O.감사	O.관리	O.식별및인증	O.정보흐름통제	O.정보누출대응	O.바이러스차단	O.잔여정보제거	O.TSF데이터보호	O.안전한알림기능	O.침해사고식별/대응	OE.물리적보안	OE.운영체제보강	OE.신뢰된관리자
T.암호해독 공격									√				
T.바이러스·웜 침해						√							
T.웹 콘텐츠 변조								√					
T.허위정보 유포					√								
P.보안감사	√												
P.운영환경 분리											√		
P.안전한 관리		√											
A.물리적 보안											√		
A.운영체제 보강												√	
A.신뢰된 관리자													√

4.6 보안기능요구사항

본 논문에서 제시하는 보안기능요구사항은 앞에서 식별한 모든 보안목적을 충족시키기 위해 공통평가기준 2부의 컴포넌트를 선정하여 사용한다[4]. TOE에서 요구되는 보안기능요구사항 컴포넌트는 표 7과 같으며, 표 8에서 보안기능요구사항과 보안목적의 매핑으로 이론적 근거를 표시 하였다.

(표 7) 보안기능요구사항
(Table 7) Security Functional Requirement

보안기능 클래스	보안기능 컴포넌트	
식별 및 인증	FIA_AFL.1	인증 실패 처리
	FIA_UAU.1	인증
	FIA_UAU.3	위조할 수 없는 인증
	FIA_UAU.4	재사용 방지 인증 메커니즘
	FIA_UID.1	식별
암호지원	FCS_CKM.1	암호키 생성
	FCS_CKM.2	암호키 분배
	FCS_CKM.4	암호키 파기
보안감사	FAU_ARP.1	보안경보
	FAU_GEN.1	감사 데이터 생성
	FAU_SAA.1	잠재적인 위반분석
	FAU_SAA.3	단순공격학습
	FAU_SAR.1	감사검토
	FAU_SAR.2	감사 검토 권한 제한
	FAU_STG.1	감사 증적 저장소 보호
	FAU_STG.2	감사 데이터 가용성 보장

(표 7) 보안기능요구사항(다시)
(Table 7) Security Functional Requirement

보안기능 클래스	보안기능 컴포넌트	
TOE 접근	FTA_MCS.1	기본적인 세션수의 제한
	FTA_SSL.1	TSF에 의한 세션 잠금
TSF 보호	FPT_ITC.1	외부전송 TSF 데이터의 비밀성
	FPT_RPL.1	재사용 공격탐지
	FPT_STM.1	신뢰할 수 있는 타임스탬프
	FPT_TST.1	TSF 자체시험
보안관리	FMT_MOF.1	보안기능 관리
	FMT_MSA.1	보안속성 관리
	FMT_MTD.1	TSF 데이터 관리
	FMT_SMF.1	관리기능 명세
	FMT_SMR.1	보안역할
사용자 데이터 보호	FDP_ACC.1	부분적인 접근통제
	FDP_ACF.1	보안속성에 기반한 접근통제
	FDP_ETC.2	보안속성을 포함한 사용자 데이터 유출
	FDP_IFC.1	부분적인 정보흐름 통제
	FDP_IFF.1	단일계층 보안속성
	FDP_RIP.1	부분적인 잔여정보 보호
	FDP_SDI.1	저장된 데이터의 무결성 검사
	FDP_UIT.1	전송 데이터 무결성

(표 8) 보안목적과 보안기능요구사항 대응

(Table 8) Correspond to Security Goal and Security Functional Requirement

보안목적 / 보안기능 요구사항	O. 감사	O. 관리	O. 식별 및 인증	O. 정보 흐름 통제	O. 정보 누출 대응	O. 바이러스 차단	O. 잔여 정보 제거	O. TSF 데이터 보호	O. 안전한 암호 기능	O. 침해 사고 식별/대응
FIA_AFL.1			√							
FIA_UAU.1		√	√					√		
FIA_UAU.3			√							
FIA_UAU.4			√							
FIA_UID.1		√	√					√		
FAU_ARP.1	√					√				√
FAU_GEN.1	√									
FAU_SAA.1	√									
FAU_SAA.3	√									
FAU_SAR.1	√									
FAU_SAR.2	√									
FAU_STG.1	√									
FAU_STG.2	√									
FPT_ITC.1								√		
FPT_RPL.1						√		√		√
FPT_STM.1	√							√		
FPT_TST.1								√		
FMT_MOF.1		√								
FMT_MSA.1		√								
FMT_MTD.1		√								
FMT_SMF.1		√								
FMT_SMR.1		√								
FCS_CKM.1									√	
FCS_CKM.2									√	
FCS_CKM.4							√		√	
FDP_ACC.1			√					√		
FDP_ACF.1			√					√		
FDP_ETC.2					√					
FDP_IFC.1				√						
FDP_IFF.1				√						
FDP_RIP.1							√			
FDP_SDI.1								√		
FDP_UIT.1				√						
FTA_MCS.1		√	√			√		√		
FTA_SSL.1		√						√		

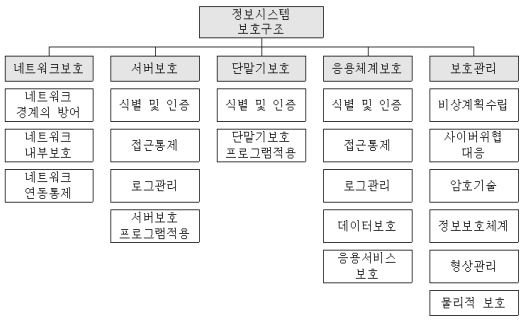
4.7 보증요구사항

4.7.1 정보가치분류

본 논문에서 제시하는 국방 SNS 보호프로파일의 보증등급은 미국의 IATF 기준을 참고하였다. IATF 기준은 보호하려는 정보의 가치와 위협의 등급에 따라 보증등급을 산출한다[20]. 국방 SNS의 자산은 군기강 훼손 또는 군사보안에 위협을 초래하는 정보로써 IATF 정보가치분류 기준에 의거 정보보호 방침을 위반하면 그 피해는 심각한(Serious) 수준의 V4 단계이다.

4.7.2 위협등급 산출

위협등급 산출기준은 “보호프로파일 개발을 위한 보증등급 산정 기준에 관한 연구”에서 제시한 위협등급 산



(그림 3) 군 정보시스템 보호구조
(Figure 3) Military Security System Protection Structure

정 방법을 적용하였다[21]. 위협등급은 위협상황 정도에 따라 수치화 평가 후 위협상황 평가의 합산한 값을 위협 유형 수로 나누어 위협상황 평균값을 구한다.

- 위협상황 평균값
  = Σ(위협상황평가) / Σ(위협 유형 수)

위 식의 위협상황 평균값에 따라 9개의 위협 등급으로 구분한다. 국방 SNS의 위협등급 산출결과 10.8점이 나왔으며, 이것은 위협등급 T4에 해당한다.

따라서 이렇게 도출된 정보가치와 위협등급을 견고성 등급에 매핑하면 국방 SNS의 보증요구사항은 EAL4 등급이 된다.

5. 결 론

본 연구는 기존 연구에서 시도되지 않았던 군을 대상으로 상용 SNS의 위협과 취약점 분석을 통해 군에 SNS 도입시 필요로 하는 보안기능요구사항을 새롭게 제시 하였다. 이 연구를 통해 기존의 군 SNS 가이드라인을 보완 및 대체함으로써 군내 SNS 보안문제를 해결할 수 있으며, 여기서 제시한 보안기능요구사항들은 상용 보안 시스템의 군내 도입이나 현재 추진중인 군사용 스마트폰 어플리케이션 개발 사업과 같은 분야에서 군내 보안요구사항의 참고자료로 충분히 활용될 수 있을 것이다.

또 국방정보화업무훈령 중 정보시스템 보호구조는 그림 3과 같이 5개 분야로 구성되어 있는데, 각 분야에 대해 보호통제항목별로 어떤 보안기능들을 적용할 것인가에 대한 내용은 명시되어 있으나 군에 필요한 기술적인 보안기능들은 아직 정립되지 않은 실정이다[12]. 따라서 본 연구를 바탕으로 군 정보시스템 보호구조에 대한 보안기능요구사항을 제시함으로써 군내 보안시스템의 평가체계 확립에 기여할 수 있을 것이다.

참고문헌(Reference)

[1] http://en.wikipedia.org/wiki/Social_network_service
[2] 강철원, 좌훈승, 한재웅 “Social Network Service”, Computing Ethics and Social Issues, pp. 3.
[3] Danah m. boyd, Nicole B. Ellison,“Socialnet work sites: Definition, history, and scholarship”, Journal of Computer-Mediated Communication, Vol 13, pp. 210-230, 2007.
[4] ISO/IEC 15408 CC:Common Criteria for ITSecurity Evaluation, R3, 2009.
[5] 이진형, “SNS(Soical Network Service)Diffusion and Trends”, Korea Communications Agency, Journal of Communication & Radio Spectrum. Vol. 44. pp. 54-59, 2012.
[6] Collaborative Thinking, “Reference Architect ure For Social Network Sites”, <2008/07/29>,http://mikeg. typepad.com/ perceptions/2008/07/reference-archi.html
[7] slideshare, <2008/05/19>http://www.slideshare.net/ linkedin/linkedins-communication-architecture
[8] Terry.Cho’s blog, <2010/03/22>, http://javamaster. wordpress.com
[9] http://nvd.nist.gov/cwe.cfm#cwes
[10] Hogben, G., Security Issues and Recommen dations for Online Social network, ENISA Position Paper No. 1, October, pp. 3-4. 2007.
[11] Symantec, “The Risks of Social Networking”, Security Response, pp. 1-28, 2010.
[12] Ministry National Defense Instruction 제130 4호, “Military Information Instruction” Appendix, pp. 225, 227. 2011.
[13] Ministry National Defense Instruction 제13 93호 (2012. 2. 13.), “Military Security Instruction”, pp. 21, 80.
[14] Facebook Security Guide, pp. 8-11.
[15] http://www.boannews.com/media/view.asp? idx=33144&kind=1 <Boannews>, 2012/10/23

[16] 김바로, “A Study on Enhanced Wireless Co nnectivity Authentication and a Security Threat Prevention in a Wireless LAN Environment”, Soongsil University, pp. 6-11. 2012.
[17] Mindi McDowell and Damon Morda, “Socializing Securely: Using Social Networking Services”, US-CERT, pp. 2. 2011.
[18] ENISA, “Online as soon as it happens”, pp. 23-24. 2010.
[19] National Computing & Information Agency, “Web Application Development Security Guide 2010”
[20] “Information Assurance Technical Framework Documents”, Release 3.1, Chapter 4. Technical Security Countermeasures, pp.32-34.
[21] 윤신숙, 장대석, 김환구, 오수현, 하재철, 김석우, “Study calculated based on the level of assurance for the development of PP”, The Korea Institute of Information Security and Cryptology 제17호, 2007.

◐ 저 자 소 개 ◑

유 덕 훈(Deokhoon Yu)

1998년~2000년 육군 제3사관학교 조직관리학과 졸업
2000년~현재 대한민국 육군
2011년~2012년 고려대학교 정보보호대학원 석사과정
관심분야 :정보보증, 개인정보보호, CC평가
E-mail : yuseojin@korea.ac.kr

김 승 주(Seungjoo Kim)

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년 KISA(舊한국정보보호진흥원) 팀장
2004년~2011년 성균관대학교 정보통신공학부 부교수
2011년~현재 고려대학교 정보보호대학원 정교수
2002년~현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재 한국정보보호학회 이사
2005년~2006년 교육인적자원부 유해정보차단 자문위원
2007년 국가정보원장 국가사이버안전업무 유공자 표창
2007년~현재 대검찰청 디지털수사 자문위원
2007년~2009년 전자정부 서비스 보안위원회 사이버 침해사고대응 실무위원회 위원
2010년~현재 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재 SK커뮤니케이션즈 보안강화 특별자문위원
2012년 중앙선거관리위원회와 서울시장후보 홈페이지 사이버테러 특별검사 자문위원
관심분야 : 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security
E-mail : skim71@korea.ac.kr