정 보 보 호 학 회 지
제24권 제3호, 2014. 6

스마트폰 보안 위협에 따른 사용자 중심의 대응방법 동향

강 성 배*, 양 대 헌**

요 약

스마트폰의 보급률이 높아지고 많은 업무가 PC에서 스마트폰으로 옮겨 가면서 개인신상정보, 금융 정보와 같은 중요한 정보들도 함께 옮겨가고 있다. 최근에 이러한 중요한 정보들을 보호하기 위한 스마트폰 보안이 다양하게 연구되고 있다. 스마트폰의 휴대성 덕분에 사용자는 언제, 어디서나 다양한 업무를 수행할 수 있지만, 공격자도 마찬가지로 사용자에게 더욱 접근하기가 쉬워졌으며 스마트폰 사용자는 PC 환경보다 더욱 다양한 취약점에 처하게 되었다. 이러한 다양한 취약점 때문에 스마트폰을 겨냥한 다양한 종류의 공격 방법들이 생겨나고 있다. 본 논문에서는 스마트폰 보안 위협으로써 네트워크, 악성코드, 훔쳐보기 공격 등의 위협이 개인정보 유출이나 금전적 손실과 같은 직접적인 피해로 이루어지기 쉬우므로 해당 위협들에 대해 설명하고, 해당 위협을 완화하거나 회피할 수 있는 사용자 중심적인 최신 기술 동향을 소개한다.

Ⅰ. 서 론

스마트폰의 보급률이 급속하게 증가하며, 스마트폰을 이용하는 모바일 뱅킹의 거래 건수 또한 상당히 증가하였다. 또한, 스마트폰은 사용상의 편리함과 휴대가 편하다는 장점이 있어 많은 스마트폰 사용자는 별다른 생각 없이 중요한 정보를 스마트폰에 저장하여 사용하고 있다. 이러한 중요한 개인정보들은 악의적인 공격자에 의한 다양한 공격으로 유출될 위협에 처해있다. PC 환경에서도 가능했던 피싱, 파밍, 훔쳐보기 공격뿐만 아니라 각종 악성코드를 이용하여 스마트폰의 정보를 가져가거나 스마트폰을 좀비 PC로 만드는 등 다양한 공격 유형이 존재한다. 또한, 스마트폰의 SMS 서비스를 이용하여 악성코드를 심어서 공격하는 스미싱(Smishing)과 같은 신종 공격도 생겨났다. 본 논문에서는 스마트폰 보안에 위협으로서 네트워크 환경, 악성코드, 훔쳐보기 공격 등에 의한 위협에 대하여 설명하고, 해당 위협에 대응할 수 있는 최신 방법들을 소개하도록 한다.

오늘날 스마트폰과 함께 노트북, 태블릿 등의 스마트 기기에서의 와이파이 연결은 필요조건이 아닌 필수조건이 되었다. 2010년 국내의 와이파이존 구축 현황은 세계 7위 정도였으나, [표 1]에서처럼 현재는 세계 2위의 보급률을 자랑하고 있다[1]. 이러한 통계 현황은 국가의 인구수와 면적에 비교하여 와이파이존이 상당히 밀집되어 있으며 매우 널리 보급되어 있음을 짐작할 수 있다. 또한 [표 1]에 따르면 와이파이존이 구축된 장소 대부분은 공공장소 이거나 공공장소에 준하는 식당, 까페, 호텔, 상가 등이 주를 이루고 있다. 스마트기기 사용자는 이러한 와이파이존의 구축으로 언제, 어디서나 편리하게 인터넷을 사용할 수 있다. 그러나 현재 널리 보급된 와이파이존에 비해 사용자뿐만 아니라 네트워크 관리자조차 네트워크 보안에 대한 인식은 턱없이 부족하다. 본 논문에서는 스마트폰 사용자에게 네트워크 보안 위협요소로서 로그 AP에 대한 위협을 설명하고 최신 대응방안을 소개한다.

악성코드를 이용한 공격은 [표 2]에서 보는 것처럼 5가지 정도의 유형이 있다[2]. 단말 장애 유발형, 배터리 소모형 등의 악성코드는 스마트폰 사용자에게 불편함을 가져올 수 있으나 개인정보유출이나 금전적 손실 등의 직접적인 피해를 주지는 않는다. 본 논문에서는 직접적인 피해를 가져오는 과금 유발형의 한 종류인 “스미싱”

* 인하대학교 컴퓨터공학과 (sbkang87@isrl.kr)
** 인하대학교 컴퓨터공학과 교수 (nyang@inha.ac.kr)

〔표 1〕 145개국 에서의 881,480개의 공공 or 사설 WI-FI 설치 지역 현황.

Top 10 Countries			Top 10 Location Type		
Rank	Countries	Location	Rank	Countries	Location
1	United States	190,352	1	Public Space / Public Building	422,134
2	South Korea	186,758	2	Cafe	89,936
3	United Kingdom	182,610	3	Hotel / Resort	89,755
4	China	104,106	4	Store / Shopping Mall	65,234
5	France	35,431	5	Other	60,054
6	Taiwan	24,148	6	Restaurant	55,657
7	Russian Federation	16,829	7	School / University	24,769
8	Japan	15,734	8	Office Building	14,934
9	Germany	15,095	9	Library	12,116
10	Sweden	9,546	10	Hotzone	7,659

과 개인정보를 유출하는 형태의 스파이웨어 형태의 악성코드를 알아보고, 악성코드에 대응하는 최신 방법을 소개한다.

〔표 2〕 모바일 악성코드의 5가지 형태

유형	설명
단말 장애 유발형	단말의 사용을 불가능하게 만들거나 장애를 유발
배터리 소모형	단말의 전력을 지속적으로 소모시켜 배터리를 고갈
과금 유발형	단말의 메시징 서비스나 전화 시도를 지속적으로 시도하여 과금을 발생
정보 유출형	감염된 단말의 정보나 사용자 정보를 외부로 유출
크로스 플랫폼형	모바일 단말을 통해 PC를 감염

마지막으로 공격자가 물리적으로 사용자의 아이디, 패스워드, PIN 번호 등을 훔쳐봄으로써 사용자인증에 사용되는 패스워드를 탈취하는 훔쳐보기 공격에 대하여 설명하고, 최신 대응방법을 소개한다.

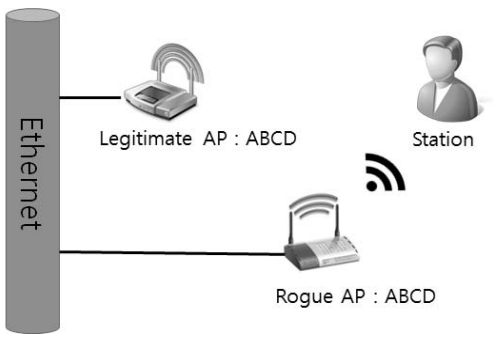
Ⅱ. 스마트폰 보안 위협

2.1. 네트워크 환경의 위협

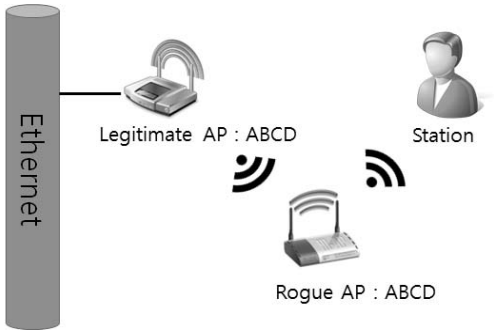
2.1.1 로그 AP

일반적으로 스마트폰 사용자는 와이파이 기능을 항상 켜놓으면서, 인증/ 암호기능 설정이 되어 있는 AP보다는 인증 없이 자동으로 간편하게 접속되는 AP에 접속하는 것을 선호한다. 이러한 사용방법 때문에 사용자는 로그 AP의 위협에 처하게 된다.

이 장에서는 PC 환경과 스마트폰 환경에서 다양한 네트워크 위협 중에서 네트워크 환경의 위협으로서 네트워크 관리자의 허가를 받지 않은 불법적인 로그 AP(Rogue Access Point)의 위협에 대해서 설명한다. 로그 AP는 [그림 1],[그림 2]에서처럼 두 가지 유형으로 분류할 수 있다. [그림 1]의 공격자는 사용자에게 인터넷을 제공하기 위하여 일단 유선망에 자신의 로그 AP를 설치한다. 공격자는 자신의 로그 AP에 합법적인 AP의 정보를 위조하여 사용자에게 자신의 로그 AP를 마치 네트워크 관리자에 의해 허가받은 AP처럼 보이게 한다. [그림 2]의 공격자는 사용자에게 인터넷을 제공하기 위하여 유선망이 아니라 합법적인 AP의 무선망에 연결하여 로그 AP를 설치한다. 이 방법도 마찬가지로 합법적인 AP의 정보를 위조하여 사용자에게 인가된 AP처럼 보이게 된다. 유선망에 연결하여 로그 AP를 설치하는 방법은 무선망에 연결하는 로그 AP보다 설치 장소에 제한을 받을 뿐만 아니라 더 강한 신호로 사용자 접속을 유도하는 것에 제한을 받는다. 그러나 일단 설치가 완료되고 사용자를 접속하도록 유도하고 나면 사용자가 네트워크 관리자의 도움이나 별도의 특별한



〔그림 1〕 유선망에 연결한 로그 AP



〔그림 2〕 무선망에 연결한 로그 AP

장치 없이는 로그 AP인지 정상적인 AP인지 구분하기가 상당히 어렵다.

공격자는 설치된 로그 AP를 이용하여 패킷을 가로채어 암호화되지 않은 문서 등을 확인할 수 있으며, 인터넷에서 사용되는 아이디, 패스워드 등의 개인정보 역시 가로챌 수 있다. 또한, 단순히 패킷 분석만을 통하여 정보를 가로채는 수동적인 공격뿐만 아니라 피싱 사이트를 만들어 제공하는 등의 능동적인 중간자 공격(Man In The Middle)이 가능하다. 이러한 공격은 사용자의 개인정보 유출, 금전적 손실 등의 직접적인 피해로 이어지기 때문에 스마트폰 사용자에게 매우 위협적이다. 〔표 3〕에서 로그 AP를 통한 피해 유형을 정리하고 있다.

〔표 3〕 로그 AP를 이용한 공격 유형

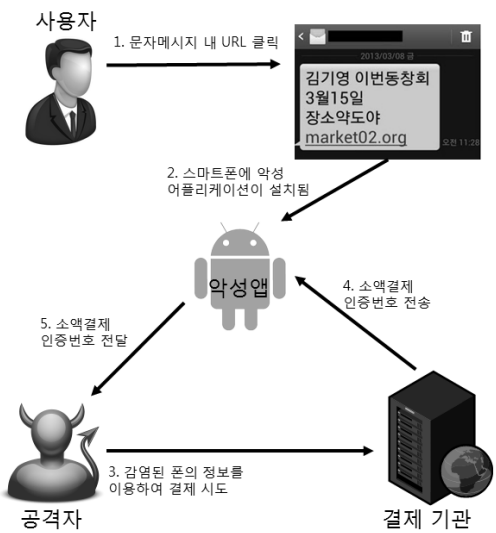
공격 유형	공격 방법
패킷 분석	사용자로부터 발생되는 패킷을 분석하여 사용자의 사용패턴 분석하여 온라인 아이디, 비밀번호 등의 유출 또는 암호화되지 않은 문서를 유출한다.
피싱(Phishing)	패킷을 제어하여 공격자가 의도한 피싱사이트로 접속하도록 유도하여 공격자가 의도한대로 사용자를 행동하게 한다. 대부분의 경우 금융사이트를 사칭하여 금전을 취하려한다.
파밍(Pharming)	피싱의 한 유형으로 사용자가 정확한 웹페이지 이름을 입력하였더라도 공격자가 의도한 사이트로 이동하도록 만들어 금전적 이득을 취한다.

2.2 악성코드로 인한 위협

2.2.1 스미싱(Smishing)

스미싱이란 SMS를 이용한 Phising의 합성어이다. 공격자는 사용자에게 동창회, 결혼식, 환급금확인 등의 친근한 문자내용과 함께 자신의 악성코드를 설치할 수 있는 URL이 담겨있는 문자메시지를 보낸다. URL을 통하여 악성코드를 설치하게 되면 공격자의 의도대로 스마트폰 사용자의 정보를 가져가거나 스마트폰의 동작을 제어할 수도 있다.

[그림 3]에서 보편적인 스미싱 공격 유형의 한 예를 보여 주고 있다. 공격자는 자신의 친근한 메시지와 함께 악성코드가 담긴 URL을 포함하여 메시지를 전송한다. 사용자가 URL을 의심 없이 클릭하면 악성코드가 설치되며, 공격자는 스마트폰 사용자의 정보를 가져가서 소액 결제를 시도한다. 사용자의 정보로 요청된 소액 결제 인증번호는 사용자의 스마트폰으로 전송되지만, 이 인증번호는 악성코드에 의해 사용자에게 보이지 않고 공격자에게 재전송한다. 결국, 공격자는 인증번호를 이용하여 스마트폰 사용자 대신 소액결제에 성공하며 금전적 이득을 취하게 된다.



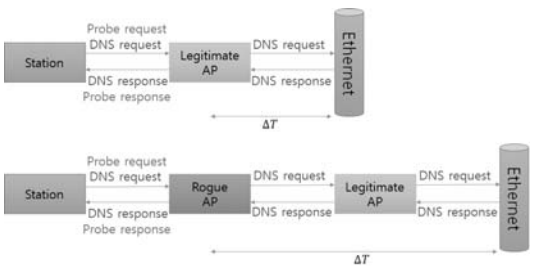
〔그림 3〕 스미싱 공격 방법

악성코드를 이용한 스미싱 공격의 경우 개인정보유출과 금전적 손실 등의 직접적 피해로 이루어지므로 이전에 소개했던 다른 악성코드들 보다 더욱 위협적이다.

2.3. 훔쳐보기 공격

스마트폰은 항상 휴대할 수 있으며 PC에 버금가는 성능으로 많은 업무를 처리할 수 있다는 장점이 있다. 그러나 스마트폰의 사용은 고정된 PC 환경이나 은행의 ATM기기와 달리 항상 가지고 다니며 업무를 처리한다는 점에서 훔쳐보기 공격에 노출되는 확률을 높이고 있다.

훔쳐보기 공격은 사용자가 PIN이나 아이디, 패스워드 등을 스마트폰에서 입력할 때에, 공격자가 옆이나 등 뒤에서 입력하는 모습을 보는 것만으로 간단하게 수행 가능한 공격 방법이다.



〔그림 4〕 H.Han 등의 로그 AP 탐지 방법

공격자는 알아낸 사용자의 PIN이나 아이디, 패스워드 등을 가지고 사용자의 디바이스를 직접 이용하여 저장된 정보를 유출할 수 있다. 또는 보편적으로 사용자는 자신의 PIN이나 아이디, 패스워드 등을 여러 가지가 아닌 하나로 통일하여 사용하기 때문에 공격자는 훔쳐보기 공격으로 알아낸 아이디, 패스워드를 이용하여 다른 포털 사이트에 접속하여 사용자의 정보를 유출할 수도 있다.

Ⅲ. 취약점에 따른 대응방법 동향

3.1 로그 AP 탐지 방법

앞장에서 로그 AP의 두 가지 공격 형태를 설명하였다. 그 중 첫 번째 형태인 유선망에 연결하여 인터넷을 제공하는 로그 AP는 공격자에게 많은 제한이 있으며, 일단 공격자가 설치하여 사용자를 접속에 유도하고 나면, 네트워크 관리자의 도움이나 별도의 장치 없이 사용자가 직접 로그 AP를 판별해내기는 어렵다. 따라서 본 논문에서는 공격자가 더 수행하기 쉬우며 사용자에게는 더욱 위협적이지만, 사용자 측면에서 로그 AP를 탐지하는 방법이 활발하게 연구되고 있는 공격 유형인 무선망에 연결하여 인터넷을 제공하는 로그 AP의 공격 유형을 탐지하는 최신 방법에 대하여 소개한다.

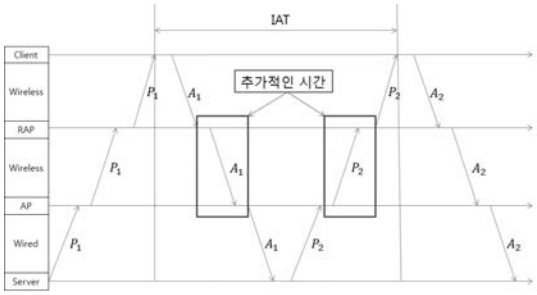
3.1.1 H. Han등의 탐지 방법

[그림 4]에서 H. Han 등의 로그 AP 탐지 아이디어를 보여주고 있다. H. Han 등은 합법적인 AP와 여기에 무선으로 연결한 로그 AP 사이에 반드시 발생할 수밖에 없는 무선구간에서 발생하는 지연시간을 이용하여 로그 AP를 탐지한다[3]. H. Han은 사용자가 자신이 접속한 AP까지의 왕복 거리를 측정한 RTTprobe와 사용자와 DNS 서버까지의 거리를 측정한 RTTdns를 이용하여 RTTdns - RTTprobe 값인 델타T 값을 구하여 통계적으로 합법적인 AP일 때의 값보다 크게 되면 로그 AP로 판단하는 방법이다. 이 방법은 짧은 시간 내에 사용자가 직접 로그 AP를 판단할 수 있다는 장점이 있다. 별도의 장비를 필요로 하지 않으며 Pcap을 이용한 패킷을 전송할 수 있는 리눅스 기반의 스마트폰과 같은 장치만 있으면 탐지할 수 있다. 그러나 이 방법은 사용자가 연결된 무선망의 채널이 혼잡할 때에 탐지율이 현저하게 떨어지는 단점이 있다.

3.1.2 C. Yang 등의 탐지 방법

[그림 5]에서 C. Yang 등의 로그 AP 탐지 아이디어를 보여주고 있다[4]. C. Yang 등은 DNS, 웹 호스트 등의 다양한 서버에 서버프로그램을 두고 사용자에 호스트 프로그램을 두어 TCP 연결을 설정하고. 서버프로그램에서 전송한 P1을 받는 동시에 사용자 프로그램은 A1을 전송한다. A1을 받은 서버는 바로 P2를 사용자에게 전송한다. 사용자는 P1을 받은 시간부터 P2를 받은 시간까지를 측정하여 IAT(Inter Arrival Time)이라 부르고 이 값이 합법적인 AP에서는 측정될 수 없는 값일 때에 로그 AP로 판단한다. 서버와 사용자 사이에 TCP 연결이 설정되어 있으므로 일반적인 TCP 통신에서와는 달리 공격자가 TCP에 대한 ACK 패킷을 대신하여 전송하는 방법의 회피방법으로는 간단하게 회피할 수가 없다. 이 방법은 TCP 통신이 가능한 단말이면 스마트폰 사용자 외에도 사용이 가능한 방법이며, 단 한 번의 패킷전송을 통한 시간측정으로 1초 이내에 로그 AP 탐

지가 가능하다. 그러나 이 탐지 방법 역시 채널이 혼잡하거나 무선망의 신호세기가 약한 경우 탐지율이 낮아지는 단점이 있다.



〔그림 5〕 C. Yang 등의 IAT(Inter Arrival Time)을 이용한 로그 AP 탐지 기법

3.2 사용자 중심의 스미싱 대응 방안

3.2.1 출처가 불분명한 APP 설치 차단

[그림 6]에서 안드로이드에서는 출처가 분명하지 않은 애플리케이션을 설치하지 않도록 차단하는 기능이 있다. 악성코드는 인증된 제작자에 의해 만들어진 애플리케이션이 아니므로 사용자는 이 기능을 활성화하지 않음으로써 출처가 분명하지 않은 애플리케이션을 설치하지 않을 것을 본인이 선택할 수 있다. 그러나 이 기능은 일반적인 설정에 있지 않아서 찾기가 쉽지 않고, 이 기능을 활성화하지 않고 사용하게 되면 국내 은행 애플리케이션의 경우 제대로 설치되지 않아 사용할 수 없는 등의 불편함을 겪어야 한다.

〔그림 6〕 출처가 불분명한 APP 설치 차단 화면

따라서 이러한 방법은 사용자 측면에서 스미싱을 방지할 수 있는 좋은 방법이지만. 금융 애플리케이션과 같이 출처가 불분명하지만 설치할 수밖에 없는 애플리케이션도 존재하므로 사용자가 애플리케이션을 설치할 때에 해당 애플리케이션이 악성코드인지 아닌지 판단하여 해당 기능을 on/off 해야 하는 것은 뛰어난 보안 방법이라고 생각되지 않는다. 따라서 악성코드가 설치되는 권한 및 책임을 사용자가 짊어져야 하고, 실제로 활용되기 힘들다는 단점이 있다.

3.2.2 스미싱 차단 애플리케이션 설치

스마트해지는 공격자에 의해서 스미싱의 방법도 다양해지고 있다. 스미싱을 방지하는 가장 좋은 방법으로는 스미싱의 피해를 줄이기 위해서 스미싱 차단 애플리케이션을 설치하는 것이다. 사용자는 각 통신사에서 제공하는 스미싱 차단 애플리케이션을 사용하거나, 앱스토어에 더욱 강력한 기능을 제공하는 스미싱 차단 애플리케이션을 사용하면 된다.

스미싱을 차단하는 애플리케이션은 크게 URL/문자열 검사를 거쳐 스미싱을 판단하거나 악성 앱 권한을 검사하여 스미싱으로 판단하는 두 가지 방법이 있다.

〔표 4〕

탐지 방법	스미싱 차단 앱 이름
URL/문자열 검사	S-GUARD
	SMS 피싱
	피싱캅
	링크스캔
	뭐야 이 문자
	피싱 제로
	Smishing Defender
	유후
	엠엔 메시지 통
설치된 앱 권한 검사	올레 스미싱 차단
	뭐야 이 문자
	앱 보안관
	라인 백신
	알약 안드로이드
	스파이 수사대

URL/문자열 검사의 경우 단순히 URL에 스미싱 관련 문자열이 포함되어 있거나 악성코드 관련된 앱으로 연결하도록 하는 URL로 판별될 경우 사용자에게 알림을 주도록 한다. 악성 앱 권한을 검사 하는 방법은 URL에 연결된 애플리케이션이 일반적인 애플리케이션에서는 필요하지 않은 과다한 권한을 가지고 있을 때, 이러한 권한이 스미싱을 유발할 수 있는 권한과 비슷할 때에 사용자에게 알려준다.

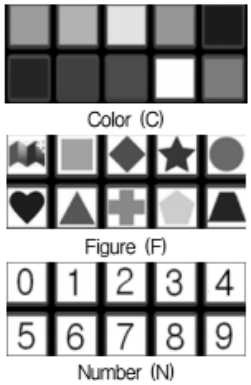
[표 4]에서 스미싱을 탐지하는 애플리케이션들을 탐지 방법에 따라 분류해 놓았다[5]. URL/문자열 보다 권한 검사의 경우가 스미싱을 탐지해 내는데 더욱 성능이 좋다.

3.3 훔쳐 보기 공격 대응 방안

3.3.1 임수민 등의 훔쳐보기 공격을 고려한 연구

임수민 등은 [그림 7]에서처럼 패스워드로 색깔, 도형, 숫자를 사용하여 세 요소 간에 어떤 차이가 있는지 살펴보기 위하여 실험을 통해 사용성 및 보안성을 살펴보았다[6].

이 연구는 알파벳으로 구성된 패스워드는 패스워드의 길이가 길어져도 사용자가 사용하기 쉽지만, 공격자도 훔쳐보기 공격에 성공했을 때에 사용자의 패스워드를 알아내기 쉽다는 점에 착안하여, 알파벳을 사용자가 알아볼 수 있는 간단한 도형으로 바꾸어 사용하여도 사용성과 보안성에서 뒤떨어지지 않음을 확인하기 위해 실험하였다.



〔그림 7〕 임수민 등의 실험에 사용된 색깔(C), 도형(F), 숫자(N) 패스워드

〔그림 8〕 아래쪽 왼쪽 : 패스 인증 성공,
아래쪽 오른쪽 : 패스 인증 실패

실험 결과로 색깔, 도형, 숫자의 순으로 4.16, 4.09, 7.23개를 맞췄다. 표준편차는 0.94, 0.94, 1.73으로 나타났다. 이러한 결과는 숫자는 7개 이상으로 구성해야 하고 색깔, 도형의 경우 5개 이상으로 구성된 패스워드가 훔쳐보기 공격에 안전할 것으로 예측할 수 있다. 따라서 단순한 이미지나 도형을 이용하면 적은 개수로도 패스워드를 구성할 수 있다. 이 실험 결과에서 패스워드의 길이가 숫자나, 도형에 차이가 없을 때에, 공격자는 훔쳐보기 공격에 성공하더라도 해당 패스워드가 단순히 숫자일 때보다 더 외우기 힘들어서 훔쳐보기 공격에는 강한 것으로 볼 수 있다.

또한 기존의 숫자 키패드를 이용한 PIN시스템에서 배열의 위치만을 변화 시켰을 때에 사용자가 2배정도 더 어려움을 겪었음을 실험 하였다. PIN 번호를 입력하는 숫자 배열을 랜덤하게 재배치하면 PIN 번호를 알고 있는 사용자와 PIN번호를 모르는 공격자와 비교를 하였을 때, 공격자가 훔쳐보기 공격에 성공하였더라도 PIN 번호를 유추하기가 더욱 어렵다는 점에서 랜덤하게 재배치하는 것에서 보안성을 높일 수 있음을 보여주고 있다.

3.3.2 문건영 등의 그래픽 패스워드 인증 기법

문건영 등은 한붓그리기를 이용한 새로운 그래픽 패스워드 방식을 제안하였다[7]. [그림 8]에서 이 기법은

여러 모양의 이미지를 그리드 형식으로 배열하며, 각 이미지를 시작이미지, 종료이미지, 패스이미지, 마인이미지를 두고 시작이미지에서 종료이미지까지 한붓그리기를 한다. 단, 패스이미지 3개를 반드시 순서대로 지나야 하며 마인이미지 1개는 절대로 지나가면 안 된다. 또한, 한붓그리기의 경로에 제한은 없으며 중복된 이미지를 선택할 수 있으므로 패스워드의 길이는 무한해질 수 있다. 이러한 방법 때문에 사용자는 자신의 패스워드인 패스이미지 외에 다양한 더미이미지를 추가할 수 있으며, 공격자는 훔쳐보기 공격에 성공하더라도 패스이미지와 더미이미지를 구별할 수 없다.

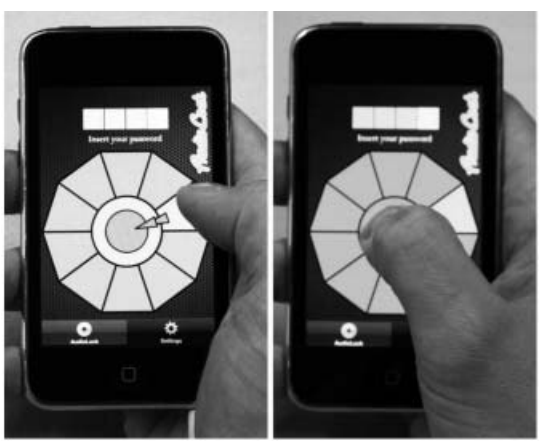
이 방법은 이미지의 배치에 따라서 인증이 불가능한 배치가 발생하기도 하지만 간단하게 이미지를 재배치해 줌으로써 해결가능하다.

이 방법은 기존의 패턴이나 PIN방식, 알파벳 배열식 패스워드 방식과 비교하면 경로가 인증 때마다 변경되므로 스머지 공격에 강하며, 패스이미지와 함께 더미이미지가 들어가게 되므로 훔쳐보기 공격에 상당히 강하다는 것을 알 수 있다. 그러나 시뮬레이션 결과 일반적으로 쓰이는 4자리의 PIN 방식보다 무작위 대입 공격에는 약하다는 것이 단점이다.

무작위 대입 공격에 대한 대책으로서, 그리드의 크기와 패스이미지 수, 마인이미지 수 등의 요소에 관한 고려는 추후 연구에서 진행할 것으로 보인다.

3.3.3 A. Bianchi 등의 훔쳐보기 공격에 강한 PIN인증 기법

A. Bianchi 등은 공격자가 훔쳐보기 공격에 성공하여 패스워드를 입력하는 화면을 보더라도 사용자의 패스워드를 알아낼 수 없는 방법을 제안하였다[8]. [그림 9]에서 이 방법은 가운데 하나의 원과 원을 둘러싸고 있는 10개의 도형이 있다. 이 10개의 도형에 손가락을 가져다 대면 이어폰을 통해 숫자를 영어로 불러주게 된다. 이 10개의 도형에 매칭되는 숫자는 매번 입력할 때마다 변경되지만, 숫자의 순서는 시계방향으로 오름차순으로 정렬되어 있다. 따라서 사용자는 10개의 도형 중에 한 곳을 터치했을 때에 다음 위치의 숫자를 예측할 수 있으며 다음 위치뿐만 아니라 다음 몇 개의 위치의 숫자도 예측할 수 있다. 따라서 사용자는 자신이 입력해야 하는 PIN 번호에 맞게 손가락을 가져다 댈 수 있다. 자신이 원하는 PIN 번호에 손가락을 가져다 대었으면 PIN 번호를 입력하기 위해 해당 도형에서 손가락을 떼지 않은 채 가운데로 드래그한 다음, 가운데 원에서 손가락을 떼면 PIN 번호를 성공적으로 입력한 것이다.



〔그림 9〕 B. Andrea의 PIN 인증 기법

이 방법은 공격자에게 패스워드 입력화면을 보여주더라도 실제 사용자가 입력하는 PIN 번호에 대한 정보는 알려주지 않으므로, 공격자의 훔쳐보기 공격은 무작위 공격과 다르지 않게 된다. 이 방법은 사용자의 시각적인 인증뿐만 아니라 청각도 이용하여 인증하므로 일종의 2채널 인증이라고 볼 수 있다.

훔쳐보기 공격에 매우 강한 이 방법은 사용자 인증을 위해 PIN 번호를 입력할 때마다 이어폰을 착용해야 한다는 단점이 있다.

Ⅳ. 결론

본 논문에서 소개한 스마트폰에서 보안 위협 외에도 더욱 많고 다양한 위협이 있다. 여기서는 그중에서도 사용자에게 직접적인 피해로 이루어지는 위협들에 대해서 설명하였다. 인증/암호화하지 않은 네트워크에서의 위협, 스미싱을 이용하여 악성코드 설치에 대한 위협, 훔쳐보기 공격에 대한 위협 등을 살펴보았다. 사용자는 보안에 대한 지식이 거의 없거나 보안에 민감하지 않기 때문에 자신의 개인정보가 유출되거나 직접적인 피해를 받지 않는 이상 이러한 위협에 의해 피해가 올 것을 짐작하지 못할 것이다. 실제로 앞에서 설명한 위협들이 얼마나 위험하며 예방하지 않고 일단 당하고 나면 되돌릴 수 없는 위협들인지 제대로 인식하지 못하고 있다.

최신 연구들은 보안 전문가로서 스마트폰 사용자들

에게 보안인식을 심어주고 해당 위협들을 사전에 예방하고자 하는 연구가 주를 이루고 있다. 최근의 위협에 대응하기 위한 방안들은 사용자가 보안에 대한 지식이 많지 않아도 이해할 수 있는 수준에서 연구되거나 사용자가 사용하기 쉽도록 구현되어 있다. 또한, 사용성이 뛰어나면서도 보안성이 뒤떨어지지 않는 대응 방법들이 꾸준히 연구되고 있다.

관리자나 제조사 입장에서 사전에 위협을 예방해야 하는 예전의 연구와는 달리 최근의 연구들과 앞으로의 연구들은 보안성은 뒤처지지 않으며, 사용자의 편의성과 사용자와의 상호작용을 고려해야 하는 것이 연구의 관건이 될 것이다.

참 고 문 헌

[1] http://v4.jiwire.com/search-hotspot-locations.htm

[2] 조성제, “모바일 보안 및 저작권”

[3] H. Han, B. Sheng, C. Tan, Q. Li, and S, Lu, “A Timing-Based Scheme for Rogue AP Detection”, IEEE trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1912-1925, Nov 2011.

[4] C. Yang, Y. Song, and G. Gu, “Active User-side Evil Twin Access Point Detection Using Statistical Techniques.”, IEEE Transactions on Information Forensics and Securiy, vol. 7, no. 5, pp. 1638-1651, Oct. 2009.

[5] 박상호, 이준형, “인증 및 사전 권한 검증을 통한 스미싱 방지 시스템 제안”, 정보보호학회논문지, 23(6), pp. 5-12, Dec 2013

[6] 임수민, 김형중, 김성기, “Shoulder Surfing 공격을 고려한 패스워드 입력 시스템 구현 및 통계적 검증”, 전자공학회논문지, 49(9), pp. 215-224, Sep 2012.

[7] 문건영, 김종욱, 홍만표, “모바일 환경에서 훔쳐보기 공격에 강한 그래픽 패스워드 시스템.”, 정보과학회논문지, 18(1), pp. 90-94, Jan 2012

[8] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, “The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices.”, Proc. Conf. on Tangible, embedded, and embodied interation, TEI ‘11, pp. 197-200, January 2011.

〈저 자 소 개〉

강 성 배 (SungBae Kang)
학생회원

2012년 2월 : 인하대학교 컴퓨터공학과 학사
2014년 2월 : 인하대학교 컴퓨터공학과 석사
2014년 3월~현재 : 인하대학교 컴퓨터공학과 박사
관심분야 : 무선 인터넷 보안, 네트워크 보안, 사용자 인증 보안

양 대 헌 (DaeHun Nyang)
정회원

1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자공학과 졸업
1996년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 컴퓨터정보공학과 부교수
관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, 네트워크 보안