# 블루투스를 이용한 스마트폰 데이터 해킹 트로이목마 어플리케이션 개발

허 준[O], 위동현[*], 이성원[**], 조태남[***]
[O*]우석대학교 정보보안학과
[**](주)아이제론
[***]우석대학교 IT전자융합공학과
e-mail: gjwns8502@naver.com[O], dnlehdgus2@naver.com[*], forensic@izerone.co.kr[**], tncho@ws.ac.kr[***]

# Developing a Trojan Horse Application for Smartphone Data Hacking using Bluetooth

June Heo[O], Donghyun Wee[*], Seongwon Lee[**], Teanam Cho[***]
[O*]Dept. of Information Security, Woosuk University
[**]Ltd. Izerone
[***]Dept. of IT&Electronics Engineering, Woosuk University

● 요 약 ●

본 논문에서는 스마트폰과 스마트폰이 블루투스로 연결할 때 페어링 진행을 최초 1회만 하는 것에 대한 위험성에 관하여 연구하였다. 본 연구를 통하여 구현한 트로이목마 어플리케이션은 희생자 스마트폰과 페어링이 되어 있을 경우, 실행과 동시에 공격자의 스마트폰과 블루투스로 연결되도록 하였다. 희생자 스마트폰의 어플리케이션은 스마트폰의 카메라를 작동시켜 사진을 촬영하고 스마트폰에 저장된 주소록 데이터를 추출하며, 촬영한 사진과 추출한 주소록 데이터를 공격자의 스마트폰으로 전송한다. 공격자는 희생자의 스마트폰에서 탈취한 정보를 확인할 수 있다.

**키워드:** 트로이목마(Trojan horse), 블루투스(Bluetooth), 페어링(Pairing), 사회 공학적 기법(Social engineering)

## I. Introduction

스마트폰의 블루투스 인증은 페어링을 통해 이루어진다. 최초 페어링이 진행되면 서로의 블루투스 연결이 정상적인 방법으로 이루어진 것인지 확인하기 위해 핀 번호를 출력하고 해당 핀 번호를 두 스마트폰 사용자가 확인한 후 연결을 승인한다. 하지만 최초 페어링 이후의 연결은 서로의 스마트폰 기기가 신뢰할 수 있는 기기로 등록이 되어있기 때문에 페어링 없이 진행하게 된다. 본 논문은 사회공학적 기법을 이용하여 최초 페어링을 진행한 후, 희생자 스마트폰에 저장된 데이터를 탈취하도록 공격자와 희생자의 스마트폰에서 작동되는 트로이목마 어플케이션을 구현하였다.

## II. Preliminaries

### 1. Social engineering

사회 공학적 기법은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격기법을 통칭한다. 시스템의 한 요소로서의 사람은 취약점을 가진 요소로 작용될 수 있다. 최근 모바일 기기의 발전과 대용량화로 인해 모바일 기기 안에 중요한 정보들을 저장할 수 있게 되었는데, 이로 인해 모바일 기기 또한 새로운 공격 목표물이 될 수 있다는 위험성을 가지게 되었다. 사회 공학적 기법은 접근 수단을 무엇으로 하느냐에 따라서 인간 기반과 컴퓨터 기반으로 나누어진다. 인간 기반 공격은 대상에게 직접적인 접근을 통해 이루어지고 컴퓨터 기반 공격은 공격 대상에게 악성코드나 프로그램, 웹 사이트 등의 수단을 이용해 접근을 통해 이루어진다. [1]

### 2. Trojan horse

트로이 목마는 정상 프로그램으로 가장하여서 악의적인 행위를 실행하는 프로그램 또는 코드를 말한다. 주로 사회 공학적 기법을 이용하여 배포되며 사용자 몰래 공격자가 원하는 정보를 빼내 가거나 키 로그 기능을 수행하기도 한다. 최근에 이슈가 되고 있는 APT 공격에서도 트로이목마 악성코드를 활용하는 공격이 대다수이다. [2] 암호화화폐 트로이목마는 컴퓨터를 모니터링하면서 암호화화폐 계좌 번호로 보이는 정보가 나타나길 기다렸다가 사용자가 전송하려는

순간 원래의 계좌를 공격자의 계좌 번호로 바꿔 피해를 준다. [3]

### 3. Bluetooth connection [4][5]

스마트폰이 블루투스 장치와 연결하기 위한 절차는 다음과 같다.

장치검색 : 블루투를 연결하기 위해 주변에 있는 블루투스가 활성화된 장치를 검색한다.

페어링 : 선택한 장치와 연결하기 위해서는 페어링이라는 간단한 인증절차를 거친다.

장치연결 : 한번 페어링을 진행한 장치와는 페어링 과정 없이 목록에 있는 장치를 선택하는 것만으로도 블루투스 연결이 완료된다.

Fig. 1와 같이 스마트폰 LG G5가 Samsung Galaxy S7과 페어링을 진행 하고나면, 다음에 블루투스를 연결할 때 연결 가능한 기기 목록에 Samsung Galaxy S7가 표시되므로, 이후부터는 목록에서 선택하여 연결 할 수 있다.

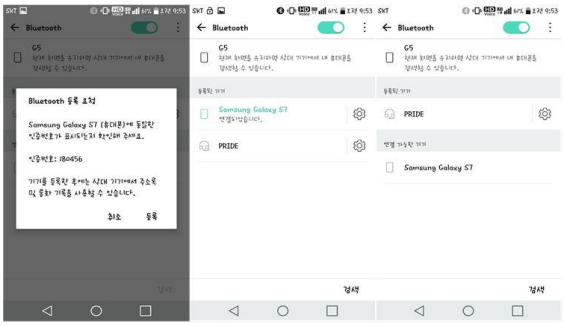


Fig. 1. 스마트폰 블루투스 페어링 과정

## III. Trojan horse application

본 연구에서 제작한 트로이목마 어플리케이션은 희생자의 스마트폰에서 실행과 동시에 공격자의 스마트폰과 블루투스로 연결되며, 크게 2가지 기능을 가지고 있다. 첫 번째로 희생자의 주소록 데이터를 탈취하여 전송하는 기능과 두 번째로 희생자의 카메라를 작동시켜 사진을 촬영하여 전송하는 기능이다. 공격 시나리오는 모의로 진행하였으며 두 개의 스마트폰을 준비하여 진행 상황을 캡처하였다. 탈취한 데이터들은 테스트를 위해 제작된 데이터이다.

### 1. Application configuration and environment

트로이목마 어플리케이션은 Fig. 2와 같이 공격자의 스마트폰에서 실행하는 서버 어플리케이션(CnCServer)과 희생자의 스마트폰에서 실행하는 클라이언트 어플리케이션(ISCommunity)으로 구성되어있다.

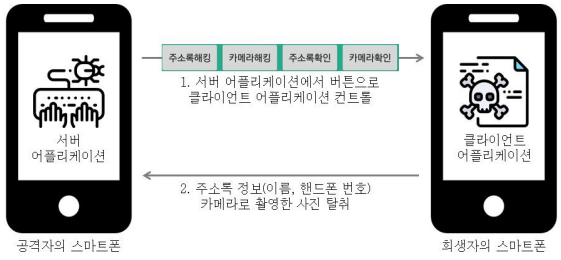


Fig. 2. 서버와 클라이언트 어플리케이션 통신 구조

어플리케이션 개발환경은 Table 1과 같다.

Table 1. 트로이목마 어플리케이션 개발 환경

| 환경 | | 이름 |
|---|---|---|
| 개발 tool | | Android Studio |
| 스마트폰 기종 | 서버 | Galaxy S7 |
| | 클라이언트 | LG Gx2 |
| 안드로이드 Version | 서버 | 안드로이드 8.0.0 |
| | 클라이언트 | 안드로이드 4.4.2 |

### 2. Attack scenario

공격은 Fig. 3와 같이 사회 공학적 기법을 이용하여 희생자들에게 접근한 후, 블루투스 연결을 시도하는 것으로 시작된다. 이후엔 학과 커뮤니티 어플리케이션을 가장해 데이터를 탈취하는 기능을 가진 클라이언트 어플리케이션을 학과 학생들(희생자)에게 배포한다. 공격자는 희생자의 스마트폰을 컨트롤 할 수 있는 서버 어플리케이션을 실행한 후 희생자에게 접근한다. 희생자가 클라이언트 어플리케이션을 학과 커뮤니티 어플리케이션이라고 착각하고 실행하는 순간 공격자의 스마트폰과 블루투스로 연결되고 공격자는 희생자의 스마트폰에서 정보를 탈취할 수 있다.

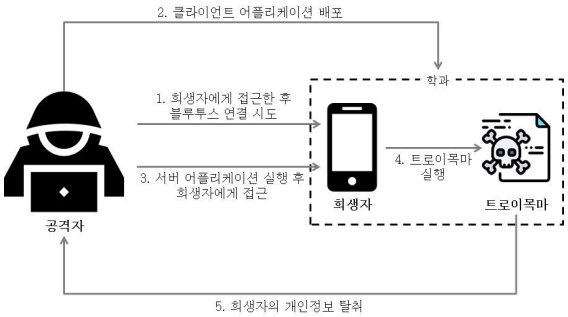


Fig. 3. 공격 시나리오

### 3. Server and client applications

[server application]

공격자는 Fig. 4에서와 같이 서버 어플리케이션에 있는 4개의 버튼으로 클라이언트 어플리케이션을 컨트롤 할 수 있다.

- 주소록해킹 : 클라이언트 어플리케이션이 희생자의 스마트폰에 저장된 주소록 데이터에서 이름과 전화번호를 추출하여 서버 어플리케이션으로 전송하도록 한다.
- 카메라해킹 : 클라이언트 어플리케이션이 희생자의 스마트폰 전면 카메라를 작동시켜 희생자를 촬영하도록 한다.
- 주소록확인 : 클라이언트 어플리케이션이 전송한 희생자의 주소록 데이터를 공격자 화면에 출력한다.
- 카메라확인 : 희생자의 스마트폰에서 촬영한 사진을 서버 어플리케이션으로 전송하도록 하고 공격자 화면에 출력한다.

[client application]

클라이언트 어플리케이션은 실행과 동시에 공격자의 스마트폰

MAC주소로 블루투스 연결을 시도한다. 공격자의 스마트폰에 서버 어플리케이션이 실행 중이라면 바로 블루투스로 연결된다. 블루투스 연결에 성공하면 Fig. 5와 같이 서버 어플리케이션에 연결된 희생자 스마트폰 정보가 출력되고, 이후에는 희생자가 인지하지 못하는 사이에 공격자의 서버 어플리케이션의 제어에 따라 정보를 공격자에게 보낸다.

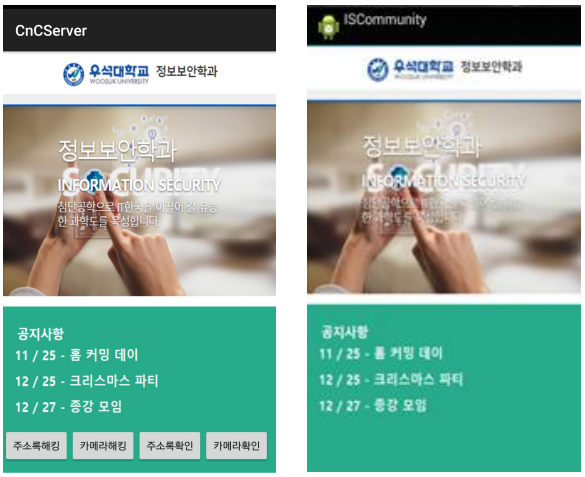


Fig. 4. 서버와 클라이언트 어플리케이션 실행화면

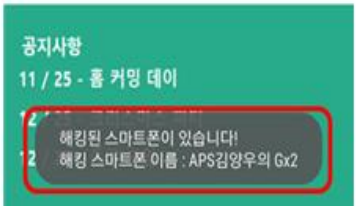


Fig. 5. 서버 어플리케이션 블루투스 연결 확인

4. Taking smartphone address book

공격자가 [주소록해킹] 버튼을 클릭하면 클라이언트 어플리케이션으로 주소록 데이터를 추출하는 신호를 보낸다(Fig. 6). 신호를 받은 클라이언트 어플리케이션은 스마트폰에 저장된 주소록에서 이름과 전화번호를 추출하여 배열에 저장하고, 배열에 있는 데이터를 순서대로 블루투스를 통해 전송한다. 서버 어플리케이션은 들어오는 주소록 데이터를 순서대로 다시 배열에 저장한다. 서버 어플리케이션에서 주소록확인 버튼을 클릭하면 공격자 화면에 희생자 스마트폰에서 추출한 주소록 데이터를 출력한다(Fig. 7).

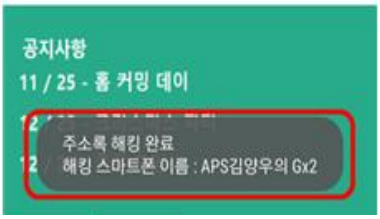


Fig. 6. 서버 어플리케이션에서 주소록해킹 버튼 클릭

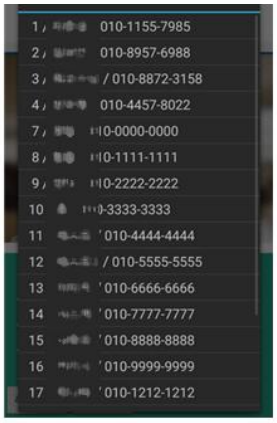


Fig. 7. 희생자의 스마트폰에서 탈취한 주소록 확인

5. Taking smartphone camera picture

서버 어플리케이션에서 [카메라해킹] 버튼을 클릭하면 클라이언트 어플리케이션으로 카메라 작동 신호를 보낸다. 신호를 받은 클라이언트 어플리케이션은 스마트폰 전면 카메라를 작동시켜 희생자를 촬영한다. 클라이언트 어플리케이션에 카메라 기능을 추가했기 때문에 카메라 어플리케이션을 실행시키지 않고 바로 사진을 촬영할 수 있다. 서버 어플리케이션에서 [카메라확인] 버튼을 클릭하면 희생자 스마트폰에서 촬영한 사진을 블루투스를 통해 전송한다(Fig. 8). 전송이 완료되면 공격자 화면에 희생자 스마트폰에서 전송받은 사진을 출력한다(Fig. 9).

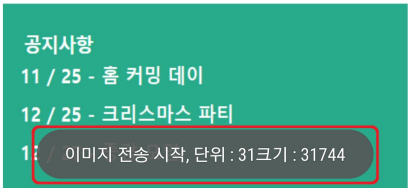


Fig. 8. 서버 어플리케이션으로 이미지 전송

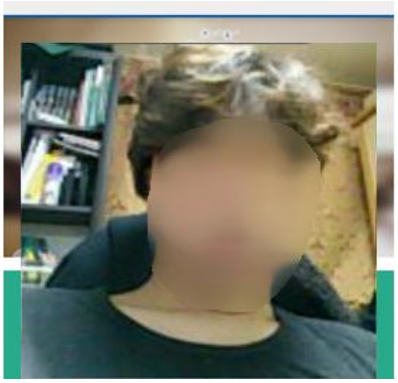

Fig. 9. 희생자 스마트폰에서 촬영한 사진 출력

IV. Conclusions

본 논문에서는 스마트폰이 블루투스로 연결할 때 페어링을 최초 1회만 진행하는 것에 대한 취약점을 분석하였다. 사회 공학적 기법을 이용하여 최초 페어링을 진행한 후, 학과 커뮤니티 어플리케이션을

가장한 트로이목마 어플리케이션을 통하여 공격 대상의 스마트폰에 담긴 중요한 개인정보를 탈취하는 시나리오를 설계하였고, 이를 위한 트로이목마 서버 및 클라이언트 어플리케이션을 구현하여 그 위험성을 보였다.

## REFERENCES

[1] Changing aspects of social engineering hacking, Policy Planning 08-04, Korea Information Security Agency Policy Planning Team
[2] TeanamCho, Introduction to information security, infinit ibooks, 2009. 02.
[3] ITWorld Korea, http://www.itworld.co.kr/news/107732
[4] Specification of the Bluetooth System, v5.0 ,Bluetooth SIG
[5] Specification of the Bluetooth System, v4.0 ,Bluetooth SIG