Truth and Falsity of Various Services

AhnLab, Inc
Silverbug

Agenda

- Wi-Fi
- SMS
- Android Key/Pattern Unlock
- CSRF

WIFI

Hotstats as of January 25, 2010 289,834 free and pay Wi-Fi locations in 139 countries

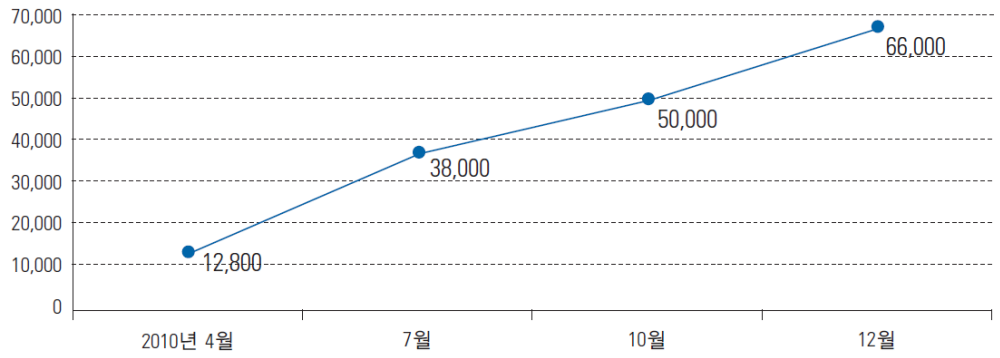
Top 10 Countries			Top 10 U.S. Cities			Top 10 Location Types		
Rank	Countries	Locations	Rank	Cities	Locations	Rank	Type	Locations
1	United States	69,757	1	New York	883	1	Hotel/Resort	65,701
2	China	35,115	2	San Francisco	870	2	Other	51,086
3	United Kingdom	28,041	3	Chicago	798	3	Cafe	41,710
4	France	26,283	4	Houston	641	4	Restaurant	41,702
5	Germany	14,759	5	Seattle	609	5	Public Space/ Public Building	22,874
6	Russian Federation	14,700	6	Los Angeles	511	6	Store/Shopping Mall	15,525
7	South Korea	12,815	7	Atlanta	463	7	Office Building	10,232
8	Japan	11,833	8	San Diego	448	8	Hotzone	6,634
9	Sweden	7,124	9	San Antonio	428	9	Pub	5,206
10	Switzerland	5,485	10	Austin	425	10	Airport	3,368

출처 : JiWire Global Wi-Fi Finder(2010. 1. 25. 기준)

이동통신사	2009년 말	2010년 7월	2010년 11월
KT	약 12,000	27,000	40,000
SKT	-	5,000	14,000
LG U+	-	-	16,000
계	약 12,000	32,000	70,000

※출처: 각 사업자 발표, 언론보도

[국내 Wi-Fi Zone 추이]



*Soure : 지와이어, 매일경제 재인용
*출처 : http://www.wi-fi.org

각 통신사별 Wi-Fi 정책

KT – only Subscribers
SKT – only Subscribers
LGT – Subscribers AP

Telecom WiFi

- Phone Register.
  - IMEI & Mac Address Register(White List)
- USIM + Wifi (Secure)
  - Most phone does not support
- Insecure Wifi(Not Secure)

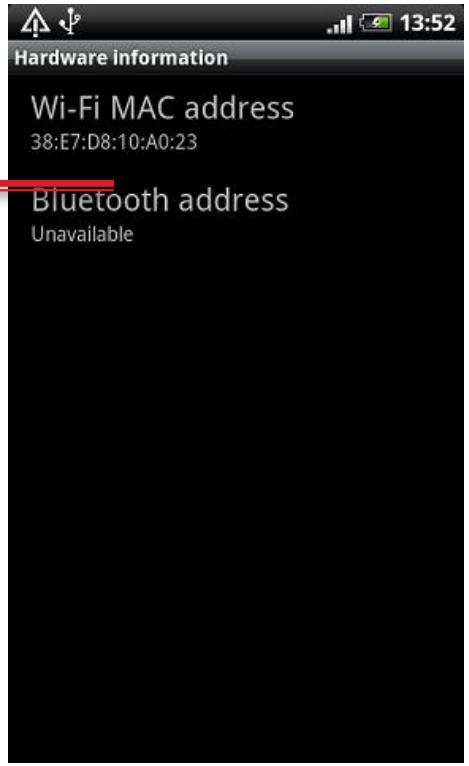
Wi-Fi Security Issues

- Firesheep
  - Easy…
  - Mozilla Firefox add-ons
  - HTTP Session Hijacking Attack

- Countermeasures
  - Blacksheep
  - VPN, HTTPS
  - Wireless network security

Mac Address – Unique?

refurbished phone?

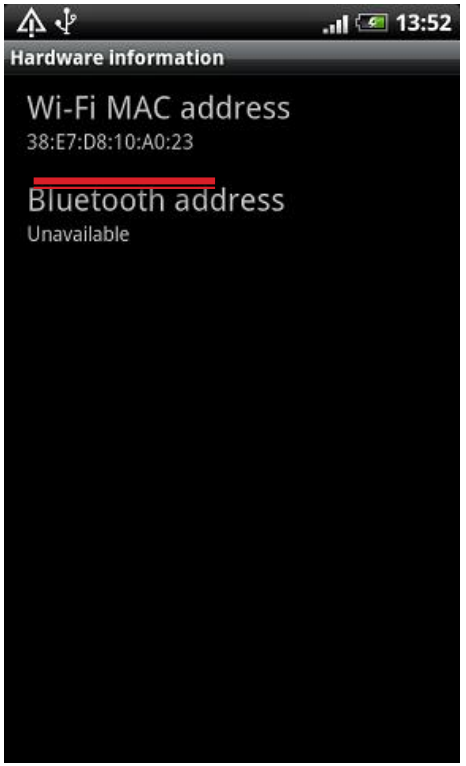


=

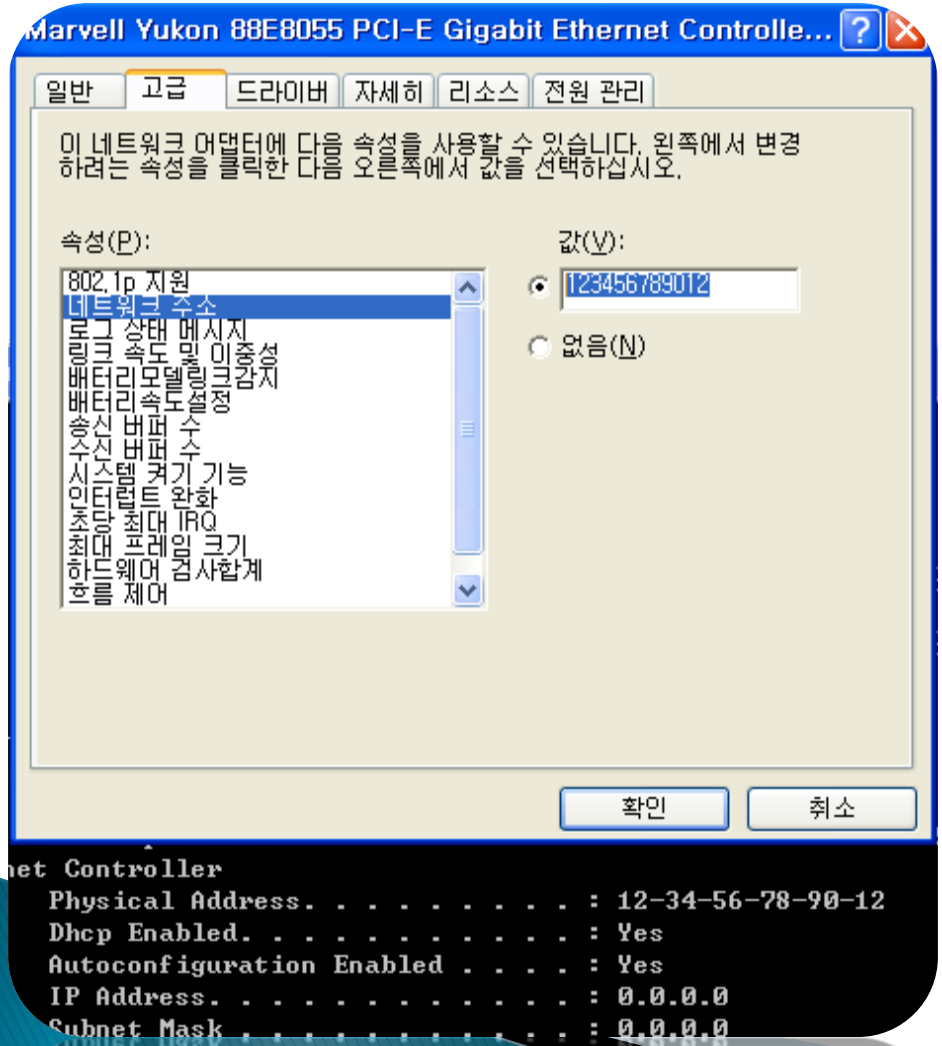
Mac Address

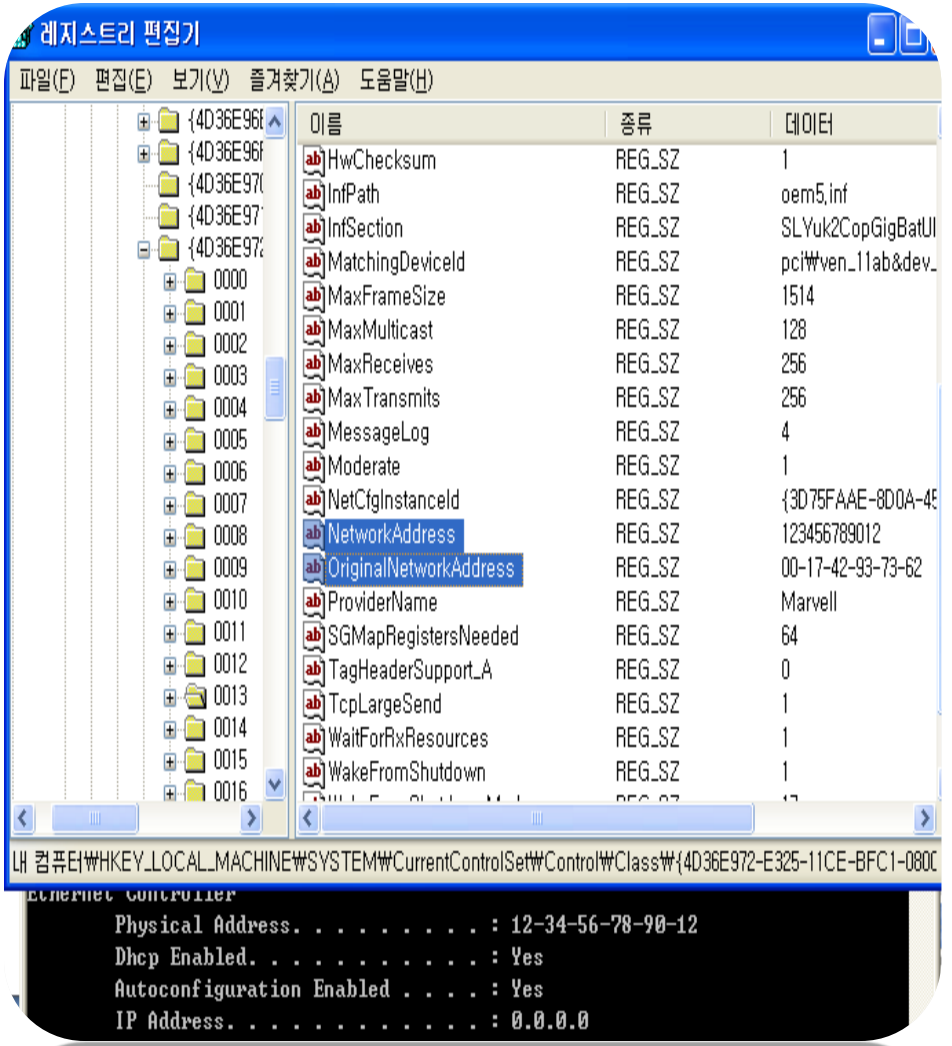
xx:xx:xx:xx:xx:xx

Magic Mac Address?



Mac Change – Windows





Mac Change – Linux/BSD

- BSD

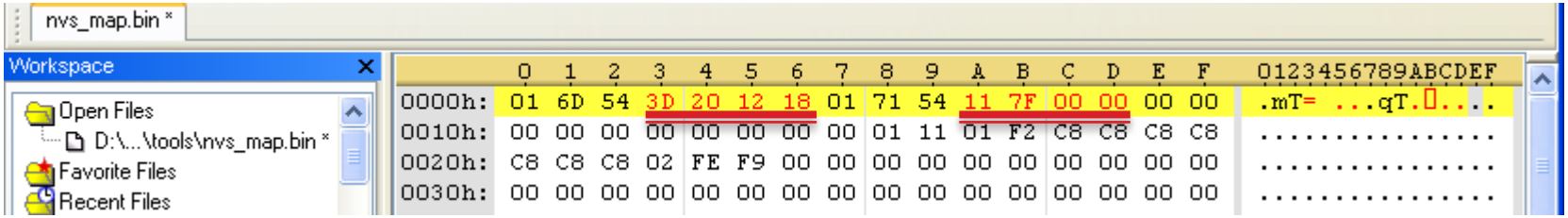
- Bring down the interface: "ifconfig xl0 down"
- Enter new MAC address: "ifconfig xl0 link AA:BB:CC:DD:EE:FF"
- Bring up the interface: "ifconfig xl0 up"

- Linux

Bring down the interface: "ifconfig eth0 down"
Enter new MAC address: "ifconfig eth0 hw
ether AA:BB:CC:DD:EE:FF"
Bring up the interface: "ifconfig eth0 up"

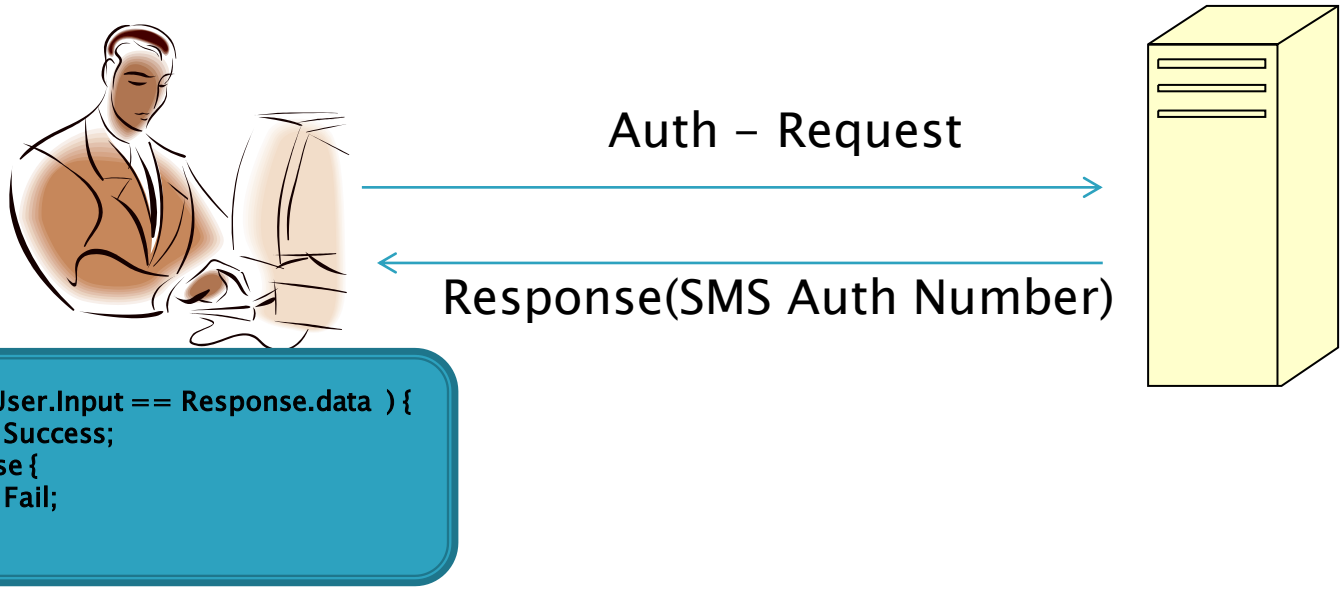
Mac Change – Android

- Android
  - eeprom image file
  - /pds/wifi/nvs_map.bin



SMS Authentication

- Client Side Script – Authentication



Android Key/Pattern Unlock

- com.android.internal.widget.LockPatternUtils
  - /data/system/gesture.key

Settings.db

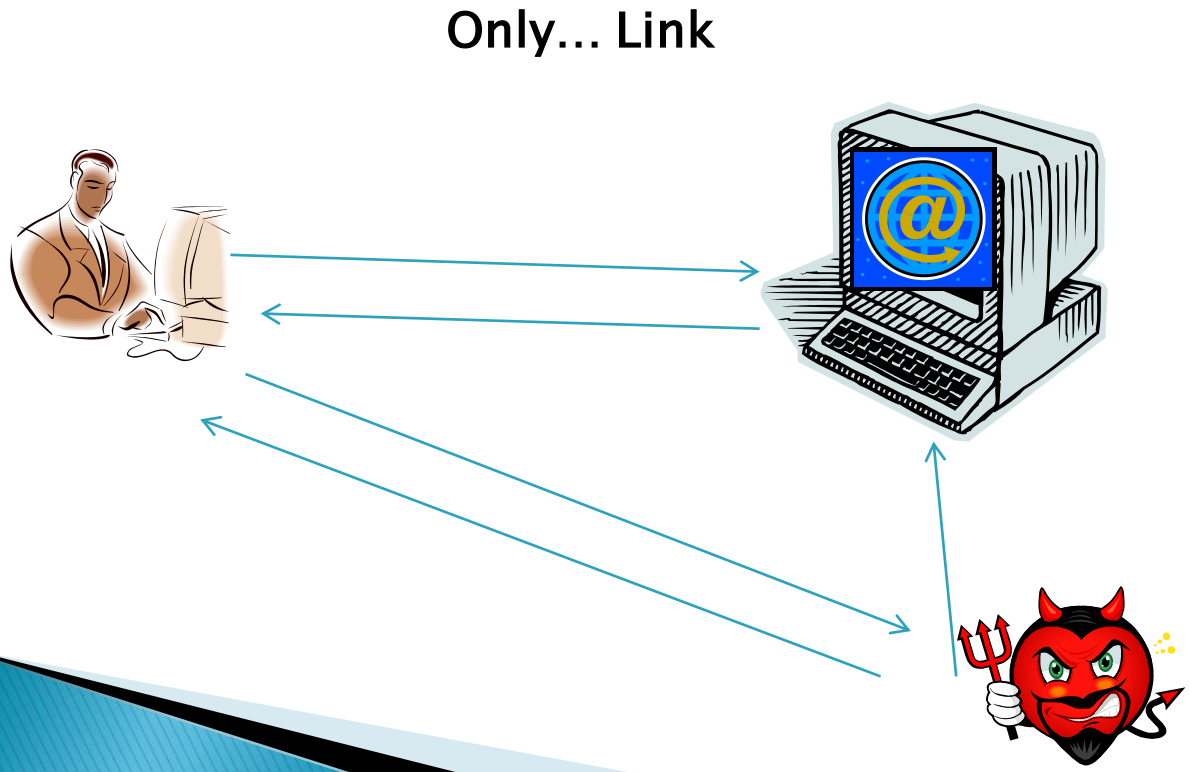
```
for (int i = 0; i < patternSize; i++) {
    LockPatternView.Cell cell = pattern.get(i);
    res[i] = (byte) (cell.getRow() * 3 + cell.getColumn());
}

MessageDigest md = MessageDigest.getInstance("SHA-1");
byte[] hash = md.digest(res);
return hash;
```

  - /data/system/pc.key

```
byte[] saltedPassword = (password + getSalt()).getBytes();
byte[] sha1 = MessageDigest.getInstance(algo = "SHA-1").digest(saltedPassword);
byte[] md5 = MessageDigest.getInstance(algo = "MD5").digest(saltedPassword);
hashed = (toHex(sha1) + toHex(md5)).getBytes();
```

CSRF

- Attack
  - Cross Site Request Forgery



여기에 넣을 수 없는 것!

- 법적인 문제로...


THE
END