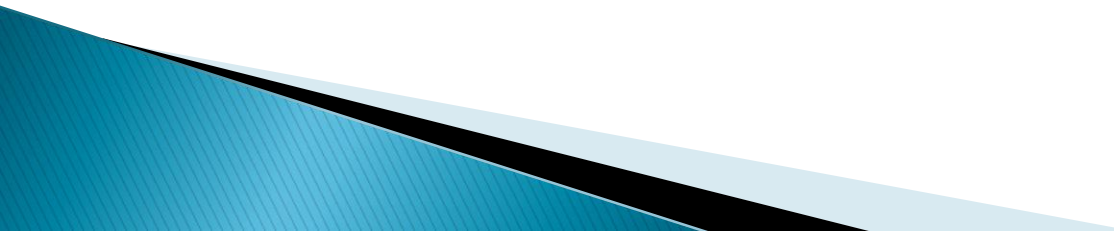


# Truth and Falsity of Various Services

AhnLab, Inc  
Silverbug

# Agenda

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



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

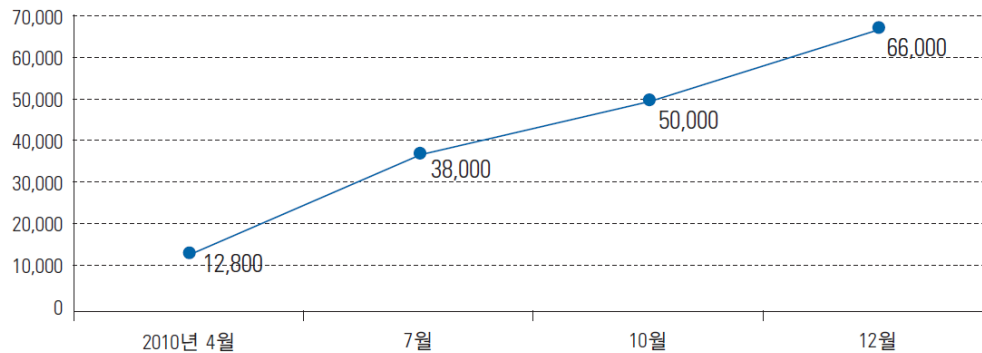
Top 10 Countries			Top 10 U.S. Cities			Top 10 Location Types		
Rank	Countries	Locations	Rank	Cities	Locations	Rank	Type	Locations
1	United States	69,757	1	New York	883	1	Hotel/Resort	65,701
2	China	35,115	2	San Francisco	870	2	Other	51,086
3	United Kingdom	28,041	3	Chicago	798	3	Cafe	41,710
4	France	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]



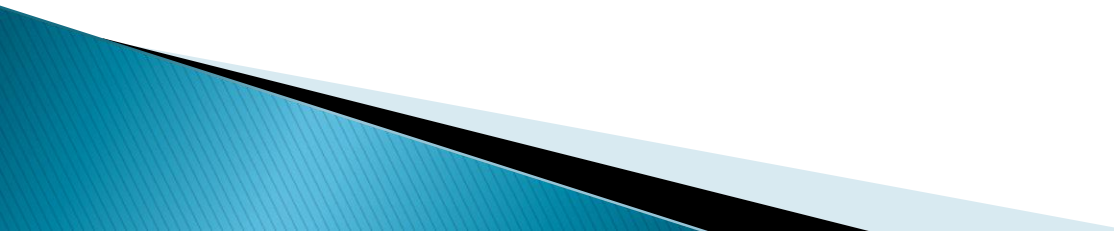
\*Source : 지와이어, 매일경제 재인용

\*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

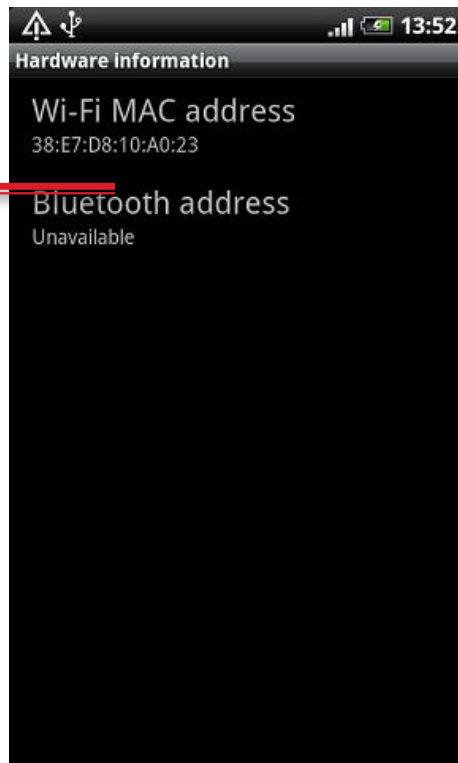


## Countermeasures

- Blacksheep
- VPN, HTTPS
- Wireless network security

# Mac Address – Unique?

refurbished phone?

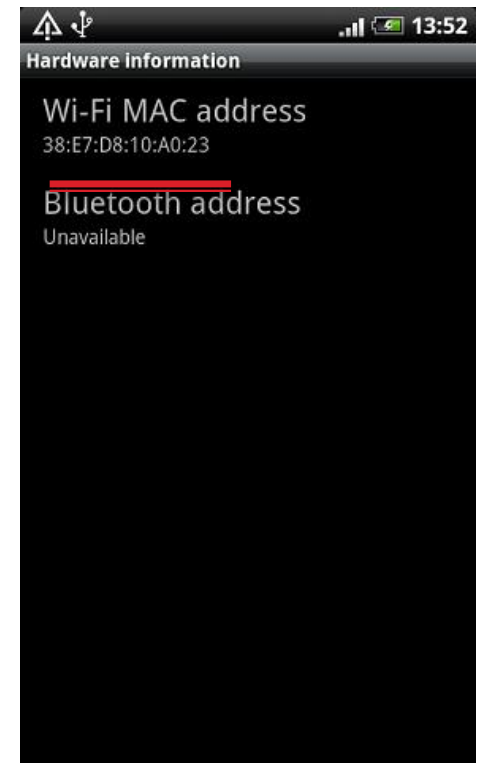


=

Mac Address

**XX:XX:XX:XX:XX:XX**

Magic Mac Address?



# Mac Change - Windows

Marvell Yukon 88E8055 PCI-E Gigabit Ethernet Controlle...

일반 고급 **드라이버** 자세히 리소스 전원 관리

이 네트워크 어댑터에 다음 속성을 사용할 수 있습니다. 왼쪽에서 변경하려는 속성을 클릭한 다음 오른쪽에서 값을 선택하십시오.

속성(P):

- 802.1p 지원
- 네트워크 주소**
- 로그 상태 메시지
- 링크 속도 및 링크 감지
- 배터리 리모컨 링크 감지
- 배터리 리모컨 링크 감지
- 송신 버퍼 수
- 수신 버퍼 수
- 시리얼 커넥터 기능
- 인터럽트 완화
- 초당 최대 IRQ
- 최대 프레임 크기
- 하드웨어 검사합계
- 호환

값(V):

123456789012

없음(N)

확인 취소

```

net Controller
Physical Address. . . . . : 12-34-56-78-90-12
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0

```

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

이름	종류	데이터
{4D36E96F}		
{4D36E96F}		
{4D36E970}		
{4D36E970}		
{4D36E970}		
0000		
0001		
0002		
0003		
0004		
0005		
0006		
0007		
0008		
0009		
0010		
0011		
0012		
0013		
0014		
0015		
0016		
ab]HwChecksum	REG_SZ	1
ab]InfPath	REG_SZ	oem5.inf
ab]InfSection	REG_SZ	SLYuk2CpGigBatUI
ab]MatchingDeviceId	REG_SZ	pci\ven_11ab&dev_...
ab]MaxFrameSize	REG_SZ	1514
ab]MaxMulticast	REG_SZ	128
ab]MaxReceives	REG_SZ	256
ab]MaxTransmits	REG_SZ	256
ab]MessageLog	REG_SZ	4
ab]Moderate	REG_SZ	1
ab]NetCfgInstanceId	REG_SZ	{3D75FAAE-8D0A-4E...
ab]NetworkAddress	REG_SZ	123456789012
ab]OriginalNetworkAddress	REG_SZ	00-17-42-93-73-62
ab]ProviderName	REG_SZ	Marvell
ab]SGMapRegistersNeeded	REG_SZ	64
ab]TagHeaderSupport_A	REG_SZ	0
ab]TcpLargeSend	REG_SZ	1
ab]WaitForRxResources	REG_SZ	1
ab]WakeFromShutdown	REG_SZ	1

```

LH 컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-0800...
net Controller
Physical Address. . . . . : 12-34-56-78-90-12
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 0.0.0.0

```

# 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"



# SMS Authentication

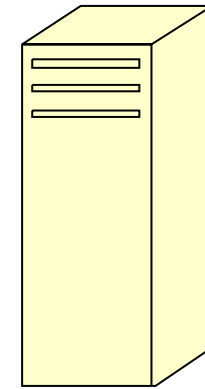
## ▶ Client Side Script – Authentication



Auth – Request



Response(SMS Auth Number)



```
if( User.Input == Response.data ) {  
    Success;  
} else {  
    Fail;  
}
```

# 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;
```

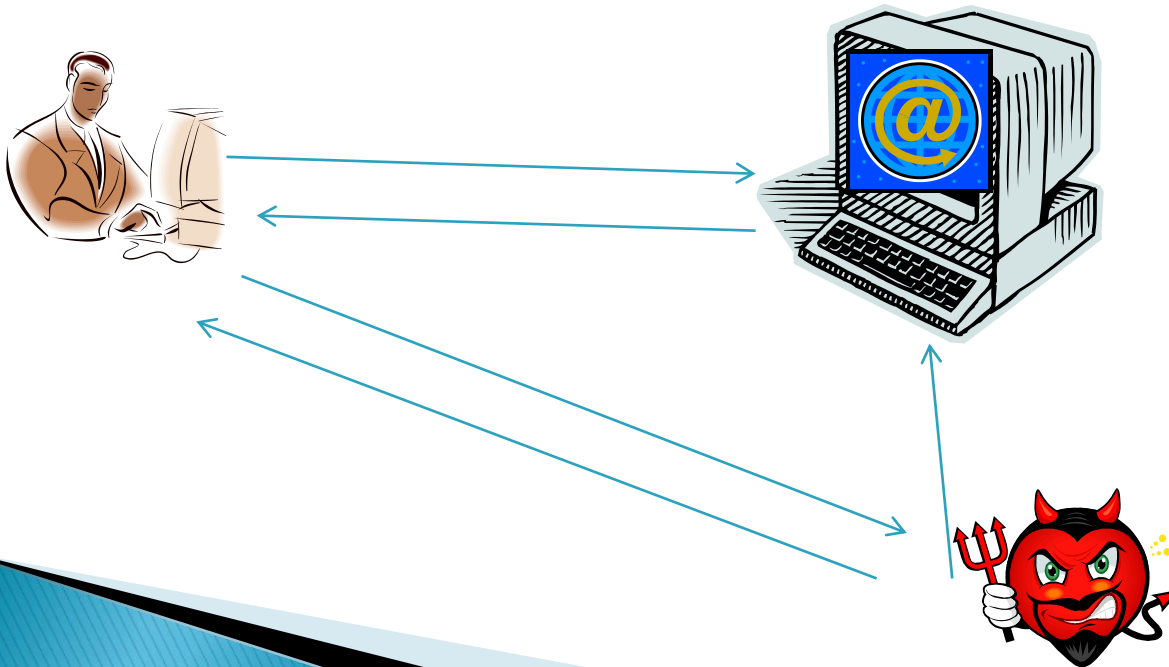
- `/data/system/pc.key`

```
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

Only... Link



# 여기에 넣을 수 없는 것!

- ▶ 법적인 문제로...

