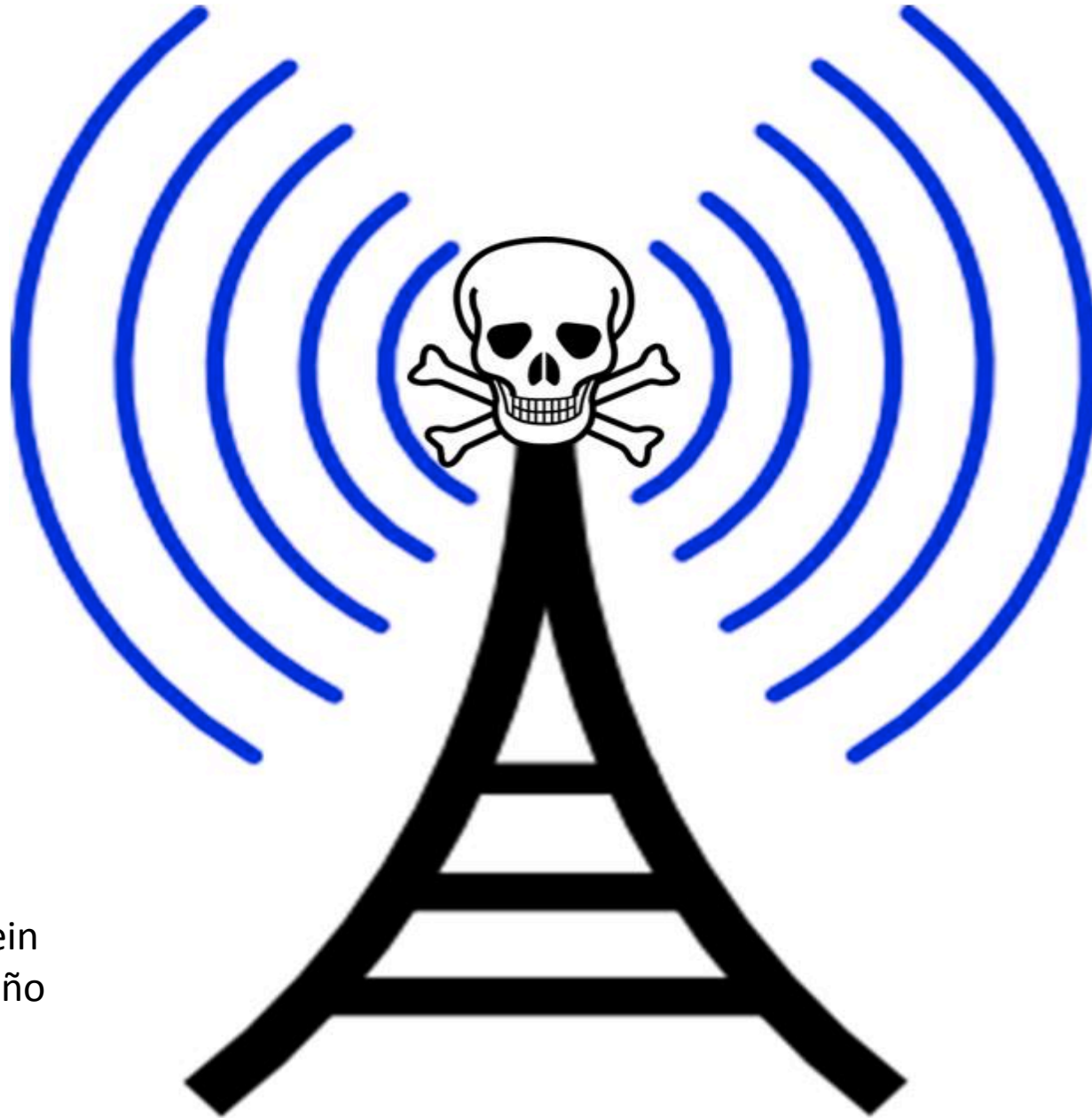
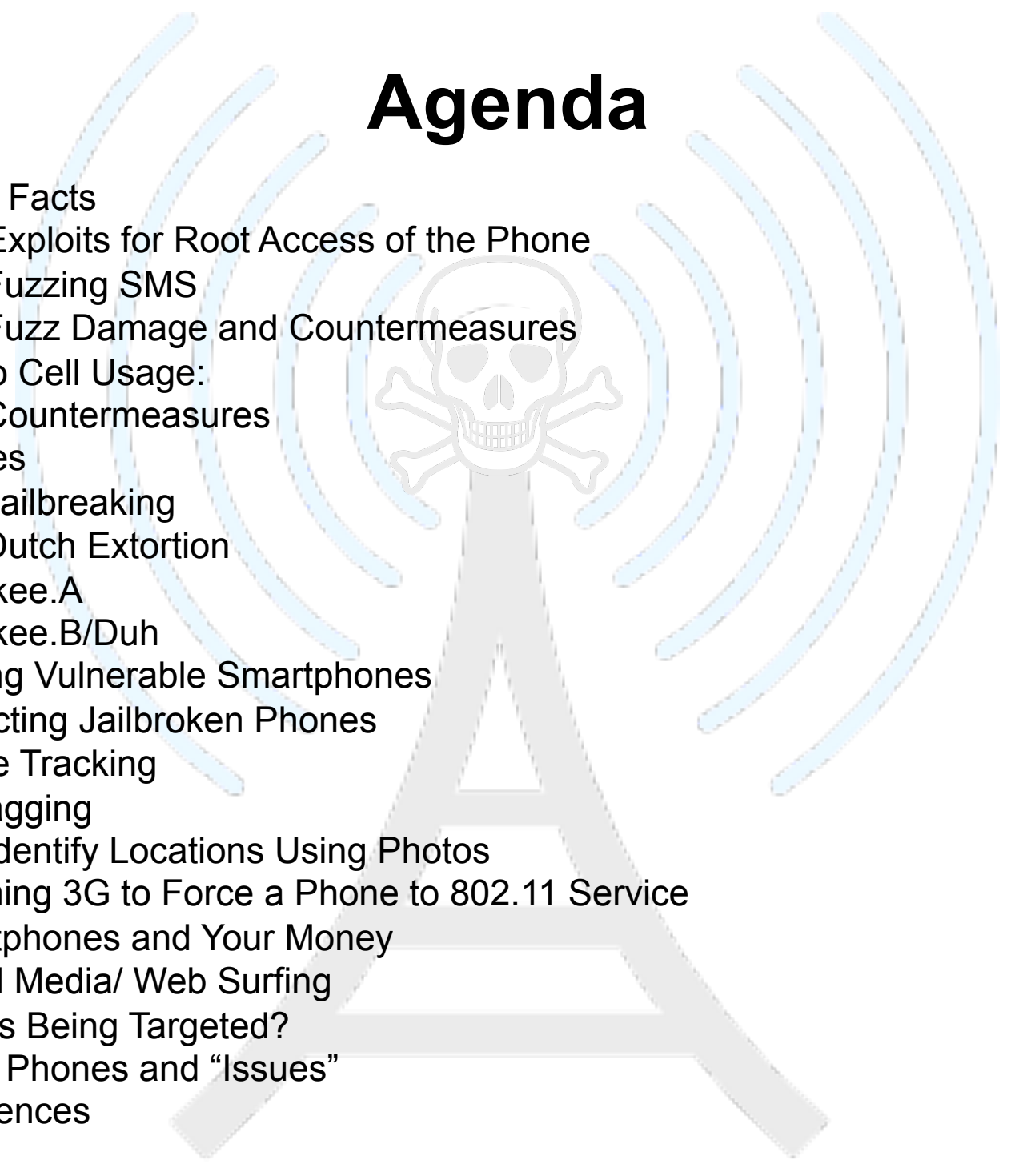


# YOUR SMART PHONE HATES YOU



Mike Klipstein  
Rafael Cedeño  
Li Li

# Agenda

- Quick Facts
  - SMS Exploits for Root Access of the Phone
    - Fuzzing SMS
    - Fuzz Damage and Countermeasures
  - Femto Cell Usage:
    - Countermeasures
  - iPhones
    - Jailbreaking
    - Dutch Extortion
    - ikee.A
    - ikee.B/Duh
  - Finding Vulnerable Smartphones
  - Protecting Jailbroken Phones
  - Phone Tracking
  - Geotagging
    - Identify Locations Using Photos
  - Jamming 3G to Force a Phone to 802.11 Service
  - Smartphones and Your Money
  - Social Media/ Web Surfing
  - Who is Being Targeted?
  - Other Phones and “Issues”
  - References
- 

**What People Want From Their Phone**

**FREE PORN!!!!**



# What They Get From Their Phone



Really? But He Seems Really Friendly....

# Quick Facts



- Over **3.3 BILLION** active cell phones worldwide
- Over 2 billion users of SMS worldwide
- Korean teenagers 15-19 average **20,000** text messages per year (60.1 per day)
- On 2 FEB 2011, over **1 BILLION** text messages were sent in Beijing, China in one day
- **101.2 MILLION** smart phones sold in 2010
- SMS (Text Messages) protocol outlined in 3GPP TS 24.011 as part of GSM standard in 1985
- Limited to 160 7 bit characters (140 bytes)
- Uses extra bandwidth in the control channels – essentially free for the provider

# SMS Exploits



- Presents a serious problem because of the “always on” nature of the SMS service.
- Attacker could render a phone unusable.
- If written properly, will give root access to the phone OS
- Attacker will have access to even encrypted data on phone
- The iPhone CommCenter process is responsible for handling SMS and telephone call, running as root with **no application sandbox!**
- Android uses a **Java application** for SMS
- **NO WAY TO FIREWALL** without blocking calls or data transmission

# Fuzzing SMS

- Fuzzing originally used to test software for input vulnerabilities.
- Random and oversized data streams used to locate and pinpoint vulnerabilities.
- The whole process consists of 3 steps: generation, delivery and monitoring.
- Local injection of SMSs at the application level provides a cost-efficient way to systematically test implementations by avoiding the mobile network (SMS cost money!)
- The “generation” step involves modifying the structure of SMS messages and its stack.
- Vulnerabilities found can theoretically affect more than half the mobile phones in general US usage.
- Former NSA employee Collin Mulliner demonstrated that an SMS may be sent and no notification will be presented to the phone user.

# Fuzzing Damage & Countermeasures

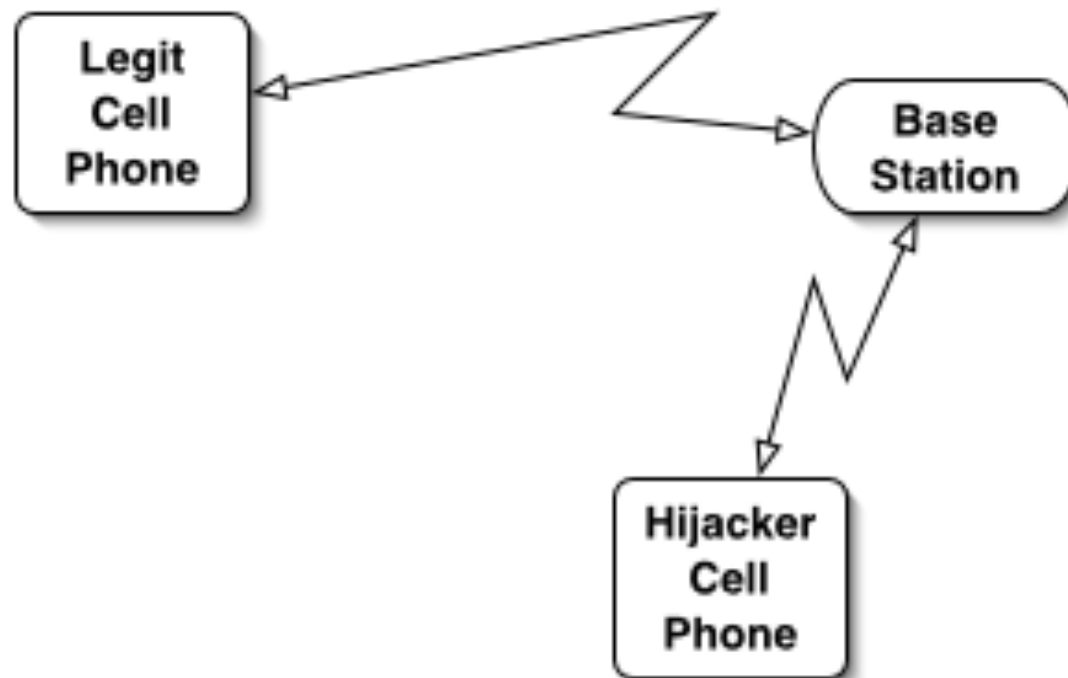
- By fuzzing SMSs, researchers have found that it's possible to lock phones, interrupt calls, switch devices off, brick (destroy) phones & reboots.
- Providers may also be forced to create other type of filter methods due to privacy issues. Some countries may not allow invasive screening of data.
- iPhones can be kicked off the network and lose **all** connections (bluetooth, WiFi, 3G); phone cannot join the network for about 15 seconds
- Android phones can be kicked off the network and if the SIM has a PIN, will not register with the network until the user notices (owner is unreachable)
- Mulliner demonstrated at a Black Hat conference by locking a random iPhone in the audience for the duration of his presentation and for 2 ½ hours after by sending SMSs.
- Repeatedly send SMSs will queue and continue attacking
- Very little can be made to avoid these attack from the customer side.
- Customers only hope is for providers to adopt a filtering scheme at the core network level.

# Femto (Pico) Cells & Eavesdropping

- Pico cell are low power “base stations” on which potential devices can connect to.
- The vulnerability of the A5/1 & A5/2 cyphers have paved the road for researchers and aficionados to create means of individual targeting and eavesdropping.
- Although the equipment needed to implement such attack was prohibitively high, nowadays a whole kit can be put together with a relatively low cost.
- Two main approaches can be taken: create a relay base station or “listen” to the data traveling through a specific carriers base station using a modified GSM handset.
- Cheap handsets can have their firmware swapped for a modified open source version that allows it to listen to all the data going through the legitimate base station it's connected to.
- On the other hand, by creating a relay base station, attackers can force users in close vicinity to hop on their station. Afterwards, the communication is then relayed to a legitimate base station (e.g. AT&T, T-Mobile, etc.)

# Pico Cells & Eavesdropping

- At the JAN 2011 Black Hat Conference, Ralf-Philipp Weinmann demonstrated how to hack and steal information from iPhones with a laptop acting as a base station for less than \$100.
- Could monitor all voice and data exchanges with laptop used for Man-in-the-Middle Attack



# Countermeasures

- Since the algorithms that “protect” our calls are vulnerable, there’s not much customers nor providers can do until other technologies provide better security means.
- 2G-only GSM handsets are the most vulnerable group, since they are potential targets to anyone with mal-intent. Users with 2G/3G handsets can be able to locally force the device to only use 3G and thus mitigate the exploit.
- However, the standard cryptographic algorithm KAZUMI (A5/3) used over 3G UMTS networks has been cracked recently. Although the initial crack was done under unoptimized conditions in a little under two hours (hardly on-the-fly), it’s still a matter of concern.
- As far-fetched as it may sound, we should try and move towards more recent technologies like LTE (pre-4G) and subsequently to Advanced LTE (4G) which provide stronger algorithms.

# iPhone – The Breakthrough of Smartphone



- Runs on the iOS
- Thousands of applications – making your phone to be a handheld computer
- Consumers download **9 paid apps per month**
- Other applications can't be installed on iOS, except jailbreak or unlock iPhone.
- U.S. declares iPhone jailbreaking **legal**
- **7%** of the iPhone users have jailbroken their devices
- **2.3 million** jailbroken iPhones in 2009

# Why People Jailbreak the iPhone?

- Allows to install 3<sup>rd</sup> party applications on iPhone via Cydia and Installer
- Makes your iPhone more customizable
- Full control of your iPhone system
- The precondition for unlock



# Jailbreaking Brings Security Threats



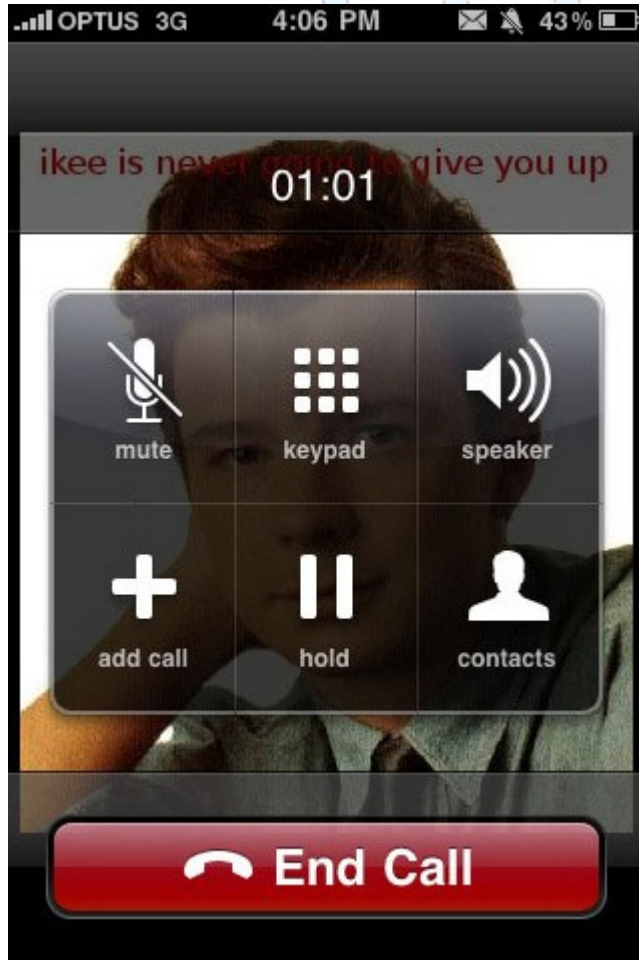
- “Jailbreak **removes 80%** of the iPhone’s **security precautions**”
  - Charlie Miller, SyScan 2009
- **OpenSSH** is used to jailbreak, gives backdoor access to iPhone.
- The default password of OpenSSH is ‘alpine’
- The jailbroken iPhone is completely open to other hack attempts, if user fails to change the default password.

# Dutch Extortion



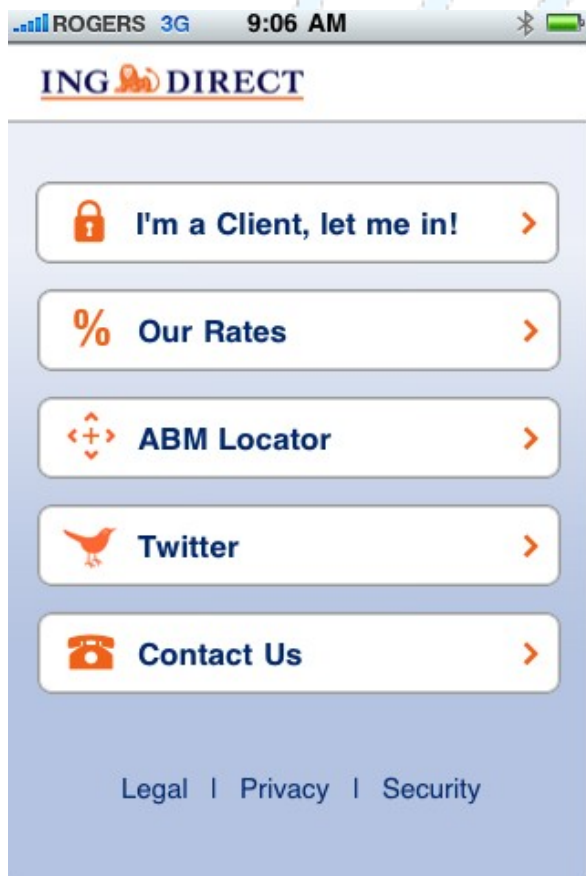
- In November 2009, Dutch users of jailbroken iPhones in T-Mobile's 3G IP range began experiencing extortion popup windows.
- The hacker made use of **port scanning method** to find jailbroken iPhones in his country Netherlands **running with SSH**.
- *"Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your iPhone right now! Right now, I can access all your files."*

# First iPhone Worm – ikee.A



- iPhone owners in Australia have reported that their smartphones have been infected by a worm that has **changed their wallpaper** to an image of 1980s pop crooner Rick Astley.
- A 21-year-old Australian hacker released the initial innocuous iPhone worm using the very same SSH vulnerability.
- the malware did not just infect jailbroken iPhones, but would then convert the iPhone into a self-propagating worm, to infect other iPhones, an estimated 21,000 victims within about a week.

# Second iPhone Worm --ikee.B/Duh



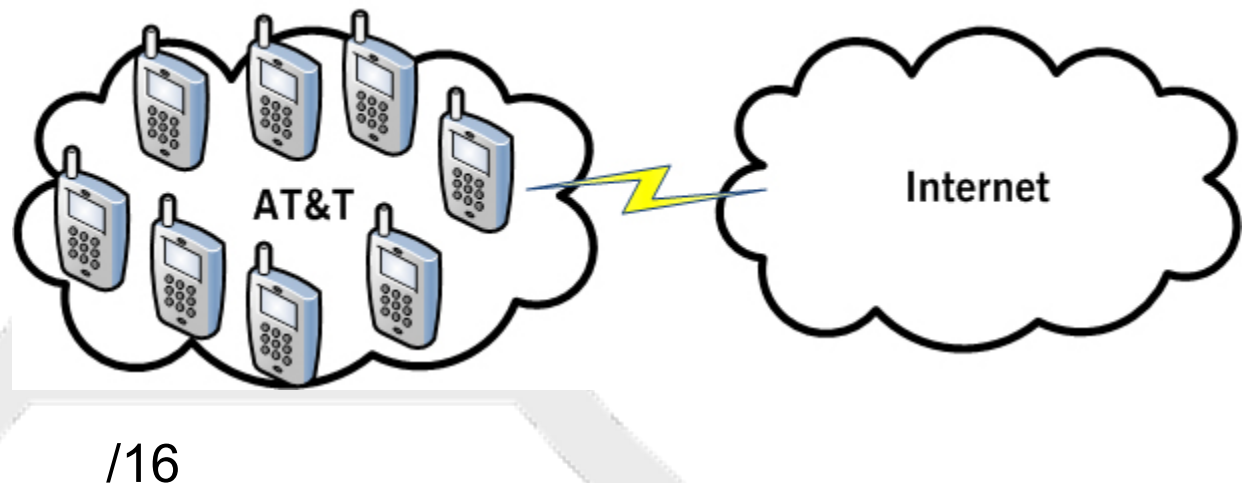
- To target the financial data of customers using **online bank ING Direct**
- The worm redirects ING Direct users to a **phishing site**
- To harvest online banking login details
- More complex than simple phishing and seems to involve an attempt to **snatch SMS messages** associated with online banking transactions

# How Do They Find the Vulnerable Smartphone?

People think the IP looks like this:



Actually, it looks like this:



# How Do They Find the Vulnerable Smartphone?

- Take AT&T as an example. Until Oct. 16, 2009 AT&T didn't filter device to device IP network traffic.
- The smarphone (laptop/blackberry) has been on one giant flat network.
- The default SSH port number is 22
- Attacker can use port scanner software to probe the devices that are running SSH.
- To avoid being scanned:

Change the port number. The best port number should be more than 1024. Because most port scanner software cannot scan the port number more than 1024.

# Protect Your Jailbroken iPhone



- What is clear is that the "Duh" or Ikee-B worm exploits an SSH backdoor on jailbroken handsets in order to spread.
- All iPhones have same default root password 'alpine' and who forget to change after jailbreaking, leaving their phone vulnerable to intrusion and hacking.
- The easiest thing one can do to secure his or her iPhone is to **change default root password** or **by disabling SSH**.

# What's Scariest -- Secretly Tracking Location

- The latest operating system powering the iPhone keeps a log of everywhere you go, recording both **the location** and **time** you were there
- The feature has been around since June 2010.
- You can turn off the GPS function on your iPhone, but it can still figure out its location by looking at nearby cell phone towers and Wi-Fi signals.

-- What can we do if we want to ensure our data is safe?

-- The simplest method is just not to use a fancy phone.

As of now there is no known way to stop an iPhone with OS 4 from logging locations.

# Geotagging

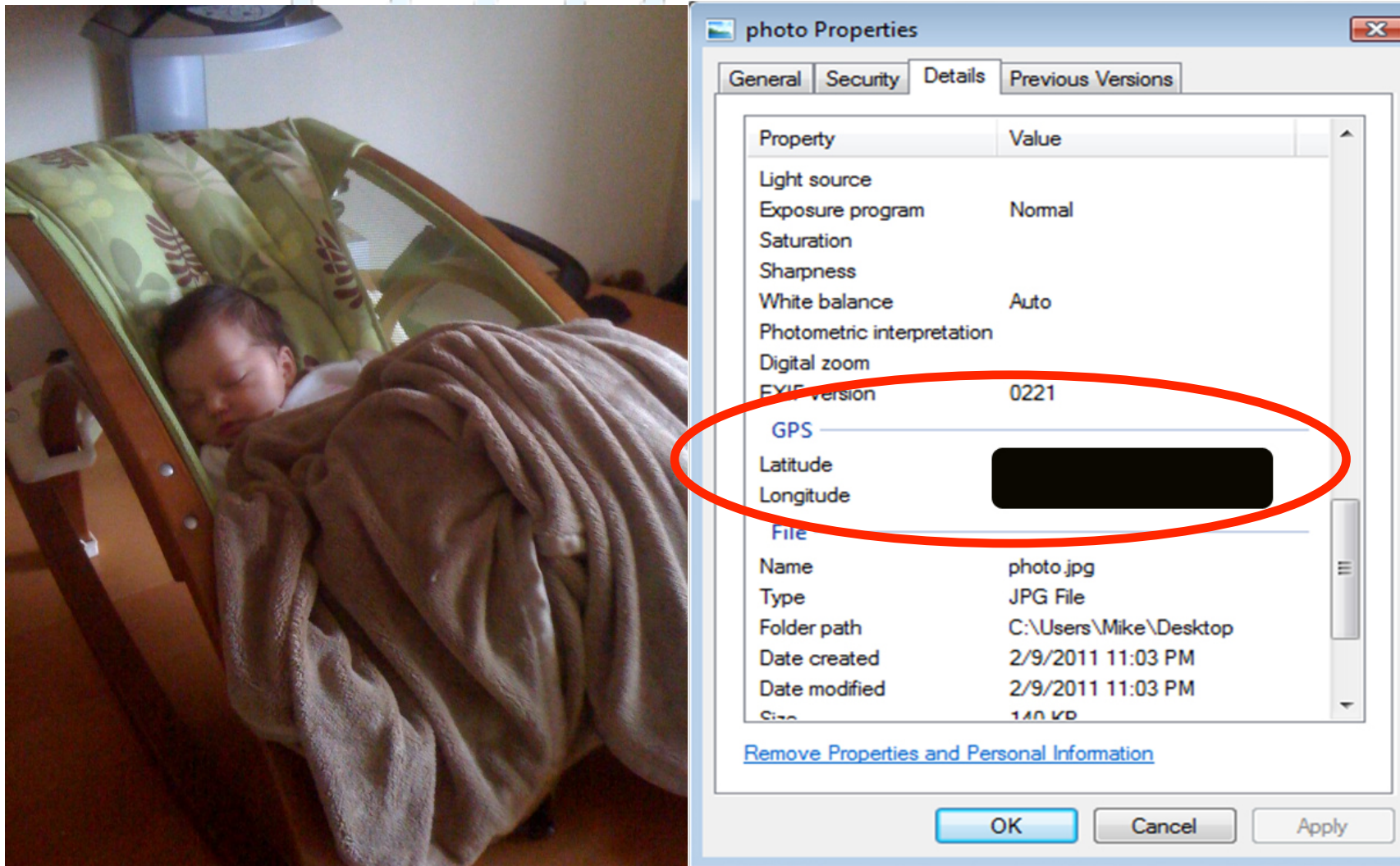
Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a grid coordinate to everything you post on the internet.

- Flickr <http://www.flickr.com/>
- Facebook Places <http://www.facebook.com/places/>
- Picasa <http://picasa.google.com>
- Foursquare <http://foursquare.com/>
- Gowalla <http://gowalla.com/>
- Scvngr <http://www.scvngr.com/>

# Geotagging

This is a picture of my now four month old niece, Madison, taken with my wife's iPhone 3G at Madison's home.

By default, iPhones have the geotagging feature turned on.



# Geotagging – Wired Magazine JAN 2009

“I ran a little experiment. On a sunny Saturday, I spotted a woman in Golden Gate Park taking a photo with a 3G iPhone. Because iPhones embed geodata in/ to photos that users upload to Flickr or Picasa, iPhone shots can be automatically placed on a map. At home I searched the Flickr map, and score—a shot from today. I clicked through to the user’s photostream and determined it was the woman I had seen earlier. After adjusting the settings so that only her shots appeared on the map, I saw a cluster of images in one location. Clicking on them revealed photos of an apartment interior—a bedroom, a kitchen, a filthy living room. Now I know where she lives.”

# Geotagging – Myth Busters

In August of 2010, Adam Savage, of “Myth Busters,” took a photo of his vehicle using his smartphone. He then posted the photo to his Twitter account including the phrase “off to work.” Since the photo was taken by his smartphone, the image contained metadata revealing the exact geographical location the photo was taken. So by simply taking and posting a photo, Savage revealed the exact location of his home, the vehicle he drives and the time he leaves for work.



# Cellular Jamming/ Forcing to 802.11

## Handheld Cell Phone Jammer HPJ01



MORE IMAGES

SHARE

Email a friend

### Specifications

### Product Gallery

### Customer Reviews

### You May Also Like

The hand heldphone jammer HPJ-01 is small and light, it can be easily put inside your pocket or hand bag. It can disable all types of cellular signals including the new 3G band. The isolating radius is up to 10 meters. It comes with rechargeable Li-Ion battery, an AC charge and a car charger.

### SPECIFICATIONS

Cover interface:	Digital-IDEN,TDMA,CDMA,GSM,UMTS, Analog-AMPS,NMT,N-AMPS,TACS
Isolating range:	CDMA 850-894MHz GSM 925-960MHz DCS 1805-1880MHz PHS 1900-1930MHz CDMA1900 1930-1990MHz 3G 2110-2170MHz
Output power:	0.5 watt
Antennas:	External,omnidirectional
Power supply:	Rechargeable Li-ion battery,1100mAh,2-3 hours'work time
Humidity:	5%-80%
Effective range:	Radius 2-10 meters,depending on the strength of the signal
Dimension:	96mm x 45mm x 18mm
Weight:	126g

### Ordering Information

Unit Price: **\$33.00**

Shipping Cost: View shopping cart

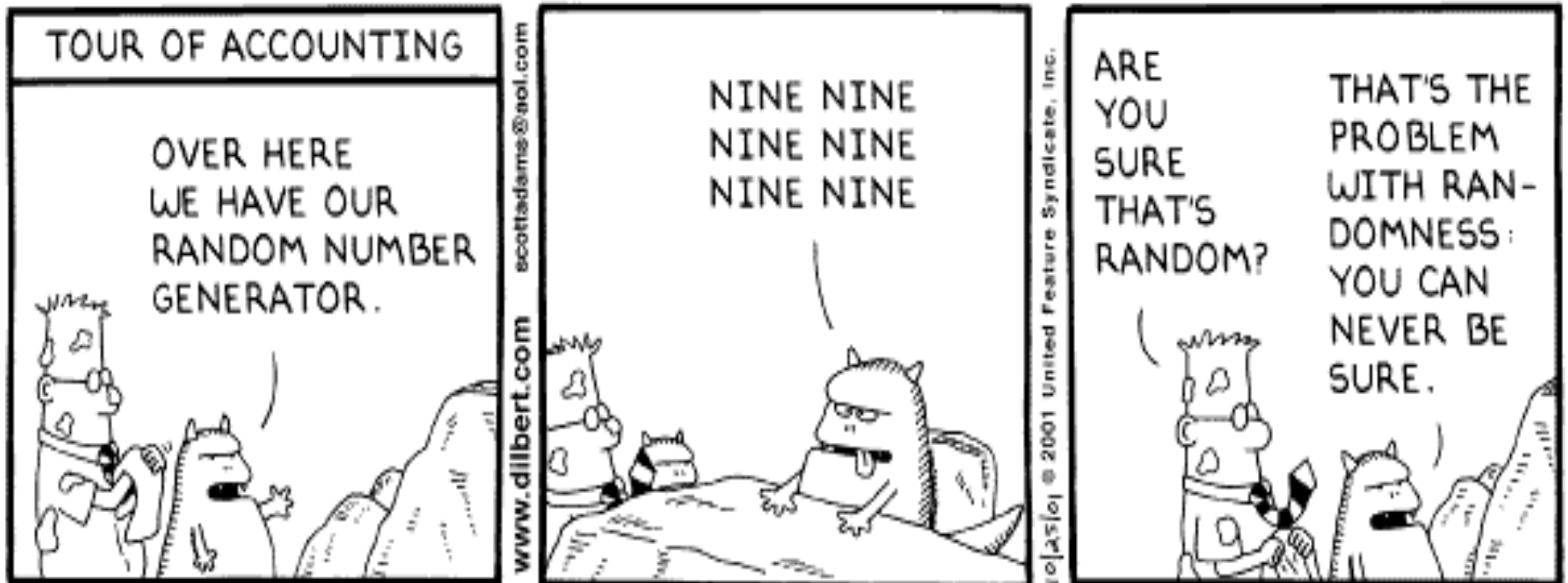
Usually Ships: Within 2 days

Quantity:

BUY NOW

By using inexpensive devices, smartphones can be forced to use 802.11 connectivity, making data vulnerable, just like on any other computer.

# Your Phone Encryption Algorithm?



Copyright © 2001 United Feature Syndicate, Inc.

# Smart Phones and Your Money

- Estimated diffusion in Europe/North America: 2013 (already beginning)
- Estimated financial transaction market: \$75BN
- NFC Tech: 13.56mhz, data rates 106kbit/s, multiple rfid tags
- NFC Tag transmit URI by proximity to the phone that prompt user for action given the protocol:

URI

SMS

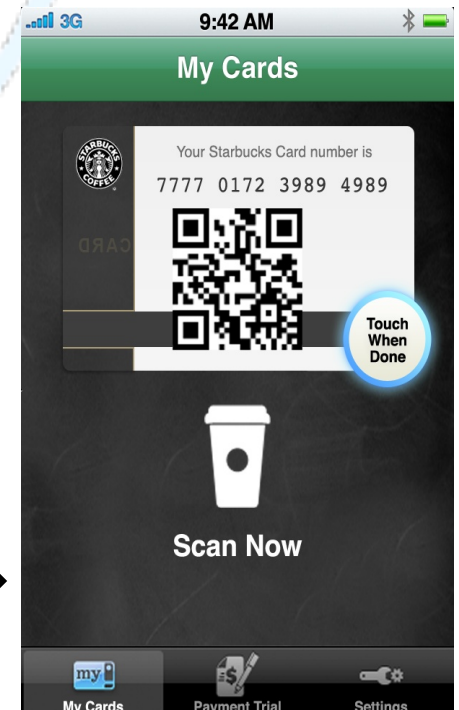
TEL

SMART Poster (ringtone, application, network configuration)



**Whole Foods Checkout In Baltimore**

**Starbucks App For Phone Payment**



# Smart Phones and Your Money

Using an item like this and a netbook computer, would only have to walk near a person to steal their banking info if linked to the RFID.



## Socket Communications CompactFlash RFID Reader Card 6E (RF5400-542)

by [Socket](#)

[Be the first to review this item](#) | [Like](#) (0)

List Price: ~~\$250.00~~

Price: **\$178.99**

You Save: **\$71.01 (28%)**

**In Stock.**

Ships from and sold by [onSale](#).

Only 8 left in stock--order soon.

[5 new](#) from \$177.61   [2 used](#) from \$139.99

### What Do Customers Ultimately Buy After Viewing This Item?



**58%** buy the item featured on this page:

Socket Communications CompactFlash RFID Reader Card 6E (RF5400-542)  
**\$178.99**



**13%** buy

Travelon RFID Blocking Card Sleeve Travelon ★★★★★ (7)  
**\$9.99**



**11%** buy

Travelon RFID Blocking Passport Case Travelon ★★★★★ (15)  
**\$12.18 - \$18.95**



**10%** buy

Travel Smart By Conair RFID Blocking Passport Wallet, Black by Travel Smart by Conair ★★★★★ (8)  
**\$12.99**

[Explore similar items](#)

**\$178.99** + \$3.98 shipping

In Stock. Sold by **onSale**

Quantity:



Add to Cart

or

[Sign in](#) to turn on 1-Click ordering.



Add to Wish List

### More Buying Choices

ANTOnline

[Add to Cart](#)

**\$177.61** + \$6.98 shipping

The Price Pros

[Add to Cart](#)

**\$183.00** + \$6.44 shipping

Beach Audio

[Add to Cart](#)

**\$183.11** + \$8.51 shipping

[7 used & new](#) from **\$139.99**

Have one to sell?

[Sell yours here](#)

[Share](#)



# Social Media/ Web Surfing

- Facebook – Not beating this horse anymore
- Amazon.com – Many smartphones will keep cookies when users sign into accounts and will automatically sign in when site is accessed or not completely sign out/ log off.
- Color ([www.color.com](http://www.color.com)) – New social media model using photo sharing

“Color creates new, dynamic social networks for your iPhone or Android wherever you go. It is meant to be used with other people right next to you who have the Color app on their smartphone. This way, you can take photos and videos together that everyone keeps.”

“Color is a completely open network. This means that **any Color user can see your content. It also means that any photo taken within about 150ft. of other users of the Color app are automatically shared to their devices.** It’s a great way to extend the way you experience your day. If you have a private moment that you don’t want shared with the people around you, please use your device’s native camera app”

- ***It is unclear what vulnerabilities exist with this application and what access could be gained.***

# Who is Targeted and How?

- Corporate Executives – Corporate Espionage
- Government Officials – Espionage, Lobbyist Activities/ Targeting, Potential for Blackmail
- Everyday People – Financial Theft, Identity Theft
- Business Cards with cell phone numbers
- Professional social networks (Linkedin, ISC2, etc)
- OpenBTS
  - Ralf-Philipp Weinmann used a laptop and OpenBTS to create a rouge basestation
  - Negotiated all phones to use A5/0 encrytion (plain text only)
  - Total cost for project: less than \$2000.<sup>00</sup>

# Not Only iPhone – Android

- Android is a mobile operating system based on Linux. Google and other members of the Open Alliance collaborated on Android's development and release.
- Android phone **collected its location** every few seconds and transmitted the data to Google at least several times an hour.
- Google let virtually **anyone complete control** over when and how they make their applications available
  - help the OS gain traction against Apple
  - malware hijacked tens of thousands of Android phones
- The openness of the platform and the availability of alternative application markets makes Android-based devices more difficult to secure

# JAN 2010 Detected Vulnerabilities



BlackBerry.  
BlackBerry.  
BlackBerry.  
BlackBerry.  
BlackBerry.

symbian OS  
symbian OS  
symbian OS  
symbian OS  
symbian OS

Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile  
Windows Mobile



# REFERENCES

1. <http://www.puremobile.com/communityblog/cell-phones/10-things-you-probably-didnt-know-about-cell-phones/>
2. <http://www.cellular-news.com/story/47808.php>
3. <http://www.wired.com/gadgetlab/2011/01/android-os-leading-smartphone/>
4. <http://www.wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/>
5. <http://eprint.iacr.org/2010/013.pdf>
6. <http://cryptome.org/jya/a5-hack.htm>
7. <http://www.nytimes.com/2009/12/29/technology/29hack.html>
8. [http://blog.washingtonpost.com/securityfix/2008/02/research\\_may\\_spell\\_end\\_of\\_mobi.html](http://blog.washingtonpost.com/securityfix/2008/02/research_may_spell_end_of_mobi.html)
9. [http://threatpost.com/en\\_us/blogs/second-gsm-cipher-falls-011110](http://threatpost.com/en_us/blogs/second-gsm-cipher-falls-011110)
10. <http://eprint.iacr.org/2010/013.pdf>
11. <http://www.bbc.co.uk/news/technology-12094227>
12. <http://www.bbc.co.uk/news/technology-13013577>
13. <http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf>
14. [http://www.mulliner.org/collin/academic/publications/counteringsmsattacks\\_golde\\_mulliner.pdf](http://www.mulliner.org/collin/academic/publications/counteringsmsattacks_golde_mulliner.pdf)
15. <http://www.securitynewsdaily.com/new-hack-turns-cell-phones-into-spying-devices-0442/>
16. <http://www.sectechno.com/2011/01/20/baseband-apocalypse-new-way-for-hacking-smartphones/>

# REFERENCES

18. <http://www.npr.org/2011/04/21/135610178/your-iphone-may-be-logging-your-physical-positions>
19. <http://petewarden.github.com/iPhoneTracker/>
20. <http://www.foxnews.com/scitech/2011/04/21/apple-google-receive-phone-users-locations/>
21. <http://www.foxnews.com/scitech/2011/04/20/apple-iphone-users-beware-location-tracking/>
22. *Mobile Security* Presentation by Fabio Pietrosant
23. *Wifi Security -or-Descending Into Depression and Drink* Presentation by Mike Kershaw
24. *Geotags and Location-Based Social Networking* by US Army
25. <http://nyti.ms/917hRh>
26. *The New World of Smartphone Security* Presentation by Trevor Hawthorn