

The Current State of Mobile Security



Ministério da
Educação

Ministério da
Ciência e Tecnologia



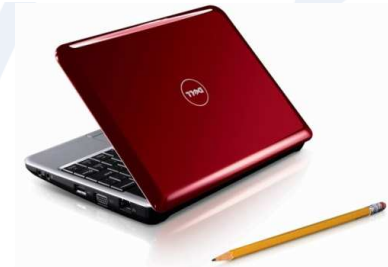
Ronaldo Vasconcellos, Security Analyst
Brazilian Academic and Research Network CSIRT – CAIS/RNP

- **Agenda**

- Introduction
 - Smartphone definition, main players, popularity
- A look at the recent security conferences
- Smartphone security
- Future scenarios and conclusion

- **Introduction**

- Smart phone
 - mobile phone with advanced capabilities, no industry standard
 - standardized interface / platform for application developers
 - complete operating system
- In short: a really mobile computer with phone capability
 - Netbooks: small, but you need to carry an AC/DC adapter and it doesn't fit your pocket



- **Introduction (2)**

- The main players: Hardware
 - Apple iPhone
 - iPhone OS (Darwin based, as Mac OS X)
 - iPod Touch: Same OS, Unix in the end
 - RIM BlackBerry
 - Nokia
 - Symbian
 - HTC
 - MS Windows Mobile, Google Android

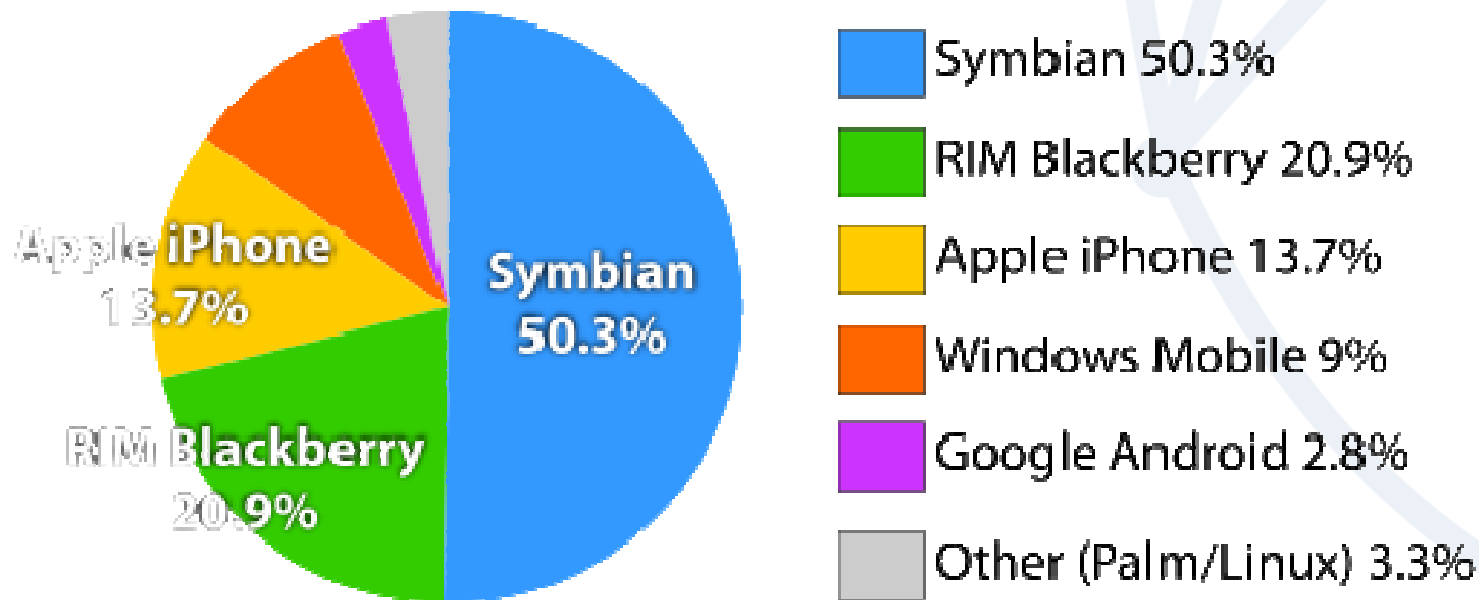
- Introduction (3)



- **Introduction (4)**

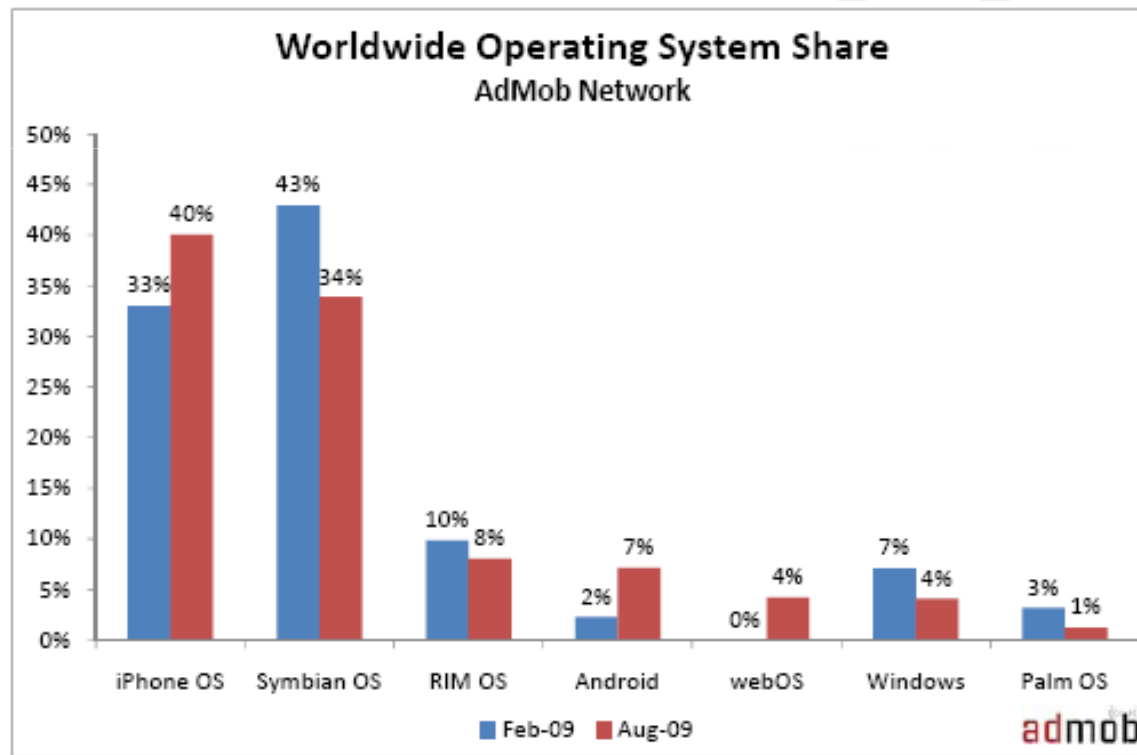
- The main players: Operating System
- Q2 2009 Marketshare data from Canalys
<http://www.canalys.com/pr/2009/r2009081.htm>

Global Smartphone Sales, Q2 2009



- **Introduction (5)**

- August 2009 Mobile Metrics Report
<http://metrics.admob.com/>



- **Introduction (6)**

- Opera State of the Mobile Web Report (March 2009)
<http://www.opera.com/media/smw/2009/pdf/smw032009.pdf>
- Chile jumped from #9 to #1 over the past year!
 - Chilean mobile web use increased by **3200%**
- Top Sites: 1)facebook.com 2)google.com 3)live.com
4)msn.com 5)fotolog.com 6)hotmail.com 7)youtube.com
8)wikipedia.org 9)ebuddy.com 10)my.opera.com



- **A look at the recent security conferences**

- Mobile security research in the past 2 years in the mainstream security conferences
- DEFCON (USA), Black Hat (USA, Europe, Japan), CCC (DE), ShmooCon (USA), YSTS (BR), HITB (May), CanSecWest (CAN), EuSecWest (NL), GTS (BR), Ekoparty (AR), DeepSec

- **A look at the recent security conferences (2)**

- 2008

- DEFCON 16 - Taking Back your Cellphone

Alexander Lash

- BH DC / BH Europe – Intercepting Mobile

Phone/GSM Traffic

David Hulton, Steve

- BH Europe - Mobile Phone Spying Tools

Jarno Niemelä

- BH USA - Mobile Phone Messaging Anti-Forensics

Zane Lackey, Luis Miras

- **A look at the recent security conferences (3)**

- 2008 (2)

- Ekoparty - Smartphones (in)security
Nicolas Economou, Alfredo Ortega

- BH Japan - Exploiting Symbian OS in mobile devices
Collin Mulliner

- GTS-12 - iPhone and iPod Touch Forensics
Ivo Peixinho



GTS Grupo de Trabalho em Segurança

- **A look at the recent security conferences (4)**

- 2008 (3)

- 25C3

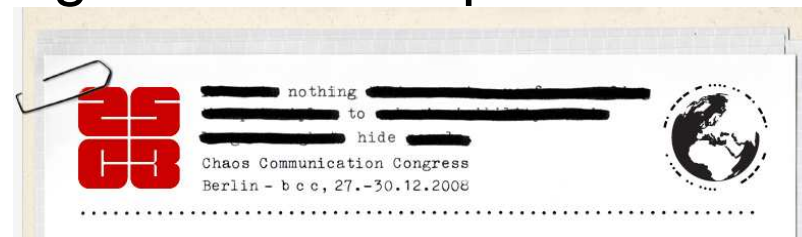
- Hacking the iPhone - MuscleNerd, pytey, planetbeing

- Locating Mobile Phones using SS7 – Tobias Engel

- Anatomy of smartphone hardware – Harald Welte

- Running your own GSM network – H. Welte, Dieter Spaar

- Attacking NFC mobile phones – Collin Mulliner



- **A look at the recent security conferences (5)**

- 2009

- ShmooCon

- Building an All-Channel Bluetooth Monitor
Michael Ossmann and Dominic Spill

- Pulling a John Connor: Defeating Android
Charlie Miller



- **A look at the recent security conferences (6)**

- 2009 (2)

- BH USA



- Attacking SMS - Zane Lackey, Luis Miras

- Premiere at YSTS 3.0 (BR)

- Fuzzing the Phone in your Phone - Charlie Miller, Collin Mulliner

- Is Your Phone Pwned? - Kevin Mahaffey, Anthony Lineberry & John Hering

- Post Exploitation Bliss - Loading Meterpreter on a Factory iPhone - Vincenzo Iozzo & Charlie Miller

- Exploratory Android Surgery - Jesse Burns

- **A look at the recent security conferences (7)**

- 2009 (3)

- DEFCON 17

- Jailbreaking and the Law of Reversing - Fred Von Lohmann, Jennifer Granick

- Hacking WITH the iPod Touch - Thomas Wilhelm

- Attacking SMS. It's No Longer Your BFF - Brandon Dixon

- Bluetooth, Smells Like Chicken - Dominic Spill, Michael Ossmann, Mark Steward

DEFCON®

- **A look at the recent security conferences (8)**
 - 2009 (4)
 - BH Europe
 - Fun and Games with Mac OS X and iPhone Payloads - Charlie Miller and Vincenzo Iozzo
 - Hijacking Mobile Data Connections - Roberto Gassirà and Roberto Piccirillo
 - Passports Reloaded Goes Mobile - Jeroen van Beek



- **A look at the recent security conferences (9)**

- 2009 (5)

- CanSecWest

- The Smart-Phones Nightmare
Sergio 'shadown' Alvarez

- A Look at a Modern Mobile Security Model:
Google's Android
Jon Oberheide

- Multiplatform iPhone/Android Shellcode, and other
smart phone insecurities
Alfredo Ortega and Nico Economou



- **A look at the recent security conferences (10)**

- 2009 (6)

- EuSecWest - Pwning your grandmother's iPhone

Charlie Miller

- HITB Malaysia - Bugs and Kisses: Spying on Blackberry Users for Fun

Sheran Gunasekera

- YSTS 3.0 / HITB Malaysia- Hacking from the Restroom

Bruno Gonçalves de Oliveira

- PacSec: The Android Security Story: Challenges and Solutions for Secure Open Systems

Rich Cannings & Alex Stamos

- **A look at the recent security conferences (11)**

- 2009 (7)

- DeepSec

- Security on the GSM Air Interface
David Burgess, Harald Welte

- Cracking GSM Encryption
Karsten Nohl

- Hijacking Mobile Data Connections 2.0:
Automated and Improved
Roberto Piccirillo, Roberto Gassirà

- A practical DOS attack to the GSM network
Dieter Spaar

- **Smartphone security**

- Rogue GSM Network
 - That's right, I didn't mean Rogue Wi-Fi AP (also a threat)
- Hacking at Random 2009 (HAR2009)
 - The Netherlands
- GSM network available in the conference
 - test license from the dutch regulatory authority
 - OpenBSC
 - <http://openbsc.gnumonks.org/trac/>
 - <https://wiki.har2009.org/page/Network#GSM>



- **Smartphone security (2)**

- Security at the link layer
- “Don’t use Wi-Fi, use GSM instead. It’s safer.”
 - May be a misconception in the near future
- GSM encryption is under cracking
- AirProbe - GSM-Sniffer project. The goal is to build an air-interface analysis tool for the GSM (and possible later 3G) mobile phone standard.
<https://svn.berlin.ccc.de/projects/airprobe/>

- **Smartphone security (3)**

- Client side security
 - Sun Java ME (former J2ME)
Some vulns may be cross-platform
 - Adobe Flash Player
- Flash available in smartphones soon
 - mobile-ready Flash 10.1 for Windows Mobile and Palm Pre late 2009
 - Android, Symbian and BlackBerry phones early 2010
 - No iPhone (“closed device”)
 - Good and **Bad** news at the same time: frequent Adobe Flash vulnerabilities




- **Smartphone security (4)**

- Gigs and gigs of data
- Backup
- Sensitive data
 - Private photos, open sessions / saved password (Google Gmail client, Fring, Gravity Twitter client, etc.)
 - Encryption needed!
- Forensics is not as simple as downloading SMS messages, logs and photos
 - **SANS Mobile Device Forensics (SECURITY 563)**
<http://www.sans.org/security-training/mobile-device-forensics-1297-mid>



- **Smartphone security (5)**

- Mobile security suites are not for paranoids
 - Antitheft
 - Probably one of the most personal and exposed of your devices
 - Recover using GPS – good luck! 
 - Block, find, wipe, watch where your SIM is remotely via SMS
 - Encryption
 - Antispyware
 - Firewall

- **Smartphone security (6)**

- Mobile malware: Sexy Space / Sexy View worm (2009)
 - Symbian SIS package sent via SMS
 - Prompt: “Install Sexy Space? Yes or No”
 - Symbian Express Signing ☺
- iPhone users looking for SMS vulnerability in Google
 - Search Engine Optimization
 - iPhone Blackhat SEO Poisoning Leads to Total Security Rogue Antivirus

<http://securitylabs.websense.com/content/Blogs/3483.aspx>

- **Smartphone security (7)**

- Mobile anti-virus is not as useless as you may think
 - F-Secure Mobile Security
<http://mobile.f-secure.com/>
 - Kaspersky Mobile Security
http://www.kaspersky.com/kaspersky_mobile_security



- **Smartphone security (8)**

- Vulnerabilities
 - Popular discovery method: Fuzzing
 - Today you **must** update the firmware of everything you own
 - performance, bugs, denial of service (DoS), security vulnerabilities
 - DoS = offline
 - #2009-014 Android denial-of-service issues
<http://www.ocert.org/advisories/ocert-2009-014.html>
 - About the Java Vulnerability on S40 Phones
<http://www.f-secure.com/weblog/archives/00001483.html>

- **Smartphone security (9)**

- Vulnerabilities (2)

- SMS vulnerability

- Black Hat USA 2009, Charlie Miller and Collin Mulliner

- iPhone “owned” after a series of specially crafted SMS messages

- Apple quickly released iPhone OS 3.0.1 (July 31)
<http://support.apple.com/kb/HT3754>



- **Smartphone security (10)**

- Wi-Fi & Bluetooth
 - The same old vulnerabilities
 - 802.11 Denial of Service (DoS), sniffing, Man in the Middle (MITM)
 - A smartphone in a hotspot is even more unsafe
 - Browsers are tiny
 - Worm spreading itself via BT + MMS
 - Worm:SymbOS/Commwarrior A-Q (2005-?)
<http://www.f-secure.com/v-descs/commwarrior.shtml>



- **Smartphone security (11)**

- Jailbreaking is common practice
 - Mobile companies lock devices
 - Car GPS, Videogames, etc. – people are hackers customers for a long time
 - People don't pay attention to URLs
 - Backdoors may be installed
 - Camera, Mic, GPS, Compass, Wi-Fi
 - Well known: DEV-TEAM BLOG
<http://blog.iphone-dev.org/>
- Backdoors already on the market
 - iSpy an iPhone Spy
<http://www.f-secure.com/weblog/archives/00001565.html>

- **Smartphone security (12)**

iPhone Devices

Mobile Spy is the world's first spy software for the iPhone. For anyone who wants to monitor the text message and call activity of their Apple phone in stealth, this software is the only method available. Mobile Spy is the world's first and only spy software!

The iPhone version works for second generation iPhones only. It is not compatible with the first generation. If your iPhone is a 3G 2.x phone then it is compatible. You do not need 3G access to use Mobile Spy. However your phone needs to be the 3G model.

Apple iPhones



3G 8GB



3G 16GB

Additional Requirements

Note that your phone should be jailbroken to enable the software's functionality. We provide the easy and reversible instructions to do this at no cost upon ordering. The phone must have the Internet enabled so the Mobile Spy software can upload logs to your account.

- **Smartphone security (13)**

- ≡ Read SMS, Call Logs and Email and GPS locations
- ≡ Simple to install
- ≡ iPhone versions 2 and 3 supported
- ≡ AVAILABLE 21st December 2008

FlexiSPY iPhone spyphone - Secretly captures events and sends to your secure web account

SMS Messages call history & other phone data are uploaded directly from the mobile phone to the FlexiSPY server.

All data received by FlexiSPY can be accessed 24 hours a day, 7 days a week via any computer connected to the internet.



Remotly read SMS, Call Logs, Emails and GPS on the iPhone.

FlexiSPY LIGHT is a premium iPhone spyphone product, and lets you secretly read iPhone SMS, Email, Call Records and GPS locations inside a secure web account. You can then carry out powerful searches and view locations on a map.

- **Smartphone security (14)**

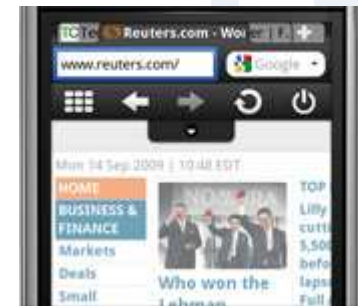
- Privacy
- GPS and compass is cool
 - Augmented reality
- Cool for malware and malicious purposes, too.
 - Reports where you are
 - At least 3 ways to “call home”
 - SMS/MMS, Wi-Fi, GPRS
 - How Much Latitude?

<http://www.f-secure.com/weblog/archives/00001599.html>



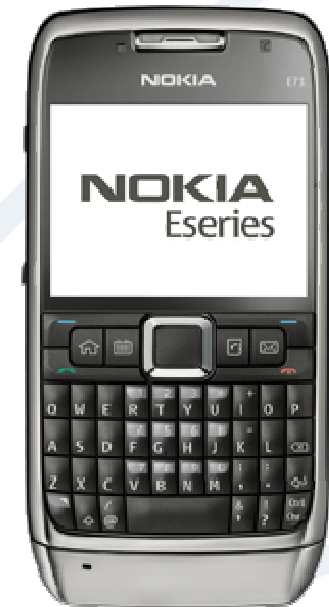
- **Smartphone security (15)**

- Browsers are becoming more capable
 - Web 2.0
- Still limited security features
 - More security features in desktop browsers
- Mobile browsers vulnerabilities
 - Identifiable by User-Agent HTTP header field
- Opera is paying attention to mobile web
 - Opera Mini 5 beta
<http://www.opera.com/mini/next/>



- **Smartphone security (16)**

- Not all mobile applications offer SSL encryption
 - Unsafe for Wi-Fi hotspots, WEP
- Mobile are more vulnerable to Wi-Fi Rogues
- Try to sniff / capture the traffic
- Typical toolkit in a Symbian
 - Gravity (best Twitter client), Gmail client, Google Maps, fring (passwords!), Qik (privacy!), JoikuSpot / JoikuBoost (3g → Wi-Fi), Orkut (BR), Opera Mini beta 5, Btbrowser, Bloover, Barbelo
- Check Bruno Gonçalves presentation HITB
<http://conference.hackinthebox.org/hitbsecconf2009kl/materials/>



- **Future scenarios and conclusions**

- IPv6 and every mobile device routable on the Internet
 - bots online 24x7x365 using GSM/3G (as Apple Store NYC!)
- Smartphones tend to be even more powerful, Netbooks are getting bigger
 - Remember: mobile phones are really portable



• Future scenarios and conclusions (2)

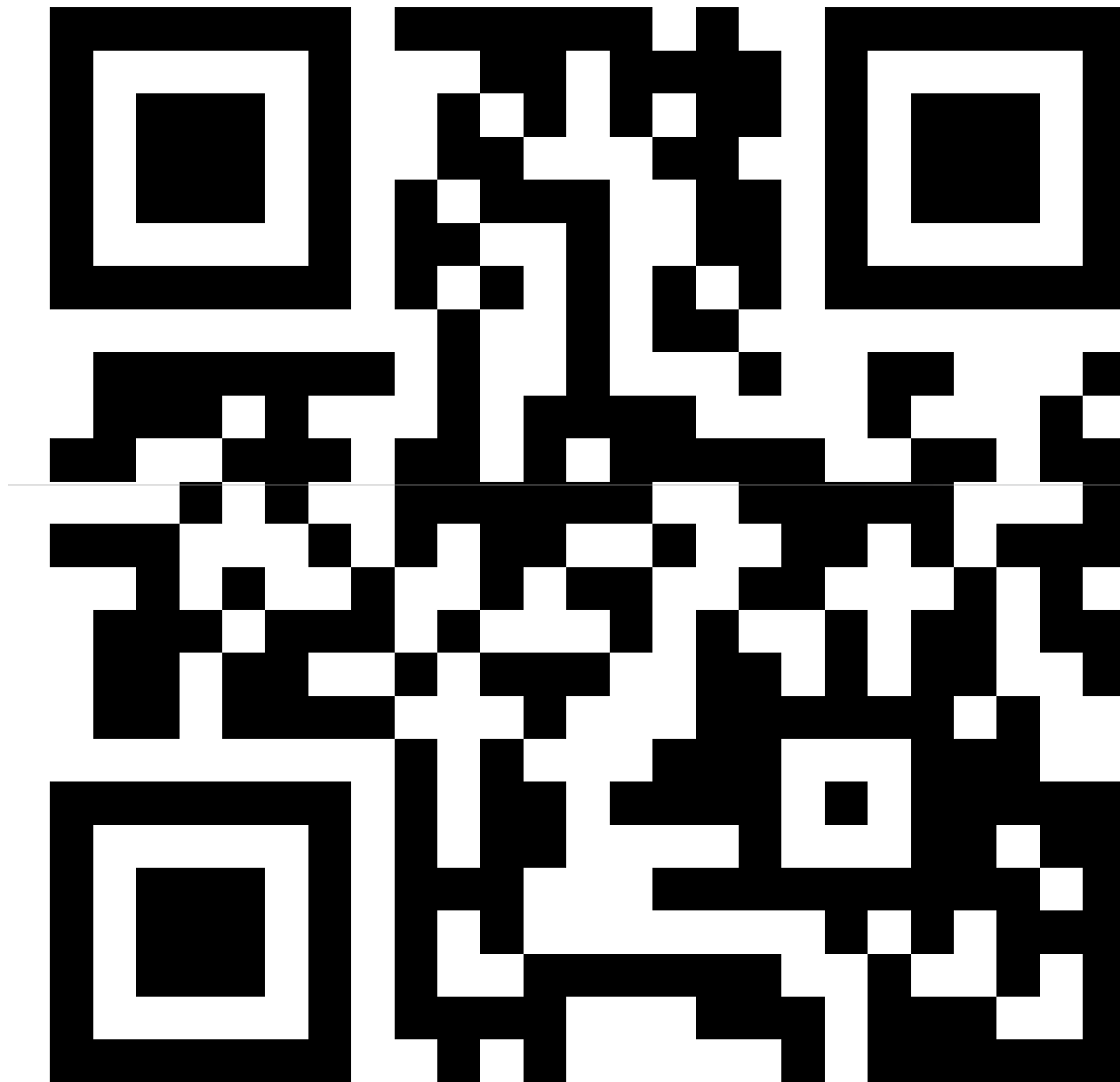
- Spam over SMS (and malware)
 - Anti-spam for mobile not as useless as you may think
 - Spam fraud
 - What's w03.v762.net?
<http://www.f-secure.com/weblog/archives/00001793.html>
 - Update on Finnish SMS Spam case
<http://www.f-secure.com/weblog/archives/00001785.html>
 - Many companies in Brazil send SMS without permission
- Cell phone for payment and banking
 - Vulnerable applications
 - Backdoor is even more dangerous

- **Future scenarios and conclusions (3)**

- iPhone and Google Android, the most “hackable” platforms today, tend to be the leaders
 - Mono cultures and complexity are bad to security
 - October 2009: Gartner forecast puts Android ahead of iPhone, BlackBerry, Windows Mobile by 2012
 - 50+ Android Phones expected in near future
 - <http://wiseandroid.com/NewsItem.aspx?itemid=14>
 - Social media is becoming even more popular
 - Twitter, Facebook, FriendFeed
 - Vulnerabilities in mobile clients
 - Malware propagation via social media



The Current State of Mobile Security



- **Future scenarios and conclusions (4)**

- Try <http://j.mp/iDo9E> or <http://j.mp/info/iDo9E>
- The BIG problem of URL size, even bigger in mobile phones
- QR Code (Quick Response)
 - Matrix code / 2-D barcode
 - Created by DENSO Co. (JP) in 1994
 - More popular in Nokia and Japan
- URL shorteners
 - bit.ly / j.mp, TinyURL, is.gd, others
 - around since around 2002 (TinyURL)
- QR Code would be great for mobile malware
 - “Win a Wii / iPhone / other desired gadget”



- **Useful References**

- Independent Security Evaluators - Exploiting the iPhone
<http://securityevaluators.com/content/case-studies/iphone/>
- Independent Security Evaluators - Exploiting Android
<http://securityevaluators.com/content/case-studies/android/>
- Independent Security Evaluators – Publications
<http://securityevaluators.com/content/publications/>

- **Useful References (2)**

- SMS (short message service) Security Research Page
<http://www.mulliner.org/security/sms/>
- iPhone Security Research
<http://www.mulliner.org/iphone/>
- Collin Mulliner Blog (Mobile Security News)
<http://www.mulliner.org/blog/>
- NIST Guidelines on Cell Phone and PDA Security (SP800-124)
<http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>

Thank you!

Brazilian Academic and Research Network CSIRT –
CAIS/RNP

<http://www.rnp.br/en/cais/>

 @cais_rnp

Ronaldo Castro de Vasconcellos
ronaldo at cais.rnp.br



Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil
<http://www.rnp.br>

Ministério da
Educação

Ministério da
Ciência e Tecnologia



Incident Reporting

Report security incidents on RNP backbone:

1. E-mail: cais@cais.rnp.br

Please use CAIS PGP public key if you need to send sensitive data:
<http://www.rnp.br/cais/cais-pgp.key>

2. Incident Reporting - Web:
http://www.rnp.br/cais/atendimento_form.html

Hotline INOC-DBA (Inter-NOC Dial-By-ASN): 1916*800

CAIS Advisory (CAIS Alerta): To subscribe CAIS Alerta, a service offered to the brazilian security community since 1998, please use the form below. Advisories in brazilian portuguese.

<http://www.rnp.br/cais/alertas/>



Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil
<http://www.rnp.br>

Ministério da
Educação

Ministério da
Ciência e Tecnologia

