HACKING THE BIG BROTHER

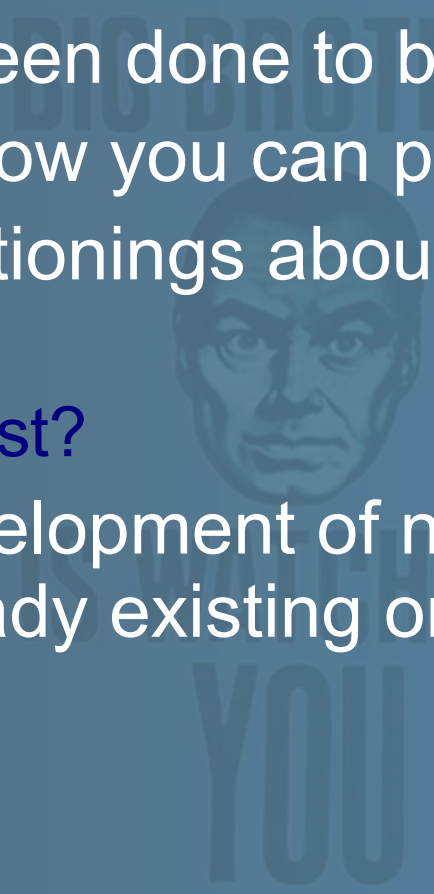
When intelligence defeats the iron fist

João Batista C. G. Moreira
joao@livewire.com.br

Júlio César Fort
julio@rfdslabs.com.br

Main Goals

- What is this lecture about?
  - Show what has been done to break your privacy...
  - ...but also show how you can protect yourself
  - Raise some questionings about anonymity and privacy in digital era
    - Who can you trust?
  - Stimulate the development of new techniques and tools and improve already existing ones

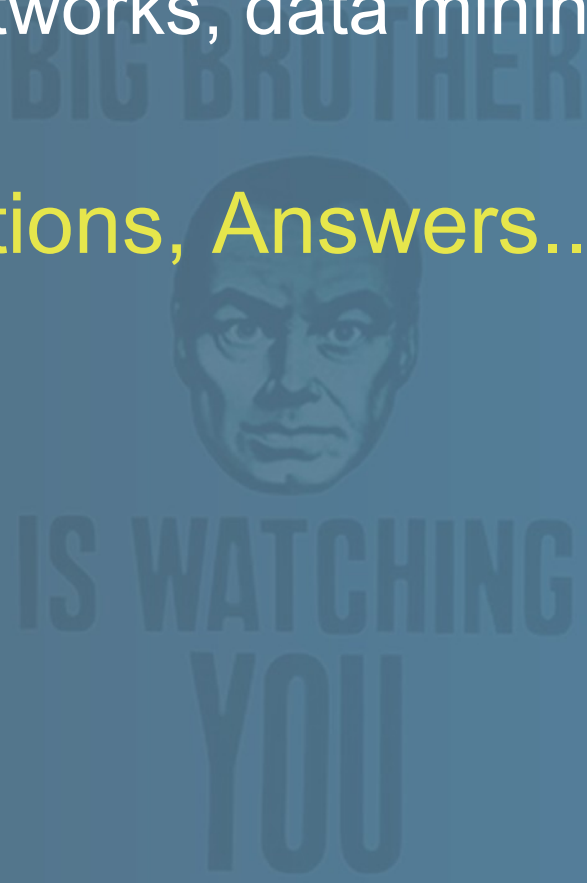


Breakpoints

- The Network Eye
  - Eavesdropping, traffic analysis and shapping, Narus
  - SSL, public-key cryptography, Tor, privacy boxes
  - Telephony
    - Wiretapping, satellites
    - Voice cryptography, secure phones
- Defective by Design?!
  - DRM, trusted computing
  - Reverse engineering, hardware hacking
- Personal Tracking
  - RFID and its hacks, BSN, WSN

Breakpoints

- Personal Information
  - Google, social networks, data mining, direct marketing.
- Recent News...
- Discussion, Questions, Answers...



The Network Eye

The Network Eye

- Internet communication is unsafe
  - Unknown gateways
  - Corporate gateways
  - Unsafe gateways
- Gateways are not neutral
  - Store communication data
  - Store network requests
  - Allow analysis of the stored data
  - May change its behavior
  - May stop some kinds of connections, allow others
  - May capture data like passwords, logs, etc...

The Network Eye

- Eavesdropping
  - Snooping on someone else's conversation
    - Landline and mobile phone, e-mail, instant messaging...
  - Used in corporations, universities, internet cafes, home networks, government agencies... and everywhere else where there is communication
  - ECHELON (and its counterparts)
    - International eavesdropping system evolving USA, UK, Canada, Australia, New Zealand (AUSCANZUKUS)
    - Many interception stations in ground and orbit
    - Rumors about data being captured for commercial endings

The Network Eye

- Telephony
  - Wiretapping in landline telephones are very well known
  - Mobile telephony (GSM) can also be tapped
    - Attacks are more sophisticated, yet possible
    - Carriers (and attackers) can spy on your conversations, SMS and stuff alike
  - Eavesdropping on VoIP is also possible
    - Many available freeware and open source tools can do the task

The Network Eye

- Traffic Analysis
  - Intercept communication and deduce information from patterns
  - Can be performed on encrypted systems
  - In computer networks
    - Focus on packet headers (they are not encrypted)
    - Are usually used against anonymity systems – aims to compromise its security properties
      - Tor, re-mailer servers
    - Can be used to decrease time of brute forces
  - In telephone networks
    - Narus, AT&T's Hancock and others are also crafted to provide CDRs with accuracy

The Network Eye

- Traffic Shapping
  - Network favors or harms some kinds of traffic
  - Can interfere on some services communication
  - Reduced or no bandwidth at all for some kinds of traffic
  - Main affected services: VoIP, P2P
  - Reasons?
    - VoIP threatens conventional telephony
    - ISPs sell more bandwidth than what they can support
    - P2P keeps bandwidth completely full
  - Used by many ISPs in Brazil and throughout the world, even though they do not admit publicly

The Network All-Seeing Eye

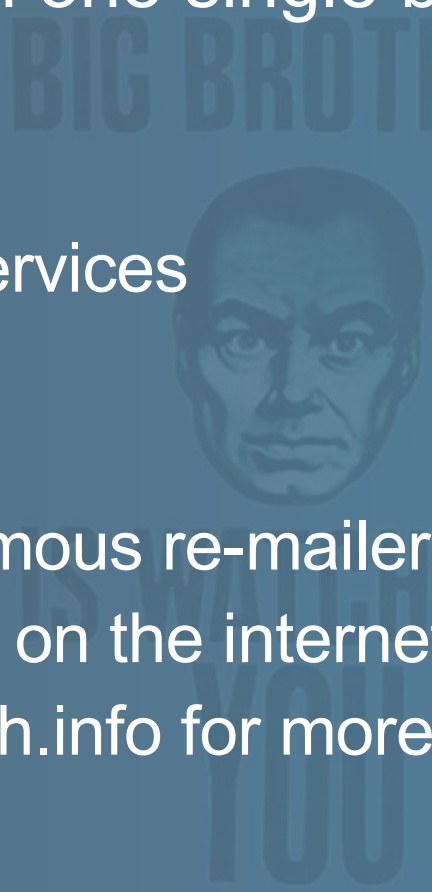
- Narus
  - Private company founded in 1997
    - Currently has a former big shot NSA spook as chairman
  - Created NarusInsight, a massive surveillance system
    - Among its clients in Brazil are our beloved carriers BrasilTelecom and Oi
  - Focus on network and application layer traffic
  - Collects data from different sources
    - Perfectly suited for high speed networks
  - Analyzes and correlates captured data to provide detailed information about the network users, applications, protocols...

Hacking the Network Eye

- Cryptography
  - Hiding traffic from the watchers
  - Use of secure protocols, like TLS, SSL
  - Use of tools, like PGP
- Onion Routing
  - Using P2P networks to route the network traffic
  - Provides anonymous navigation
  - Most popular countermeasure against traffic analysis
  - Recently hacked by ha.ckers.org guys
  - P2P nodes used to route the traffic are not neutral
  - How to improve Tor?

Hacking the Network Eye

- Privacy Boxes
  - Closed boxes with one single button
  - What it provides:
    - Firewall
    - Local network services
    - Web server
    - Mail server
    - Supports anonymous re-mailers and privacy services
    - Different models on the internet
    - See winstonsmith.info for more information



Hacking the Network Eye

- ECHELON
  - Artificial intelligence system and data miner
  - Based on pattern analysis to define...
  - Echelon spoofer use known Echelon patterns to generate fake matching messages
    - See echelonspoofer.com for more information
  - Attach the generated words to all your unimportant messages and help flooding the Echelon system
  - Eg.:
    - Preheat the oven to 350 degrees BOMB In a large bowl, mix the flour WHITE HOUSE 3/4 cup sugar, 1/4 cup cocoa PRESIDENT Stir in the milk, oil, and vanilla RED CELL Spread in the prepared pie plate VIRUS

Hacking the Network Eye

- Secure telephony
  - Voice mixing, scrambling and encryption exist but are not popular
    - Secure telephones are very expensive and mostly require ISDN lines
  - There are many commercial solutions for encrypting voice and text on smartphones
  - You can try to avoid traces with caller ID spoofing
    - Can be done fairly easy with VoIP
    - Harder to perform on POTS yet possible with orange box

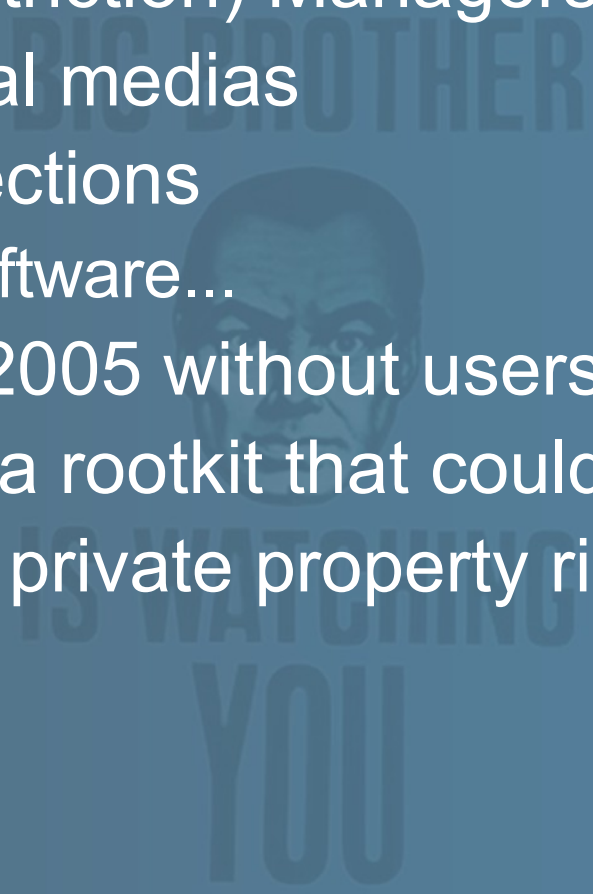
Defective by Design?!

Defective by Design?!

- Trusted Computing
  - Computers will behave in well-known ways
  - Behavior enforced by hardware and software
  - “Computers will be much safer against viruses”
  - Also a hardcore DRM system
  - Users will not chose who they trust, or how to work
  - Complete absence of anonymity
  - Trusted Platform Module
  - Needs authentication provided by TPM to execute code
  - Switching software will become less simple
  - Security or freedom? Never both, maybe none...

Defective by Design?!

- DRM
  - Digital Rights (restriction) Managers
  - Used to limit digital medias
  - Lots of copy protections
    - Movies, CDs, software...
  - Used by Sony in 2005 without users knowledge
  - Sony's DRM was a rootkit that could be exploited
  - DRMs breaks the private property rights



Fixing It!

- Reverse Engineering
  - Process of discovering internal details of a system through a top-bottom point of view
  - Understand how systems work is the main task before hacking it
  - Might be useful to understand DRMs and TC modules
  - Blackest box ever...
- Hardware Hacking
  - Changing default hardware to work as you wish
  - Used to hack hardware DRMs (like iPhone's)
  - A way to hack the Trusted Platform Module?

Personal Tracking

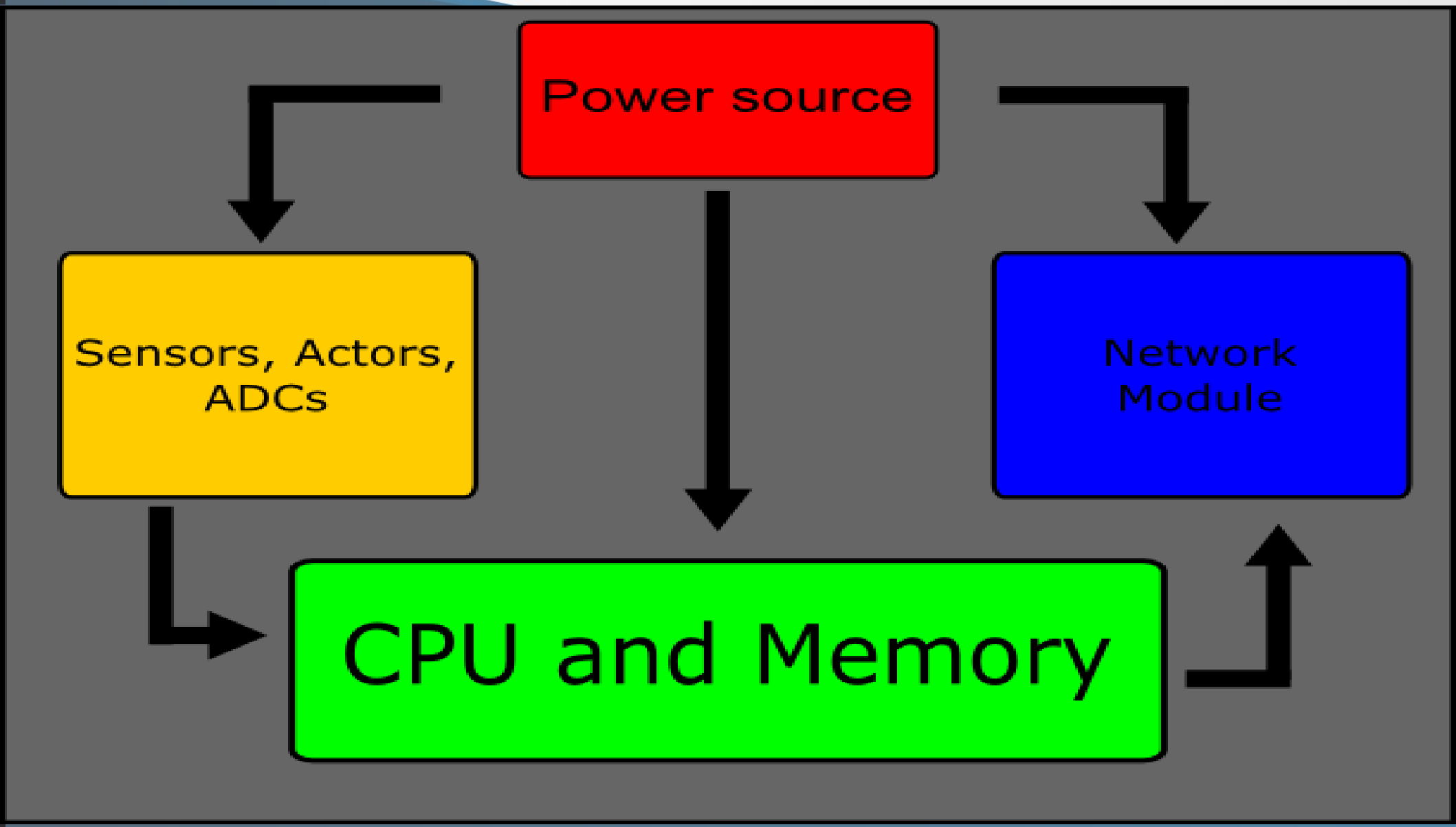
Personal Tracking

- RFIDs
  - RFID architecture consists of a reader and tags
  - Reader queries tags, receive information and act
  - All data transmitted through radio waves
  - Access cards, credit cards, passports, AVI, pets...
  - Could be used to track and identify people
    - THE MARK OF THE BEAST?! Ph33r!
  - Enables full-time tag tracking

Personal Tracking

- Wireless Sensor Networks
  - WSN Arch consists of sensor nodes and main node
  - Sensor nodes have processing capabilities
  - Commercial, industrial, scientific, military applications
  - New tech, lots of bugs
- Body Sensor Networks
  - BSN are WSN covering a body area
  - Able to sense changes in body behavior or health
  - Can be capable of self medicating
  - System can use cell phones to send data

Sensor Nodes Basic Architeture



Stealth Yourself

- Lots of RFIDs well known hacks
  - Easily blocking the RFID signal with metallic material
  - RF noise can be a very good jammer
  - Many RFIDs can be easily read
  - Tags and reader communication can be intercepted
  - RF manipulation allows spoofing, replays and jamming
  - Perhaps you want more than being undetected, but also making trackers think you are somewhere else

Stealth Yourself

- Sensor Networks
  - Sensor nodes have processing capabilities
  - Many nodes have embedded operating systems
    - TinyOS, FreeRTOS, Linux, Windows...
  - We all know that softwares have security flaws
    - Where did I put my PIC18F4550 shellcode, damn it?!
  - Analogic sensors also can be easily deceived
  - Power supply might be easily disconnected
  - Network modules are also susceptible to the RF manipulation attacks, like spoofing, replays and DoS

Building Profiles

Building Your Profile

- Google
  - Store data about your searches
  - Own your Gmail e-mails
  - Track lots of your steps over the Internet
  - The new Big Brother?
  - Also a tool used to research about someone else
- Social networks
  - Is there another way to be more exposed nowadays?
  - Tons of personal information exposed
  - Very used in social engineering attacks

Building Your Profile

- Data mining
  - Correlation of data to define behaviors and patterns
    - When buying beer many people also buy nuts...
    - ...this pattern shows that placing beers in the same shelf as the nuts may help increase sales
  - Patterns might help on building profiles
- Direct marketing
  - After building your profile, they know what you like
  - It is much easier to know what try to sell to you
  - Extensively used by Google
  - They know your e-mails, they know what you are interested in, thus they make the right advertisement

Hiding Yourself

- Hide and seek with Google?
  - Free e-mail providers and ISPs are not neutral, never trust their privacy policy (Gmail is not the only one)
    - Keeping your e-mails on your own server is much safer
  - Tor can help you anonymizing your navigation
  - If you are famous, probably you cannot hide from Google
  - If you are not famous, try to not write too much about yourself on your blog, or ask your friends not to do it
  - Leave social networks. Or, keep a low info profile

Hiding Yourself

- Hiding from profilers?
  - It is really hard to run away from behavior patterns
  - Beer with nuts is nice, and that's why the pattern exists
  - Being wacky or exotic might be a good choice, but it may not be easy
  - Breaking patterns is the only way if you do not want to be profiled (perhaps you can buy beer with eggs)
  - It is easier to confuse profilers based on text, using a random word generator
  - Maybe you can move to the mountains too...

Recent News

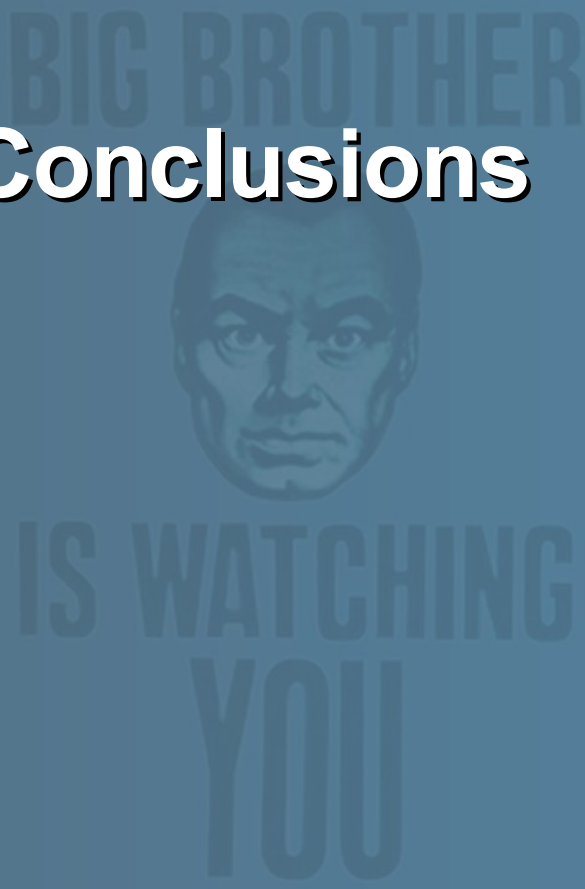
Recent News...

- Apple is tracking iPhone usage
  - *“Hidden in the code of the “Stocks” and “Weather” widgets is a string that sends the IMEI of your phone to a specialized URL that Apple collects.”*
  - *“Apple knows which app you are using ... IP address you were using ... so they can track down their customers all around the world.”*
  - *“attempts to modify the URL to exclude the IMEI information will not allow you to retrieve any information in the “Stocks” and “Weather” apps.”*
  - http://uneasysilence.com/archive/2007/11/12686/

Recent News...

- Hushmail contributing with police investigations
  - *“Hushmail claims to offer unreadable email as it uses PGP encryption technology ... However it seems the Canadian company has been divulging keys to the American authorities.”*
  - *“The document describes the tracking of an anabolic steroid manufacturer who was being investigated ... The DEA agents received three CDs of decrypted emails which contained decrypted emails for the targets of the investigation”*
  - http://www.itnews.com.au/News/65213,hushmail-turns-out-to-be-anything-but.aspx

Conclusions



Conclusions

- “Buy yourself a rifle, encrypt your data and prepare for revolution”
- Paranoia can be healthy sometimes
- Encrypt everything you consider classified, as well as your communication
  - GnuPG, PGP mainly for e-mail
  - SIMP, OTR for instant messaging, SSL'd IRC, SILC for relay chat
  - VoIP VPN, voice and text encryptors for smartphones
  - TrueCrypt, PGP Disk for file encryption
    - and do not forget to wipe your files!

Other Cool Related Stuff

- AXIS Cameras
  - Public XSS exploits for AXIS 2100 Cameras, allowing video stream replace (like in the movies)
- Matelgo
  - Tool to perform information gathering
- Keyloggers
  - Tons of keyloggers, with screenshots, ftp connection available for download
- Orkut Stalking
  - Tools that download someone's scraps (before they delete), that allow invisible navigation, etc...

References and Links

- Books
  - 1984, Animal Farm (George Orwell)
  - Brave New World (Aldous Huxley)
  - Discipline & Punish (Michel Foucault)
- Links
  - bigbrotherawards.org
  - eff.org
  - dataretentionisnosolution.com
  - openbeacon.org
  - defectivebydesign.org
  - bigbrotherstate.com
  - research.att.com/~kfisher/hancock
  - burks.de/tron/tron.htm (Tron's cryptophon thesis – in german)
    - ftp://ftp.ccc.de/cryptron
  - blog.wired.com/27bstroke6
  - duplipensar.net

Kudos

- Daddy, mommy, pets and friends in Brazil!
- Los hermanos en Ekoparty staff
- Rodrigo Rubira Branco, Domingo Montanaro and H2HC staff
- Very special kiss to Keyra Agustina
- Ex-rfdslabs, ex-gotfault and The Bug! Magazine guys
- Plebe Rude (for being the soundtrack of this work)
- Bruno Cardoso
- Luiz Eduardo (for the insightful comments)
- Bárbara Lopes
- Júlio Auto de Medeiros
- Robert Connolly (did you think you were for real?)
- Chaos Computer Club and all the privacy-concerned people around the world
  - And a special thanks to you for your patience

Questions?

HACKING THE BIG BROTHER

When intelligence defeats the iron fist

João Batista C. G. Moreira
joao@livewire.com.br

Júlio César Fort
julio@rfdslabs.com.br