Smart Phone Monitoring and Malware

Up close and personal

by Pierluigi Paganini, Ron Kelson, David Pace , Benjamin Gittins



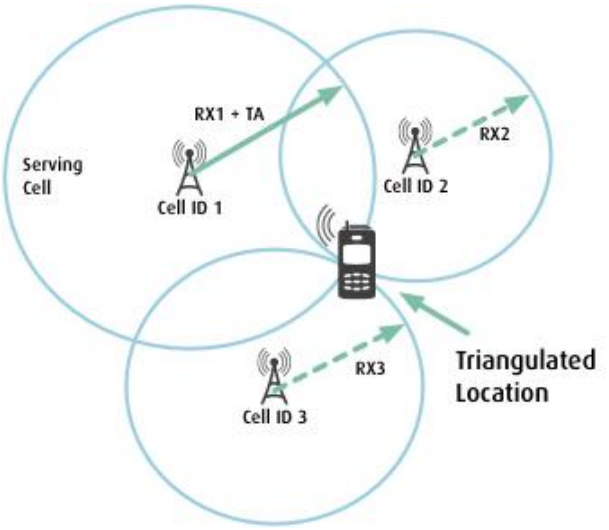
Ron Kelson *Pierluigi Paganini* *David Pace*

Published: 29nd July 2012

Mobile phones were once the status symbols of high-flying business executives. Today, mobile phones have nestled intimately into the fabric of our day to day lives. We often forget how indispensable they are to us, or how much they reassure us... that is until we can't urgently contact a business colleague, or one of our children, instantly. As mobile phones evolved from their clunky "brick" form factor to today's featherweight devices, they have progressively dazzled us with improved functionality, multi-media wizardry, Internet connectivity and ease of use. It's hard to imagine modern life without one...

As the price of owning and using phones has decreased, the number of people dependent upon them has grown. Activation is easy: just provide the telco your credit card details, passport and/or your National ID card details.

As the functionality of mobile phones increased, they became more convenient and valuable to us. Slowly, and subconsciously, they became an integral extension of our persons. Mobile phones follow us around everywhere, know our business and personal network (phone numbers and email addresses) and manage our event diaries. If left on, they track our location 24 hours a day, 7 days a week by systematically recording our position, through *triangulation* or by logging which cell stations within range of our phone.



Many of us have placed our unquestioning trust in these fantastic consumer devices (and the mobile phone operators that provide us services). We have been reassured by sales people that our mobile phone calls are encrypted, yet GSM security schemes are trivially breakable in practice. We have been lulled through decades of television advertising into feeling safe enough to openly communicate our most personal thoughts and feelings through these devices to our loved ones and family. As we surf the Web, we are increasingly exposing our individual habits and personal tastes...

With today's technology, and thanks to the technical assistance ("lawful interception") provided by mobile phone carriers, it is trivial for any Government to capture:

1) every mobile phone holder's physical location 24/7
2) every text message sent and received, and
3) every phone call made in their country.

Governments can choose to store all these activities in a large database for the duration of the mobile phone owner's natural life (100+ years). More than just the ability to recall any data they want on any person, they can perpetually mine this database for any changes in behaviour of any civilian, or group of civilians. After doing a quick search on "big data" and then "data mining" you will be ready to visit http://jeffjonas.typepad.com/ and read Jeff's expert analysis on just how grave the situation is.

How secure are the interception technologies used to implement this Total Information Awareness / Panopticon-like strategy? Search for "*Can they hear me now*?" by Matt Blaze and "*U.S. Enables Chinese Hacking of Google*" by Bruce Schneier, on Google, for the opinions of two information security experts.

How secure are Government networks from unauthorised third party access? According to Debora Plunkett, Director of the Information Assurance Directorate of the U.S. National Security Agency, "***There is no such thing as secure any more***."

According to James R. Clapper, Director of U.S. National Intelligence, in his statement to the U.S. House Permanent Select Committee on Intelligence (Feb 2012):

"*We assess that trusted insiders using their access for malicious intent represent one of today's primary threats to US classified networks." ... "We judge that evolving business practices and information technology will provide* ***even more opportunities*** *for FIS (foreign intelligence services), trusted insiders, hackers, and others to collect sensitive US economic data*."

Dr. James S. Peery, director of the Information Systems Analysis Center at U.S. Sandia National Laboratories, testified before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities (21 March 2012). *"I think we have to go to a model where* ***we assume that the adversary is in our networks****. It's on our machines, and we've got to operate anyway."*

With the introduction of smart phones, malware presents unique opportunities for Governments to dramatically increase their ability to monitor civilian targets. Surveillance malware can be used to turn on the smart phone's microphone (and video

camera) and transmit that data to Government servers over the mobile phone network.

How extensive is Government monitoring? No civilian is authorised to know. Some Governments in the EU, such as the UK Government, have laws and practices that allow the Government to collect and use intelligence in legal cases without disclosing their sources or methods. To quote chapter 8 of the Crown Prosecution Service's Disclosure Manual, this includes: "*the ability of the law enforcement agencies to fight crime by the use of covert human intelligence sources, undercover operations, covert surveillance, etc*" and "*the protection of secret methods of detecting and fighting crime*".

What is particularly disturbing is that this is exactly the same strategy used by the Military. To quote Ch. 17, Rec. 45, of the Unclassified Report of the U.S. Defence Science Board Task Force on the use of Biometrics in Defense: "*Often, it is wise to protect, sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This is a classic feature of intelligence and military operations; ... [W]e must seek to preserve the security of what the intelligence community calls 'sources and methods'* ...".

According to whistleblower William Binney, former director of the U.S. NSA's World Geopolitical and Military Analysis Reporting Group), Binney estimates the U.S. NSA alone has assembled 20 trillion "*transactions*" — phone calls, emails and other forms of data — just from Americans (April, 2012). Binney says: "*the point is, the data that's being assembled is about everybody. And from that data, then they can target anyone they want*."

According to Thomas Andrews Drake, a former senior executive of the U.S. NSA and whistleblower: "*When you open up the Pandora's Box of just getting access to incredible amounts of data, for people that have no reason to be put under suspicion, no reason to have done anything wrong, and just collect all that for potential future use or even current use, it opens up a real danger — and to what else what they could use that data for, particularly when it's all being hidden behind the mantle of national security,*" Drake said.

Recall the U.S. FBI's COINTELPRO program in the 1950's and 1960's which targeted non-violent civil-rights groups, and the recent activities of the U.S. Government against whistleblowers exposing crimes within Government. Also search Google for: "How the west built Iran's lawful intercept functionality". We can safely assume that other democratic Governments are enthusiastically following the precedent set by the United States.

Government agencies are not the only organisations interested in the personal data stored on, or transmitted through, your mobile phone... Self styled cyber criminals are now jumping on the bandwagon to reap benefits previously enjoyed only by Government and intelligence agencies.

In fact, recently the cyber security industry has observed an exponential growth of malware designed to attack smart phones, steal sensitive information, and exploit that data in successful

Classification of mobile threats by Trend Micro

Types	Technique	User Implication
Data Stealer	Steals information stored in the mobile device and sends it to a remote user	Stolen information may be used for malicious purposes
Premium Service Abuser	Subscribes the infected phone to premium services without user consent	Unnecessary charges for services not authorized by the user.
Click Fraudster	Mobile devices are abused via clicking online ads without user's knowledge (pay-per-click)	Cybercriminals gain profit from these clicks
Malicious Downloader	Downloads other malicious files and apps	Mobile device is vulnerable to more infection
Spying Tools	Tracks user's location via monitoring GPS data and sends this to third party	Cybercriminals track down location of users
Rooter	Gains complete control of the phone, including their functions	Users' mobile devices are exposed to more threats.

attacks, such as against mobile banking transactions. Today, the "Malware report" from Kindsight Security Labs estimates that one out of every 140 devices on mobile networks is infected with malware.

In the last 3 months, the cyber security industry has measured a 300% increase in malware targeted for mobile phones (and tablets) running the Android Operating System. In the Trend Labs Quarterly Security Roundup: "*Security in the Age of Mobility*" report the Trend Micro security firm focused on mobile threat incidents related to the first quarter of 2012. We will extensively quote Trend Micro's report below.

According to Trend Micro, the Android platform is the most dangerous platform today, with more than 5000 new malicious apps available. These malicious apps are made available for download through the Android Market store and unofficial software distribution channels. Downloading Android applications from unofficial channels is several times more dangerous than through the official Android Market store. The official Android Market store has the ability to remove malware once detected, reducing the chances of you downloading it.

However, unofficial distribution channels have no such security controls working in your favour. The Android Market is considered LESS secure than Apple's application store because the Android Market has LESS restrictions when it comes to registering as a software developer. Apple's more rigorous vetting process holds developers MORE accountable, which encourages malware vendors to target Android devices where they are less likely to be held accountable for their actions. Of

course, Apple users can choose to circumvent Apple's security controls by "*jail-breaking*" their phone and expose themselves to similar and worse types of malware problems...

One of the more interesting types of mobile phone attacks that exist on both Android Devices and Apple's iOS devices is the "*Data Stealer*" attack.

The UK's "The Sunday Times" published a news article that studied the behavior of approximately 70 widely-used mobile phone applications:

"*Twenty-one Transmitted the phone number, six sent out email addresses, six shared the exact co-ordinates of the phone and more than half passed on the handset's ID number.*"

The survey found that the data was sent to countries outside the EU such as China, Israel, India and America. Just how many (mobile phone and desktop) applications are leaking your personal data behind your back, nobody knows...

The sorry state of affairs is that both State and Non-state actors are cashing in on vulnerabilities and weaknesses in the design and implementation of today's (smart) mobile phones.

In the past (and even today) some Governments discourage or proscribe strong security in mobile phone standards and devices. The U.S. DARPA's "*Plan X*" (2012) seeks to explicitly track and exploit weaknesses in all electronic devices connected to the Internet.

What is clear, is that when Governments and organizations do not act to protect the legitimate interests of all stakeholders, the average civilian will continue to be exposed and exploited.

The question is: D*o you continue to consent to this type of behavior against you, your loved ones, and your community*?

This article was first published in the Malta Independent on Sunday – Original article below.

About the Authors :

Pierluigi Paganini, Security Specialist, CISO Bit4ID Srl, is a CEH Certified Ethical Hacker, EC Council and founder of Security affairs - http://securityaffairs.co/wordpress .
Ron Kelson is Vice Chair of the ICT Gozo Malta Project and CEO of Synaptic Laboratories Limited.

Ben Gittins is CTO of Synaptic Laboratories Limited.
David Pace is Project Manager of the ICT Gozo Malta Project, and a freelance IT Consultant.

ICT Gozo Malta is a joint collaboration between the Gozo Business Chamber and Synaptic Labs, part funded in 2011 by the Malta Government, Ministry for Gozo, Eco Gozo Project, and a prize winner in the 2012 Malta Government National Enterprise Support Awards. The web portal at www.ictgozomalta.eu *provides extensive links to free cyber awareness resources for all age groups.*

To promote Maltese ICT, we encourage all ICT Professionals to register on the ICT GM Skills Register and keep aware of developments, both in Cybersecurity and other ICT R&D initiatives in Malta and Gozo.
For further details contact David Pace at dave.pace@ictgozomalta.eu

Other Articles in the Series

Insider perspectives on the Global Cyber Safety and Security Status – Part 1
Insider perspectives on the Global Cyber Safety and Security Status – Part 2
Insider perspectives on the Global Cyber Safety and Security Status – Part 3
Insider perspectives on the Global Cyber Safety and Security Status – Part 4
A Picture of the Hacktivism Phenomenon
Serious Safety and Security Problems in Automotive, Aviation, Aerospace and other Cyber-Physical Systems – Part1
Serious Safety and Security Problems in Automotive, Aviation, Aerospace and other Cyber-Physical Systems – Part2
The Cyber War Era Began Long Ago
Are your Business Operations Secure?
Cyber Security at Large Sporting Events
Malware – It's all about you!
Phishing the Financial and Banking seas
Understanding the risks of Mobile Banking Transactions
Social Networking series Part 1: Who exactly are you disclosing your story to?
Social Networking series Part2: Have you been infiltrated?
Social Networking series Part3: Are you unnecessarily exposing yourself to physical threats?
...

All the above articles, and more, are available at www.ictgozomalta.eu/events/documents-list. They may also be available from the respective author's websites.