Emerging Threats in Mobile Computing

Adam Meyers - SRA International

Significant Work. Extraordinary People. SRA.

Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion
- Q & A

Who are you, and what are you doing here?

- SRA
  - Leading provider of technology and strategic consulting services and solutions - including systems design, development and integration; and outsourcing and managed services.
  - Comprehensive cyber security practice integrating security architecture, risk assessments, and certification & accreditation. SRA's IA practice currently rated at NSA-CMM Level 3.
- Adam
  - Security Consultant
  - Penetration Test Team
  - Forensic Technician
  - Security Architect
  - Reverse Code Analysis

Hacker Fail

- Fall 2008 a promise is made
- Meet JK Benites
- This ‘genius’ left his name (unobfuscated) in the malware he wrote to steal banking credentials and ended up at a certain US Government Agency

Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion
- Q & A

Disclaimer

- Standard legal-mumbo jumbo.
- You have the right to remain silent. Anything you say or do can and will be used against you in a court of law. You have the right to an attorney. If you cannot afford an attorney, one will be appointed to you.
- Prohibition on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
- (2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
- (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- (B) information from any department or agency of the United States; or
- (C) information from any protected computer;
- I pledge allegiance to the flag of the United States of America, and to the republic for which it stands, one nation under God, indivisible, with liberty and justice for all
- Energy can be transformed (changed from one form to another), but cannot be created or destroyed.

Agenda

- Introduction
- Disclaimer

- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion
- Q & A

How We Got Here

- Why mobile computing
  - Allows us to tackle problems where they occur
  - Facilitates (e)commerce
  - Economic advantages of working remotely
    - Not to mention traffic reduction
- Major milestones facilitating mobile computing
  - Global Cellular Networks
    - Groupe Spécial Mobile (GSM) 1991
  - Reduced Instruction Set Computer (RISC) Processors
    - ARM 1983
  - NAND Memory retains data when powered off and improved I/O
    - Toshiba 1987
  - Consumerization of Internet
    - Lets call it the 90's

SRA INTERNATIONAL, INC.

Honesty and Service®

Summary

SRA INTERNATIONAL, INC.

Honesty and Service®

Multitude of Devices

Mobile Players

- Who are the mobile players?

Worldwide smartphone market share, Q3 2010 by platform						
Company	3Q09 units (,000)	3Q10 units (,000)	growth in units %	3Q 09 share %	3Q 10 share %	change in share (%)
Symbian	18314.8	29480.1	60.96	44.6	36.6	-8
Android	1424.5	20500	1339.1	3.5	25.5	22
iOS	7040.4	13484.4	91.53	17.1	16.7	-0.4
Research In Motion	8522.7	11908.3	39.72	20.7	14.8	-5.9
Microsoft Windows Mobile	3259.9	2247.9	31.04	7.9	2.8	-5.1
Linux	1918.5	1697.1	11.54	4.7	2.1	-2.6
Other OS	612.5	1214.8	98.33	1.5	1.5	0
Total	41093.3	80532.6	95.98	100	100	0

source: Gartner

Why do we care?

- Gartner - 172,373,100 mobile sales 2009!
- Users arbitrarily install software ‘vetted’ by vendor markets/app store
- Implied security by expensive hardware constraints
  - Do you have a GSM base station?
  - These aren’t the droids you’re looking for
- Not many security products for smartphone
  - A/V? HBSS? HIDS?
- Enterprise users are bringing them onto the enterprise - despite policy

Enterprise Use Case

- Mobile devices primarily originated as consumer personal devices
- Many popular ones developed solely for consumer market with no interest in enterprise markets
- Putting consumer devices with limited security capabilities on the enterprise makes the network defenders job harder
- These devices are on the network - whether you like it or not
  - Plugged in for power
  - Connected to enterprise wireless
  - Backed up/synced to enterprise computers

Agenda

- Introduction
- Disclaimer
- Background

- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion
- Q & A

SRA INTERNATIONAL, INC.

Honesty and Service®

Mobile Security Concerns

Trojanized Applications

Data at Rest

Mobile Malware

Data in Motion

Social Engineering Attacks

Voice Communication Security

Browser Based Attacks

Security on Mobile

- Components
  - Device (Pad/Phone)
  - Network (Cellular/WiFi)
  - Operating System (IOS/Android/BB/Symbian/WinMo)
  - Applications (3rd Party)
  - Browser
  - Enterprise Applications (Custom/Mail/Web)
- Limitations
  - OS API limitations
  - Limited 3rd party application validation
  - No carrier authentication for device (GSM Um)
  - Not all devices support data encryption
  - No mandatory security controls out of the box
  - No updates for security (a la Windows Update)

Data at Rest

- Blackberry
  - Content Protection = 1 (AES256)
- Android
  - Fail
- iPhone
  - Device level encryption (AES 256)
  - (2 bypasses already)
- Symbian
  - Software based
- WM7?

Data in Motion

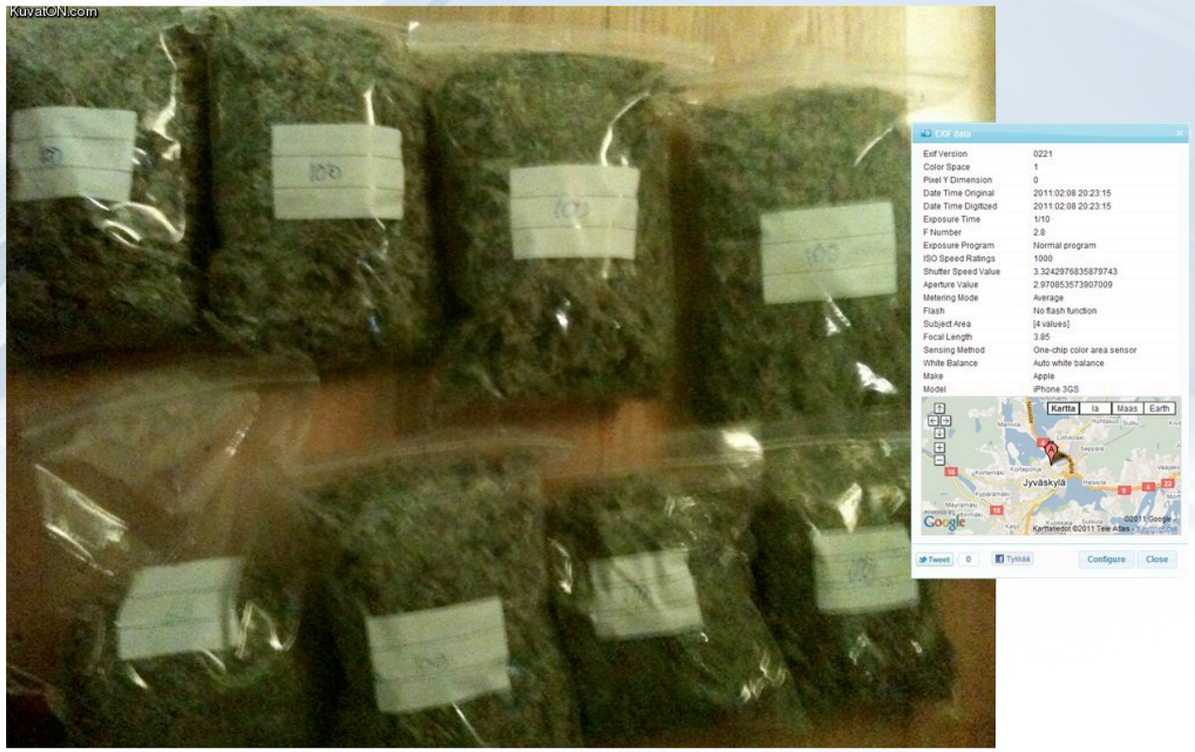
- Depends on device and what communication medium being used
  - Blackberry Enterprise - AES256 tunnel
  - Others - rely on protocol security GPRS/UMTS/EDGE/EV-DO/ HSPA/WiMax
  - WiFi
- Tools
  - Difficult to implement due to restricted API on mobile devices
    - Implement Enforce VPN for devices
    - Restrict user capabilities

Voice

- Device Dependent in many cases
- Latency issues
- Software Based
  - Whisper Systems (OTR) - Free
- Hardware Enabled
  - AT&T Encrypted Mobile Voice
  - SRA One Vault Voice

Personnel Security Concerns

- Social Networking and Realtime updating can compromise operations
- WiFi networking on untrusted networks can compromise data and identity
- GSM account information can be compromised and allow tracking of personnel
- Remote Access Tools can allow for tracking of personnel and remote listening



Perimeter Security Concerns

- Perimeter security model standard across enterprises
  - Gateway/Firewall to delineate trusted zones
- Devices are moving towards ‘blackberry model’
  - Blackberry Enterprise Server builds secure connection between devices and enterprise
- Persistent connection to corporate network
  - Provide ‘secure’ access to corporate resources
  - Manage device from corporate enterprise
- Demonstrated issue - Jesse D’Aguanno BBProxy
- Perimeter is effectively pushed out to every mobile device

Who owns the data

- Users are increasingly bringing their devices to the party
- CEO Ipad Birthday
- Once the door is open to personnel devices
- Life cycle of personnel devices used for enterprise data
  - Secure removal?
  - Policies/NDA/Other?
  - Forensics
  - Retention
  - Backups
- Emerging problems for management of mobile exist in addition to technical security concerns

Detection/Mitigation Concerns

- How to monitor realtime when the devices are not on enterprise infrastructure
- No real auditing capabilities for installed applications
- Monitoring user behavior (insider threat) are difficult to track
- How can we remove (if we knew about them) malicious software from a mobile device

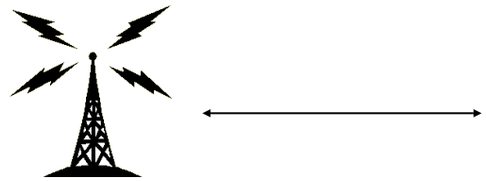
Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion
- Q & A

Attack Surface

- Physical Access
- Cellular Communications Channels
- Browser
- Operating System
- Applications
- Social Engineering

Cellular Phone Attack Surface

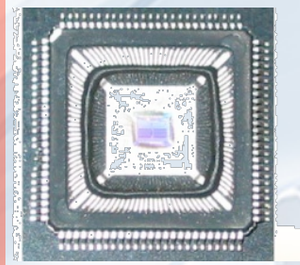


Attack Command Set (AT commands)

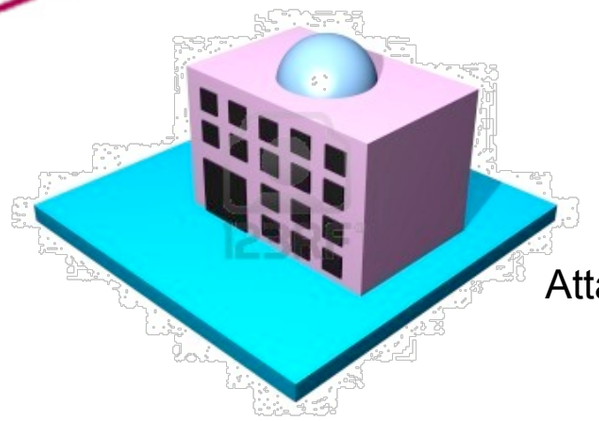
Receive controls from Carrier

Encode Voice Communication (GSM/ CDMA/etc)

Interception/Man-in-the-Middle



SmartPhone Attack Surface

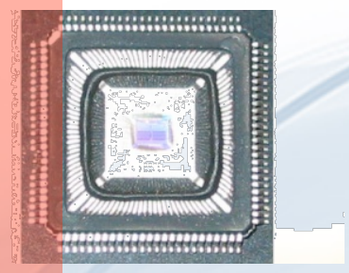


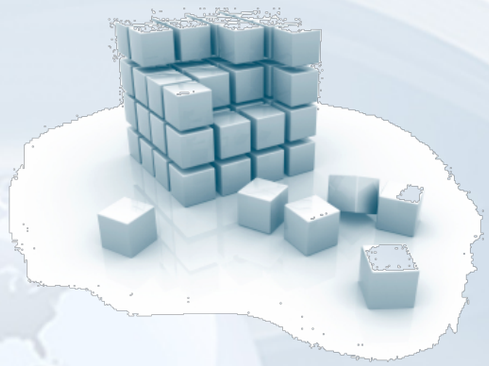
Attack Command Set (AT commands)

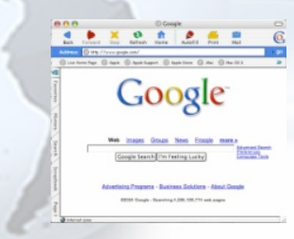
Receive controls from Carrier

Encode Voice Communication (GSM/ CDMA/etc)

Interception/Man-in-the-Middle







Browser

- Browsers continue to be targeted applications on mobile devices
- Browser is primary attack surface exposed to the most threats
- Browser issues
  - Javascript
  - Cross Site Scripting (XSS)
  - Iframe injection
  - Browser Vulnerabilities (Memory corruption attacks etc)
- Browser as an attack mechanism
  - pwn2own 2010
  - CVE-2009-1680
  - CVE-2009-0961
  - CVE-2009-0959
  - ...

Applications

- Applications are being developed by anyone and there is little validation
  - Who is designing that App you just installed?
- 3rd Party App Stores
- Few options to monitor/remove malicious apps
- Latent functionality?

Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors

- Emerging Threats
- Conclusion
- Q & A

20XX the year of mobile malware

- Vendors and analysts have been proclaiming *this* will be the year of mobile malware for the last several years
- FUD?
- Increasing cases of malware over the last few years
- Threat is present
- Rapid expansion of technology and platforms provides ‘target rich environment’
- First some news:

Mobile Malware Will Grow in 2011, Predicts IT Security Firm ...
Mobile Malware Will Grow in 2011, Predicts IT Security Firm. By Matthew Harwood. 11/29/2010 -. Cybercriminals will feast on the insatiable demand for ...
www.securitymanagement.com/.../**mobile-malware**-will-grow-2011-predicts- it-security-firm-007899 - Cached

Will 2010 Be the Year of **Mobile Malware**? | News & Opinion | PCMag.com
Feb 16, 2010 ... One of the perennial predictions for security is that it will be the year of **mobile malware**. This year just might.
www.pcmag.com/article2/0,2817,2359780,00.asp - Cached - Similar

Geimini

- December 2010 Chinese Android market applications are trojanized with mobile malware
- Malware capabilities
  - Initiate calls
  - Full control of SMS messaging
  - Access to Contacts and Application Databases
  - Download and Execute arbitrary files
  - Launch browser to a target URL
  - Cryptographic C2 (DES)
  - Obfuscation

Soundminer

- Proof-of-Concept Malware
- New concept - “sensory malware”
- Malware requests access to microphone
- Identifies Interactive Voice Response (IVR) System
- If found it begins to record and exfil recorded content to Command and Control
  - “Please say or enter your account now.”
- http://www.cs.indiana.edu/~kapadia/papers/soundminer-ndss11.pdf

Flashlight App

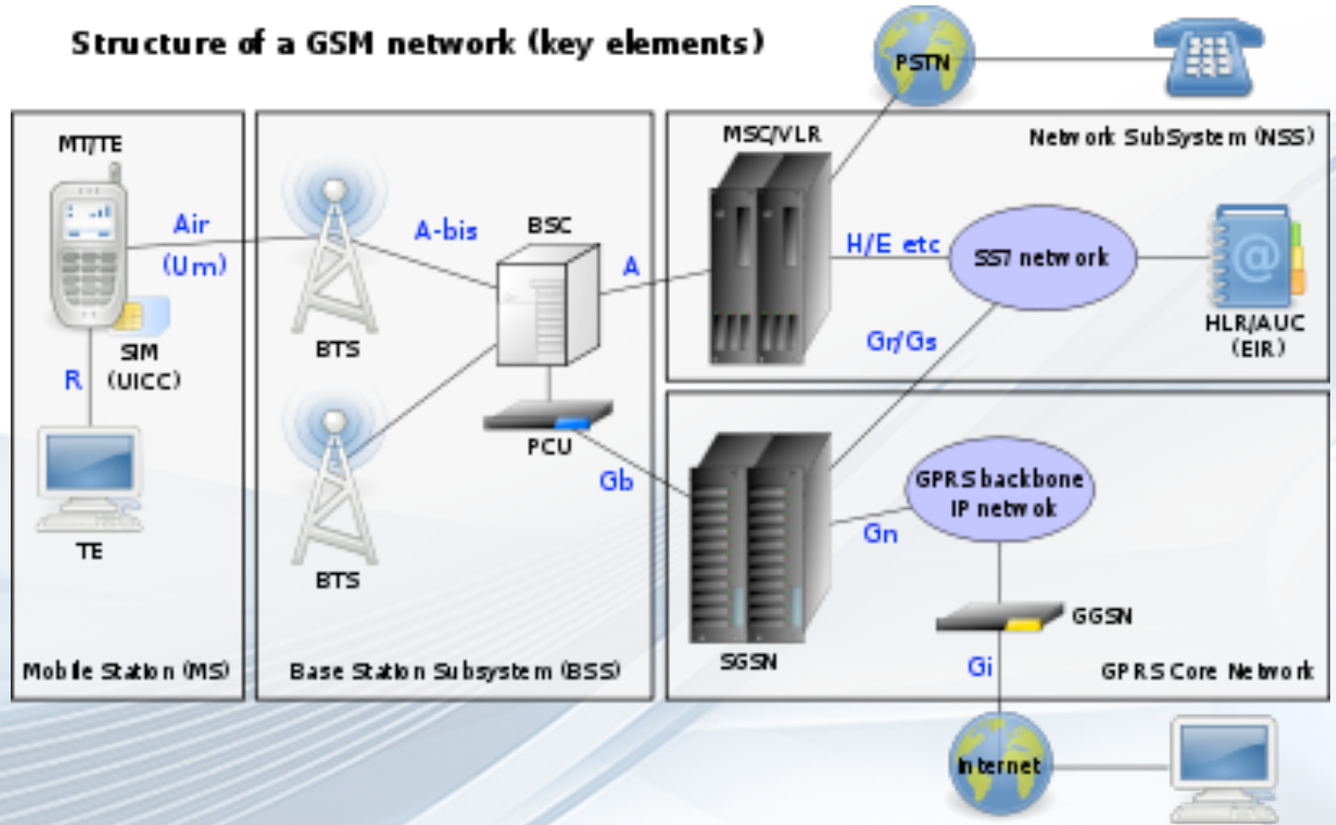
- July 2010 Handy Light
- 15 Year Old Nick Lee
- Standard flash light app
  - if you include tethering
- Indicative of the amount of analysis going into app validation

Cellular Interception

- Cellular interception is not new
- Hackers used to routinely intercept analog cell phone traffic
- Newer protocols (GSM/CDMA/3G/etc) have kept attack costs high requiring carrier level equipment
- Some of these protocols still keep attack costs high

Groupe Spécial Mobile

- Cellular technology first deployed in 1991
- Still prevalent in cellular technology today ‘2G’
- Many devices support only 2G mode (e.g.: Blackberry)



GSM Interception

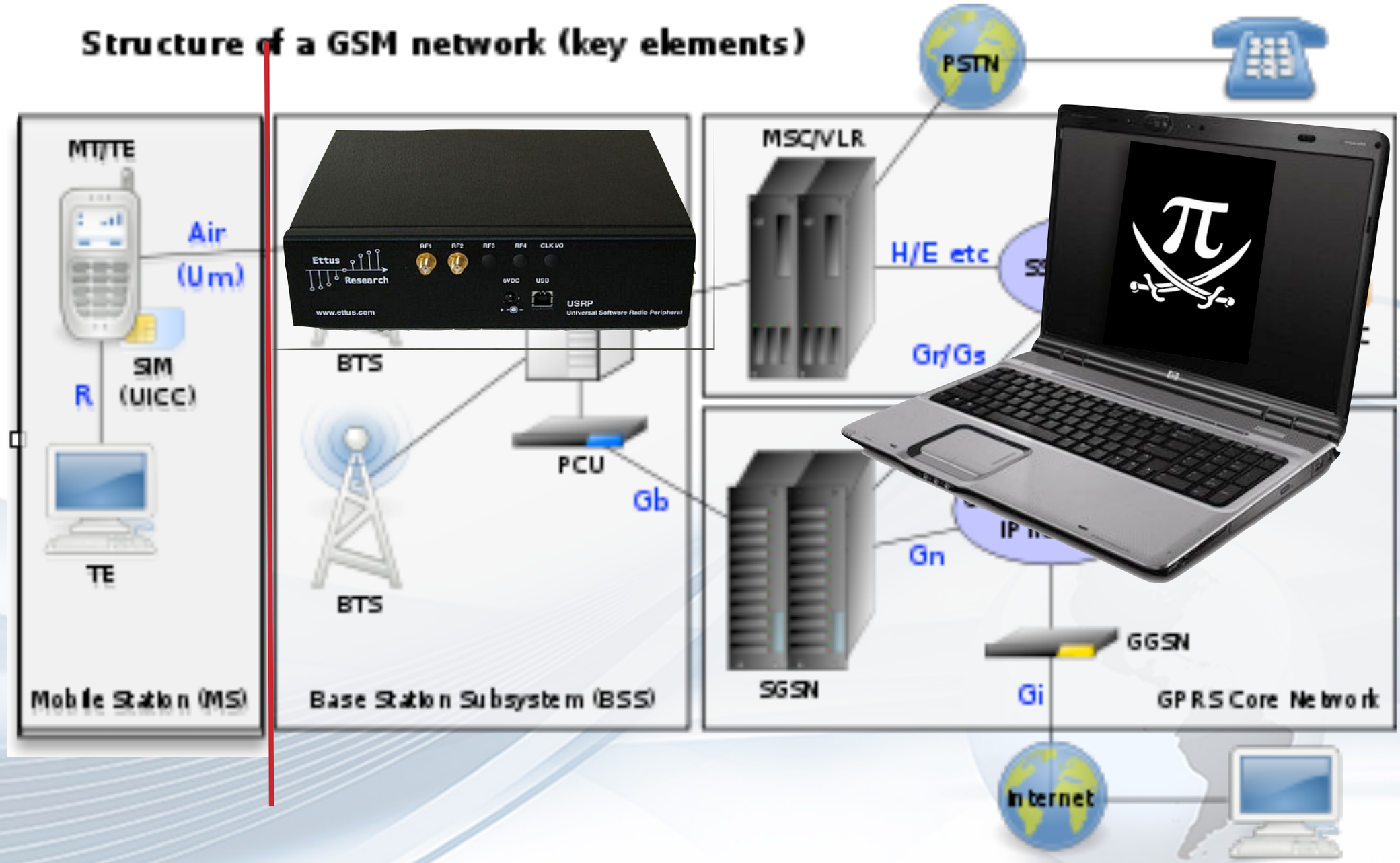
- Sniffing Attack
  - Monitor passively for GSM traffic
  - Compounded by encryption algorithms
    - GSM uses A5 Stream Cipher
  - Luckily for us A5 is broken
    - Golic 1997
    - Alex Biryukov, Adi Shamir and David Wagner 2000
    - Karsten Nohl and Sascha Krißler 2009 Blackhat
- Man-in-the-Middle
  - “IMSI Catcher” commercialized by Rohde & Schwarz.
  - 2010 Chris Paget Defcon Demo

GSM Interception Under $2000

- GSM operates on commonly available consumer bands 850Mhz, 900Mhz, 1800Mhz, 1900Mhz
- Meet the Universal Radio Software Peripheral
  - USRP - $700
  - RFX900 - $275 (x2)
- Other requirements
  - Antenna
  - Accurate Clock (~$275) or build your own
  - Computing device with OpenBTS, Asterisk, Python

Honesty and Service®

IMSI Catching



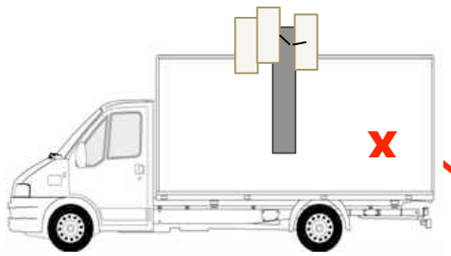
Demo Time

- 404 Error - Demo Not Found
- The demo you requested could not be found!

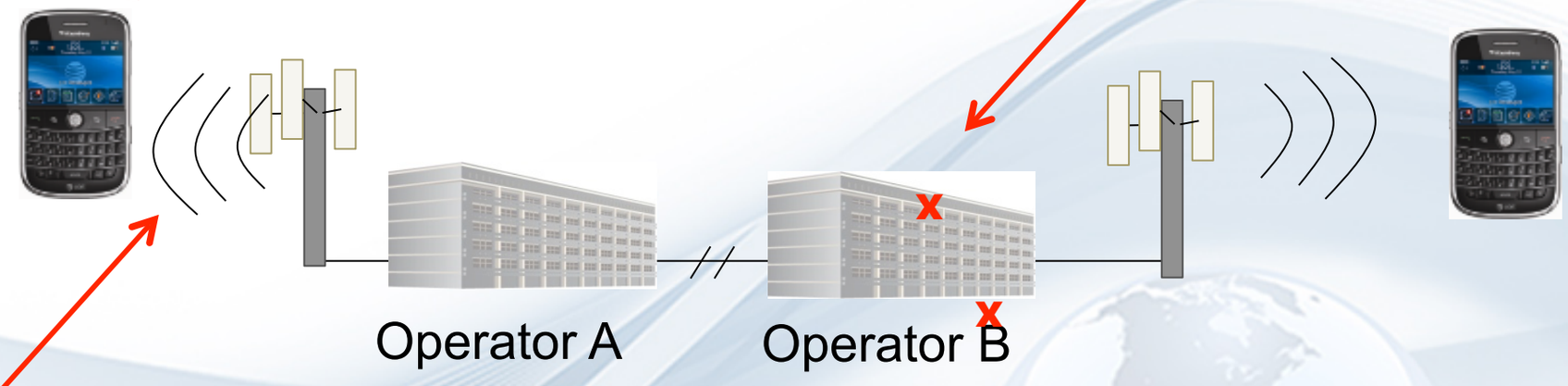
Mobile Intercept: Attack Vectors

3rd party application exploits

Tower Spoofing



Access at Network Facility



Illegal Monitoring

Unwanted Surveillance by a Foreign Government

Hacker Exploit of Lawful Call Monitoring Taps

Other GSM Attack Vectors

- Current cellular infrastructure designed in late 80's early 90's
- GSM 1991
- BaseBand Radio legacy code
- 'Baseband Apocalypse' Ralf-Philipp Weinmann Blackhat Federal 2011
  - Baseband code written poorly and few changes since 1990's
  - Shared Memory (worst case) on mobile devices between CPU and BB
  - Demonstrated effective attack using one GSM Um packet to turn iPhone on with Autoanswer
  - Utilized rogue base station

Remote Access Tools

- Commercial and Open Source
  - Flexispy
  - Mobile Spy
  - Open Source
- RAT's provide capabilities to monitor
  - Ambient Audio (Hot Mic)
  - Message Traffic
  - Voice Conversations
  - API access to OS
- RAT Installation
  - Unauthorized access to device
  - Social Engineering
  - Exploit?

Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats

- Conclusion
- Q & A

Conclusion

- Mobile Computing is over 15 years old
- Numerous attack vectors to target mobile
- Cellular infrastructure has some inherent issues
- Limited access to third party developers to build security tools
- Bad things are beginning to target mobile devices
- Applications are not being vetted 100% and users are installing anything that seems fun
- Enterprises need to prepare for users and their devices increasing the risk to them

Agenda

- Introduction
- Disclaimer
- Background
- Mobile Security Concerns
- Mobile Attack Vectors
- Emerging Threats
- Conclusion

- Q & A

Questions?

Adam Meyers
Adam_meyers@sra.com
Twitter: Cyber_Adam_SRA