



Emerging technologies and threats for the IS Auditor

Stan Barber, B.Sc., FIA
Director Education and Technology
MindGrove Ltd, UK



Summary of Session

- 1 – The Wireless Revolution
- 2 – Dangers and Vulnerabilities
- 3 – The Dilemma
- 4 – Taming the Revolution





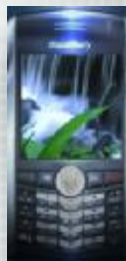
1 – The Wireless Revolution

- An updating tour
- On the move computing – solutions on a chip
- Cut out commuting – bring the network to the user
- The global virtual user



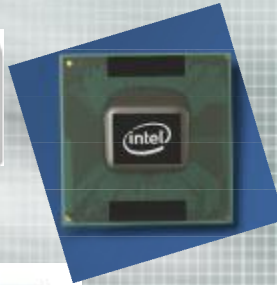
The evolving world of cell phone technology...

- 1 billion + cell phones sold June 2006 – May 2007
 - 2bn+ worldwide cell phone users
 - Most consumers have two or more phones in storage
 - 300bn SMS sent in 1Q 2007





Wireless computing – very powerful integrated network solutions on a chip...
802.11a/b/g



Or a UMPC if it's small you want...





Inexpensive data capture...

- Multiple low cost storage solutions – prices are in freefall



ISACA



And storage need not be passive...



- StarNet is shipping a USB-key-based PC X server that lets Windows PC users run graphical applications that reside on remote Linux systems, and carry their sessions with them.
- The product launches an X Window server application when plugged into a host PC running Microsoft Windows.



ISACA



USB – U3 Specification permits applications to run directly from USB device



The Launchpad makes the drive smart:

- Comes with **pre-loaded software**
- Carry and access your files **easily!**
- Get more U3 smart software at software.u3.com
- Keep your data **safe and secure**
 - Anti-virus comes bundled on most drives
 - Built-in password protection
 - Unplug the drive and leave no personal data behind



And PC Cards bring fast networks to the user...

- No device with a PC Card slot is too far from a network

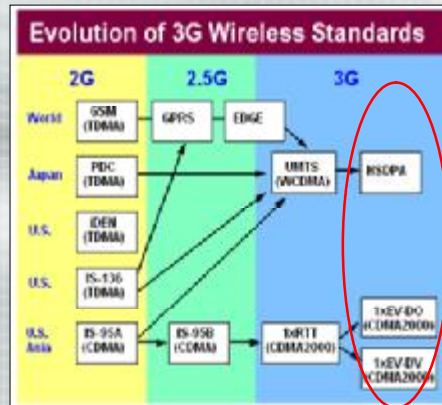




Convergence of wireless technologies in the chipset...

- At the core of (Qualcomm's) Snapdragon is the Scorpion 1-GHz microprocessor. Scorpion is paired with a 128-bit multiple-data capability and a 600-MHz digital signal processor to handle various multimedia applications
- Snapdragon supports a variety of 3G cellular technologies, including EV-DO, deployed by Sprint and Verizon Wireless in the United States, and UMTS/HSDPA, deployed by Cingular, as well as Wi-Fi and Bluetooth

snapdragon



ISACA



And for those who need applications on the move – Software as a Service

- Software as a Service (SaaS) provides functionality without operational overheads; it's a delivery method that provides network-based access to, and management of, software
- SaaS is part of a wider move towards Internet-based automated services
- Unlike some ASP offerings, SaaS applications generally perform better across the web
- Gartner Research claims that by 2011 the SaaS market will top 25% of all software
 - Google Docs & Spreadsheets

Google
Docs & Spreadsheets BETA

ISACA

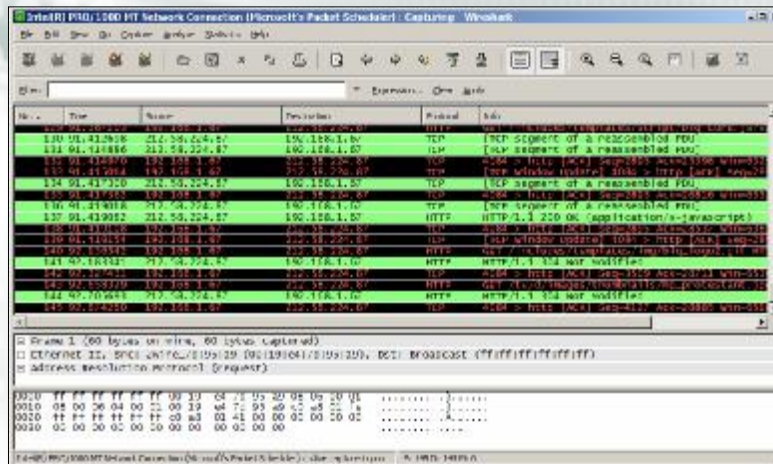


Yet wherever the mobile user goes their wireless signal can be detected...

- For law enforcement
- Or less legitimate reasons



Or your traffic can be watched...





And wherever the mobile user operates...

- They represent a potential threat to your corporate systems safety or your corporate data security



ISACA



2 – Dangers and Vulnerabilities

- The five stupidest (preventable) things that people do with mobile technology
- Attacks on wireless technology – social and technical mechanisms
- Attacks on mobile technology – the trends and shapes of things to come
- Attacks using mobile technology – new possibilities in the wireless era
- Combinatorial attacks fusing new technologies

ISACA



The five stupidest (preventable) things that people do with mobile technology

1. Leave devices and storage media on open display

- Theft – from person, vehicle, or working location
including “switch” and “coat” heists
- Interference – deliberate exchange of media cards or SIM
- Loss - from internet lost and found
 - Found 2 ipods on the Heathrow Express, Around 6:3 AM Sep16
 - Monday night I lost business critical travel documents on the overground train from Waterloo to Wimbledon. It was the 12:15am train. Reward offered.
 - Lost Nokia 6021 at Gatwick airport on 25th August. Left it in tray at the walk through security gate during early morning check-in on to First Choice Airlines to Verona. Grateful for its return. Contains Vodaphone SIM on business contract.
 - I left my Nokia E90 into a black cab right in front of London Heathrow airport on August 12, 2007 around 11:30am - 12:00pm. I would ask the founder (sic) to contact me asap.



The five stupidest (preventable) things that people do with mobile technology

2. Not using vendor supplied security mechanisms incorporated in the device

- PIN and SIM access protection (one in two cell phones do not have these protections set)
- Power up passwords – notebooks and pocket PC
- Biometrics
- Timeout and Timer resets – cell phone and pocket PC





The five stupidest (preventable) things that people do with mobile technology

3. Allowing screens to be viewed by strangers

- On train or in public locations such as coffee shops
- When away from device
 - According to a recent UK survey, there are 2.4million notebook users daily at risk from prying eyes.
 - What's more, 8 out of 10 of us may already have become victims of shoulder surfing.



The five stupidest (preventable) things that people do with mobile technology

4. Giving away information by engaging in audible discussions

- Conducting business in a public place – airport, rail carriage, taxi cab, restaurant, hotel lobby
- We are no longer *overhearing*, which implies accidentally stumbling upon a situation where two people are talking in presumed privacy. Now we are all simply *hearing* eavesdropping is the new norm.





The five stupidest (preventable) things that people do with mobile technology

5. Not being aware of broadcast range

- Bluetooth Class II – 10m; but Bluetooth Class I – 100m
- WiFi under good conditions and appropriate aerial up to 2km – maybe more with amplification
- Lack of signal attenuation



ISACA



Attacks on emerging technology – social mechanisms

- Loan to make a call or calculation
- The person that stands behind you is not a good guy
- Extortion, blackmail and threats of violence
- Phish to Phone
- BlueJack

“This is the prize notification message service of the National Lottery. Please note down telephone number 0207 434 8000 for future use and please enter 5657 to confirm you have done this when asked to enter your PIN.”

ISACA



Attacks on emerging technology – technical mechanisms

- Retrieving contents of SIMs and Phone memories through hacking software
 - Name and address
 - Including non-registered private addresses
 - Private ex-directory numbers
 - Including landline, cell and VoIP numbers
 - Personal id data including...
 - Bank
 - Household alarm codes
 - Vehicle codes
 - Discovering that the user has synchronised all PINS



ISACA



Read any SIM



- WE CAN DO THE FOLLOWING:
 - Copy their phone book onto your PC
 - You can find deleted text
 - You can view up to last 10 numbers dialed.
 - Transfer data from one SIM card to another
 - Back up phone numbers and SMS messages
 - Examine your SIM card to find deleted text messages/numbers
 - Program your SIM card to only dial numbers and make calls that you permit. (Good for controlling children's calls or company employees.)
 - Allows you to backup restore and edit your phone book.

Contact Us Today Results within 48hrs: 1234icu@gmail.com





Attacks on emerging technology – technical mechanisms

- Retrieving contents of unprotected storage devices
 - SmartMedia (SM)
 - CompactFlash Type I (CF)
 - CompactFlash Type II (CF)
 - Microdrive (MD)
 - MultiMedia Card (MMC)
 - Reduced Size MultiMedia Card (RS-MMC)
 - Dual Voltage Reduced Size MultiMedia Card (DVRS-MMC)
 - MultiMedia Card Mobile (MMCmobile)
 - Memory Stick (MS)
 - Memory Stick Pro (MS Pro)
 - Memory Stick Duo (MS Duo)
 - xD Picture Card (XD)
- Use simple software and multi-way reader



Attacks on emerging technology – technical mechanisms

- Man-in-middle attack
 - Route browser through local rogue proxy – supplied as part of configuration set
 - Monitor using Paros or similar M-i-M review and replay agent





M-i-M monitor

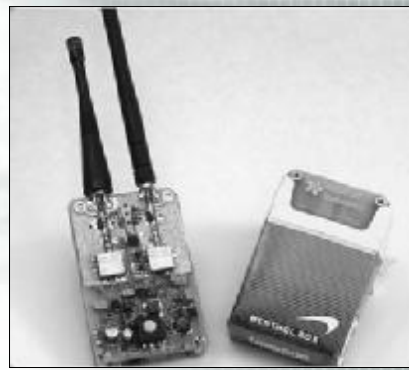
The screenshot shows a network monitoring interface. The top part displays a list of IP addresses and their associated domains. The bottom part shows a detailed view of a specific IP address, including its parameters and values.

Parameter Name	Value
Product Name	ZonMIn Security Suite
Product Version	3.4.722.R0C
URL OR	DL:40075008/82000-1C20
Product Author	Andreas Holmstrom (andreas@zonm.com)
License	?
Language	EN
OS	Linux



Attacks on emerging technology – the trends and shapes of things to come

- Direct attacks on the network to disrupt users – denial of service attacks by unnatural means
 - Block Wi-Fi, Bluetooth, GPS, GMS; witness the arrival of the 25\$ Jammer





Attacks on emerging technology – the trends and shapes of things to come

- John Hering and his BlueSniper rifle, which he claims can sniff and hack Bluetooth-enabled wireless devices more than a mile away

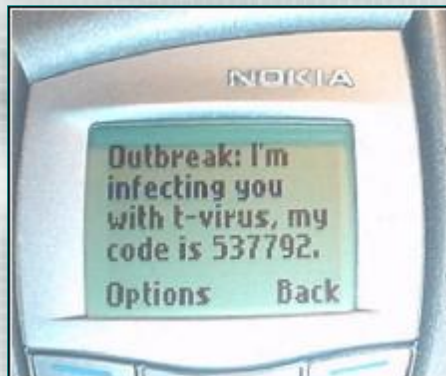


ISACA



Attacks using mobile technology – new possibilities in the wireless era

- Hoaxes and jokes
 - Spread through SMS for fear or fun (SMS pyramid attack)
 - Flood users' mailbox systems and deny access to corporate networks (Auto-voicemail attack)
 - Deliberate transmission of large files to fill media storage (Blackberry Dump)



ISACA



Combinatorial attacks fusing new technologies

- Image or audio to storage
- Storage to network
- Transfer to accomplice
- Transfer to incriminate

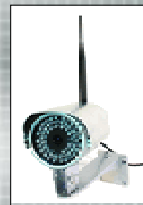


ISACA



Combinatorial attacks fusing new technologies

- Tracking individuals through GPS or Wireless Video



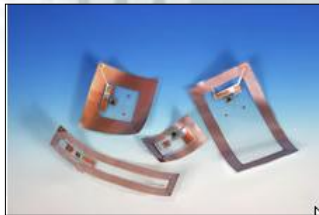
2.4 GHz colour pinhole wireless camera 23x24x23mm with audio complete kit includes transmitters, 4 channel receiver, mains adaptors and 9v battery clip. Range (good conditions) 500m.

ISACA



Combinatorial attacks on new technologies

- Breaking RFID codes and retrieving or subsuming identity



ISACA



It's only an iPod!

- Researchers have discovered critical vulnerabilities involving Apple's QuickTime media player software and the download application for Apple's iTunes music store. The flaws create a means for hackers to take control of affected systems.
- All four security issues are exploitable via iTunes. The cross platform flaw affects Windows 2000, Windows XP and Apple Mac OS X systems running vulnerable versions of iTunes. Fortunately there is a fix.



ISACA



Media applications have vulnerabilities just like other software

- Apple QuickTime remote command execution vulnerability (21 September 2007)
- Unpatched bug bites QuickTime (3 January 2007)
- Apple update fixes 'critical' security bug (2 March 2006)
- Mac OS X malware latches onto Bluetooth vulnerability (17 February 2006)
- Apple adds MiniStore monitor warning to iTunes (19 January 2006)
- Apple downplays iTunes 'spyware' fears (12 January 2006)



4 – Taming the Revolution

- Creating a security architecture that binds the moveable, the unknown and the invisible
- If it can't be audited then its not accountable or acceptable
- Our message on preparedness to management





Creating a security architecture that binds the moveable, the unknown and the invisible

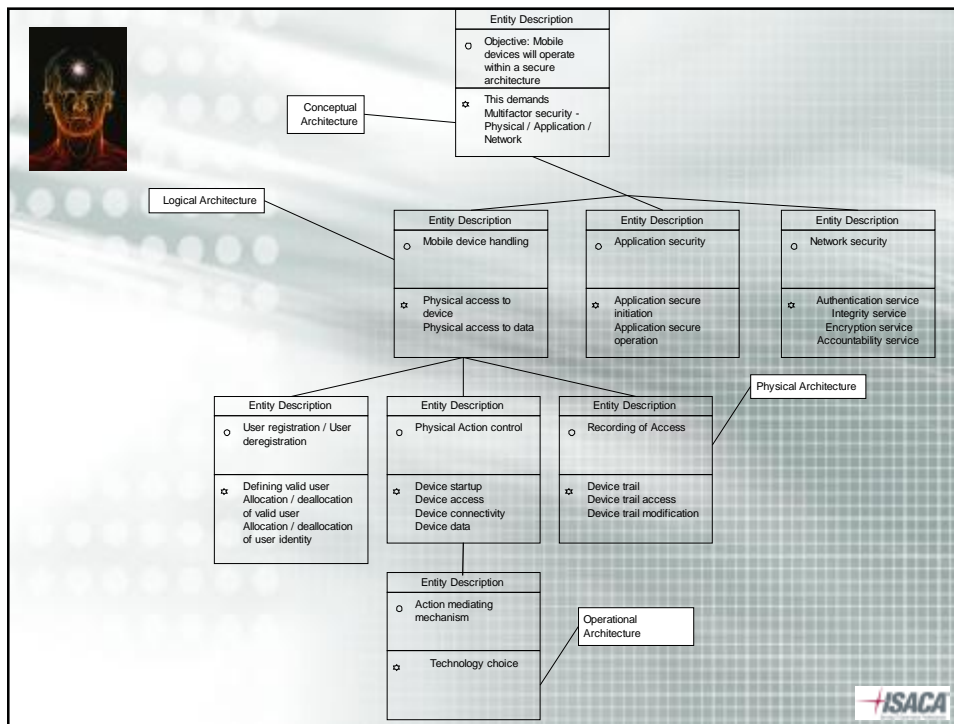
- Mobile ITSec policy required to define and control
 - What you can and can't bring into the office
 - Personal equipment and storage solutions
 - What you can and can't do with mobile technology
 - Connectivity and usage
 - European human rights conventions
 - Constraints over corporate data
 - In flight and in-storage



Creating a security architecture that binds the moveable, the unknown and the invisible

- Need to ensure that prescriptive security mechanisms stay one jump ahead of technology
 - COBIT 4.0 and beyond
 - NIST 800
 - ISO 17799/27005
 - ESF
 - Etc.
- Need to learn to engineer formal architecture to ensure competent and adequate coverage
- Need to presume that systems will be attacked outside of the framework and control we decide on





If it can't be audited then its not accountable or acceptable

- Device held trails are limited and often non-existent
- Identity of user is more doubtful for a mobile device where only the most primitive of access control methods is available and its very mobility presumes transfer of device from place to place (person to person)
- Software to extract, compare and scan through storage files held on mobile devices is hampered by slow access speeds to stored devices

The ISACA logo is visible in the bottom right corner of the slide.



Our message on preparedness to management

- It is inevitable that Moore's Law concerning technology will apply to mobile devices, leading to extremely high performance multifunctional devices that do not depend on wired connections or corporate hosts for their usefulness...



ISACA



Our message on preparedness to management

- It is inevitable that control solutions will follow retrospectively in the path of connectivity...
- Hackers and abusers will take advantage of weaknesses in structures and learn how to exploit technically and socially the mobile workforce...

ISACA



Summary of Session

- 1 – The Wireless Revolution
- 2 – The Dangers and Vulnerabilities
- 3 – The Dilemma
- 4 – Taming the Revolution



For more information

Stan Dormer

Director Education and Technology

MindGrove Ltd, UK

stan.dormer@mindgrove.co.uk

www.mindgrove.co.uk

MindGrove
TRAINING CONSULTANCY





Emerging technologies and threats for the IS Auditor

Stan Dornier, B.Sc., FIA
Director Education and Technology
MindGrove Ltd, UK

