Bluetooth Security
Issues, threats and consequences

Mark Rowe, Tim Hurman
Pentest Ltd.

Agenda

- Issues and origins
- Threat sources
- Risks
- Demonstration

A common misconception

- No practical Bluetooth vulnerabilities
- The core Bluetooth protocol has maintained its integrity
- A correctly implemented Bluetooth stack should have no vulnerabilities
- Analogy: Blaming TCP/IP for an IIS vulnerability

So what are the issues

- RFCOMM services
- Host Bluetooth implementation
- Most major Bluetooth platforms have vulnerabilities

Specifics

- Bad host stack implementation
- Incorrect IrMC filesystem permissions
- Badly implemented services
- Open channels

Vulnerability origins

- Bad coding practices when developing RFCOMM services
- Lack of knowledge regarding Bluetooth or other (OBEX) security protocols
- Re-use of older services for different protocols
- “Bluetooth is secure” - just plug in and go

Affected devices

- A small number of Bluetooth implementations are common across many platforms
- The most popular devices are vulnerable
- Result is a large number of affected devices in public
- Tests show between 85% and 94% vulnerability

IrMC permissions

- IrMC defines a set of access permissions for common objects
- Objects viewable on non-paired services
- Permissions not followed
- Intentionally open
- Allows exploitation of open IrMC services

Stack/Service errors

- Failures in basic stack implementation
  - Buffer overflows
  - Manufacturers have chosen to ignore and not release patches
- Failures in Service implementations
  - OBEX length checking
  - OBEX packet integrity
  - NULL termination

Hidden services

- Highly privileged services left open but hidden
- Back channels for other devices “to make life easier”
- Complete access to AT command set and therefore mobile equipment

Availability

- Knowledge of the vulnerabilities and exploits is common
- Numerous applications can exploit
  - btscanner, btxml, Gnokki, OpenOBEX, Redfang,
  - … and many more

Public Discussion 1

- June 2003.
  - Ollie Whitehouse releases Redfang
- October 2003
  - Bruce Potter talks on Bluetooth vulnerabilities at Defcon
- October 2003
  - Grimm, Holtmann and Vedral discuss Bluetooth OBEX vulnerabilties, later known as Bluesnarfing
  - Pentest Limited release btscanner

Public Discussion 2

- November 2003
  - 'Bluejacking' comes to public attention
  - AL Digital authors advisory on mobile phone “Bluetooth” vulnerabilities. Coined “Bluesnarfing”
  - Pentest Limited release a followup advisory
- February 2004
  - Pentest Limited release Nokia DoS advisory
  - Multiple “Bluetooth vulnerability” articles

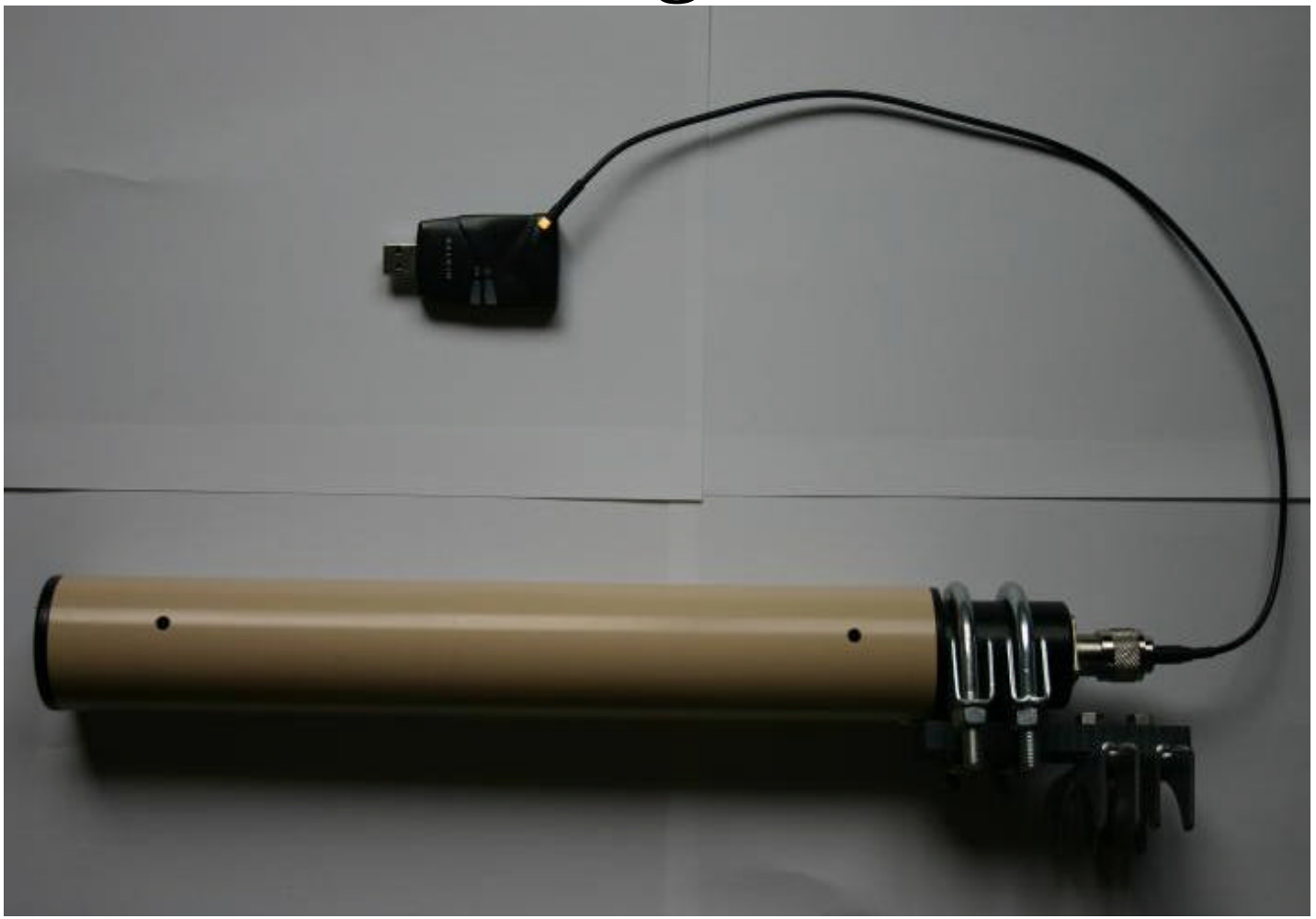
Public Discussion 3

- March 2004
  - Integralis release Nokia and Ericsson Serial profile advisory
  - Martin Herfurt scans for Bluesnarfing vulnerabilities at CeBIT
- June 2004
  - Pentest Limited and A.L. Digital give talks at Wicon
- August 2004
  - Pentest Limited release Widcomm vulnerabilities

Myths debunked

- *Bluetooth needs pairing*
  - Not in all cases. Vulnerable services generally do not.
- *Short range*
  - No, standard dongles have a much greater range than advertised. Easy to modify dongles
  - http://www.pentest.co.uk/documents/bt_dongle_mod/bt_dongle_mod.html
  - 1.1 Miles (1.77 km) achieved

Modified Dongle



More myths debunked

- *Only mobile devices affected*
  - False. More serious vulnerabilities exist for PCs.
- *Non-discoverable saves me*
  - Again, not really. It only makes exploits more difficult.
  - Device is sometimes less secure in non-discoverable mode.
- *Secure, as Encryption is used*
  - Encryption is only active if you ask for it (certain profiles require it)

Threats

- Am I vulnerable?
- Who is a threat?
- What is the impact?

Am I vulnerable?

- Both individuals and Corporations
- Owners of various popular phones. Nokia 6310, Ericsson T6x0
- PC owners (Not SP2 Bluetooth as yet)
- IpaQ, and other PocketPC owners
- Symbian device owners
- Embedded devices, Bluetooth heating systems etc.

Who is a threat

- Individuals
  - Large scale scammers
  - Advertisers
- Corporate
  - Dedicated crackers
  - Groups/Individuals with precise goals

Impact

- What exploits are possible
- What exploits exist

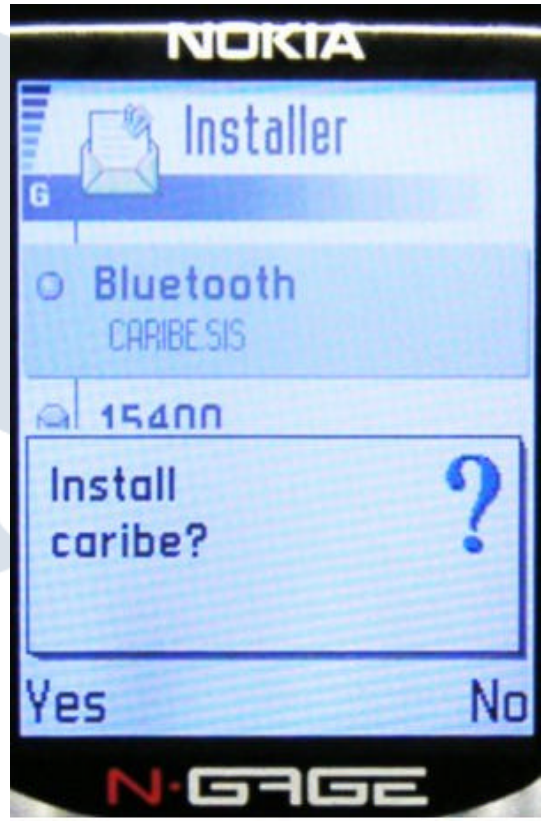
What is possible

- Theft of information, personal or corporate
- Device DoS
- Remote code execution
- Corporate espionage
- Airborne viruses or worms
- Unwittingly introduce un-firewalled network connections

Worms already exist!

- PocketPC(Duts/Dust) and Symbian (Cabir)
  - “Nice”; asks permission before installing
  - No real damage other than battery
  - Only PoC ... so far
- More virulent worms could attack open services
- Exponential rate of infection
- No ability to track the origins

Worm pictures



Copyright F-Secure Corp. 2004

Impact on Individuals

- Information theft by advertisers
- Location based SPAM
- ID theft (IMEI, contacts, appointments)
- Theft through billing
- Call theft

Corporate Impact

- Information theft
- Corporate espionage
- Bribery
- News/Media investigators

Law enforcement

- 6 degrees database of targets
  - Phonebook
  - Call history
- Tracking of individuals
- Device data
  - Phone number
  - IMEI
  - Any file on the device

Demonstration

- Please turn off Bluetooth
- Btscanner 2
- AT command exploit
- OBEX DoS exploit