State of Bluetooth Security

By:

- Peter Zebühr
- Joakim Karlsson

Background

- Developed by Bluetooth Special Interest Group formed in 1998.
- Original members was Ericsson, Nokia, Intel, IBM and Toshiba.
- Became a standard in the summer of 1999.

Modes of Security

- Security mode 1:
  - No active security enforcement.
- Security mode 2:
  - Service level security.
  - On device level no difference to mode 1.
- Security mode 3:
  - Link level security.
  - Enforce security for every low-level connection.

Bluetooth CIA

- Confidentiality
  - Possibility to read data.
- Integrity
  - Possibility to modify data.
- Availability
  - Possibility to delete data.
- Authentication
  - Possible to bypass completely.

Bluetooth Attacks - 1

- BlueStumbler (2003)
  - Getting hold of data anonymously. E.g. Address book, calendar and pictures.
  - Bug in the implementation.
- BlueSnarf
  - Pull known objects from OBEX PUSH channel.
  - No authentication required.

Bluetooth Attacks - 2

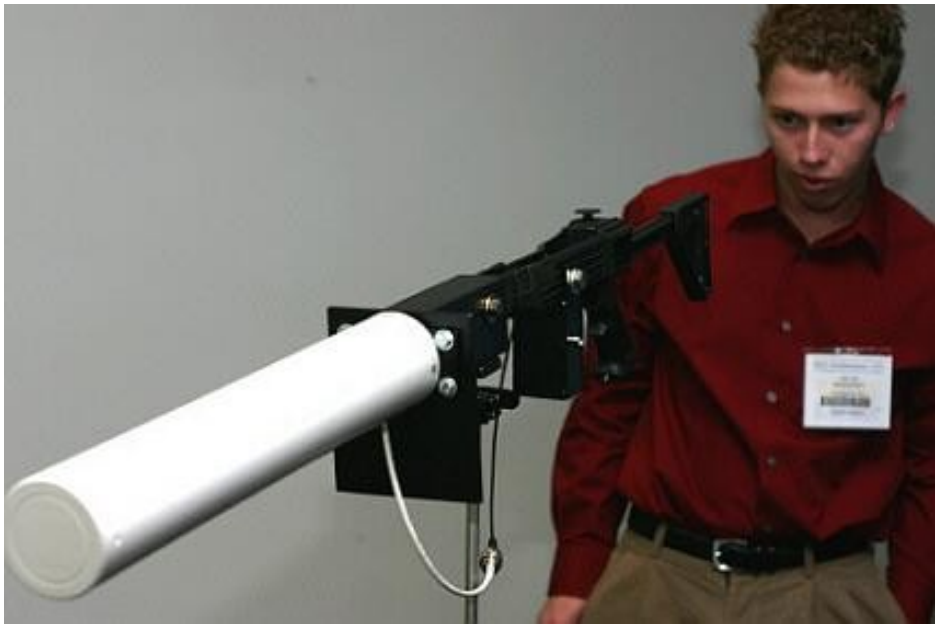
- BlueBug (2003/2004)
  - Initiate phone calls, read/send SMS, read or write to phone book, set call forward ...
  - Found when trying to replicate BlueSnarf.
  - Bug in the implementation.
- HeloMoto
  - Exploits weakness to be added as a trusted device without interaction.
  - Connects as headset and can execute AT commands (as BlueBug).

Cracking the PIN

- First know attack on the protocol.
- Decrypt all traffic.
- Our implementation finds four digit PIN in 0.7s.

#	Src	Dst	Data	Length	Notes
1	A	B	*IN_RAND*	128 bit	plaintext
2	A	B	LK_RAND_A	128 bit	XORed with K_{init}
3	B	A	LK_RAND_B	128 bit	XORed with K_{init}
4	A	B	AU_RAND_A	128 bit	plaintext
5	B	A	*SRES*	32 bit	plaintext
6	B	A	AU_RAND_B	128 bit	plaintext
7	A	B	*SRES*	32 bit	plaintext

BlueSniper



- First presented at DEFCON, LA 2004.
- Extends the attack range for attacks.
- From 10m to 1,78km.

Summary

- As mobiles continue to merge with PDAs more and more sensitive information is accessible.
- BT weaknesses are in most cases caused by bad implementations.
- The BT pairing process is limited because of the use of short PIN codes.

Mobile Poker over BT

- D3 project this year.
- Secure Texas Hold 'em written in Jif.

http://www.dtek.chalmers.se/~tox/d3proj/

The End

Thank you!