Blue Track

Imperceptible Tracking of Bluetooth Devices

Motivation

- Bluetooth de facto standard for short-range wireless communication of mobile devices
- Often enabled by default and never turned off by users
- Can Bluetooth devices be tracked imperceptibly?
- What are the implications for user privacy?

Approach

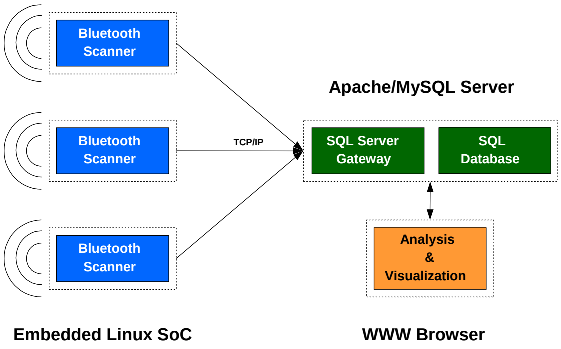
- Distributed periodic search for Bluetooth devices
- Results forwarded to a central database
- Tracking by concatenation based on unique Bluetooth device addresses
- Web-based analysis and visualization

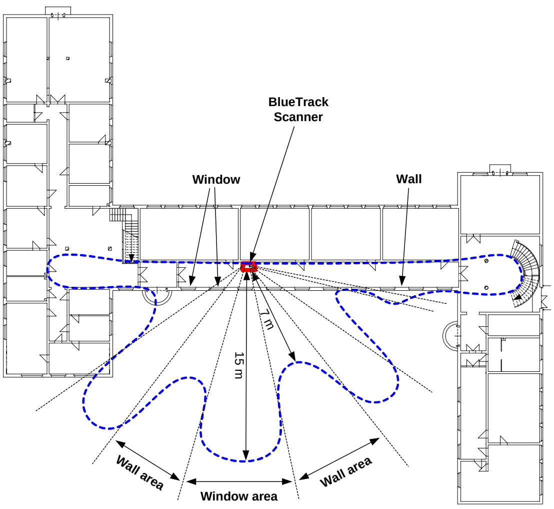
Results

- CeBIT 2004: total 5294 devices (7 days) and 500 devices during a 4-hour walkabout
- Devices detectable within 2 seconds
- 1% of detected devices disclose real user name
- Personalized traces recorded

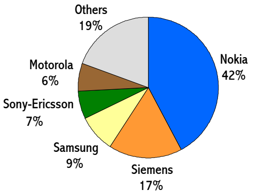
Implications

- Bluetooth devices can be (mis)used to track people imperceptibly
- Bluetooth tracking information is neutral as long as it can't be linked to a natural person
- Commercially available Bluetooth devices are vulnerable against malicious attacks

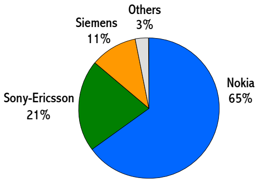




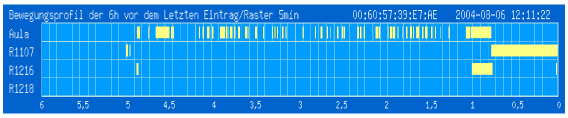
Market-Shares Mobile Phones 3rd Quarter 2003, Western Europe



Detected Devices at CeBIT2004



Personalized Trace



University of Rostock

Faculty of Computer Science and Electrical Engineering

Marc Haase, Matthias Handy, Dirk Timmermann