BlueTrack – Imperceptible Tracking of Bluetooth Devices

Marc Haase, Matthias Handy
University of Rostock
Richard-Wagner-Str. 31
18119 Rostock-Warnemünde
+49 381 4983535
[marc.haase, matthias.handy]@etechnik.uni-rostock.de

ABSTRACT
Bluetooth enabled devices are potentially vulnerable against passive tracking attacks because of their unique and invariant device address. The contribution of this paper is the exploration of tracking vulnerability of Bluetooth devices. We implemented BlueTrack, a tracking system based on off-the-shelf components. We tested our system at two sites, at a university building with several lecture rooms and at a CeBIT 2004 exhibition stand. The results show that astonishingly many Bluetooth devices can be detected and personalized traces can be recorded.

Keywords
Privacy Aspects, Bluetooth, Distributed Computing, Wireless Ad hoc networks

INTRODUCTION
Bluetooth is a short range wireless communication technology for home, office and mobile ad hoc networks. The main objective of the Bluetooth Special Interest Group (SIG) was to develop a cable replacement radio technology for mobile devices. In the last two years Bluetooth has been successfully integrated into various mobile devices and handsets, e.g. mobile phones and personal digital assistants (PDAs).

Considering factory default settings of mobile devices, we observed that Bluetooth as a new feature is often enabled by default. Many users are not aware of the state of their devices. Furthermore, the user doesn't change the default setting because he wants to benefit from new Bluetooth capabilities, e.g. ad hoc PIM synchronization, mobile gaming and ad hoc messaging. The low power consumption of Bluetooth chipsets has not a great impact on battery life time and therefore the user is not induced to disable Bluetooth.

At first glance there is no need for the user to disable Bluetooth, however, each Bluetooth device is characterized by a unique and invariant device address. An active Bluetooth chipset in visible mode (Inquiry Scan Mode enabled) is disclosing the unique address to devices searching for Bluetooth devices, because this is the fundamental prerequisite for establishing Bluetooth connections.

At the same time this renders Bluetooth devices to be potentially vulnerable against passive tracking attacks. To explore the practical tracking vulnerability of Bluetooth devices we developed BlueTrack, a tracking system based on off-the-shelf components and installed it at two sites: at a university building with several lecture rooms and at the CeBIT 2004 on a university exhibition stand.

The poster contribution will present the Bluetooth tracking approach, the architecture and actual results from both sites.

APPROACH
The motivating question at the beginning of this research project was: Is it possible to imperceptibly track Bluetooth enabled mobile devices at public places? The research objective is to determine the implication on user privacy and to derive policies for mobile security management.

The tracking process is based on a periodic search for Bluetooth devices in the vicinity at different locations (inquiry procedure). As a result the inquirer gets a list with addresses of visible Bluetooth devices. Detected devices are tagged by a first-seen/last-seen timestamp and a location-stamp. All results are forwarded to a central tracking database and concatenated based on the unique Bluetooth device address (BDADDR).

The tracking system consists of distributed Bluetooth inquiry scanners connected to a central tracking MySQL database, a NTP server for time synchronization and an analysis and visualization front-end based on an Apache web server.

PRACTICAL RESULTS
We tested the BlueTrack-system at two locations: inside a university building and at the CeBIT 2004 on a university exhibition stand. The experimental setup of the first location (university) illustrates Figure 1. We used three fixed sensors attached to the ceiling with overlapping sensing regions and one mobile sensor (Compaq iPAQ). We monitored 359 different Bluetooth-devices over a period of 6 months. The temporal distribution of detections depicts Figure 2a. A result of a successful concatenation of a student attending two consecutive lessons is shown in Figure 2b.

We conducted the second experiment at a CeBIT 2004 exhibition stand with one fixed and one mobile sensor. We

detected more than 700 new devices per day (total count 5294 for seven days). With the mobile sensor we detected more than 500 devices during a 4-hour walkabout.

IMPLICATIONS

As long as the gathered information include only the fixed Bluetooth device addresses, date, time, and location, the results of the BlueTrack system do not compromise user privacy, because the traces can not be linked to a natural person. Based on this premise, beneficial tracking systems designed for anonymous users tracking purposes can be built on top of the BlueTrack architecture. The sensing process is fast enough to track passing devices.

However, beside the BDADDR a Bluetooth device holds a device name, which can be chosen by the user itself. Just like gathering the BDADDR the device name can be fetched imperceptibly. As we can see from our experiments 1% of users chose their real name as device name. At that point profound privacy threats arise, because BlueTrack traces can be linked to natural persons.

Indeed, giving a Bluetooth device an artificial name or a pseudonym, protects the user against passive attacks, however the BDADDR can be used to mount active attacks gathering personal information from mobile device, e.g. address book, calendar information. As mentioned in [2],[3] various Bluetooth devices are vulnerable against SNARF attacks. Approximately 70% of tracked devices at the CeBIT 2004 were potential candidates for malicious attacks.

FUTURE RESEARCH

Our future research activities focus on how to better protect the privacy of users of Bluetooth-enabled devices. How can users prevent unwanted tracking and what countermeasures have to be implemented? We embark on a strategy that changes static device characteristics into dynamic ones, keeps wireless silence and provides broadcast functionality.

At the same time we intend to look at the advancement of Bluetooth technology in terms of privacy threats. For example, the new Bluetooth standard 1.2 proposes an “Inquiry with RSSI” mechanism, that measures the signal strength of incoming FHS packets sent by devices that respond to the inquiry [1]. RSSI information can be used to locate Bluetooth-devices more accurate than our BlueTrack approach.

CONCLUSION

The deployed and tested BlueTrack system demonstrates that an imperceptible tracking of Bluetooth-enabled devices is feasible. The results show that astonishingly many Bluetooth devices that randomly pass the installed Bluetooth inquiry sensors can be detected and personalized traces can be recorded. Furthermore devices staying longer times at a certain location are susceptible to detailed scans exposing informational parameters, service profiles, or even personal data [2],[3].

REFERENCES

1. Specification of the Bluetooth System 1.2, Bluetooth SIG, 2003.
2. Ben Laurie Adam Laurie. Serious flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd., http://bluestumbler.org/, January 2004.
3. Martin Herfurt, BlueSnarf @ CeBIT 2004, Technical Report, Salzburg Research Forschungsgesellschaft mbH, 2004.

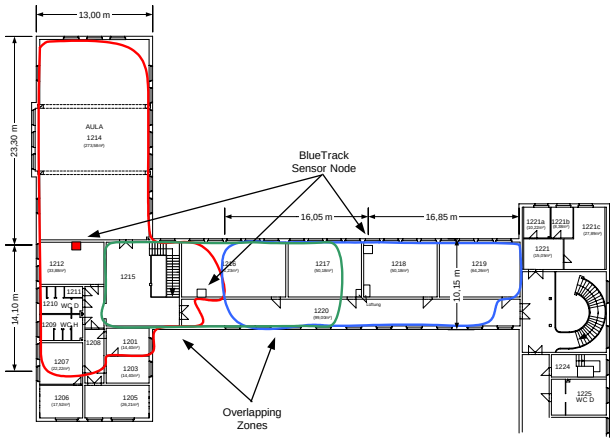

Figure 1: BlueTrack installation at the University

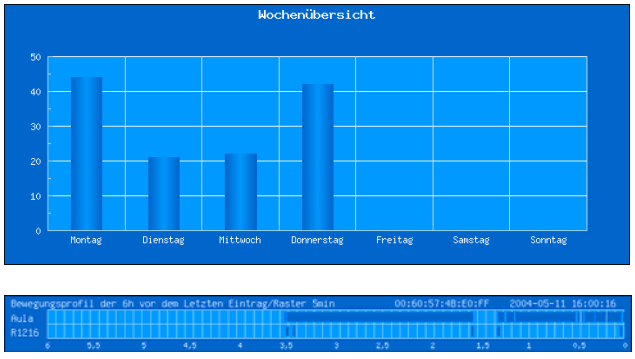

Figure 2: (a) Temporal distribution of detections at the University (top) and **(b)** a student’s detection profile (bottom)