Access Control Using Bluetooth

Authors – Marvyn Mei and Agus Salim
Supervisor – Dr. Tim Moors

This thesis project proposes a method of access control using Bluetooth. Currently access control methods require physical contact to a device, such as a swipe-card. Bluetooth is a wireless technology that could be used to replace such applications, and provide the convenience of wireless access control. The purpose of this thesis is to demonstrate that such a concept is feasible, by implementing one such application.

The application developed in this thesis involves regulating the access of people who enter a “silent” zone, by disabling the ringing tones of mobile phones that they carry. Such a policy is enforced by a Bluetooth access point situated in this “silent” zone. The access point will send out a “beacon” signal to the mobile phone, via Bluetooth, telling it to shut down its ringing tone. Another focus of this thesis is to ensure that this procedure is secure. Both the mobile phone and access point will have to carry out an authentication procedure, designed in this thesis.

With the success of this thesis, such a concept could be extended to other forms of access control applications.

1. What is Bluetooth?
Bluetooth is a short range wireless radio that operates in the 2.4 GHz band. It is embedded in many of today’s mobile devices, such as mobile phones (e.g. the Sony Ericsson P800 used to develop our prototype) and personal digital assistants.

2. Advantages of Bluetooth
• Low power consumption
• Noise resilience
• Inherent security features

The security features makes it hard to listen to data transmissions. However, Bluetooth security is insufficient for this thesis because it does not stop other Bluetooth devices from “attacking” the system. An additional application-layer authentication protocol will be needed to filter out these malicious users.

3. Mobile Phone
The mobile phone starts off by listening for incoming connections. Once a connection is established, the authentication procedure is carried out. If successful, the mobile phone turns off its ringing tone and continues to scan for the access point, to determine if it is still within its coverage area. If it is not, the mobile restores its ringing tone.

4. Access Point
The access point first scans for all nearby Bluetooth devices in its vicinity. If it finds any Bluetooth devices, it attempts to authenticate with them. Once authenticated, it stores the Bluetooth addresses of these devices into its database, so that it does not repeat the procedure with these devices. Up to seven devices can be authenticated simultaneously.

5. Authentication Protocol
An application-layer authentication protocol was designed to secure communications between the mobile phone and access point, and so prevent denial of service attacks (e.g. someone impersonating an access point and so “unlawfully” disabling the ringing tones of mobile phones. It uses the RSA algorithm for encryption, and also adds a “nonce” to prevent playback attacks to the system.

Conclusion
This thesis has successfully demonstrated the use of Bluetooth in an access control application. Although a commercially viable solution may take some time to materialise, this concept is an interesting idea that may someday lead to a practical solution.