A Trusted Device to Secure a Bluetooth Piconet

[Published in *Proc. of Gemplus Developer Conference*, Paris, France, June 20–21, 2001.]

Ludovic Rousseau, Christophe Arnoux, and Cédric Cardonnel

GEMPLUS, B.P. 100, 13881 Gémenos cedex, France
{ludovic.rousseau, christophe.arnoux, cedric.cardonnel}@gemplus.com

1 Introduction

Bluetooth [6] is a wireless protocol used for short-range communications. The Bluetooth devices talking to each other form a piconet. A piconet is composed of one master device and up to seven slave devices. The master device is not the most powerful one but just the one initiating the connection. Two or more piconets form a scatternet.

All these Bluetooth devices use cryptographic keys to guarantee confidentiality, integrity and authentication between the devices. The problem is there is nothing in the Bluetooth specifications about the management of all these cryptographic keys. Also there is nothing about a security policy inside a piconet or between two piconets. However a white paper describing a security manager [4] is available. We propose to improve the security policy described in this document and to implement such a security manager.

Bluetooth devices will generally be personal objects with strongly personal data. It is very important to define and control which device will have access to which other device. This is the problem we propose to tackle.

2 Bluetooth Security

The security FAQ on the Bluetooth Web site [5] is very short:

> "Are transmissions secure in a business and home environment?
> Bluetooth wireless technology has built-in sufficient encryption and authentication and is thus very secure in any environment. In addition a frequency-hopping scheme with 1600 hops/sec is employed. All of this, together with an automatic output power adaptation to reduce the range exactly to requirement, makes the system extremely difficult to eavesdrop."

We have different security problems here:

- The *automatic output power adaptation* is not enough to forbid eavesdropping. It will limit the ease of eavesdropping and augment the size and power consumption of the antenna used to eavesdrop but will not forbid it. Only cryptography can be used to make eavesdropping useless.

– Bluetooth provides a *sufficient encryption and authentication* scheme. This is not true when two devices have never met each other and have no shared secret or other way to authenticate.

2.1 Key exchange

The key exchange in Bluetooth is based on a PIN from 1 to 16 bytes long. "Typically, it may consist of only four decimal digits" [6, page 152]. The use of a short PIN code is the result of a limited man-machine interface for some very small Bluetooth devices.

All the security of the generated keys is based on the knowledge of this PIN. A different shared PIN should be used for each pair of Bluetooth devices.

2.2 Security problems

Some Bell Labs researchers have already pointed out some security weaknesses in version 1.0B of the Bluetooth protocol [3]. The attack found can either search the PIN exhaustively (this is very fast with a 4-digits PIN) or mount a man-in-the-middle attack to steal the authentication and encryption keys used between two Bluetooth devices.

3 The Solution: a Trusted Device

As you can see the security of Bluetooth depends greatly on the secrecy of the PIN. Unfortunately some devices will not have a man machine interface to enter a PIN code and it will be very tiring to enter a PIN code for each new Bluetooth device. The default PIN may even be 0000 in some cases.

We propose to simplify the management of all the PIN codes by using a device devoted to this task: a SmartManager. This device is in charge to securely establish a secret shared PIN code with each devices of the user's piconet.

3.1 Secure PIN exchange

To securely exchange a PIN between two devices we use a Bluetooth secure bubble [1]. We consider the bubble is secure by limiting the emitting radio range to a few millimetres around the antenna. In fact the emission power will grow up to be able to contact the other device or reach the limit of a few millimetres. The two devices exchanging the shared PIN code will need to be physically in contact or very close.

Furthermore this mode will only be activated by the user using a physical button. Pairing two Bluetooth devices will only take place one time and we can make the assumption that an attacker will not be present at that time with a very big antenna to eavesdrop the communication.

4 Security Policy

The security policy defines which device has access to which one and for what kind of access.

For each of my devices my SmartManager will store:

- What other device is allowed to access it;
- Is this access subject to an acceptance from the user or is it automatic;
- The key generated for this access is permanent or transient;
- Etc.

4.1 User interface

The user can authorise or not the connection of a new device to his piconet. The SmartManager need to interact with its user. We then need a small screen and at least two buttons: Yes, No.

To edit the security policy a more complex interface may be required. We could plug a keyboard and a screen on a USB connector of the SmartManager.

We cannot use a windows program on a PC since this platform is far from being secure. The security policy the user is editing must be the one stored in the SmartManager. The user shall only use trusted hardware and software to edit its security policy.

4.2 Secure storage

The security policy and all the secrets managed by the SmartManager are stored in a smart card. This protects the secret when the SmartManager is switched off. The user has to enter a PIN code to unlock the access to the data stored in the smart card.

The use of a smart card also facilitates the deployment of SmartManager in a company. Each employee has a SmartManager allowing him to access corporate Bluetooth devices. The security policy and initial pairings can easily be done off line in batch mode for smart cards. The SmartManager device is generic and only the smart card contains the configuration.

5 Access Rights Delegation

The role of the SmartManager is to allow or forbid the communication between two Bluetooth devices. In many cases this authorisation may not be forever. For example I may allow you to use my headset for one of your communication but you should not be able to ear my communications afterwards.

My SmartManager will give you a key valid only for a period of time. The decision to accept or deny a communication by my SmartManager is defined in my security policy. The decision to extend the validity of the session key after expiration is also defined in the security policy. The Fig 2 describes this protocol.

6 Our Reference Piconet

During the entire article, we will illustrate our analysis with examples. All these examples will reuse the same reference piconet:

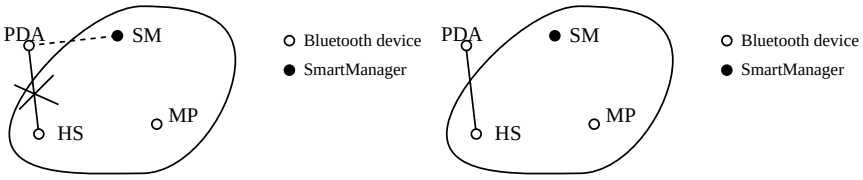
- A SmartManager (SM1)
- A Mobile Phone (MP)
- A Headset (HS)

This Piconet will evolve at the contact of other Bluetooth devices:

- A second SmartManager (SM2)
- A Personal Digital Assistant (PDA1)
- An second Personal Digital Assistant (PDA2)
- A third SmartManager (SM3)

7 One Piconet

A new Bluetooth device cannot communicate with a device of a piconet without being recognised and accepted by your SmartManager.



Before After

In this example, the piconet's owner wants to add a PDA in his piconet. The first task is pairing the PDA and the SmartManager. This step is described in Fig 1.

The communication between the PDA and the Headset (to play music for example) is not allowed until the user permit the security policy change. This update will respect the protocol described in Fig 2.

Now, the PDA can directly communicate with the Headset without the mediation of the SmartManager. This protocol chain is the only possibility, for an external Bluetooth device, to communicate with an internal device.

During the communication rights attribution, the user gives a parameter called "duration". This field will contain the key validity time. If the new device is an external device that must have a temporary permission, this value fixes the duration of this permission. If the new device will permanently integrate the piconet, this value may contain a special value "Unlimited" for example.

You will only have to exchange a PIN code between your new Bluetooth device and your SmartManager to allow it to communicate with any other device of your piconet.

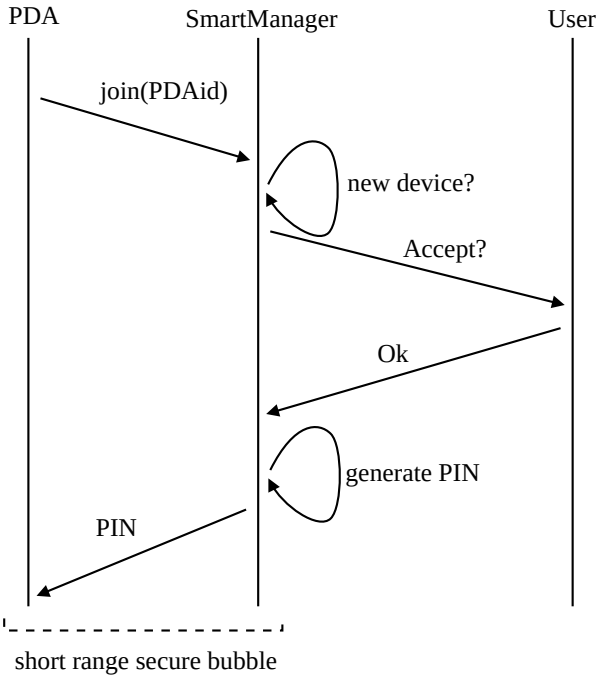


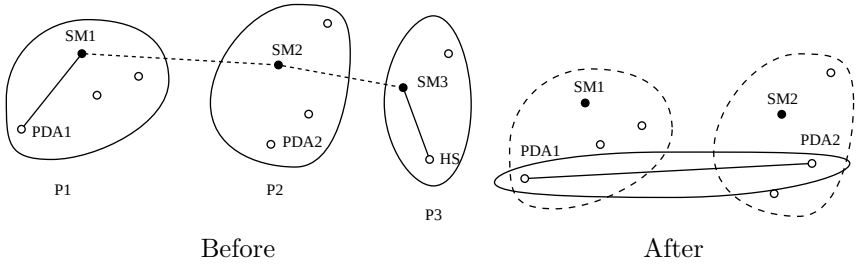
Fig. 1. Pairing

The secure pairing between the new device and the SmartManager will be used to transfer a secret shared key (if the security policy allows it) between the new device and one other Bluetooth device of the piconet.

The trusted SmartManager is the only interface with devices from outside the piconet.

8 Two Piconets

The communication between two piconets is controlled by the SmartManagers of both piconets.



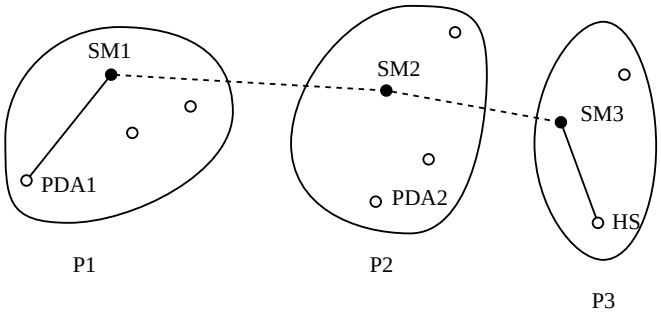
To illustrate this chapter, we will take the case of two PDAs, in two different piconets, which have to communicate together.

Once the two SmartManagers are paired and a new connection key (with a "duration" parameter) is generated by the called SmartManager (SM2) for its PDA (PDA2). This key is sent to SM1, that will relay it to PDA1. Now PDA1 and PDA2 share a secret that permits communication. They form a new piconet (PDA1 may be the master and PDA2 the slave). See Fig 3 for a description of the protocol.

This configuration avoid the situation where two people with their own piconet are in relation, it may not desirable that the GSM phone of one person will use the headset of the other.

9 Three Piconets

The case three piconet is a generalisation of the previous case.



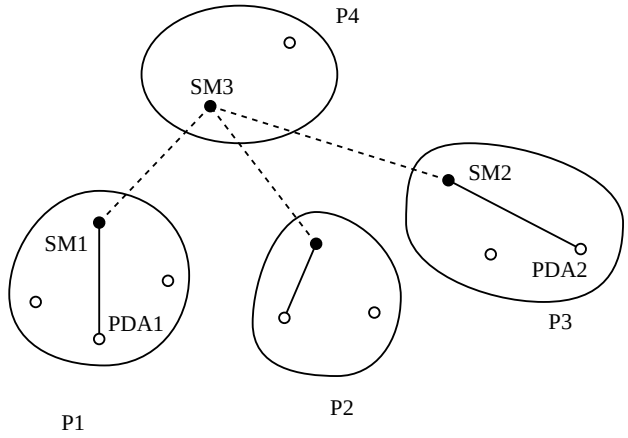
The piconets P1 and P2 are already in relation. The piconets P2 and P3 are also already in relation. But the piconets P1 and P3 do not know each other yet. P2 is the intermediate between P1 and P3.

The trust relationships may not be transitive. For example SM3 may not trust SM2 to introduce SM1. SM3 may suspect a man-in-the-middle attack.

The access rights are not transitive either. If SM3 allows PDA2 from P2 to use the Headset HS of P3, PDA2 cannot give this right to PDA1 from the piconet P1.

9.1 Hierarchy

We can even improve our scheme. It may be easier and faster to use a hierarchy of SmartManagers to link many people.



For example, in a company, if every salesman have a personal piconet like our reference one. The PDA contains a phonebook with all the customers and employees phone numbers. If the telecommunication team wants to update this phonebook, it can use special devices locates in the company, that will become "Super" SmartManagers. This SM3 will establish a connection with each SmartManager. Then, it will be able to update PDA's phonebooks.

10 Conclusion

A SmartManager as described here allows managing all the interactions between Bluetooth devices. Bluetooth devices will be personal objects and those objects will contain personal information. It is very important to control the communications between our devices and the other ones. The SmartManager gives the possibility to realise this barrier. It will define a security bubble where personal devices and data will be protected from external connections.

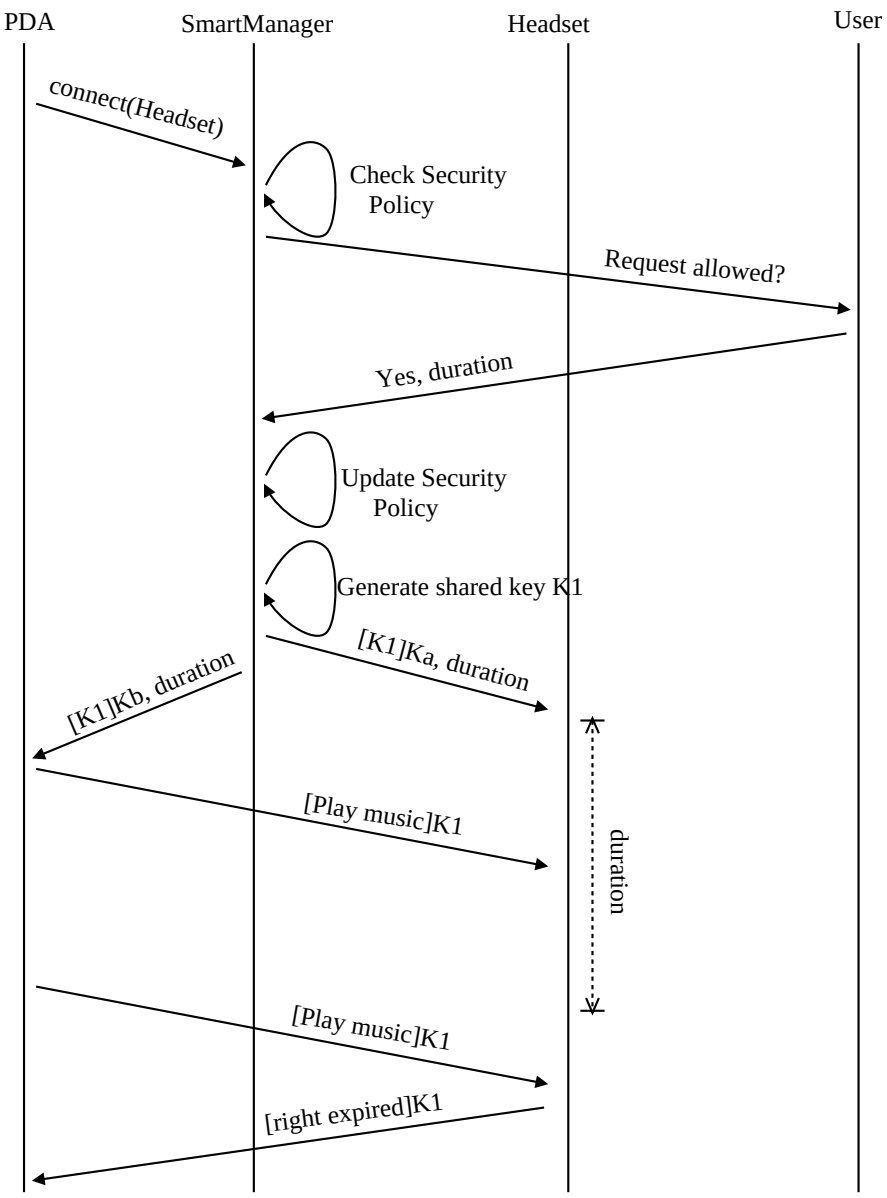
Today we can devise a SmartManager as a small personal device (like a pager), with a small screen and two or three buttons (to select the duration and accept or refuse connections). In the future, the SmartManager function may be included inside a personal device that everybody keeps with him all the time (watch, mobile phone, etc.).

The SmartManager, as an independent device, can also provide other security services. For example the SmartManager can detect and identify objects entering and leaving a predefined range [2]. This can trigger an alarm if an object is leaving the range without "authorisation" because the object is being stolen. This proximity feature may also be used to automatically lock your computer when you are out of the range.

References

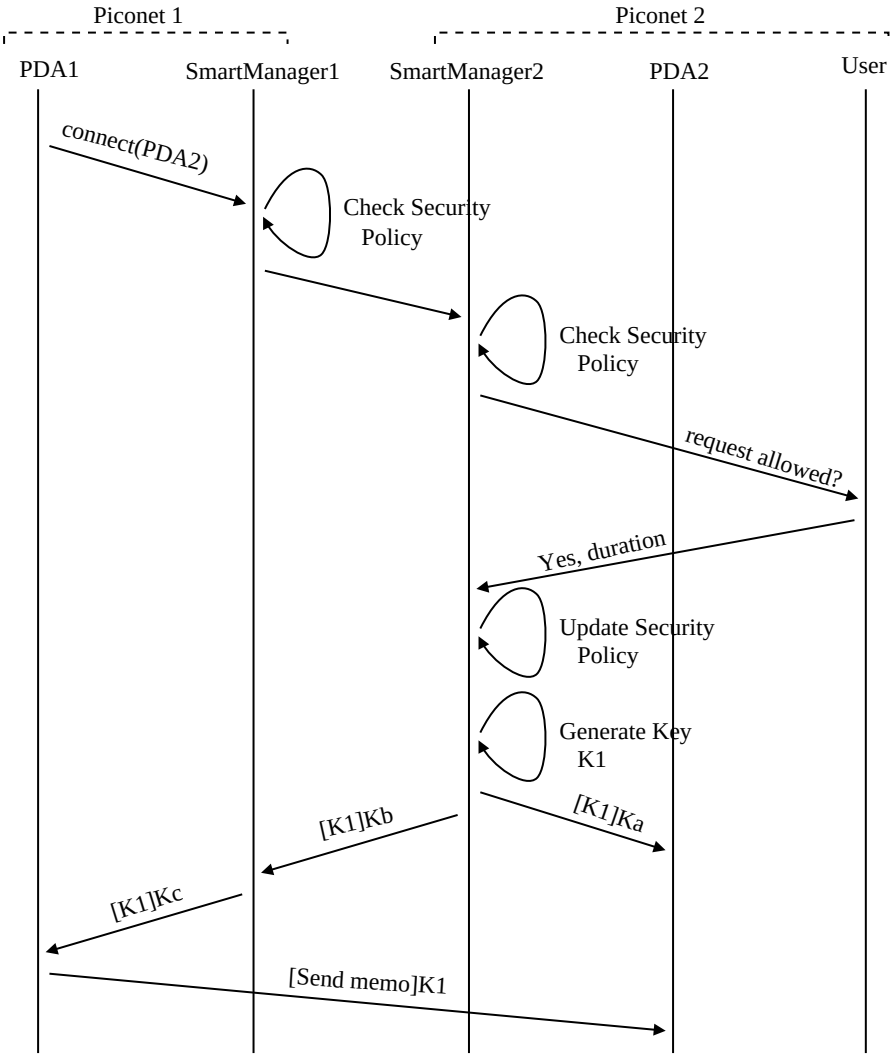
1. Christophe Arnoux. Procédé de reconnaissance sécurisée entre deux appareils d'un réseau radiofréquence. Patent, 2000.

2. Bluetags A/S. The bluetag travel. Available at <http://www.bluetags.com/html/product_concepts/travel.html>, 2001.
3. Markus Jakobsen and Suzanne Wetzel. Security Weaknesses in Bluetooth. In *RSA Conference 2001*, San Francisco, California, USA, 8 - 12 April 2001. Available at <http://www.bell-labs.com/user/markusj/bt.html>.
4. Thomas Müller. Bluetooth Security Architecture. White Paper, available at <http://www.bluetooth.com/developer/download/download.asp?doc=174>, 15 July 1999.
5. Bluetooth SIG. FAQ - Security. Available at <http://www.bluetooth.com/bluetoothguide/faq/5.asp>.
6. Bluetooth SIG. Specification of the Bluetooth System. version 1.1, available at <http://www.bluetooth.com/developer/specification/specification.asp>, 22 February 2001.



Ka : shared key between Headset and SmartManager
Kb : shared key between SmartManager and PDA
K1 : session key between PDA and Headset

Fig. 2. Connect PDA and Headset



Ka: shared key between SM2 and PDA2
Kb: shared key betwenn SM2 and SM2
Kc: shared key between SM1 and PDA1
K1: session key between PDA1 and PDA2

Fig. 3. Connect two PDAs