Relay Attacks on Bluetooth Authentication and Solutions

Albert Levi[1], Erhan Çetintaş[2], Murat Aydos[3],
Çetin Kaya Koç[4], and M. Ufuk Çağlayan[5]

[1] Sabanci University, Fac. of Eng. & Nat. Sci., Orhanli, Tuzla, TR-34956, Istanbul, Turkey
levi@sabanciuniv.edu
[2] TUBITAK – UEKAE, National Research Institute of Electronics and Cryptology
Gebze, TR-41470, Kocaeli, Turkey
cetintas@uekae.tubitak.gov.tr
[3] Pamukkale University, Dept. of Computer Engineering, Denizli, TR-20020, Turkey
maydos@pamukkale.edu.tr
[4] Oregon State Univ., School of Electr. Eng. & Comp. Sci., Corvallis, OR 97331 USA
koc@ece.orst.edu
[5] Boğaziçi University, Dept. of Computer Engineering, Istanbul, TR-34342, Turkey
caglayan@boun.edu.tr

Abstract. We describe relay attacks on Bluetooth authentication protocol. The aim of these attacks is impersonation. The attacker does not need to guess or obtain a common secret known to both victims in order to set up these attacks, merely to relay the information it receives from one victim to the other during the authentication protocol run. Bluetooth authentication protocol allows such a relay if the victims do not hear each other. Such a setting is highly probable. We analyze the attacks for several scenarios and propose practical solutions. Moreover, we simulate attacks to make sure about their feasibility. These simulations show that current Bluetooth specifications do not have defensive mechanisms for relay attacks. However, relay attacks create a significant partial delay during the connection that might be useful for detection.

1 Introduction and Background

Bluetooth [1] is a promising short-range radio link technology for wireless connectivity of portable electronic devices, such as mobile phones, laptop computers, palm computers and digital cameras. The Bluetooth system operates in the 2.4 GHz ISM (Industrial Scientific Medicine) band. In order to avoid interference with other piconets (piconet is Bluetooth's personal/local area network) and/or other devices using the ISM band, the master of a piconet synchronizes its slaves to hop among several RF channels in a pseudo-random sequence.

Bluetooth specification defines link level security mechanisms to provide confidentiality, integrity and authentication between Bluetooth devices. However, there are some vulnerabilities in the Bluetooth security as proposed in [2, 3, 4].

In this paper, we point to relay attacks on Bluetooth authentication protocol. In relay attacks, the attacker places itself in two distinct piconets and picks two victims, one in each piconet. The attacker impersonates those victims by forwarding

C. Aykanat et al. (Eds.): ISCIS 2004, LNCS 3280, pp. 278–288, 2004.

authentication messages generated by one of them to another between the piconets. As opposed to the man-in-the-middle attacks described in [2], the attacker does not need to know any shared secret between the victims in order to set up our relay attacks. We simulate relay attacks to assess their feasibility. Moreover we use simulation to evaluate the delays caused by the attack and to see if these delays could be used as a detection mechanism. We propose two other low-cost solutions as well.

The rest of Section 1 gives an overview of Bluetooth key management and authentication scheme. Relay attacks are explained in Section 2. Mechanisms to detect relay attacks are proposed in Section 3. Simulation results are presented in Section 4. Conclusions and some discussions are in Section 5.

1.1 Key Management and Authentication in Bluetooth

There are several key types in Bluetooth, but the attacks described here depend on the initialization and combination keys. Initialization key (K_{init}) is calculated at both sides of communication using a pre-shared PIN, a random number and a Bluetooth Device Address (BD_ADDR). K_{init} is used to exchange the *Combination Key*, which is one of the members of the Bluetooth "Link Key" family. These keys are used for authentication. Both ends of communication, say *A* and *B*, contribute to the combination key (K_{AB}) in a secure way by encrypting some random numbers. Current link key or K_{init} is used as the key for this encryption. Link keys are stored in Bluetooth devices and they are reused whenever necessary.

Bluetooth uses a simple challenge-response authentication scheme. The verifier sends a 128-bit random number called AU_RAND to the claimant. Claimant calculates the authentication response called SRES, which is a cryptographic function of AU_RAND, its own BD_ADDR, and the current link key. Claimant sends SRES to the verifier. Meanwhile the verifier computes the same SRES and checks whether the computed one is equal to the received one. If so, that means the claimant is really who it claims to be.

2 Relay Attacks

In this section, we describe relay attacks proposed in the paper. In the relay attacks, adversary *C* talks to victim *A* posing as victim *B*, and to *B* posing as *A*. All authentication messages that *C* needs are generated by real *A* and *B*. *C* conveys these messages from *A*/*B* to *B*/*A*. We present two types of relay attacks: (i) two-sided, and (ii) one-sided. In a two-sided relay attack, both victims are impersonated. In a one-sided attack, only one victim is impersonated.

In [2], some man-in-the-middle and impersonation type of attacks are proposed where the attacker knows or can guess the PIN or existing link key between victims. Relay attacks are similar to man-in-the-middle attacks. There exists an adversary located between the sender and receiver, but the only activity of the adversary is to relay information that it receives from one to another without changing the content. Unlike the attacks in [2], the adversary does not need to know a shared secret.