Formal Modeling and Analysis of the Bluetooth 4.0 Pairing Protocol

David (Wei) Jia
Stanford University
djia@stanford.edu

Richard Hsu
Stanford University
rhsu@cs.stanford.edu

ABSTRACT

Bluetooth is a wireless technology for exchanging data over short distances and is built into many of the devices used in daily life such as smartphones and laptops. For devices to actually communicate through Bluetooth the devices must establish a pairing. The pairing is done through Bluetooth's pairing protocol known as Secure Simple Pairing (SSP) which has been established since Bluetooth 2.1+. We employ a model checker to verify the design properties of the pairing protocol used in the latest iteration version 4.0 of Bluetooth. We demonstrate already known attacks on Bluetooth 4.0 SSP and discuss a new attack found by our model and discuss the implications and begin a discussion on the possible fixes that could be employed. Through this formal modeling we expand on the verification process of securing the Bluetooth pairing protocol.

1. INTRODUCTION

Bluetooth is a wireless technology that is ubiquitous in our computing world. Many users rely on it to transfer data between smartphone devices, laptops, on-board car systems, and headsets. Bluetooth technology also exists in more peripheral items such as printers, mice, keyboard, and speakers. Due to the proliferation of the concern of data security, any communication channel should be thoroughly tested for security. Therefore focusing on Bluetooth, we want to be sure that the Bluetooth pairing protocol and communication channels are secure as any compromise to the system can cause confidential information to be exposed.

We focus our attentions on the Bluetooth 4.0 Protocol [**?**] which is the most recent version implementation of the technology at the time of writing.

2. RELATED WORKS

Because of BluetoothÕs prevalence and the emergence of mobile technology, several related works have been done in an effort to analyze the security of Bluetooth. Most recently, in 2010, Phan and Mingard [3] analyzed the Bluetooth 4.0 protocol in ÒAnalyzing the Secure Simple Pairing in Bluetooth v4.0Ó which hand modeled and analyzed Bluetooth 4.0 and described three Man in the Middle (MitM) attacks for the NC and PE modes. In their 2007 paper, ÒFormal Analysis of Authentication in Bluetooth Device PairingÓ, Chang and Shmatikov [4] modeled Bluetooth 2.0 using ProVerif cryptographic protocol verifier and verified a known guessing attack and discovered a potential vulnerability which produces concurrent execution of authentication. Similarly, Haataja and Toivanen [8] discussed in ÒPractical man-in-the-middle attacks against bluetooth secure simple pairingÓ two more MitM attacks on Bluetooth 2.0 handsets and hand-free devices as well as modeled a vulnerability on the OoB mode given that the attacker has visual contact to the victim devices. Other papers are more general and informative, presenting a high-level view of the Bluetooth protocol, or suggesting potential vulnerabilities and risks associated with Bluetooth without providing formal analysis or proof.

While these papers present a good starting point for modeling Bluetooth 4.0, they are insufficient. First, many of the analysis of Bluetooth are either not formal or performed on outdated versions, such as v2.x. The most up-to-date analysis of Bluetooth 4.0 by Phan and Mingard encapsulated a formal analysis of only the NC and PE modes without formal modeling with a cryptographical tool such as Murphi. Furthermore, the paper focused on MitM attacks between only two pairing devices, and did not discuss eavesdropping, denial of service attacks, or multiple devices.

6. ANALYSIS, RESULTS, AND DISCUSSION

7. CONCLUSIONS

8. REFERENCES

[1] Bluetooth, SIG. Bluetooth core specification v4.0.30. `https://www.bluetooth.org/Technical/Specifications/adopted.htm`, June 2010.