Pervasive and Mobile Computing 5 (2009) 734–749

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

A comparative study of secure device pairing methods☆

Arun Kumar[a], Nitesh Saxena[a], Gene Tsudik[b], Ersin Uzun[b,*]

[a] Computer Science and Engineering Department, Polytechnic Institute of New York University, United States

[b] Computer Science Department, University of California, Irvine, United States

ARTICLE INFO

Article history:
Received 1 March 2009
Received in revised form 6 June 2009
Accepted 3 July 2009
Available online 18 July 2009

Keywords:
Usable security
Device pairing
Human-assisted authentication
Man-in-the-middle attacks
Key agreement

ABSTRACT

"Secure Device Pairing" or "Secure First Connect" is the process of bootstrapping a secure channel between two previously unassociated devices over some (usually wireless) human-imperceptible communication channel. Absence of prior security context and common trust infrastructure open the door for the so-called *Man-in-the-Middle* and *Evil Twin* attacks. Mitigation of these attacks requires some level of user involvement in the device pairing process. Prior research yielded a number of technically sound methods relying on various auxiliary human-perceptible out-of-band channels, e.g., visual, acoustic and tactile. Such methods engage the user in authenticating information exchanged over the human-imperceptible channel, thus defending against MiTM attacks and forming the basis for secure pairing.

This paper reports on a comprehensive and comparative evaluation of notable secure device pairing methods. This evaluation was obtained via a thorough analysis of these methods, in terms of both security and usability. The results help us identify methods best-suited for specific combinations of devices and human abilities. This work is an important step in understanding usability in one of the rare settings where a very wide range of users (not just specialists) are confronted with modern security technology.

1. Introduction

Ubiquitous wireless communication, based on technologies, such as Bluetooth, WiFi, Zigbee and WUSB, is very popular and will likely become even more so in the near future. Concurrently, increasing proliferation of personal wireless gadgets (including PDAs, cell phones, headsets, cameras and media players) continuously opens up new services and possibilities for ordinary users.

There are many common everyday scenarios where two devices need to "work together." One particularly common case occurs when both devices are controlled by a single user, e.g., a Bluetooth headset and a cell phone, a PDA and a wireless printer, or a laptop and a wireless access point. Whereas, in the "two-user" case, communication is between two devices, each controlled by its owner, e.g., a pair of cell phones.

The surge in the popularity of personal wireless devices triggers various security risks. The wireless communication channel is relatively easy to eavesdrop upon and to manipulate, which raises the threat of the so-called *Man-in-the-Middle* (MiTM) and *Evil Twin* attacks. Therefore, it is important to secure this channel. However, secure communication must be bootstrapped, i.e., devices must be securely paired or initialized. (We use the term "pairing" to refer to the bootstrapping of secure communication between two devices communicating over a wireless channel.)

☆ A previous version of this paper appeared in Kumar, Saxena, Tsudik, Uzun [A. Kumar, N. Saxena, G. Tsudik, E. Uzun, Caveat emptor: A comparative study of secure device pairing methods, in: IEEE International Conference on Pervasive Computing and Communications, PerCom, 2009].

* Corresponding author.
E-mail addresses: aashok01@students.poly.edu (A. Kumar), nsaxena@poly.edu (N. Saxena), gts@ics.uci.edu (G. Tsudik), euzun@ics.uci.edu (E. Uzun).

1574-1192/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.pmcj.2009.07.008

One of the main challenges in secure device pairing is that, because of the diversity of devices and lack of standards, no global security infrastructure exists today and none is likely for the foreseeable future. Consequently, traditional cryptographic means of secure channel establishment (e.g., SSL/TLS) are insufficient for the problem at hand, since unfamiliar devices have no prior security context and no common point of trust. Moreover, most types of wireless communication (e.g., RF-based) are not perceivable by humans. To this end, the research community has already recognized that some form of user involvement is necessary to address the problem of secure device pairing.[1]

One prominent research direction is the use of auxiliary – also referred to as "out-of-band" (OOB) – channels, which are both perceivable and manageable by the user(s) who own and operate the devices. An OOB channel takes advantage of human sensory capabilities to authenticate human-imperceptible (and hence subject to MiTM attacks) information exchanged over the wireless channel. OOB channels can be realized using senses such as audio, visual and tactile. Unlike the main (usually wireless) channel, the attacker cannot remain undetected if it actively interferes with the OOB channel.[2]

Since some degree of human involvement is unavoidable, usability of pairing methods based on OOB channels becomes very important. Also, because a typical OOB channel is low-bandwidth, there is an incentive to minimize the amount of information to be transmitted, for reasons of both usability and efficiency. Recently proposed pairing methods (overviewed in Section 2) typically require transmitting a few (e.g., 15) bits over an OOB channel to achieve a reasonable level of security. However, many devices (e.g., Bluetooth headsets) have limited hardware facilities and/or user interfaces, which makes it challenging to communicate even a few bits and, in turn, complicates user involvement.

At the same time, many current methods require hardware or interfaces not common across the entire spectrum of devices, including: photo/video cameras, infrared or laser transceivers, accelerometers, speakers, microphones, NFC transceivers, USB ports, keypads or displays. Such features, though present on some devices, are not universal. Whereas, certain other methods require truly minimal interfaces – e.g., LED(s) and button(s) – and are thus applicable to many common devices and pairing scenarios. However, using primitive interfaces tends to impose heavier burden on the user.

Motivation: The current situation can be described as *a state of flux*. Although many methods have been proposed, each having certain claimed advantages and shortcomings, no comprehensive and comparative usability study has been conducted. There are several reasons motivating a study. First, usability of current device pairing methods remains very unclear. Even methods that have been tested in terms of usability (e.g., [22,3]) have not been contrasted with other methods, i.e., testing was stand-alone and not comparative. Second, prior methods have been developed by security researchers who, not surprisingly, are experts in security and not usability. What appears as simple or user-friendly to a seasoned professional might not be either to an average user. This is because a non-specialist user is often initially clueless about manipulating new devices. A more important issue is that a user might have insufficient comprehension of security issues and the meaning of participation in secure device pairing. Since this topic has matured enough, it is also the right time for experimental assessment of usability factors.

Contributions: We overview prominent device pairing methods, implement them using a common software platform and conduct the *first* comprehensive and comparative field study, focusing on both usability and security. The scope of our study is the most common pairing scenario where a single user controls both the devices.[3] Our study yields some interesting results which help us identify most appropriate method(s) for a given combination of devices. We believe that this topic is very important since it sheds light on usability in one of the rare settings where most users (not just specialists) are confronted with security techniques. Also, since most device pairing methods are developed by highly-skilled specialists who are clearly not representative of the general user population, there is a certain gap between what seems to be, and what really is, usable. We hope that our work will help narrow this gap.

Compared to its prior conference incarnation [4], this paper makes several new contributions. In general, we present thorough statistical analysis of data gathered in the course of our usability study, in addition to the more informal treatment provided in [4]. Specifically, we perform statistical tests to explore and compare tested pairing methods in terms of robustness (i.e., error tolerance) and usability (i.e., speed, ease-of-use and likelihood of successful completion of pairing). In addition to investigating the effect of each usability measure separately for different methods, we study the combined effect of all measures taken together, via principle component and cluster analysis. The new analysis offers insights and statistical evidence about security and usability of individual methods as well as their comparative qualities.

Organization: Section 2 summarizes notable cryptographic protocols and secure device pairing methods. Section 3 discusses some pre-study design choices and criteria, followed by usability testing details in Section 4. Next, in Section 5, we present our logged usability study data. In Section 6, we discuss the analysis of the data and attempt to interpret the observations. We conclude with the summary and future work in Section 7.

2. Background

We now summarize notable cryptographic protocols and device pairing methods. The term *cryptographic protocol* denotes the entire interaction involved, and information exchanged, in the course of pairing. The term *pairing method* refers

[1] Indeed, this has been the subject of recent standardization activities [1].

[2] It is important to note that this approach only requires the OOB channel to be authenticated but not secret, in contrast to the standard Bluetooth pairing based on "user-selected" secret PINs. Recall that the Bluetooth pairing protocol is insecure against an eavesdropper [2].

[3] A similar study in the context of the two-user scenario is of independent interest; it is being addressed in our on-going work.