Poster: Security Through Entertainment: Using a Memory Game for Secure Device Pairing

Alexander Gallego
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
agalle01@students.poly.edu

Nitesh Saxena
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
nsaxena@poly.edu

Jonathan Voris
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
jvoris@isis.poly.edu

1. INTRODUCTION

Wireless communication channels are easy to eavesdrop upon and manipulate. Securing them is therefore a fundamental security objective. "Pairing" refers to the operation of bootstrapping secure communication between two wireless devices. An established research direction to solving the pairing dilemma is to leverage an out-of-band (OOB) channel, which is governed by device users. Unlike classical radio channels, OOB channels are "human-perceptible." That is, a user can validate the intended source of an OOB message and an adversary can not manipulate them in transit. However, prior work shows that this approach to pairing can be prone to human errors of different forms that may directly or indirectly translate into man-in-the-middle attacks.

The challenges associated with pairing motivate the design of a radically different solution. Our central research question is: *can we design pairing methods that in some way incentivize users to correctly take part in the pairing process, thus improving both security and the user experience?* To address this issue, we propose that the pairing process be reframed not as a tedious procedure that puts a burden on users, but rather as a game that is enjoyable and entertaining to complete. It is our aim to transform the operation of device pairing from one that users seek to avoid or complete as quickly as possible into one that they relish. As a result, users will be more attentive while pairing and perform better at it. Furthermore, if a game involves competitiveness between individuals, this will provide added motivation.

In essence, we are suggesting that by contextualizing a security task as a game rather than a chore, the usability burden of this task can be greatly reduced. We dub this the *Tom Sawyer Effect* after a well known event in Mark Twain's literary classic, "The Adventures of Tom Sawyer" [3]. In this novel, the boy Tom Sawyer is chastised by his Aunt Polly by being forced to paint a fence on his day off. Tom resents the fact that he must complete this task instead of enjoying his free day by playing games with his friends. To escape his plight, the clever Sawyer acts as though he is having a good time performing his task rather than resenting it. Upon observing his supposed delight, his friends insist that they be given an opportunity to paint the fence so that they can enjoy it as well, going as far as to trade him trinkets for the opportunity to do so.

Much in the same way that Tom convinces his friends to complete what would otherwise be considered an uninteresting job by treating it as a game, we seek to persuade users to be attentive during security operations, such as device pairing, by making them as interactive and entertaining as possible. To this end, we develop "Alice Says," a pairing game based on Simon, a popular memory game. This game is designed for a setting where there are two users, each of which is in control of his or her own mobile phone or other personal device.

2. RELATED WORK

Our work was inspired by Halprin and Naor [5], who recently proposed the use of games to address the problem of random number generation. The pairing mechanism that we present in this work is an example of a "Game with a Purpose" as conceptualized by von Ahn [2]. This is because it is not simply a game for its own sake, but rather a form of entertainment that simultaneously achieves a computational result without the explicit awareness of its users.

3. DESIGN OF A PAIRING GAME

Devices may establish two types of communication channels between each other. The first is a traditional wireless connection, characterized by a large bandwidth capacity and bidirectionality, but also a short range nature. The second variety compromise the set of OOB channels, which feature relatively modest bandwidths but are physically authenticatable. That is, OOB channels are crafted from forms of output which can be perceived by unassisted humans, providing users with the power to verify the transmission source themselves. This implies that any malicious entity who wishes to manipulate data in transit over an OOB channel would not be capable of modifying any messages. OOB channels are not generally secret, however, so adversaries can observe the OOB transmission in any other way they see fit. In contrast, opponents have unfettered control of the conventional wireless channel.

To leverage the Tom Sawyer effect to improve the device pairing experience, a suitable game had to be designed. We took inspiration from Hasbro's Simon [1]. This game was selected as a basis for several reasons. This game is relatively uncomplicated when compared with contemporary computer games. This was desirable both due to its ease of implementation as well as its suitability for players of all ages and levels of experience. Another important factor in the selection of this game is its close relation to existing device pairing solutions. Previous work has established the use of patterns of synchronized audio and visual output [4, 6] as a viable method of securely associating devices. At its core, playing Simon involves nothing more than the short term memorization of audiovisual patterns and thus minimal changes were required to adapt it for use in pairing.

We dubbed our Simon variant Alice Says. To demonstrate the suitability of this game for the task of pairing mobile devices, we implemented it on two Nokia N97 phones. A picture of this implementation is provided in Figure 1 Upon initially starting the game, users are provided with two menu options: a single player training mode and a two player pairing mode.

Figure 1: Alice Says Running on Two Nokia N97 Phones

3.1 Single Player Mode

To promote the Tom Sawyer effect, a single player mode is provided to allow users to unwittingly train themselves to improve their pairing performance. This mode is essentially the classic version of Simon, only adapted to the context of a mobile device. Users are shown a screen with four adjacent squares which fully occupy the screen, dividing it into quadrants. Each of these squares is a unique and distinctive color. Besides these color coded screen segments, the only other item visible to the user while the game is underway is a counter which tracks the length of the pattern that a user has matched thus far.

One of these four quadrant buttons is randomly selected by the device during each round. The selection is indicated to the user in two ways. First, the screen section is lit by increasing its luminance. Secondly, a tone corresponding to that quadrant is played. Since the Simon user interface consists of four color quadrants, each step of the pattern can be used to encode two OOB bits in the following straightforward manner: "00" corresponds to green, "01" is indicative of red, "10" means blue, and "11" is aligned with yellow.

If a user presses the screen quadrant that correctly corresponds to the one that had just been selected by the device, it then constructs a pattern of colors and sounds by displaying the first screen segment followed by a new, randomly chosen one, again conveyed to the user by brightening the relevant portion of the screen and playing a corresponding melodic tone. This process continues until the user makes an error in the pattern or a certain predetermined pattern length threshold value is reached. At this point a "Game Over" message is provided to the user.

3.2 Two Player Mode

The two player mode accomplishes device pairing. It differs from the single player version in two ways. First, the game does not conclude when a mistake is made. It continues until a sufficient number of OOB bits have been relayed. Secondly, the game is split across two devices. One device displays the pattern to the user, but does not handle input. The other does not display the pattern, but instead accepts input. A two player pairing game was selected because the need to pair two wireless devices implies that there will be two parties present to participate in the pairing. A two player game will also reap the security benefits of fostering competition between its players.

3.3 Security Guarantees

One important aspect to this design is how to handle attacked sessions. If a session has been attacked or an error has occurred, the OOB strings will be different on the two devices. Thus, even if a user "correctly" matches the displayed pattern, Alice Says will still register an error. The attacked bit will end up as the first bit of a pattern, and users will be unable to proceed by identifying the displayed single color pattern.

Thus, users will need to be provided with a mechanism for restarting the pairing session from scratch. After a certain threshold of single color pattern mismatches have occurred, an error message is displayed. At this point, users can scrap the entire session and start over. Note that single color pattern mismatches should be very unlikely in unattacked sessions, as users are anticipated to be able to handle matching at least one color. Thus, the only way for a critical error to occur in this system is for users to incorrectly match a single color. There is only a 1 in 4 chance of this occurring, even if the user is not paying any attention whatsoever, yielding a high level of practical security.

4. CONCLUSIONS

In this poster abstract, we considered the problem of designing pairing methods that provide users with incentive to put forth more effect during the pairing process, thus providing improved security and enhancing the user experience. We dubbed this the Tom Sawyer Effect. To this end, we proposed a general direction of the application of computer games to solve the problem of wireless device pairing. The incentive that we provide is fun and entertainment. As an example of this, we developed "Alice Says," a pairing game based on Simon.

5. REFERENCES

[1] Simon. Available at `http://www.boardgamegeek.com/boardgame/5749/simon`, 1978.

[2] L. von Ahn. Games with a Purpose. In *IEEE Computer Magazine*, 2006.

[3] M. Twain. The Adventures of Tom Sawyer, 1876.

[4] R. Prasad and N. Saxena. Efficient Device Pairing using "Human-Comparable" Synchronized Audiovisual Patterns. In *ACNS*, 2008.

[5] R. Halprin and M. Naor. Games for Extracting Randomness. In *SOUPS*, 2009.

[6] V. Roth, W. Polak, E. Rieffel, and T. Turner. Simple and Effective Defense Against Evil Twin Access Points. In *ACM Conference on Wireless Network Security (WiSec)*, 2008.