SECURE DEVICE PAIRING: A USABILITY STUDY

[1]Yasir Arfat Malkani, [1]Ayaz Keerio and [2]Lachhman Das Dhomeja

[1]Institute of Mathematics and Computer Science
University of Sindh, Jamshoro, Pakistan

[2]Institute of Information and Communication Technology
University of Sindh, Jamshoro, Pakistan

{yasir.malkani, ayaz, lachhman}@usindh.edu.pk

ABSTRACT

Ubiquitous computing systems are becoming more common nowadays. Usually, these systems are composed of several modern hand-held devices, which support wireless communication in some form, such as WiFi, IrDA, Bluetooth, etc. Since wireless communication is open to everyone, the issue is how to pair two unassociated devices securely. Consequently, a wide community of industrial as well as academic researchers have proposed more than two dozen schemes and protocols that use various forms of out-of-band channels to pair the two devices securely. The main goal of the research community working on this issue has been to develop and/or propose such pairing systems/schemes, which should be automatic, secure and usable. One such system is proposed by Malkani et. al. [1]. The main goal of this research was to design a generic system that facilitates association of two co-located devices by demonstration of physical proximity in ubiquitous computing environments. In this paper, we are presenting the usability study of several pairing schemes and the proposed system, which was carried out to evaluate the overall system.

KEYWORDS

Usable Security, Authentication, Device Association, Generic Framework, Proof-of-Proximity

1. INTRODUCTION

During last decade significant research efforts [2-31] have addressed the issue of secure device pairing. The main goal of the research community working on the secure device pairing issue has been to provide mechanisms that give assurance of the identity of the devices participating in the pairing process and to secure them from being victims of eavesdropping attacks, such as MiTM attack. Achieving this goal is a challenging problem from both the security and the usability points of view [32-33]. Consequently, Malkani et. al. [1] have proposed a generic framework for secure device pairing. Authors [1] advocated that a common pairing infrastructure for ubiquitous computing environments can improve the usability and security of the pairing process. The proposed system integrates device discovery, several pairing schemes and a protocol selection mechanism into a single model that facilitates association of any pair of devices in a wide range of scenarios by using the devices' existing capabilities and user preferences, and also assists the user to select an appropriate pairing protocol and relieves him/her from choosing between more than two dozen [2-31] of pairing schemes. The interested readers can find the detailed analysis of these existing schemes in [32-33] and the detailed system architecture of the proposed system in [1]. The focus of this paper is the usability study of eight pairing schemes as well as the proposed system, which integrates them. It is carried out in order to evaluate the proposed system and to

DOI:10.5121/iju.2012.3203

support the argument that the integration of discovery mechanism and several proof-of-proximity protocols into a single device pairing system is an effective approach for ordinary users from both security and usability points of view.

The remaining part of this paper is organised as follows: section 2 presents brief summary of the proposed system [1], section 3 discusses the implementation, section 4 presents the details of usability study, section 5 describes the results and presents the evaluation of the proposed system, and finally section 6 concludes the paper.

2. PROPOSED SYSTEM

The proposed system considers ubiquitous computing environments, in which devices communicate with each other through short-range wireless technology, such as 802.11 or Bluetooth. They discover each other using the proposed registration and discovery mechanism. Authors do not consider extremely resource constrained devices, such as sensor nodes. Instead, they consider those ubiquitous computing devices, which have reasonable battery power and computational capabilities, e.g. mobile phones, cameras, PDAs, laptops, printers etc. These devices are capable of symmetric encryption/decryption, public key based encryption, hashing, signature verification, and have unique device-id or address. Further, devices know their location through some location system already installed in the environment or through their own hardware/software, such as GPS (Global Positioning System). The location information is useful in the discovery process. We assume that the co-location server is a trusted, uncompromised and tamper resistant (or at least tamper evident) device. It is also capable of performing symmetric and asymmetric cryptographic operations. Since, the co-location server is very light-weight; it might be run with other local services (e.g. DNS, print) or any other server, which is part of some existing security infrastructure to limit the deployment costs. Alternatively, it could also be installed into a dedicated low-cost small device. Then each device needs to perform one time demonstrative discovery of the server device in order to build trust. We are considering all the devices registered with the same co-location server as potentially co-located and each co-location server is responsible for handling a particular domain or location. We believe that due to the modern low-cost small ubiquitous computing devices that have now reasonable battery and computational power, one co-location server per scope is feasible.

The three main design goals of the proposed system are: usability, security and generality. From usability point of view, the system should be simple to understand and easy to use for an ordinary user. Security goal is twofold: firstly, the system should be capable of establishing the secure session between two previously unassociated devices through demonstrating the physical proximity of the devices involved in pairing process; secondly, all the communication between several entities of the system must be secured. From generality point of view, the system should be applicable in a wide range of device pairing scenarios in ubiquitous computing environments, capable of incorporating existing pairing schemes and can be extended without major modifications in the design.

The proposed system consists of three phases. The first two phases are registration and discovery of the device(s), and the third phase is selection, initiation and execution of the PoP protocol. The registration, discovery and proof of physical proximity are integrated into Co-Location (CoLoc) protocol, which is core part of the proposed system. The details of CoLoc protocol can be found in [1], however we are presenting the overview of the overall system as below:

1. First of all resource device(s) register their capabilities with an easily found database stored on the co-location server. New devices can be added while the system is running.

2. When two devices need to associate, the client queries the co-location server to acquire the required information of suitable resource device(s).

3. The co-location server prepares a device list containing necessary information for selecting and contacting the resource device in order to initiate the proof-of-proximity phase.

4. Based on the information from the co-location server and user preferences, the client first goes through the Proof-of-Proximity (PoP) protocol selection process and then initiates the secure association process with the selected resource device. Different interactions to demonstrate physical proximity are possible and the selection requires a selection criterion along with device capabilities, constraints on pairing schemes and/or user preferences.

5. Both of the devices (i.e. client and resource) execute the commonly agreed PoP protocol for the purpose of demonstrating their physical proximity in order to establish the secure session. Note that secure pairing is achieved only when physical proximity between both of the devices is proved.

3. IMPLEMENTATION

To evaluate the proposed system, we built a prototype implementation of the system and conducted a usability study. The details of the usability study are given in next section. We have designed simple user interfaces for the client and the resource applications and avoided any complexities. The implementation of the proposed system is carried out using Java (version 1.6) and Windows XP operating system. In the coding and implementation process, we have used Eclipse Galileo (version 3.5) as a Java IDE. As an apparatus, we have used two 1.9GHz Dell Machines with 1GB RAM, two PhidgetInterfaceKits [34] and a camera. PhidgetInterfaceKits and camera are the requirement for some of the PoP protocols. At server-side Oracle Berkeley DBXML [35-36] is used to maintain and keep record of the devices' profiles. The implemented system integrates 14 different pairing schemes to demonstrate the physical proximity of the devices. Since, system implementation is not the focus of this paper, interested readers can find additional details of the implementation in [1].

4. USABILITY STUDY

In order to evaluate the proposed system and to support our main argument that the integration of discovery mechanism and several proof-of-proximity protocols into a single device pairing system is an effective approach for ordinary users, we conducted a usability study. This is a study of the eight pairing schemes as well as the proposed system, which integrates them. The results of the usability study are useful to test three hypothesis: 1) are the users good at identifying an appropriate (right) pairing scheme when they have to choose between large number of pairing schemes; 2) To what extent users like to be involved in the pairing process; and most importantly to evaluate that 3) is the integration of discovery mechanism and the pairing schemes into a single system an effective solution for ubiquitous computing environments from the user's point of view, and are they perceiving it as usable. In this section, firstly we discuss the prior work on usability of device pairing schemes, and then we describe the test cases that are selected as part of this study followed by describing the demographic information of test's participants, test procedure, and the results.

4.1 Prior Work on Usability of Device Pairing Schemes

More recently the usability issue of secure device pairing schemes has got significant attention from researchers and there exist some recent work on the usability of device pairing schemes in the literature. Below are described some of the notable work in this area.

In the literature, Uzun et al. [37] are considered to be the first who performed the usability analysis of secure device pairing methods followed by [38-39]. Uzun et al. [37] presented a comparative usability analysis of some of the conventional paring schemes. In their study, the participants were asked to compare strings displayed on mobile devices, copy a PIN displayed on one device and enter it onto another, and select a PIN from among 4 numeric values that matched a string displayed on another device. Their findings were that participant perceived copying and entering as booth secure and professional while comparing was perceived as easy to use. They recommended using a PIN of not more than 7 digits and that the user interface should be designed in such a way that the default option is the most secure. More recently, Kumar et al. [39] presented an experimental evaluation of a large set of device pairing schemes. Their [39] results showed that some simple schemes, such as number comparison, were quite attractive overall in terms of speed, security and usability. Subsequently, in [40] authors argued that the participants of prior study [39] comprised of mostly young males (70%) and the test organizers were experts in security relevant research as well as developers of some of the tested pairing schemes. They argued that the results of the study [39] were valuable, however it required further experimentation (usability tests) with more diverse participants, and more diverse scenarios. Many of the tested pairing schemes in [40] overlapped with the already tested schemes in [39], however this study differed from [39] in that the focus of this study was on within subjects analysis. The results of the study [40] were helpful in indentifying the pairing schemes, which were not feasible for some specific groups of users with regard to age, gender and prior experience with device pairing. More recently, Kainda et al. [41] also performed a usability and security evaluation of the pairing schemes. The main focus of this [41] work was on comparison of the usability and the security of those pairing schemes, which used more recently proposed and identified out-of-band channels together with some of the conventional ones as presented in [37]. The four classes of pairing schemes that were covered in this study are: Comparing (compare and confirm), Selecting (compare and select), Entering (copy and enter), and Barcode (taking a picture of a barcode using a camera). This work differed from [37] in the sense that authors also took into account the scenarios where the compared strings were nearly similar (i.e. mismatched by only one or two digits, characters or words depending on the scheme). Our work is similar to [41] in terms of the methodology used to carry out the usability study, however the selected pairing schemes in our study are different from those tested in [41].

4.2 Selection of Test Cases

We have selected eight PoP schemes for our experiment. The reason for conducting the user study with a reduced number of PoP schemes rather than all fourteen implemented schemes is to avoid user fatigue. With all PoP schemes, a single experiment takes around an hour, which causes for unrealistic/unproductive data, especially for a few of the last test cases/tasks. Therefore after a careful analysis, 6 pairing schemes are eliminated from this usability study. During elimination process, we considered the results of some of our previous experiments [42] conducted with 15 users and 4 button-based schemes, and also referred the prior work [37-41] on usability of device pairing schemes. For example some of those schemes, which produce/require synchronized audio/visual signal did not perform well in prior evaluations due to high error rate and user-annoyance [9, 43], so we eliminated Beep-Beep and Speaker-Speaker and Blink-Beep. According to the results of our previous experiments [42], the users perceived Beep-to-Button scheme as harder compared to the other three button-based schemes, so we eliminated the Beep-to-Button scheme as well. Digits comparison is too simple approach and hash comparison is not such a user-friendly approach [41], so we preferred Display-Display over these two schemes. In summary, the following are the short-listed PoP protocols that we have selected for the usability study.

- **Category - 1**
  Button-to-Button, Blink-to-Button, Seeing-is-Believing (SiB)
- **Category - 2**
  Blink-Blink, Display-Display, Display-Speaker
- **Category - 3**
  Selective Image Comparison (SiC), Capture and Show (CaS)

4.3 Participants

It is widely accepted that any user study that is performed by 20 users captures over 98% of usability issues [44], so a total of 20 volunteers were recruited. The majority of the participants are students of the University of Sussex and most of them are proficient computer users. The background profile information of the participants is summarized in table 1.

Gender	
Male	55%
Female	45%
Age	
18 - 25	40%
26 - 40	40%
41 or above	20%
Education	
High School/College	15%
Bachelor	40%
Masters	35%
Doctorate (PhD)	10%
Pairing Experience	
Yes	90%
No	10%
Daily Computer Usage	
2 or less hours	15%
3 - 5 hours	50%
6 or above hours	35%

Table 1: Test participant's demographic information

4.4 Test Procedure

The tests were conducted in a lab-based environment. Before the start of each experiment, we explained briefly the goals of the experiment along with the description of each pairing method to the participant; however we had already provided a leaflet to each participant in either hardcopy or through email before the actual day of the experiment that contains all the details of the experiment. Each participant filled a pre-test questionnaire before starting the test cases. The pre-test questionnaire was used to collect the demographic information of the participants.

Each experiment consisted of two parts. In the first part, each participant performed the tasks of executing the eight PoP protocols, which are mentioned earlier in section 4.2. These eight protocols were programmed to work independently from the proposed system and do not include device registration and discovery phase. Every participant performed each of the tasks twice. The first execution of each of the tasks was without any attack, while the second execution was under an attack scenario, in which users had to identify the mismatches. From the data of the first execution of each user, safe errors (i.e. identifying a match as a mismatch) are identified, while second execution provides data for fatal errors (i.e. identifying a mismatch as a match). Note that for the pairing schemes in which user is involved in generating the PoP data, fatal errors are not applicable. Thus, in that case both of the executions were performed without the attack scenario. Timing information was also recorded and stored in the test log file along with the other data. At the end of first part, each participant was given an After Scenario Questionnaire-1 (ASQ-1) to record his/her satisfaction with the performed tasks. In the second part of the experiment, each participant performed two executions of the proposed implemented system, which is described in section 2. At the completion of this part of experiment, each participant is given an After Scenario Questionnaire-2 (ASQ-2) to record his/her satisfaction with the proposed implemented system, which is denoted as CoLoc in the results of the usability study. Finally, at the end of overall experiment every participant also filled a post-test questionnaire that contains two scenario-based questions and one question regarding the ranking of each category of pairing schemes.

4.5 Results

The usability study results are obtained from the collected data by means of questionnaires (i.e. two ASQs and one Post-Test questionnaire) as well as by the log files generated during the experiment. Two separate log files were created for each participant during the experiment; one for first phase of the experiment and the other for second phase of the experiment. The first log file recorded 16 lines of data and each line contained 7 data items. These include test date and time, pairing scheme name, completion duration in seconds, expected completion result, actual completion result, error information, and information about the successful completion of task. There are 20 participants, so we got 2240 data items in total from first set of log files. The second log file recorded 2 lines of data and each line contained 8 data items, so we got 320 data items in total from the second set of log files. The seven data items are similar as in first log file and the eighth data item records information about the user input/preference. Further, we got 35 data items from the three questionnaires for each participant, thus we got total of 700 data items for 20 participants. Overall we got 3260 data items for analysis from questionnaires and log files. All of the data was transferred and recorded into Microsoft Excel workbooks for analysis and evaluation.

6. ANALYSIS OF RESULTS AND EVALUATION

In this section, we present the evaluation of the proposed system through the analysis of the system's design features and the results obtained from the usability study. In the view of our previously defined goals (section 2) and objectives of this research, we consider the three major metrics for evaluating the proposed system. These are usability, security, and generality. Usability evaluation will provide an assurance that the system is easy to use for the users and they are satisfied with the way system works. Security evaluation will make sure that the objective of securing communication between several entities of the system is achieved, along with providing confirmation of the physical proximity of the devices involved in the pairing process. Generality evaluation will ensure that the system is applicable in a large set of device pairing scenarios in ubiquitous computing environments, capable of incorporating existing pairing schemes, and can be extended without substantial effort.

5.1 Usability Evaluation

The data obtained from both of the ASQs and post-test questionnaires revealed the participant's opinion of each of the test cases and their capability to perceive an appropriate pairing scheme for a given device pairing scenario. The participant's opinion is expressed in terms of rating scores on a scale of 1 to 7 in which 1 is representing the lowest score and 7 is representing the highest or the most satisfactory score. The selection of seven-step scale is based on the fact that it captures proper balance between reliability of scale and discriminative demand on the participants [45-47].

The graphs shown in figures 1 and 2 are drawn from the data obtained from ASQ-1 and ASQ-2. Every participant recorded their satisfaction opinion for each of the test case by giving a score (i.e. 1-7) to each of the three measures on the ASQs. The graph in figure 1 shows the participants' rating view for each of the three measures. However in order to calculate the single score and to present the overall satisfaction of the participants for each of the test case, these scores are averaged and presented in figure 2. The results show that Button-to-Button pairing scheme is on top with the users average satisfaction score of 6.216. Display-Display and SiB has an average score of 6.1 and 6.15 respectively followed by CoLoc and CaS with the average satisfaction score of 5.616 and 5.556 respectively. Display-Speaker has the lowest average satisfaction score of 4.85, while Blink-to-Button and Blink-Blink stands with an average satisfaction score of 5.416 and 5.106 respectively.

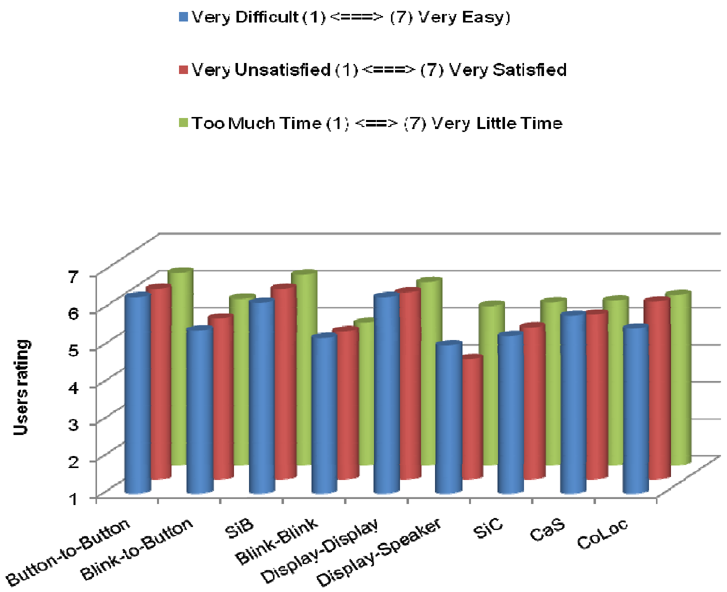

Figure 1: Users average rating score on a 7-step scale for the three measures of user's satisfaction

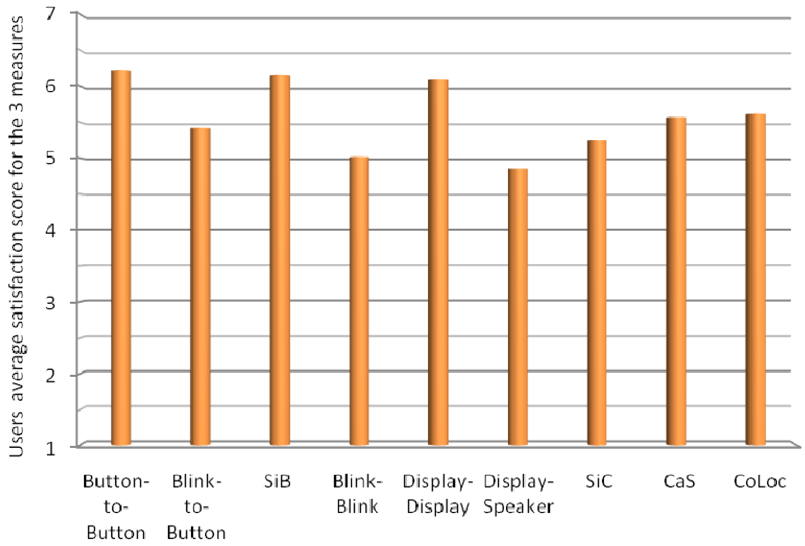

Figure 2: Users average satisfaction score on a 7-step scale for three measures

It is well known in the literature of usability evaluations that an average score of 5.6 on a 7-step scale is considered to be satisfactory and acceptable for a system or product, while an average score of 4 is the acceptable score on a 5-step scale [48]. CoLoc has an average satisfaction score of 5.616 for the three measures of usability, which indicates that the proposed system is usable and practically feasible for its users.

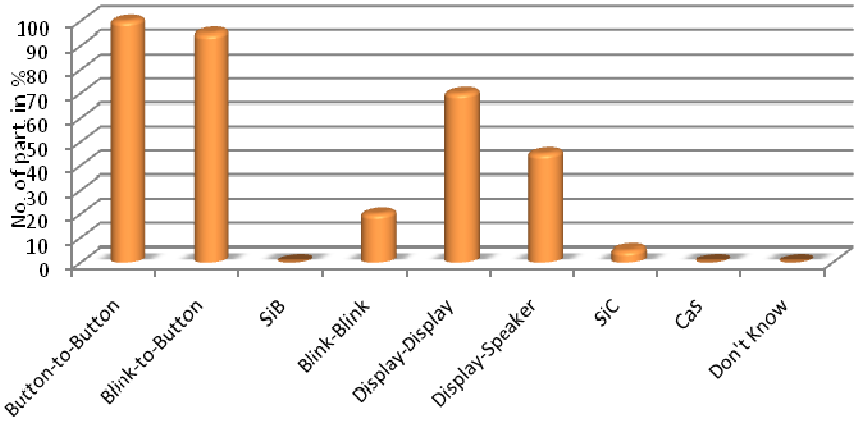

Figure 3: Participants response to a question of the post-test questionnaire

The graph in figure 3 is drawn from the data collected as response to a scenario-based question. A scenario is presented to the participants on post-test questionnaire with a number of options and asked to select all of the possible pairing schemes. The correct response was Button-to-Button and Blink-to-Button. However, results in figure 3 show that many participants have selected the wrong pairing schemes as well along with the correct ones.

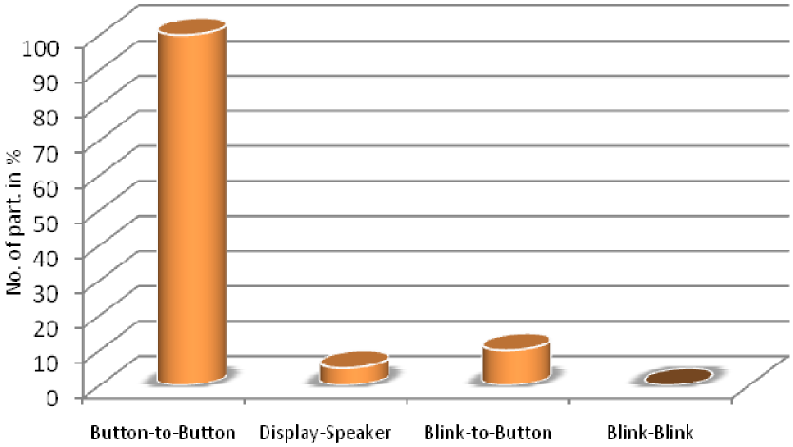

Figure 4: Participants response to a question of the post-test questionnaire

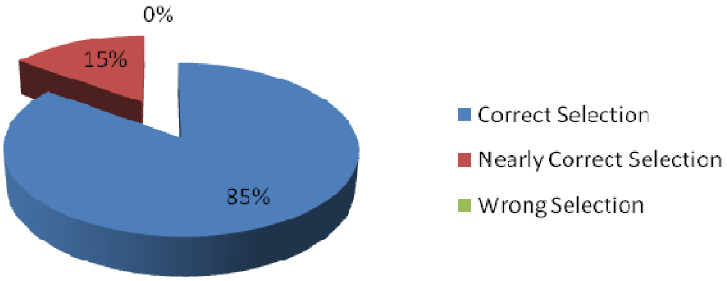

Figure 5: Interpreted results for response to a scenario-based question of the post-test questionnaire

Graphs in figure 4 and figure 5 are drawn from the data collected as response to another scenario-based question on post test questionnaire. The scenario is presented to the participants with a smaller number of options and asked to select one of the best possible pairing schemes. The correct response is Button-to-Button. Results show that all of the participants (100%) selected Button-to-Button scheme, however 5% selected the Display-Speaker and 10% selected the Blink-to-Button scheme along with the Button-to-Button scheme. Considering the fact that Button-to-Button is the correct choice, it can be concluded that 85% of the participants have selected the right choice, while 15% of the participants have selected nearly correct response, but none has selected a totally wrong choice.

The results presented in figure 3 reveal the fact that users are not good at identifying which pairing schemes are applicable in which scenarios. However, when users are given short listed pairing schemes, they performed well at identifying the suitable pairing schemes (figures 4 and 5). These results support our argument related to usability that ordinary users are not good at identifying appropriate schemes in a situation when they have to choose between many different pairing schemes; however if the cognitive overhead in terms of deciding/thinking an appropriate pairing scheme could be reduced, they are capable of performing very well in the pairing process. This result clearly supports our hypothesis that assistance in choosing a pairing scheme has value.

5.2 Security Evaluation

As stated earlier, the objective of security evaluation is to ensure that the proposed system is integrating the PoP protocols well and also securing the overall communication between several entities of the system. The security of device pairing schemes, where users are involved in security-related interactions, is evaluated in terms of safe errors and fatal errors [49]. Safe error denotes the systems inability to pair two legitimate co-located devices due to system error or user error in case of use of out-of-band channels. User errors are due to either very complicated steps of pairing, unclear instructions for the user to what to follow to achieve successful pairing or user's own carelessness during the pairing process. Fatal error denotes the systems inability to prevent pairing of an adversary with a legitimate device of the system. Note that fatal errors are more dangerous and cause more serious consequences compared to safe errors. Fatal errors are not applicable in most of the schemes that involve users in only generating PoP data. In the case of our system, fatal errors are not applicable to button-based schemes and SiB. Since CoLoc incorporates these schemes and also it encrypts all the communication between the communicating partners, fatal errors are also not applicable to it.

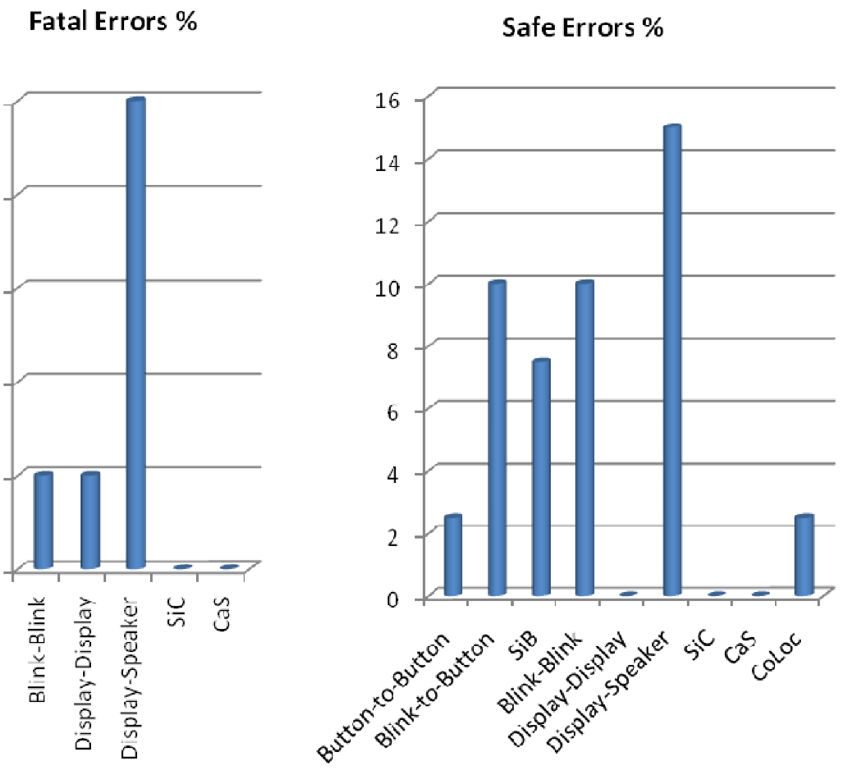

Figure 6: Safe and fatal errors for each of the test case

When looking at the safe errors in figure 6, Display-Speaker has the largest safe error rate, while Display-Display, Selective Image Comparison, and Capture and Show have not even a single safe error. Button-to-Button and CoLoc have lower error rates as compared to the other schemes. CoLoc has an average error rate of only 2.5%. When we performed a more detailed analysis of these errors, it comes to our notice that these 2.5% safe errors occurred when the participant selected Blink-to-Button as the PoP protocol during the execution of the proof-of-proximity phase, and the safe error rate of Blink-to-Button is already high in comparison to the other schemes, excluding Display-Speaker. This indicates that the rate of safe errors for CoLoc is somehow dependent on the selection of PoP protocol. These results indicate that the proposed system achieves its first security goal (i.e. demonstrating physical proximity of devices) very well.

The second security goal is to make sure that the communication between several entities of the system is secure. We have achieved this goal through encrypting all the communication from resource registration until the end of the execution of the proof-of-proximity phase [1]. The encrypted and integrity protected mode of communication used during the resource registration and discovery phase protect the pairing process from the bidding-down-attack. In this kind of attack, the goal of an adversary is to fool (bid-down) the intended pair-able devices to use weaker security than is possible. For instance, when pairing two display and camera-equipped devices, an adversary could modify the capabilities of one of the devices into a display-less and/or camera-less device (bidding-down) to force a radio-based pairing protocol to be used, which is easier to intercept without being detected. Additionally, when the proposed system is implemented considering the assumptions provided in section 2, it is also secure against MiTM attack. These facts indicate that beside the usability, the proposed system also achieves its security goals.

5.3 Generality Evaluation

The purpose of generality evaluation is to make sure that the system is capable of incorporating existing pairing schemes, as well as being extendable without substantial modifications in the design, and being applicable in a large set of device pairing scenarios in ubiquitous computing environments. Towards this, we have already shown in [1] that CoLoc is capable of integrating several pairing schemes (known as PoP protocols in this paper) to authenticate the physical proximity of the devices. Further, in addition to establishing a secure session between two previously unassociated devices, the proposed system is also capable of establishing secure group communication, creating and managing long-term pairings, and also offers a mechanism for the selection of PoP protocol that gives some control to the user. Moreover, the system is designed in a way that it can be extended without substantial effort. We are defining extension from two different points of view: the developers/programmers' point of view and the deployment point of view.

From the developers' point of view, they can add a new PoP protocol to the system by performing following steps:

- Firstly, they are required to include specifications for the new PoP protocol in the XML-based policy file.
- Secondly, they are required to write the PoP protocol implementation code in Java, which needs to be included into proof-of-proximity software component.

From a deployment point of view, the proposed system is capable of being deployed to multiple servers; thus facilitating the secure association of a pair of devices, each of which belongs to a different co-location server.

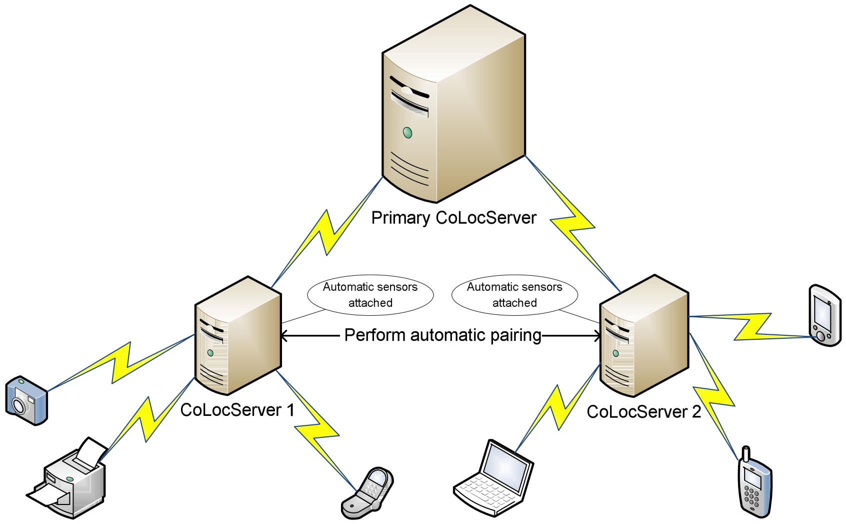
Primary CoLocServer
Automatic sensors attached
Automatic sensors attached
Perform automatic pairing
CoLocServer 1
CoLocServer 2

Figure 7: Scenario depicting the deployment of multiple co-location servers

Figure 7 shows the scenario of multiple co-location servers. In fact, it is similar to a single co-location server's scenario, where devices use the server as a mediator. Now the Primary ColocServer serves as a mediator for the other two servers (i.e. ColocServer1 and ColocServer2). These two servers can authenticate each other by either using an automatic pairing scheme, or with the help of a user/administrator using any other category of pairing schemes. Once these two servers are in a paired state, they can securely exchange the device's profiles to each other depending on the received queries from their clients.

In summary, the proposed system is designed in such a generic way that it is not restricted to any particular set of PoP protocols. It can be used with various types of PoP protocols or same PoP protocols, but with different selection criteria based on the scenario in which it is deployed. We have also shown in [1] that the proposed system is capable of getting user's preferences and considers them during the PoP protocols selection phase. The protocol selection mechanism uses an XML-based policy as PoP protocols selection criteria, which is mainly defined in terms of required device capabilities and constraints over PoP protocols. Since the criterion for the selection of PoP protocols is described in an XML-based protocol specification and selection policy file; it can be changed / modified at run-time. Moreover, we also showed that the proposed system is extendable without changing the core design of the system and without substantial effort. All of these features indicate that the proposed system is generic enough that it can cover a wide range of device pairing scenarios in ubiquitous computing environments in terms of both two device setting and group pairing.

7. CONCLUSION

In this paper, we presented the details of a usability study of eight pairing schemes and a framework developed for secure pairing of devices. The main focus of this study is to evaluate the proposed system [1]. The analysis and evaluation supports the assertion that the integration of the discovery mechanism and several proof-of-proximity protocols into a single system is a more effective approach to device pairing as compared to proposing and developing a plethora of pairing protocols that work in a totally independent fashion. We believe that our work is an important and timely first step in academic research that highlights the need of a framework based approach to device pairing. Our work helps with answering several questions relevant to secure device pairing. These include: 1) are the users good at remembering several steps of dozens of pairing schemes for a number of device pairing scenarios and situations; 2) are they capable of performing well when cognitive overhead would be reduced; 3) are the users willing to be involved in the pairing process, and if yes, then to what extent; and most importantly 4) are the frame-work based approaches feasible for tackling the issue of device pairing in ubiquitous computing environments. The task of answering these questions was at least very difficult, if not impossible, before the work presented in this paper.

ACKNOWLEDGEMENTS

This research was sponsored/funded by University of Sindh, Jamshoro, Pakistan under Mega Project Phase-I: No.SU/PLAN/F.SCH/650 and the work presented in this paper is done in the School of Informatics, University of Sussex, UK. We want to say our sincere thanks to Dr. Dan Chalmers and Dr. Ian Wakeman for their full support and guidance to make this work possible.

REFERENCES

[1] Malkani, Y.A., et al., A Generic Framework for Device Pairing in Ubiquitous Computing Environments. International Journal of Network Security and Its Applications (IJNSA), 2012. Vol. 04(02): p. 1-20.

[2] Stajano, F., The Resurrecting Duckling - What Next?, in Revised Papers from the 8th International Workshop on Security Protocols. 2001, Springer-Verlag.

[3] Stajano, F. and R. Anderson, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, in Security Protocols. 2000. p. 172-182.

[4] Stajano, F. and R. Anderson, The Resurrecting Duckling: security issues for ubiquitous computing. Computer, 2002. 35(4): p. 22-26.

[5] Naik, P., K. Ravichandran, and K.M. Sivalingam, Cryptographic key exchange based on locationing information. Pervasive and Mobile Computing, 2007. 3(1): p. 15-35.

[6] Kindberg, T., K. Zhang, and N. Shankar. Context authentication using constrained channels. in Mobile Computing Systems and Applications, 2002. Proceedings Fourth IEEE Workshop on. 2002.

[7] Saxena, N., et al., Secure Device Pairing based on a Visual Channel. sp, 2006. 0: p. 306-313.

[8] Saxena, N., M.B. Uddin, and J. Voris. Universal Device Pairing using an Auxiliary Device. in Symposium On Usable Privacy and Security (SOUPS). 2008.

[9] Saxena, N. and J. Voris. Pairing Devices with Good Quality Output Interfaces. in International Workshop on Wireless Security and Privacy (WISP) (co-located with ICDCS). 2009.

[10] Prasad, R. and N. Saxena. Efficient Device Pairing using Synchronized "Human-Comparable" Audiovisual Patterns. in Applied Cryptography and Network Security (ACNS). 2008.

[11] Saxena, N. and M. Uddin, Automated Device Pairing for Asymmetric Pairing Scenarios, in Information and Communications Security. 2008. p. 311-327.

[12] Soriente, C., G. Tsudik, and E. Uzun. BEDA: Button-Enabled Device Association. in Internation Workshop on Security and Spontaneous Interaction (IWSSI 2007). 2007.

[13] Holmquist, L.E., et al., Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts, in Proceedings of the 3rd international conference on Ubiquitous Computing. 2001, Springer-Verlag: Atlanta, Georgia, USA.

[14] Castelluccia, C. and P. Mutaf, Shake them up!: a movement-based pairing protocol for CPU-constrained devices, in Proceedings of the 3rd international conference on Mobile systems, applications, and services. 2005, ACM: Seattle, Washington.

[15] Mayrhofer, R. and H. Gellersen, Shake Well Before Use: Authentication Based on Accelerometer Data, in 5th International Conference on Pervasive Computing (Pervasive 2007). 2007.

[16] Mayrhofer, R. and H. Gellersen. Shake well before use: two implementations for implicit context authentication. in Adjunct Proc. Ubicomp 2007. 2007. Innsbruck, AT.

[17] Shaked, Y. and A. Wool. Cracking the Bluetooth PIN. in MobiSys '05: Proceedings of the 3rd international conference on Mobile systems, applications, and services. 2005. Seattle, Washington: ACM.

[18] Kirovski, D., M. Sinclair, and D. Wilson, The Martini Synch: Using Accelerometers for Device Pairing. September 2007, Technical Report MSR-TR-2007-123, Microsoft Research.

[19] Soriente, C., G. Tsudik, and E. Uzun (2007) HAPADEP: Human Asisted Pure Audio Device Pairing. Cryptology ePrint Archive, Report 2007/093.

[20] Buhan, I., et al. Secure Ad-hoc Pairing with Biometrics: SAfE. in Proceedings of First International Workshop on Security for Spontaneous Interaction (IWSSI ’07),. 2007. Innsbruck, Austria.

[21] Balfanz, D., et al. Talking to strangers: Authentication in adhoc wireless networks. in Symposium on Network and Distributed Systems Security (NDSS '02). 2002. San Diego, California.

[22] Nicholson, A., et al., LoKey: Leveraging the SMS Network in Decentralized, End-to-End Trust Establishment, in Pervasive Computing. 2006. p. 202-219.

[23] Buhan, I., et al., Feeling is Believing: a location limited channel based on grip pattern biometrics and cryptanalysis. Advances in Biometrics, 2007.

[24] Spahic, A., et al., Pre-Authentication using Infrared. Privacy, Security, and Trust Within the Context of Pervasive Computing, 2005. Vol. 780: p. 105-112.

[25] Mayrhofer, R., M. Hazas, and H. Gellersen, An authentication protocol using ultrasonic ranging : Technical Report. 2006, Lancaster University.

[26] Mayrhofer, R. and M. Welch. A Human-Verifiable Authentication Protocol Using Visible Laser Light. in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. 2007.

[27] Gehrmann, C. and C.J. Mitchell, Manual Authentication for Wireless Devices. RSA Cryptobytes, 2004. Vol. 7(1): p. 29–37.

[28] Varshavsky, A., et al., Amigo: Proximity-Based Authentication of Mobile Devices, in UbiComp 2007: Ubiquitous Computing. 2007. p. 253-270.

[29] McCune, J.M., A. Perrig, and M.K. Reiter, Seeing-is-believing: using camera phones for human-verifiable authentication. Security and Privacy, 2005 IEEE Symposium on, 2005: p. 110 - 124.

[30] Ringwald, M. Spontaneous Interaction with Everyday Devices Using a PDA. in Proceedings Workshop on Supporting Spontaneous Interaction in Ubiquitous Computing Settings, Ubicomp02. 2002. Gothenburg, Sweden.

[31] Goodrich, M.T., et al. Loud and Clear: Human-Verifiable Authentication Based on Audio. in Distributed Computing Systems, ICDCS 2006. 26th IEEE International Conference. 2006.

[32] Malkani, Y.A., D. Chalmers, and I. Wakeman, Secure Device Association: Trends and Issues, in Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, A.-S.K. Pathan, Editor. October 2010, Auerbach Publication: CRC Press, Taylor & Francis Group, USA.

[33] Malkani, Y.A. and L.D. Dhomeja. Secure device association for ad hoc and ubiquitous computing environments in 5th IEEE International Conference on Emerging Technologies (ICET'09). October 2009. Islamabad, Pakistan.

[34] Phidgets: Products for USB Sensing and Control. 2010.

[35] Claycomb, W. and D. Shin. Towards secure resource sharing for impromptu collaboration in pervasive computing. in SAC '07: Proceedings of the 2007 ACM symposium on Applied computing. 2007. Seoul, Korea: ACM.

[36] Mimaroglu, S. Java Programming with Berkeley DBXML. 2010 [cited April, 2010]; Available from: http://linux.sys-con.com/node/175405.

[37] Uzun, E., K. Karvonen, and N. Asokan, Usability Analysis of Secure Pairing Methods, in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Editors. 2007, Springer Berlin / Heidelberg. p. 307-324.

[38] Valkonen, J., A. Toivonen, and K. Karvonen. Usability Testing for Secure Device Pairing in Home Networks. in UbiComp 2007 Workshop Proceedings. 2007. Innsbruck, Austria.

[39] Kumar, A., et al., A comparative study of secure device pairing methods. Pervasive and Mobile Computing, 2009. 5(6): p. 734-749.

[40] Kobsa, A., et al., Serial hook-ups: a comparative usability study of secure device pairing methods, in Proceedings of the 5th Symposium on Usable Privacy and Security. 2009, ACM: Mountain View, California. p. 1-12.

[41] Kainda, R., I. Flechais, and A.W. Roscoe, Usability and security of out-of-band channels in secure device pairing protocols, in Proceedings of the 5th Symposium on Usable Privacy and Security. 2009, ACM: Mountain View, California. p. 1-12.

[42] Malkani, Y.A. and L.D. Dhomeja, PSIM: A tool for analysis of device pairing methods. International Journal of Network Security and Its Applications (IJNSA), October 2009. 1(3).

[43] Kumar, A., et al. Caveat emptor: A comparative study of secure device pairing methods. in IEEE International Conference on Pervasive Computing and Communications (PerCom-09). 2009.

[44] Faulkner, L., Beyond the five-user assumption: benefits of increased sample sizes in usability testing. Behavior Research Methods, Instruments, & Computers, 2003. 35(3): p. 379-383.

[45] Lewis, J.R., IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instruction for Use. International Journal of Human-Computer Interaction, L. Erlbaum Associates Inc., Hillsdale, NJ, USA, Jan-March 1995. 7(1): p. 57 - 78.

[46] Nunnaly, J.C., Psychometric Theory, ed. R.R. Wright and M. Gardner. 1978, New York, USA: McGraw-Hill, Inc.

[47] Bierton, R. and R. Bates. Experimental Determination of Optimal Scales for Usability Questionnaire Design. in Proceedings of Human Computer Interaction (HCI-2000). 2000: British Computer Society.

[48] Nielsen, J. and J. Levy, Measuring Usability: Preference vs. Performance. Communications of the ACM, April, 1994. 37(4): p. 66-75.

[49] Uzun, E., K. Karvonen, and N. Asokan, Usability Analysis of Secure Pairing Methods, in Financial Cryptography and Data Security. 2008. p. 307-324.

[50] Reynolds, F., et al., Composite Capability / Preference Profiles (CC/PP): A User Side Framework for Content Negotiation, W3C NOTE-CCPP-19990727, July 1999, url: http://www.w3.org/TR/NOTE-CCPP/.

Authors

Dr. Yasir Arfat Malkani is a Lecturer at the Institute of Mathematics and Computer Science (IMCS), University of Sindh, Jamshoro, Pakistan. He got his Master's degree in Computer Science from University of Sindh, Jamshoro (Pakistan) in 2003 and PhD from University of Sussex, Brighton, UK in 2011. His main area of research is Pervasive Computing. His research is focused on secure device/service discovery and access control mechanisms using policies and location/proximity data/information. He is also interested in sensor networks, wireless networks (including WiFi, Bluetooth, WiMAX, etc), and solutions to various issues in distributed and pervasive computing systems through the integration of tools and techniques from distinct disciplines/areas. He is also interested in the design and/or development of various tools and techniques that might be useful in giving world-wide recognition to various national languages, such as SINDH and URDU.

Dr. Ayaz Keerio is an assistant Professor at the Institute of Mathematics and Computer Science (IMCS), University of Sindh, Jamshoro, Pakistan. He got his Master's degree in Computer Science from University of Sindh, Jamshoro (Pakistan) and PhD from University of Sussex, UK in 2011. His main area of research is Speech Recognition and Synthesis systems. He is also interested in digital signal processing, data communication & networks and mobile & distributed computing systems.

Dr. Lachhman Das Dhomeja is an Assistant Professor at the Institute of Information & Communication Technology (IICT), University of Sindh, Jamshoro, Pakistan. He got his Master's degree in Computer Technology from University of Sindh, Jamshoro (Pakistan) in 1991 and PhD from University of Sussex, UK in 2011. His main research area is Pervasive Computing in general and policy-based context-awareness in particular. His other research interests include secure device pairing in ubiquitous environments, software architectures and Distributed Computing.