Sindh Univ. Res. Jour. (Sci. Ser.) Vol.45 (4) 703-710 (2013)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Performance and Usability Analysis of Proof-of-proximity (PoP) Framework

Y. A. MALKANI[++], A. KEERIO, A. W. MAHESAR* K. DAHRI*

Institute of Mathematics and Computer Science (IMCS), University of Sindh, Jamshoro.

Abstract: Security and privacy remain to be a major concern for the computing world – from traditional wired networks to modern mobile ad-hoc networks (MANETs) and ubiquitous/pervasive computing systems. Ubiquitous computing systems vary from conventional computing systems due to several reasons, such as ubiquitous computing systems are by nature ad hoc, more dynamic and there is spontaneous interaction among the devices. Most of the time, these systems are composed of modern small, handheld or embedded devices. These modern devices have support for some kind of wireless channel (i.e. WiFi, Infrared, Bluetooth, Laser etc) for communication purposes. As the wireless channels are inherently prone to security risks, the communication among the devices in these systems is not secure and these are susceptible to various attacks, such as MiTM attack. Consequently, in order to secure these systems, we need different tools and techniques than conventional security mechanisms. One of the recently addressed issues in ad-hoc and ubiquitous computing systems is the establishment of a secure channel between two devices. In literature, it is called secure device pairing. This issue is addressed by many researchers and several solutions have been proposed. We also realized the importance of this issue and proposed a framework based approach to secure device pairing. The focus of this paper is the performance evaluation and extended usability analysis of the proposed Proof-of-Proximity (PoP) framework.

Keywords: Proof-of-Proximity, Security, Device Pairing, Performance Analysis, Usability Study.

1. INTRODUCTION

The issue of device pairing for mobile ad-hoc and ubiquitous computing systems is not new any more. It has been addressed by many researchers during the last 10 years and a large set of protocols, tools and techniques have been proposed. A survey on device pairing can be found in (Malkani *et al.,* 2009a, 2010a). Apart from academic researchers, in recent years several industrial and standardization agencies have also realized the importance of this issue. These include WiFi Alliance, Universal Serial Bus (USB) Forum), Microsoft Corporation and Bluetooth SIG (Special Interest Group). The focus of these agencies on the issue of device pairing is to specify secure, usable and standard or generic procedures for device association. However, as stated in (Malkani *et al.,* 2009a, 2010a) most of the existing techniques for device pairing may differ in terms of required hardware/software capabilities, the security against several attacks and in the required level of user involvement and his/her attention. For example, some of these schemes consider devices equipped with laser, infrared, Bluetooth, and/or ultrasound transceivers, while some other schemes require embedded microphones and/or speakers, displays, accelerometers, and LEDs and /or cameras. Similarly, few schemes exploit the knowledge of radio signals to establish the secure channel of communication between two or more devices, and few schemes are those, which require significant users' involvement and attention during the pairing process.

We advocated that if we continue to multiply the pairing protocols each of which is feasible for certain scenarios only, users might be confused about the selection of appropriate pairing schemes as well as about the steps to follow them due to cognitive overhead of remembering several steps of dozens of pairing schemes. For example, while pairing two mobile phones having the capabilities of accelerometer, microphone, speaker, display, camera, infrared and Bluetooth might confuse the user about the selection of best pairing protocol, because in the given situation there are several ways to pair the two devices. It is also noted that in modern mobile ad-hoc and ubiquitous computing systems heterogeneity is unavoidable in terms of devices' capabilities and requirements, and we require mechanisms that allow the user to choose the best possible protocols without requiring the user attention and/or without considering that the user have an in-depth knowledge of the technologies used in the modern devices (Malkani *et al.,* 2009a, 2010a). Considering these facts, we proposed a framework based approach to device pairing in (Malkani *et al.,* 2009b). In this framework, several pairing protocols are integrated within a generic architecture in order to

[++]Corresponding author: Yasir Arfat Malkani email: yasir.malkani@usindh.edu.pk

*Institute of Information and Communication Technology (IICT), University of Sindh, Jamshoro.

provide a standard solution to device paring. The implementation of the proposed Proof-of-Proximity (PoP) framework (Malkani *et al.,* 2009b) and the Co-location (CoLoc) protocol1 along with the details of the software components and classification of the PoP protocols is presented in (Malkani *et al.,* 2010b, 2012a). In the context of our research, the PoP protocols are the group of protocols, which are integrated in the proposed system to achieve the goal of device pairing through the demonstration of physical proximity. This set is chosen to demonstrate the concept, not to limit the use of others. The details of the evaluation of PoP Framework were presented in (Malkani *et al.,* 2012b). The evaluation is performed through analyzing the design features of the proposed system and the usability study results. Evaluation demonstrated that the proposed system achieved its defined goals well (Malkani *et al.,* 2012b). The focus of this paper is the performance analysis of the PoP framework along with extended analysis of the usability study results, which were not covered in earlier publications (Malkani *et al.,* 2009a, 2009b, 2010a, 2010b,2012a,2012b) of this research work.

The organization of the remaining part of this paper is as follow. In section 2, a brief summary of the PoP Framework is presented, in section 3 summary of the implementation of PoP framework is presented, in section 4 methodology of system's evaluation is described, section 5 describes the performance analysis of PoP Framework and section 6 describes the extended analysis of usability study, finally section 7 concludes the paper.

2. PROOF-OF-PROXIMITY FRAMEWORK

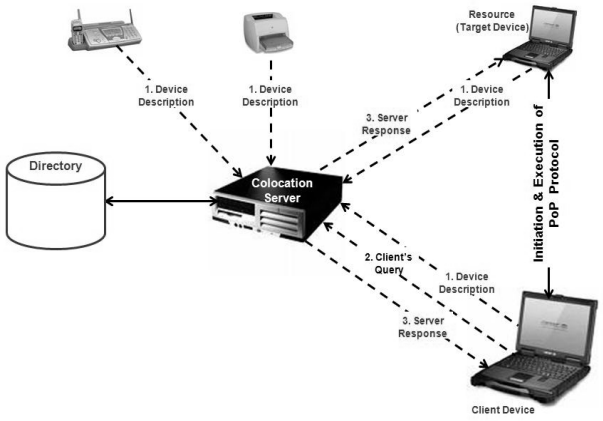


Figure 1: The high-level architecture of the PoP Framework

The high-level architecture of the PoP Framework is shown in **figure-1**. PoP Framework is composed of three parts: (1) registration, (2) devices' discovery, and (3) selection, initialization and execution of the Proof-of-proximity protocol. As stated earlier, note that all these parts are integrated and wrapped into a general protocol called CoLoc protocol. The details of CoLoc protocol can be found in (Malkani *et al.,* 2012a), however for the sake of completeness of this paper, we are reproducing the summary of the overall system in subsequent paragraphs.

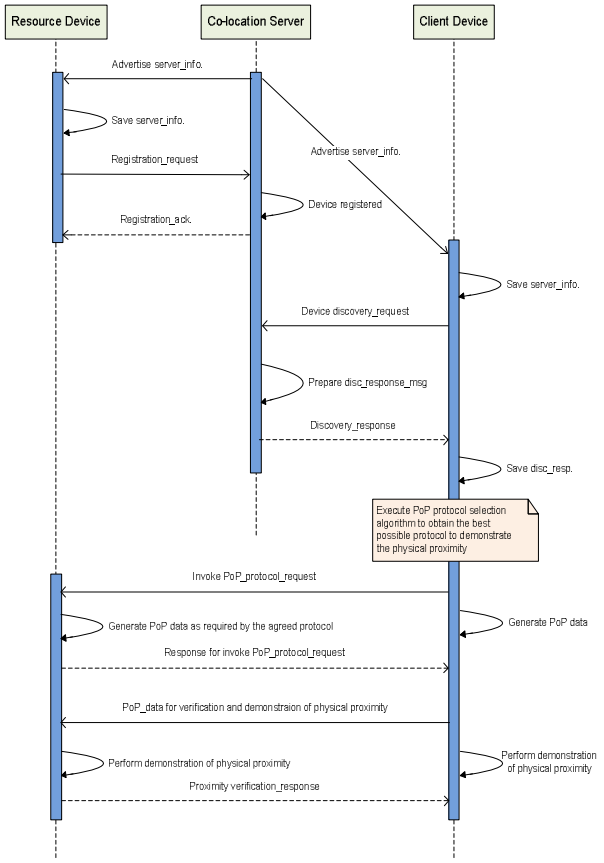


Figure 2: Message sequence diagram of the PoP Framework

The proposed PoP framework is composed of device discovery, several device pairing protocols and a protocol selection mechanism. These three parts are integrated into a generic model in such a way that allows pairing of devices using their existing capabilities. The proposed system also considers user preferences during the process of device pairing and helps the user in identifying the best pairing protocol according to the situation, thus relieves her/him from choosing between a large set (Balfanz, 2002; Castelluccia, 2005; Gehrmann, 2004; Goodrich, 2006; Holmquist, 2001; Kirovski, 2007; Mayrhofer, 2006, 2007a, 2007b; McCune, 2005; Prasad, 2008; Saxena, 2006, 2008, 2009; Soriente, 2007a, 2007b; Stajano, 2000, 2001; Varshavsky, 2007) of pairing protocols.

[1] All other sub-protocols of the proposed system are integrated and wrapped into a general protocol called CoLoc protocol, which is core part of the proposed PoP framework.

Interested reader can find the survey and detailed analysis of these existing paring schemes and protocols in (Malkani *et al.,* 2009a, 2010a). The key features of the PoP framework are below:

a) Secure and Generic: As stated, the proposed system integrates the device discovery mechanism and a set of several pairing protocols/schemes mainly identified and discussed in (Malkani *et al.,* 2009a, 2010a). Since none of the discovery systems in their original form were found to be suitable in for integration and prototype implementation of the PoP framework in terms of complexity and the features offered by these systems, Malkani *et al.,* (2009b) developed their own registration and discovery mechanism through combining several features of its own (such as confidentiality and integrity protection) and the existing well known discovery systems. This way the proposed framework is able to provide support for various PoP protocols along with integrity and confidentiality protected device discovery, and thereby comprehensively provides broader scope for device pairing in varied types of scenarios in mobile ad-hoc and ubiquitous computing environments.

b) Dynamic PoP protocol selection mechanism: The proposed framework follows a PoP protocols specification and selection policy when selecting a PoP protocol based on device capabilities and user preferences. The PoP protocol specification and selection mechanism is defined in an XML-based policy file. The XML-based policy allows modifying the protocol selection criterion at runtime. A runtime modification of the protocol selection criterion is useful for customizing the PoP protocol selection mechanism according to an individual user's or enterprise needs and preferences which were not foreseen at the time of deployment. In order to avoid redundancy, we have presented the overall working mechanism of PoP Framework in **figure 2** with the help of a message sequence diagram.

3. SYSTEM IMPLEMENTATION

For practical realization of the proposed PoP framework, a prototype implementation is carried out. The detailed description of prototype implementation of PoP framework is already published in (Malkani *et al.,* 2012a), however for completeness of this paper; we are reproducing the summary of system implementation in this section.

Total of fourteen PoP protocols are integrated in the prototype implementation of the PoP Framework. These are classified into three categories distinguishing user action(s) in the generation of PoP data and user involvement in verifying/matching PoP data. Those PoP protocols, which require some user action(s) in the generation of PoP data belongs to the category-1, the category-2 is composed of those PoP protocols, which involve user in the verification/matching of PoP data, and the category-3 contains those PoP protocols, which require user to be involved in both the generation and the verification of PoP data. **Table-1** presents the summary of the features of the implemented PoP protocols. Interested reader can find the detailed category-wise description of each of the implemented PoP protocol in (Malkani *et al.,* 2012a).

Table 1: List and features of the implemented PoP Protocols

The Implemented PoP Protocol	Device Capabilities		Human/User Involvement	Out-of-band/Location-limited secondary channel
	Device A	Device B		
Category-1: Users are involved in generating PoP data.				
Button-to-Button	A single button on each of the device		Press button on both of the devices simultaneously with random time-intervals until response signal received	Tactile
Blink-to-Button	An LED	A single button	Press and release button on device B whenever the LED of device A flashes/blinks	Visual and Tactile
Beep-to-Button	Speaker/Beeper	A single button	Press and release button on device B whenever the LED of device A flashes/blinks	Audio and Tactile
Seeing-is-Believing (SiB)	Display or Bar code sticker/label	Camera	Properly place camera of device B at the displayed bar code on device A with sufficient proximity and take the photograph	Visual
Category-2: Users are involved in verifying the PoP data.				
Blink-Blink	A single LED on each of the device		Compare the two synchronous LED blinking patterns	Visual
Blink-Beep	An LED	Speaker	Observe the synchronization of an LED blink with a beep generated from the other device	Audio and Visual
Beep-Beep	Speaker	Speaker	Compare the two vocalized MadLib sentences from both of the devices	Audio
Display-Display	Display	Display	Compare the two MadLib sentences displayed on both of the devices	Visual
Display-Speaker	Display	Speaker	Compare the MadLib sentence displayed on the screen of device A with the vocalized MadLib sentence from device B	Audio and Visual
Speaker-Speaker	Speaker	Speaker	Compare the two vocalized MadLib sentences from both of the devices	Audio
Digits Comparison	Display	Display	Compare two numbers displayed on both of the devices	Visual
Hash Comparison	Display	Display	Compare two hashes displayed on both of the devices	Visual
Category-3: Users are involved in both generating and verifying the PoP data.				
Selective Image Comparison (SiC)	Display	Display	Compare two images displayed on both of the devices	Visual
Capture and Show (CaS)	Display	Display and Camera	Take a photo of a nearby object/scene and compare it with the image displayed on the screens of both of the devices	Visual

4. SYSTEM EVALUATION METHODOLOGY

The methodology to evaluate the PoP Framework is mainly based on a usability study, which incorporates eight pairing protocols/schemes and the proposed system that integrates them. The reason for reducing the number of pairing schemes from 14 to 8 in conducting the usability study is to reduce the chances of data inconsistency caused by user fatigue. The eight PoP

protocols, which are chosen for the usability study, are: Button-to-Button, Blink-to-Button, Seeing-is-Believing (i.e. Category-1 PoP protocols), Blink-Blink, Display-Display, Display-Speaker (i.e. Category-2 PoP protocols), Selective Image Comparison, Capture and Show (i.e. Category-3 PoP protocols).

It is extensively accepted in the literature of usability study that any study, which is performed by twenty users captures over 98% of the usability issues (Faulkner, 2003). Therefore, a total of twenty participants were recruited in the usability process. All of the participants are either volunteer students or faculty of the University of Sussex, Brighton, United Kingdom. Most of the participants are good computer users. The usability study is carried out to test the three hypotheses: First, is an average user good at identifying a correct or best pairing protocol in case he/she has to choose from a large set of pairing protocols? Second, what should be the extent or level of user involvement in the process of device pairing? Third and the most important hypothesis is to check or verify that the proposed PoP framework is an effective solution of device pairing issue from user's perspective, and are they considering it as usable or not? The detail of usability study is already presented in (Malkani *et al.,* 2012b), which justifies that the proposed system meets its defined goals well. However the focus of this paper is performance evaluation of PoP Framework and the extended analysis of the usability results, which were not presented in (Malkani *et al.,* 2012b).

5. PERFORMANCE ANALYSIS

Note that the usability study results are generated from the data, which is collected through two types of questionnaires (i.e. two after-scenario-questionnaires (ASQs) and one post-test questionnaire) and two log files generated during the experiment. The data obtained from the two log files became the basis for performance analysis of the proposed system and the eight pairing schemes. Performance analysis is based on the average task completion times and the average task completion rates for each of the test cases. The graph presented in **figure 3** shows the average task completion time along with the standard deviation. It shows that Button-to-Button and SiB schemes are faster than all of the other schemes. Their average task completion times are 19.161 and 20.209 seconds respectively. Blink-to-Button and SiC have similar approximate average task completion times. Similarly, Blink-Blink and CaS have similar approximate average task completion times. CoLoc has the largest average task completion time. Since CoLoc incorporates several PoP schemes as sub- protocols, it is the fact that the task completion time for CoLoc is dependent on the chosen PoP protocol.

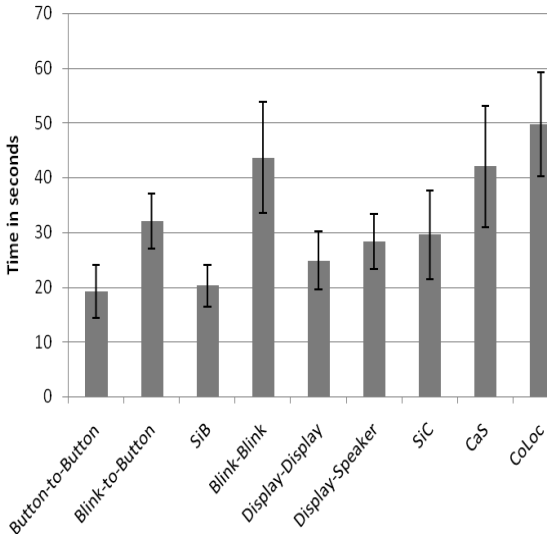


Figure 3: Average task completion time with standard deviation

Refer to the graph shown in **figure 4** for task completion rates. The task completion rate for all of the schemes is good. The only schemes that could not achieve 100% completion rate are Blink-to-Button with 95% completion rate, Blink-Blink with 85% completion rate and Display-Speaker with 90% completion rate.

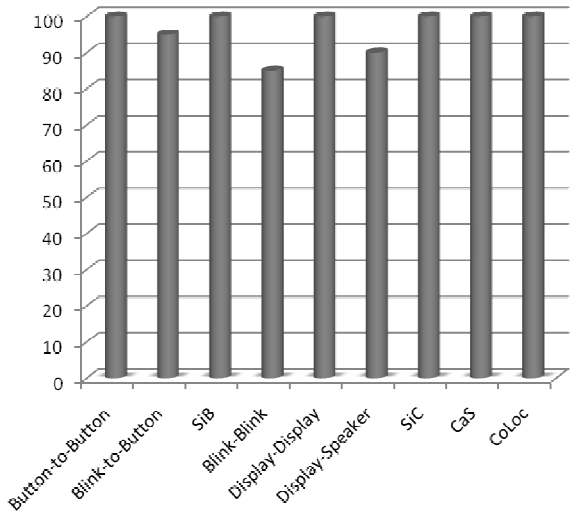


Figure 4: Task **completion rate for each of the test case**

6. EXTENDED ANALYSIS OF THE USABILITY STUDY RESULTS

Prior to performing the extended analysis, we present the categorized summary of the usability study results

in **table 2**. Some of the results (i.e. safe and fatal errors and user satisfaction) are reproduced from (Malkani, *et al.,* 2012b) for the sake of completeness.

Table 2: The categorized summary of the overall results

PoP Schemes	Average Time (sec)	Std Dev.	Safe Errors (%)	Fatal Errors (%)	User Satisfaction on Scale of 1-7	Task Completion Rate (%)
Category One						
Button-to-Button	19.161	4.857	2.5	N/A	6.216	100
Blink-to-Button	31.982	5.036	10	N/A	5.416	95
Seeing is Believing	20.209	3.778	7.5	N/A	6.15	100
Category Two						
Blink-Blink	43.608	10.153	10	5	5.016	85
Display-Display	24.841	5.342	0	5	6.1	100
Display-Speaker	28.33	5.075	15	25	4.85	90
Category Three						
Selective Image Comparison	29.587	8.05	0	0	5.25	100
Capture and Show	42.033	11.046	0	15	5.566	100
Proposed System						
CoLoc Protocol	49.738	9.414	2.5	N/A	5.616	100

(A) Combined Metrics Analysis

We calculated a single score from the collected raw data using the Single Usability Metric (SUM) model (Sauro and Kindlund, 2005a, 2010a) to rank each of the tested pairing schemes and the proposed system. SUM was originally introduced by Sauro and Kindlund (Sauro and Kindlund, 2005a). It is a single, summated and standardized usability evaluation metric, which is based on the ISO 9241 pt. 11 (Guidance on Usability, 1998) and the ANSI (Common Industry Format for Usability Test Reports, 2001) defined dimension of usability. A SUM score is calculated from the four usability evaluation metrics, which are: post-task satisfaction, task completion rate, average completion time of task, and average number of errors. These four metrics are aggregated into a single measure (known as SUM score) through the standardization process outlined in (Sauro and Kindlund, 2005b).

Table 3: Overall ranking of schemes based on SUM scores

Task Name	SUM Score			Task Completion Score	Task Satisfaction Score	Execution Time Score	Errors Score
	Low	Mean	High				
Seeing is Believing	76.8%	**83.8%**	97.9%	91.7%	97.6%	53.2%	92.8%
Display-Display	74.5%	**82.0%**	96.6%	91.7%	87.5%	53.6%	95.0%
Button-to-Button	72.8%	**80.5%**	96.3%	91.7%	83.3%	54.3%	92.8%
Coloc Protocol	61.8%	**72.2%**	89.4%	91.7%	51.1%	53.2%	92.8%
Capture and Show	60.4%	**71.3%**	87.9%	91.7%	47.2%	54.3%	91.9%
Selective Image Comparison	57.2%	**66.9%**	81.5%	91.7%	24.6%	54.6%	96.9%
Blink-to-Button	53.6%	**65.8%**	97.9%	87.7%	36.7%	52.6%	86.1%
Blink-Blink	48.1%	**59.8%**	74.9%	79.4%	14.1%	53.9%	91.9%
Display-Speaker	45.6%	**56.1%**	70.7%	83.6%	3.7%	53.0%	84.2%

In order to avoid any errors in calculation, we have used an Ms Excel utility package to calculate the SUM score, which is designed by Sauro and available from (Sauro and Kindlund, 2010b). This utility follows the original calculation process of the SUM score as outlined in (Sauro and Kindlund, 2005b) and contains the required pre-set functions, formulas and a set of sample data for illustration purposes. We entered all of the collected raw data into the downloaded spreadsheet package according to the specified rules and format, and finally got the results presented in table 3 using the confidence level of 95%. According to these results, SiB has the highest SUM score, while Display-Speaker has the lowest. PoP Framework (i.e. Coloc Protocol) is fourth with a SUM score of 72.2%, which interestingly out performs most of the schemes (even they do not include registration and discovery phases) that are tested without integrating into the PoP framework.

(B) Categories Ranking

Figure 5 shows the graphs, which are drawn from the data obtained through post-test questionnaire. Results show the ranking for each of the category of PoP scheme as given by the participants. Note (as stated earlier) that category-1 is that in which user is involved in generating PoP data; category-2 is that in which user is responsible for verifying the PoP data; and category-3 is that in which user is involved in both generating the PoP data and verifying it. Category-1 consists of Button-to-Button, Blink-to-Button and Seeing is Believing schemes. Category-2 is composed of Blink-Blink, Display-Display and Display-Speaker schemes. Category-3 consists of Selective Image Comparison and Capture and Show schemes.

Results show that 85% of the participants ranked category-1 as the number one; it is ranked as number two by 15% participants, and none has ranked it as number three. Category-2 is ranked as number one by 15% participants; it is ranked as number two by 35% participants, and 50% of the participants ranked it as number three. In the case of category-3, none has ranked it as number one, however 50% of the participants ranked it as number two and remaining 50% of the participants ranked it as number three. These results revealed that most of the participants preferred the first category of PoP protocols in which they were involved in generating PoP data. None of the participants ranked the third category of PoP protocols as their favourite, while second category has a moderate ranking as few have ranked it first, some have ranked it second and the remaining ranked it third. Further, in category-1 the most preferred or satisfactory PoP protocol is Button-to-Button, in category-2 the most preferred PoP protocol is Display-Display, and in category-3 the most preferred PoP protocol is Capture and Show. These results suggest that users usually prefer to take part and willing to be involved in the pairing process. However, some of them prefer to be involved at the beginning of the proof-of-proximity

phase in order to generate the PoP data, while others prefer to be involved during the last steps for verification of the PoP data; but majority of the users do not prefer to be involved in the process from the beginning to end of the pairing process. This advocates the fact that user involvement in the secure pairing process is unavoidable (Suomalainen *et al.,* 2007); however users do not prefer excessive and unrestrained involvement or interactions during the pairing process.

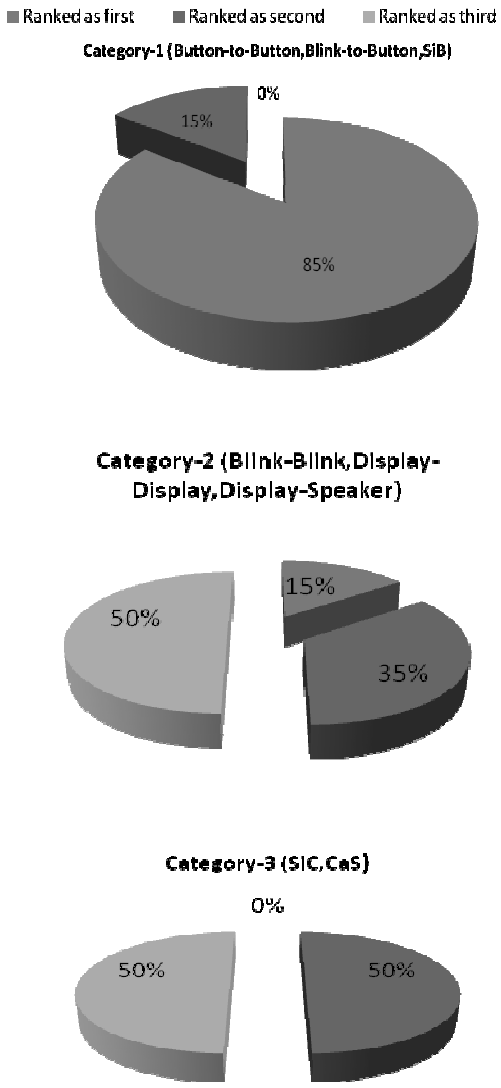


Figure 5: Category-wise ranking of pairing schemes

(C) Impact of Gender

The usability study participants' recruitment process was performed without controlling any balance on the participant dependant variables, such as age and gender. Since there was little difference in the sample size for each gender (55% male and 45% female), we performed unpaired t-tests to investigate the effect of gender on average completion time and user satisfaction rating scores. Test results revealed that there is not a statistically significant effect of gender on participants' satisfaction ratings and task completion time.

(D) Impact on the Proposed System

The usability study of the eight pairing schemes has an impact on the proposed system. The results are useful in improving the PoP protocol selection mechanism. Particularly, the SUM score can be used to prioritize the PoP protocols. In this case, the decision mechanism used to set the recommended order of the PoP protocols would also consider the ranking as produced by the SUM score.

7. CONCLUSION

In this paper, the performance evaluation and extended usability analysis of a framework for secure device pairing is presented. The performance analysis showed that the proposed PoP framework out performs most of the pairing schemes. The results obtained through the extended analysis of the usability study data are in favour of a widely accepted view on the part of academic researchers, and the device manufacturers or industrial researchers that some level of human intervention/interaction in the process of secure device pairing is inevitable; however, the results also indicated that human users are interested in moderate level of involvement or interaction. They do not want to be overburdened with human-to-device interactions. It is noted that the usability study results of eight pairing schemes are also useful in improving the protocol selection criteria in PoP Framework. Finally, we believe that the results and findings of this work including (Malkani *et al.,* 2009a, 2009b, 2010a, 2010b,2012a,2012b) motivates the research community to re-think the issue of secure device pairing and come up with a more standardized, common and universal solution.

ACKNOWLEDGEMENTS

The work presented in this paper has carried out by the first author as part of his PhD research at University of Sussex, UK. Authors want to say many thanks to Dan Chalmers and Ian Wakeman for their full support and guidance during this research. Other parts of this research work are already published in (Malkani *et al.,* 2009a, 2009b, 2010a, 2010b, 2012a,2012b).

REFERENCES:

Balfanz, D., D. K. Smetters, P. Stewart and H. C. Wong. (2002). Talking to strangers: Authentication in adhoc wireless networks. in Symposium on Network and Distributed Systems Security (NDSS '02). San Diego, California.

Castelluccia, C. and P. Mutaf. (2005). 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. ACM: Seattle, Washington.
Common Industry Format for Usability Test Reports (ANSI-NCITS 354-2001). (2001). American National Standards Institute. Washington, DC.

Ergonomic Requirements for Office Work with Visual Display Terminal (VDTs). (1998). in Part 11: Guidance on usability (ISO 9241-11:1998(E)). Geneva, Switzerland.

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

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

Goodrich, M.T., M. Sirivianos, J. Solis, G. Tsudik and E. Uzun. (2006). Loud and Clear: Human-Verifiable Authentication Based on Audio. in 26th IEEE International Conference on Distributed Computing Systems (ICDCS-06).
.
Holmquist, L.E., F. Mattern, B. Schiele, P. Alahuhta, M. Beigl and H. Gellersen. (2001). Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts, in Proceedings of the 3rd international conference on Ubiquitous Computing. Springer-Verlag: Atlanta, Georgia, USA.

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

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

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

Malkani, Y. A., D. Chalmers, I. Wakeman and Lachhman Das Dhomeja. (2009b). Towards a General System for Secure Device Pairing by Demonstration of Physical Proximity, in MWNS-09 co-located with IFIP Networking Conference, Shaker Verlag: Aachen, Germany. ISBN: 978-3-8322-8177-9. 13-24.

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

Malkani, Y. A., D. Chalmers, and I. Wakeman. (2010b). A framework for secure device pairing by demonstration of physical proximity, in ACM Proceedings of the 8th International Conference on Frontiers of Information Technology (FIT'10). Islamabad, Pakistan.1-6.

Malkani, Y. A., D. Chalmers, and I. Wakeman, and L.D Dhomeja. (2012a). A Generic Framework for Device Pairing in Ubiquitous Computing Environments. International Journal of Network Security & its Applications (IJNSA). Vol. 04, No. 02.

Malkani, Y. A., A. Keerio, and L. D Dhomeja. (2012b). Secure Device Pairing: A Usability Study. International Journal of UbiComp (IJU), Vol. 03, No. 02.

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

Mayrhofer, R. and H. Gellersen. (2007a). Shake Well Before Use: Authentication Based on Accelerometer Data, in 5th International Conference on Pervasive Computing (Pervasive-07).

Mayrhofer, R. and M. Welch. (2007b). A Human-Verifiable Authentication Protocol Using Visible Laser Light. in proceedings of second international conference on availability, reliability and security. ARES 2007.

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

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

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

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

Sauro, J. and E. Kindlund. (2005a). A Method to Standardize Usability Metrics into a Single Score, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM: Portland, Oregon, USA.

Sauro, J. and E. Kindlund. (2005b). Making Sense of Usability Metrics: Usability and Six Sigma. in Proceedings of the 14th Annual Conference of the Usability Professionals Association. Montreal, Canada.
Sauro, J. and E. Kindlund. (2010a). Using a Single Usability Metric (SUM) to Compare the Usability of Competing Products.

URL:http://www.measuringusability.com/papers/HCII2005_sauro_kindlund-V9.pdf.
Sauro, J. Measuring Usability: Quantitative Usability, Statistics & Six Sigma. (2010b). URL:http://www.measuringusability.com/SUM/index.htm.

Saxena, N., J. E. Ekberg, K. Kostiainen, N. Asokan. (2006). Secure Device Pairing based on a Visual Channel. in IEEE Symposium on Security and Privacy, 306-313.

Saxena, N. and M. Uddin. (2008). Automated Device Pairing for Asymmetric Pairing Scenarios, in Information and Communications Security. 311-327.

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

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

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

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

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

Suomalainen, J., J. Valkonen, and N. Asokan. (2007). Security Associations in Personal Networks: A Comparative Analysis. Lecture Notes in Computer Science, Springer Berlin/Heidelberg, Volume 4572/2007: 43-57.

Varshavsky, A., A. Scannell, A. LaMarca and E. de Lara. (2007). Amigo: Proximity-Based Authentication of Mobile Devices, in Ubiquitous Computing (UbiComp-07). 253-270.

.