Foreword

René Mayrhofer

Faculty of Computer Science,
University of Vienna,
Dr.-Karl-Lueger-Ring 1, A-1010 Vienna, Austria
E-mail: rene@mayrhofer.eu.org

Kaisa Nyberg

Department of Information and Computer Science,
Helsinki University of Technology,
Konemiehentie 1, FI-02150 TKK, Espoo, Finland
E-mail: kaisa.nyberg@tkk.fi

Tim Kindberg

Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford
Bristol BS34 8QZ, UK
E-mail: timothy@hpl.hp.com

Biographical notes: René Mayrhofer currently holds a guest professorship for Mobile Computing at the University of Vienna, Austria. His research interests include computer security, ubiquitous computing, and machine learning, which are combined in his recent research to create usable, intuitive, and unobtrusive techniques for securing spontaneous interaction. Before his current position, he received his Dipl.-Ing. (MSc) and Dr. techn. (PhD) degrees from Johannes Kepler University Linz, Austria and subsequently held a Marie Curie Fellowship at Lancaster University, UK. He is an author of about 30 scientific papers on context-aware systems, handling sensor data, and security protocols based on these concepts.

Kaisa Nyberg holds a chair in Cryptology at Helsinki University of Technology since 2005. She has a PhD degree in Mathematics from the University of Helsinki. Her career in Cryptography spans over about 20 years. In 1998 she joined Nokia and is now responsible for cryptographic techniques in cellular security and related applications. She is a co-author of the book ‘UMTS Security’, Wiley & Sons, Chichester 2003, and a member of the designer team of the Bluetooth Simple Pairing. She acted as an editor of international standards on digital signatures with ISO/IEC SC27 Working Group WG2 ‘Security Mechanisms’. She is an author of about 40 scientific papers and book chapters on digital signatures, design and analysis of symmetric key cryptography and security protocols.

Tim Kindberg’s research interests are in ubiquitous and mobile computing, particularly in urban settings. He has been a senior researcher at HP Labs since 1999, in Palo Alto and Bristol. He is a Visiting Professor of Computer Science at the University of Bath. Previously, he was Senior Lecturer in Computer Science at Queen Mary, University of London, and principal software engineer at start-up Zebra Parallel. He is co-author of the textbook Distributed Systems – Concepts and Design. He holds a PhD in Computer Science from the University of Westminster and a BA in Mathematics from the University of Cambridge.

IWSSI 2007, the First International Workshop on Security for Spontaneous Interaction, brought together researchers working on this topic, to define open issues, clarify the terminology, and foster cooperation between researchers in this area. The present special issue combines extended versions of workshop papers with additional, invited contributions. The latter extend previous publications in the light of newer developments, and combine multiple publications for thorough coverage of a specific topic.

One of the main issues in security for spontaneous interaction is the lack of common ground. This includes both terminology (e.g., ‘context-based authentication’ vs. ‘ephemeral pairing’) and a shared understanding of the open research issues covering various aspects like user interaction, cryptographic primitives, and dealing with limited device resources. IWSSI 2007 provided a forum for researchers to discuss these problem areas and to put forward an agenda for future research. One of the results is that, due to the diversity of application scenarios, device types, and security demands, many different approaches for securing spontaneous interactions have already been proposed.

However, there are commonalities. In the absence of a priori shared information or trusted third parties, a common approach is to support the user in connecting two devices securely. This is often based on a special type of channel with physical affordances that the user can directly understand. There are various terms for such a channel, including 'constrained channel' and 'location-limited channel'. But there is a reasonable level of agreement that this is an out-of-band channel[1] that can be directly established or manipulated by the user, and which provides authentication, and sometimes also secrecy, to some level of confidence due to its physical properties alone. One of the first suggestions was direct physical contact. Research progressed to include experimentation with infrared, lasers, audio, ultrasound, the visual channel between a camera and display or between a camera and object, and mutual movement; additionally, some physical properties of the main, in-band wireless channels have been studied.

Whatever their exact physical nature, the foregoing out-of-band channels are used to bootstrap cryptographic protocols. Many protocols have been devised specifically to exploit one such type of out-of-band channel or another. Many have recently been found to belong to the same family of protocols called MANA IV.

A strongly related common approach is for the human to validate an existing spontaneous association between two devices, one that has already been created with a reasonable probability of success. In this case, the procedure is first to exercise a cryptographic protocol such as Diffie-Hellman key exchange, and then for the human to verify that precisely the correct entities have exchanged secret material, by examining evidence on a multimedia out-of-band channel. For example, the human is asked to compare information on two displays, or to compare the musical notes that two devices emit. Another option is for humans to provide common input that can be used in cryptographic protocols to ensure that only devices having received such an input can participate in the interaction.

Whatever the particular approach to securing spontaneous interaction, we observe that an old concept in the security literature, the trusted computing base, is undergoing a transformation as we extend computing away from the enterprise and desktop. Once, we relied on security professionals to safeguard the critical system components on which the security of our systems rely. Now, in pervasive and mobile computing, we are asking users to make spontaneous judgements about the trustworthiness of devices and the auxiliary channels that researchers are devising. This is a huge step. As a research community, we will need an interdisciplinary approach that connects our understanding of user perceptions and behaviours to the technical properties of our mechanisms and protocols.

In the meantime, for this special issue, the focus lies on contributions that tie together or review various approaches and therefore provide a broader discussion of some aspect or topic of security for spontaneous interactions, as well as novel authentication techniques and protocols.

Adin Scannell, Alex Varshavsky, Anthony LaMarca and Eyal de Lara present an authentication protocol that uses wireless LANs both for in-band communication and out-of-band verification that the interacting devices are sufficiently close to each other, that is, co-located. This approach is highly interesting from a practical point of view, because it does not require any additional hardware for secure spontaneous authentication and is unobtrusive from a user point of view.

Claudio Soriente, Gene Tsudik and Ersin Uzun also present an authentication protocol not relying on additional hardware; in this case, single buttons are used to transfer or input quasi-random messages based on the length and spacing of button presses. Although it directly involves users in authentication, this approach may be of high practical relevance due to its re-use of existing hardware components.

Ileana Buhan, Bas Boom, Jeroen Doumen, Pieter Hartel and Raymond Veldhuis present the use of biometric user data as another out-of-band medium for authentication. Hand grip patterns and facial images are evaluated and a novel protocol making use of 'fuzzy' cryptographic primitives is theoretically and practically analysed. Using facial images for authentication with another user's device is interesting from a user point of view, because the same images can be used for intuitive future reference.

Jonathan M. Mcune, Adrian Perrig and Michael K. Reiter also use video cameras as out-of-band media, but for direct transfer of messages by capturing 2D bar codes displayed on another device, either statically or dynamically generated. Comparable to taking facial images, users can observe what their device captures, and thus implicitly verify physical authenticity. In comparison to their earlier publication, the presented protocol can now optionally be based on MANA IV.

Michael T. Goodrich, Michael Sirivianos, John Solis, Claudio Soriente, Gene Tsudik and Ersin Uzun present the use of audio instead of video for spontaneous device authentication, both by letting users compare English sentences spoken by the interacting devices and by using MIDI sequences played by one and captured by the other device for direct, out-of-band transmission. The use of audio also provides physical evidence of the authenticity of device interactions.

Sven Laur and Sylvain Pasini present a detailed summary and analysis of authentication protocols based on short out-of-band message transmission, for example performed by users. Different variations of protocols are analysed in a common threat model and it is shown that some of these protocols are optimal in terms of the length of the out-of-band transmission. These results seem applicable to most of the out-of-band media suggested by the previous papers, and are important for constructing theoretically secure implementations.

Jani Suomalainen, Jukka Valkonen and N. Asokan in turn analyse protocols that have already been standardised in terms of online and offline threat scenarios and present a taxonomy for classifying authentication protocols suitable for spontaneous interaction. An important insight is that, although standards may include secure authentication modes, attacks can succeed by exploiting different standard options and forcing devices into switching modes without the user explicitly noticing.

Cynthia Kuo, Adrian Perrig, and Jesse Walker complement the previous paper by specifically analysing user behaviour based on a practically relevant case study, concluding that the combination of seemingly simple security tasks can be too demanding.

This special issue therefore presents an overview of the current state of the art in security for spontaneous interaction, ranging from specific, technically oriented proposals for out-of-band transmission media to theoretical analysis and comparison of cryptographic protocols and finally the evaluation of user behaviour as the most important part of secure systems. The breadth of contributions is owed to the interdisciplinary nature of this research topic and outlines once more that research on security, especially in the challenging context of spontaneous interaction, needs to take a systems perspective, neglecting neither low-level communication channel details nor mental models and user behaviour.

Note

[1] The term out-of-band channel is commonly used in research publications to mean an auxiliary way to transmit messages besides the main (in-band) wireless communication channel. This general meaning was also agreed upon in the open panel session of IWSSI 2007 among various research groups. Some standardisation efforts, however, restrict its use to describe a secondary wireless channel.