[1] D. Balfanz, G. Durfee, D. Smetters, and R. Grinter. In search of usable security: five lessons from the field. *Security & Privacy, IEEE*, 2(5):19-24, Sept.-Oct. 2004. [bib | DOI]

A new system reduces the time to enroll in a secure wireless network by two orders of magnitude, and it also gets high marks for usability and user satisfaction. This article provides a real-world example revealing five general lessons for usable, secure system design.

Keywords: computer network management, human computer interaction, public key cryptography, security of data, telecommunication security, wireless LAN PKI, enrolling time, public key infrastructure, secure system design, secure wireless network, usability, usable security, user satisfaction

[2] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium (NDSS)*, February 2002. [bib | .html]

In this paper we address the problem of secure communication and authentication in ad-hoc wireless networks. This is a difficult problem, as it involves bootstrapping trust between strangers. We present a user-friendly solution, which provides secure authentication using almost any established public-key-based key exchange protocol, as well as inexpensive hash-based alternatives. In our approach, devices exchange a limited amount of public information over a privileged side channel, which will then allow them to complete an authenticated key exchange protocol over the wireless link. Our solution does not require a public key infrastructure, is secure against passive attacks on the privileged side channel and all attacks on the wireless link, and directly captures users' intuitions that they want to talk to a particular previously unknown device in their physical proximity. We have implemented our system in Java for a variety of different devices, communication media, and key exchange protocols.

[3] L. Eschenauer, V. D. Gligor, and J. S. Baras. On trust establishment in mobile ad-hoc networks. In *Security Protocols Workshop*, volume 2845 of *Lecture Notes in Computer Science*, pages 47-66, 2004. [bib | DOI | .pdf]

We present some properties of trust establishment in mobile, ad-hoc networks and illustrate how they differ from those of trust establishment in the Internet. We motivate these differences by providing an example of ad-hoc network use in battlefield scenarios, yet equally practical examples can be found in non-military environments. We argue that peer-to-peer networks are especially suitable to solve the problems of generation, distribution, and discovery of trust evidence in mobile ad-hoc networks, and illustrate the importance of evaluation metrics in trust establishment.

[4] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human-verifiable authentication based on audio. In *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 10-17, 2006. [bib | DOI]

Secure pairing of electronic devices that lack any previous association is a challenging problem which has been considered in many contexts and in various flavors. In this paper, we investigate the use of audio for human-assisted authentication of previously un-associated devices. We develop and evaluate a system we call *Loud-and-Clear (L&C)* which places very little demand on the human user. L&C involves the use of a text-to-speech (TTS) engine for vocalizing a robust-sounding and syntactically-correct (English-like) sentence derived from the hash of a device's public key. By coupling vocalization on one device with the display of the same information on another device, we demonstrate that L&C is suitable for secure device pairing (e.g., key exchange) and similar tasks. We also describe several common use cases, provide some performance data for our prototype implementation and discuss the security properties of L&C.

[5] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In *Proceedings of the 5th International Conference on Pervasive Computing*, volume 4480 of *Lecture Notes in Computer Science*, pages 144-161, May 2007. [bib | DOI | .pdf]

Small, mobile devices without user interfaces, such as Bluetooth headsets, often need to communicate securely over wireless networks. Active attacks can only be prevented by authenticating wireless communication, which is problematic when devices do not have any a priori information about each other. We introduce a new method for device-to-device authentication by shaking devices together. This paper describes two protocols for combining cryptographic authentication techniques with known methods of accelerometer data analysis to the effect of generating authenticated, secret keys. The protocols differ in their design, one being more conservative from a security point of view, while the other allows more dynamic interactions. Three experiments are used to optimize and validate our proposed authentication method.

[6] J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. pages 110-124, May 2005. [bib | DOI]

Current mechanisms for authenticating communication between devices that share no prior context are inconvenient for ordinary users, without the assistance of a trusted authority. We present and analyze seeing-is-believing, a system that utilizes 2D barcodes and camera-telephones to implement a visual channel for authentication and demonstrative identification of devices. We apply this visual channel to several problems in computer security, including authenticated key exchange between devices that share no prior context, establishment of a trusted path for configuration of a TCG-compliant computing platform, and secure device configuration in the context of a smart home.

Keywords: authorisation, bar codes, cameras, cryptography, mobile computing, mobile handsets, telecommunication security 2D barcodes, TCG-compliant computing platform, authenticated key exchange, camera phones, camera-telephones, computer security, demonstrative device identification, human-verifiable authentication, secure device configuration, seeing-is-believing system, smart home, trusted path, visual channel

[7] N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel (short paper). In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 306-313, 2006. [bib | DOI]

Recently several researchers and practitioners have begun to address the problem of how to set up secure communication between two devices without the assistance of a trusted third party. McCune, et al. [6] proposed that one device displays the hash of its public key in the form of a barcode, and the other device reads it using a camera. Mutual authentication requires switching the roles of the devices and repeating the above process in the reverse direction. In this paper, we show how strong mutual authentication can be achieved even with a unidirectional visual channel, without having to switch device roles. By adopting recently proposed improved pairing protocols, we propose how visual channel authentication can be used even on devices that have very limited displaying capabilities.

[8] F. Stajano and R. Anderson. The resurrecting duckling: security issues for ubiquitous computing. *Computer*, 35(4):22-26, Apr 2002. [bib | DOI]

Imagine the future: hundreds of embedded computers per person, all cooperating via ad hoc wireless networks. What will the security implications be? Peer-to-peer and ubiquitous computing systems involve many principals, but their network connectivity is intermittent and not guaranteed. Traditional approaches to authentication, from Kerberos to public-key certificates, are therefore unworkable, because they rely on online connectivity to an authentication or revocation server. The paper considers new solutions. It discusses the Resurrecting Duckling security policy model. The traditional taxonomy of security threats identifies three main classes which are considered: confidentiality, integrity or availability.

Keywords: data integrity, data privacy, security of data, telecommunication securityResurrecting Duckling security policy model, ad hoc wireless networks, authentication, availability, data confidentiality, data integrity, data security, embedded computers, peer-to-peer, ubiquitous computing

[9] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, volume 1796 of *Lecture Notes in Computer Science*, pages 172-194, 1999. [bib | www:]

In the near future, many personal electronic devices will be able to communicate with each other over a short range wireless channel. We investigate the principal security issues for such an environment. Our discussion is based on the concrete example of a thermometer that makes its readings available to other nodes over the air. Some lessons learned from this example appear to be quite general to ad-hoc networks, and rather different from what we have come to expect in more conventional systems: denial of service, the goals of authentication, and the problems of naming all need re-examination. We present the *resurrecting duckling* security policy model, which describes secure transient association of a device with multiple serialised owners.

[10] J. Suomalainen, J. Valkonen, and N. Asokan. Security associations in personal networks: A comparative analysis. Technical Report NRC-TR-2007-004, Nokia Research Center, January 2007. [bib | .pdf]

Introducing a new device to a network or to another device is one of the most security critical phases of communication in personal networks. There have been several different proposals to make this process of *associating* devices both easy-to-use and secure. Some of them have been adapted by emerging standard specifications. In this paper, we first present a taxonomy of protocols for creating security associations in personal networks. We then make use of this taxonomy in surveying and comparing association models proposed in several emerging standards. We also identify new potential attack scenarios.

Keywords: Personal networks - security association - survey

[11] E. Uzun, K. Karvonen, and N. Asokan. Usability analysis of secure pairing methods. Technical Report NRC-TR-2007-002, Nokia Research Center, January 2007. [bib | .pdf]

Setting up security associations between end-user devices is a challenging task when it needs to be done by ordinary users. The increasing popularity of powerful personal electronics with wireless communication abilities has made the problem more urgent than ever before. During the last few years, several solutions have appeared in the research literature. Several standardization bodies have also been working on improved setup procedures. All these protocols provide certain level of security, but several new questions arise, such as “how to implement this protocol so that it is easy to use?” and “is it still secure when used by a non-technical person?” In this paper, we attempt to answer these questions by carrying out a comparative usability evaluation of selected methods to derive some insights into the usability and security of these methods as well as strategies for implementing them.

[12] S. Čapkun and M. Čagalj. Integrity regions: authentication through presence in wireless networks. In *Proceedings of the 5th ACM workshop on Wireless Security (WiSe)*, pages 1-10, 2006. [bib | DOI]

We introduce *Integrity (I) regions*, a novel security primitive that enables message authentication in wireless networks without the use of pre-established or pre-certified keys. Integrity regions are based on the verification of entity proximity through time-of-arrival ranging techniques. We demonstrate how I-regions can be efficiently implemented with ultrasonic ranging, in spite of the fact that ultrasound ranging techniques are vulnerable to distance enlargement and reduction attacks. We further discuss how I-regions can be used in key establishment applications in peer-to-peer wireless networks.
