The Weakest Link: Security in Human Interactive Security Protocols.

Ronald Kainda

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford, OX1 3QD, UK

Ad hoc networks of mobile devices have posed challenges never seen before in conventional wired networks. In conventional wired networks, the use of trusted third parties or Public Key Infrastructure (PKI) has worked quite well. However, in ad hoc networks of mobile devices, there is no PKI that can cover all devices and scenarios at a reasonable cost[6]. In addition, these networks are usually created among devices that share no secrets nor know each other's identity.

The lack of a PKI that is both sufficiently universal and sufficiently available to cover all scenarios or presence of trusted third parties holding pre-shared secrets in ad hoc networks has forced researchers to look for alternative ways in which secure device association can be achieved in such environments. A common denominator among the proposed alternatives is the use of an out-of-band (OOB) or empirical channel [5].

The use of two channels has been proposed: one is a high bandwidth channel which is subject to the Dolev-Yao attacker model[1] [1] where messages that are public are exchanged between associating devices. The second channel is a low bandwidth out-of-band or *empirical* channel, which is not subject to the Dolev-Yao attacker model, through which messages that need integrity and or secrecy are exchanged.

On the normal channel, usually public keys are exchanged. These keys could be long term keys or ephemeral depending on the application. Assuming that the information exchanged on the normal channels are public keys, either one device whose key needs to be authenticated sends its public key to the other device(s) or all devices involved exchange their public keys.

The requirement on the empirical channel, that it should not be subject to the Dolev-Yao model of attack, has attracted much attention directed at finding ways in which it could be achieved. One proposal is based on the fact that two interacting human beings have a certain level of trust between them even though their devices have no previous association. In order to bootstrap security on the devices, the already existing human trust can be transferred to their devices. To this regard, humans are required to transfer information between devices that they identify as required to establish an association.

However, these proposals suffer from what will be termed here as the *weakest link problem*. Humans have, for some time now, been identified as the weakest link in a security chain [7, 8]. This is because, in many instances, security is not a primary goal for users [9] and any attempt to distract users from their primary goal in order to 'do security' may result in security being ignored or done only to get the primary goals achieved. Essentially, any security proposal that exerts mental and or physical workload on human users is likely to suffer from the weakest link problem.

The major challenge on the empirical channel is finding a trade off that achieves the required level of security for the amount of effort human users put into it. Examples of some of the proposals of implementing an empirical channels include comparing short strings [2, 3], and using an auxiliary device such as a camera phone [4] to transfer data between devices.

[1] Under the model, the attacker has control over the network; he can overhear, block, modify or insert messages on the channel.

However, these proposals not only demand human effort but also high degree of attention from users in order to achieve secure device associations. As a result some of these proposals are vulnerable to insecure actions from users, some demand too much effort from users such that they risk not being accepted in daily use while some are promising.

A usability study comparing some of the proposed methods has revealed some serious challenges to these proposals. These challenges are not only usability, but also security. They are as a result of the failure to design protocols around would be human users.

The study was conducted by recruiting participants to use a prototype of a mobile peer-to-peer payment system running on two mobile phones. Each participant interacted with all methods in the study. Objective data was collected by logging the number of errors and completion times while subjective data was collected through questionnaires and interviews.

Contrary to what most proponents of various methods claim, the results show that many of these methods are an 'added complication' that could result in usability problems and or security failures. Some of these methods, however, offer some strengths that cannot be ignored hence requires improvements and further investigations. Laboratory user studies have a weakness in that they may not reflect what is possible in a real world setting. However, this turned out to be one of the strengths of this study since in real world applications there are more challenges and if these methods can show weaknesses in an environment with fewer challenges then more could be found otherwise.

Future work will focus on developing a framework under which empirical channels that are both usable and secure may be developed. A number of factors that could help in developing this framework have already been identified. The major challenge is that the amount of data that has to be transmitted on the empirical channel entirely depends on the design of a particular protocol and as such no single empirical channel method may cover all protocols but rather a framework that would help decide what to use is necessary.

References

1. Dolev, D., and Yao, A. On the security of public key protocols. *Information Theory, IEEE Transactions on 29*, 2 (Mar 1983), 198–208.
2. Gehrmann, C., Mitchell, C. J., and Nyberg, K. Manual authentication for wireless devices. In *RSA Cryptobytes* (Spring 2004), vol. 7(1), RSA Security, pp. 29–37.
3. Goodrich, M., Sirivianos, M., Solis, J., Tsudik, G., and Uzun, E. Loud and clear: Human-verifiable authentication based on audio. In *Proc. 26th IEEE International Conference on Distributed Computing Systems ICDCS 2006* (04–07 July 2006), pp. 10–10.
4. McCune, J., Perrig, A., and Reiter, M. Seeing-is-believing: using camera phones for human-verifiable authentication. In *Proc. IEEE Symposium on Security and Privacy* (8–11 May 2005), pp. 110–124.
5. Roscoe, A. W. Human-centred computer security. Unpublished draft, 2006.
6. Sadie Creese, Michael Goldsmith, R. H. P. W. W. A. R., and Zakiuddin, I. Exploiting empirical engagement in authentication protocol design. In *Proceedings of SPPC* (2005).
7. Sasse, M. A., Brostoff, S., and Weirich, D. Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal 19*, 3 (2001), 122–131.
8. Schneier, B. *Secrets & Lies: Digital Security in a Networked World.* John Wiley & Sons, Inc., New York, NY, USA, 2000.
9. Whitten, A., and Tygar, J. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium, August 1999, Washington* (1999), pp. 169–183.