The Resurrecting Duckling — what next?

Frank Stajano

AT&T Laboratories Cambridge
http://www.uk.research.att.com/~fms/
and
University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/~fms27/

Abstract. In the context of the security of wireless ad hoc networks, we previously explored the problem of secure transient association between a master and a slave device in the absence of an online authentication server. We introduced the *Resurrecting Duckling* security policy model to address this problem.
Master-slave relationships, however, do not exhaust the range of interesting interactions. We therefore extend the Duckling model to also cover relationships between peers.

1 The Duckling: why, what, and what's missing

The range of devices that contain a microprocessor is continually expanding in every field — from consumer goods to office equipment, "white goods", vehicles and medical and scientific instrumentation. Looking ahead, the next development after endowing every device with a processor is going to be to allow all these computing nodes to communicate with each other, enabling them to co-operate and take advantage of each other's services. For convenience, in many cases this connectivity will be wireless: devices will be able to talk to each other as required by forming short-lived *ad hoc wireless networks*.

One respect in which such networks are fundamentally different from their well studied more traditional cousins is the absence of online servers for functions such as authentication. Your digital camera and your electronic organiser may spontaneously decide to communicate at any time, for example while you are taking pictures in the middle of the desert, and the ad hoc network they establish will be completely local, with no backbone infrastructure to connect it to the Internet or to anything else. This means that the problem of authentication can no longer be solved in the traditional way. The symmetric cryptography solutions in the tradition of Needham-Schroeder, Otway-Rees, Kerberos etc. explicitly require an online ticket-granting server; and even the solutions based on public key cryptography and signed certificates eventually fail if the certification authority is not online, due to the difficulty of performing timely revocation[1].

[1] Certificates may certainly be marked with an expiration date, and the interval between renewals may be made sufficiently short that timely revocation becomes pos-

B. Christianson, B. Crispo and M. Roe (Eds.). *Security Protocols, 8th International Workshop Proceedings*, Lecture Notes in Computer Science, 2000.
© Springer-Verlag Berlin Heidelberg 2000