Security in Pervasive Computing
(Abstract of Invited Talk)

Frank Stajano

University of Cambridge
http://www-lce.eng.cam.ac.uk/~fms27/

The audience of SPC 2003 needs no introduction to the Mark Weiser vision of ubiquitous computing: the etymological meaning of "computing present or found everywhere" is not to be taken in the narrow sense of "a computer on every desk" but rather in that of embedding computing and communication capabilities into all the everyday objects that surround us.

Various embodiments of this vision have been proposed over the past fifteen years by researchers from all over the world, covering the whole spectrum of implementation maturity from thought experiments to well-engineered commercial solutions. From self-contained information appliances such as Norman's hypothetical "home medical advisor" to the microscopic embedded RF-ID tags proposed by the Auto-ID Center that allow the washing machine to refuse to wash your precious white shirts until you remove the red sock that got in there by mistake, the idea of computing devices pervading our environment is now much closer to reality than to science fiction.

Moving from one computer per company in the 1960s to one computer per desktop in the 1990s to *hundreds* of computers per person in the current decade is an enormous quantitative change. So large, in fact, that it becomes also a quantitative one. Many old solutions will not scale by so many orders of magnitude. Recycling obsolete paradigms may lead to expensive mistakes—particularly in the field of security.

Authentication is an area in which the advent of pervasive computing will require new ideas and new strategies. We have relied for a long time on passwords as the primary mechanism for authenticating a user to a computer; this solution was never particularly user-friendly ("invent a password, including funny characters and numbers, that you won't forget or write down, but that nobody could possibly guess"), but it is obvious that it will never scale to the scenario of hundreds of computers per person.

Interestingly, the very first computers—of ENIAC and EDSAC vintage—did not require passwords to be accessed: one would just walk up to them and load a punched paper tape in the reader. Neither did the first personal computers, before they were linked up into LANs or the Internet. These are examples of the "Big Stick" security policy model: *whoever has physical access to the device is allowed to take it over*. In its simplicity, this policy is a very good match for many real-world situations. It is effective, sensible and reasonably easy to enforce. In many pervasive computing usage cases it will be a better strategy than passwords. Big Stick, however, is not suitable for every situation. Think of a vending machine or, for a more extreme example, a safe.

A central new problem in the pervasive computing scenario is therefore that of "Secure Transient Association": pairing up a master and a slave device so that the slave will

D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS 2802, pp. 6–8, 2004.

obey the master, will stay faithful to that master even when under physical control of hostile principals, but also will switch allegiance to a new master if the original master tells it to do so.

The solution is the "Resurrecting Duckling" security policy model. The slave device behaves like a newborn duckling that is permanently imprinted to whatever it first sees at birth. The "mother duck" master device is the only entity that can fully determine the behaviour of the duckling; this total control even allows the mother duck to order the duckling to "commit suicide" and be born again, at which point the duckling may get imprinted to a new mother duck. One crucial aspect of this policy model is its explicit reliance on a tamper resistance element in the duckling, to prevent the "assassination" case in which someone other than the mother duck attempts to cause the duckling's death so as to re-imprint it to itself. The Duckling policy fruitfully applies to a very wide range of practical applications—from universal remote control of home appliances to wireless car keys and from biomedical devices to thermonuclear warheads.

Pervasive computing brings convenience but also risk. Many things happen automatically, which is a relief, but their side effects are not always fully anticipated. Location-based services allow applications to customize their service to you based on where you are; but are you happy for the application provider to know your whereabouts on an ongoing basis, every few minutes, at city-block resolution? What about every few seconds and at sub-metre resolution? Protecting location privacy will be a challenge. We have designed a scheme based on frequently-changed pseudonyms, so that applications could provide their location-based service to customers protected by anonymity; and then we have tried to break it, simulating a malicious application that aimed to find out the identities that the users were attempting to protect. There is still much useful work to be done in this area.

Since the deployment of pervasive computing will have such a wide-ranging impact on society, we security professionals have to examine the proposed scenarios with critical eyes, imagining all the ways in which things could go wrong, and bearing in mind all the parties for whom things could go wrong.

Having previously mentioned authorization, for example, the security question that should be asked more often is: *authorized by whom?*. The obvious answer used to be *by the owner of the machine*; but this is no longer necessarily true in the new world of "Digital Restrictions Management". I bought a Sony Minidisc to record my lectures in digital format, only to discover that I can't take a backup of these discs. I am the owner of both the recorder and the copyright of the recording, and yet I can't get at my own bits... Who is the bad guy being kept out?

As architects of this new digitally endowed world of pervasive computing, we technical people have an ethical duty to pay attention to the fair requirements of all the parties involved—especially those without the money, lobbying power or technical astuteness to speak up for themselves.

This invited contribution was just a high level overview as opposed to a research paper. Readers interested in the details of my actual work on this topic may choose to follow the selected references provided below.

References

1. Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, 2002. ISBN 0-470-84493-0. http://www-lce.eng.cam.ac.uk/ fms27/secubicomp/.
2. Alastair Beresford and Frank Stajano. "Location Privacy in Pervasive Computing". *IEEE Pervasive Computing* 2(1):46–55, 2003. http://www-lce.eng.cam.ac.uk/ fms27/papers/2003-BeresfordSta-location.pdf.
3. Frank Stajano. "Security For Whom? The Shifting Security Assumptions Of Pervasive Computing", in *Software Security—Theories and Systems*, LNCS 2609, pp. 100–111, Springer, 2003. http://www-lce.eng.cam.ac.uk/ fms27/papers/2003-Stajano-shifting.pdf.