Security for Ubiquitous Computing

Frank Stajano

Computer Laboratory, University of Cambridge, UK
fms27@cam.ac.uk

Abstract. Ubiquitous computing, over a decade in the making, has finally graduated from whacky buzzword through fashionable research topic to something that is definitely and inevitably happening. This will mean revolutionary changes in the way computing affects our society: changes of the same magnitude and scope as those brought about by the World Wide Web. When throw-away computing capabilities are embedded in shoes, drink cans and postage stamps, security and privacy take on entirely new meanings. Programmers, engineers and system designers will have to learn to think in new ways. Ubiquitous computing is not just a wireless version of the Internet with a thousand times more computers, and it would be a naive mistake to imagine that the traditional security solutions for distributed systems will scale to the new scenario. Authentication, authorization, and even concepts as fundamental as ownership require thorough rethinking. At a higher level still, even goals and policies must be revised. One question we should keep asking is simply "Security for whom?" The owner of a device, for example, is no longer necessarily the party whose interests the device will attempt to safeguard. Ubiquitous computing is happening and will affect everyone. By itself it will never be "secure" (whatever this means) if not for the dedicated efforts of people like us who actually do the work. We are the ones who can make the difference. So, before focusing on the implementation details, let's have a serious look at the big picture.

C. Park and S. Chee (Eds.): ICISC 2004, LNCS 3506, p. 2, 2005.