The Security Challenges of Ubiquitous Computing

Frank Stajano

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

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.

The performance of a computer of given cost has gone up dramatically throughout the whole history of computing. Even just the last decade has brought improvements worth several orders of magnitude along such diverse dimensions as processor speed, memory capacity, disk capacity, communication bandwidth and so on. As we overtake the "a computer for everyone" milestone and march steadily towards a future in which each person owns hundreds of computing objects, we will start to explore a different region of the computer design space: keeping the performance constant and making the cost vanishingly small. Think of throw-away embedded computers inside shoes, drink cans and postage stamps.

Security engineers will face specific technical challenges such as how to provide the required cryptographic functionality within the smallest possible gate count and the smallest possible power budget: the chips to be embedded in postage stamps will be the size of a grain of sand and will be powered by the energy radiated by an external scanning device.

The more significant security challenges, however, will be the systemic ones. Ubiquitous computing is not just a wireless version of the Internet with a thousand times more computers, and it would be a naïve 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. The security challenges of the architecture are much greater than those of the mechanisms.

At a higher level still, even goals and policies must be revised. Having hundreds of computers per person changes the situation to such an extent that even the most fundamental assumptions need reexamining. There are evident issues of privacy, but also of trust and control. 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. 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.