

APPLICATIONS AND ACHIEVEMENTS OF THEORY IN TRUST, SECURITY, AND RESOURCE CONTROL FOR GLOBAL UBIQUITOUS COMPUTING

Presentation at the 1st UK UbiNet Workshop

VLADIMIRO SASSONE, UNIVERSITY OF SUSSEX

July 24, 2003

The talk illustrates the impact on applications in Ubiquitous Computing of recent developments in Theoretical Computer Science. I will focus on trust, security, and resource control, proceeding by examples through some of the most noticeable achievements. My purposes are: to pinpoint the relevance of Theory to the present research challenges, to illustrate some of the currently open problems, and to advocate for the future an integrated foundational/experimental approach to research in Global Ubiquitous Computing.

The challenge. To develop the scientific underpinnings of Ubiquitous Computing, it appears necessary to comprehend a large variety of notions. Such is the extent of the ‘Science for Global Ubiquitous Computing’ proposal for a Grand Challenge, in the context of which a thorough assessment of the state-of-the-art has been conducted. Here I will only focus on three areas: space and mobility; security and privacy; trust and resource control.

Space and mobility. *Locality* and *movement* of components are key notions in understanding a widely distributed system, and must be modelled directly. Calculi, logics and type systems are now emerging, in which the physical *space* occupied by real systems is treated as one with the virtual space of software and data structures. As evidenced by current results in language-based security (e.g. typed assembly languages), such research is likely to have a direct impact on the design of migration primitives which carry strong safety guarantees for mobile code.

Future perspectives: Within a few years we can expect calculi, logics and types, together with programming languages derived from them, to be installed for experiment in prototypical systems (e.g. a sentient building).

*Extracted from the case for support for ‘Science for Global Ubiquitous Computing’, a fifteen year Grand Challenge for computing research, http://www.nesc.ac.uk/esi/events/Grand_Challenges/proposals/Ubiq.pdf and the respective platform paper ‘Theories of Ubiquitous Processes and Data’ <http://www.cl.cam.ac.uk/users/rm135/plat.pdf>.

Security and privacy. *Safe languages* – typically based on static typing techniques – can demonstrably provide protection against security attacks, such as buffer overruns and unauthorised operations. The foundational approach has been the key to reveal new attacks to *security protocols*, and fix them. Currently, model-checkers and symbolic techniques based upon logical proof or bisimulation can verify security protocols.

Future perspectives: Within a few years we can expect to derive directly from theories the designs of safe languages close to C, to which existing C code can be ported with minor adjustment, and which are immune to various classes of attacks. We can also expect the verification via semi-automated tools of implemented security protocols, not only their abstract descriptions, and important principles for the design secure protocols will arise from work in semantics.

Trust and resource control. Mobile agents in ubiquitous systems must expect to acquire resources as necessary from the environment they visit. Access to resources can be controlled in terms of *boundary crossing* in current spatial model of the global network, and access policies expressed by type constraints. Methods based upon logics and types now exist to control allocation and deallocation of *resources*. As certainty is a commodity often unavailable on the global network, interactions will have to be based on *trust* and risk assessment. Logics and languages have been proposed for expressing the trust essential for resource allocation, in terms of notions such as *belief* and *authority*.

Future perspectives: Within a few years we can expect the development of protocols, based upon present research, for mobile agents to acquire and to manage resources. This involves *access negotiation* based upon *trust evaluation*; the latter will vary, under dynamically varying knowledge and belief about agents.