

Understanding, Managing and Securing Ubiquitous Computing Environments

Proposed by: Raquel Hill, Roy Campbell

Department of Computer Science, University of Illinois, Urbana Champaign

Moderated by: Roy Campbell, (rhc@uiuc.edu)

Panelists: Raquel Hill, Christine Julien, Xiaolan Zhang

(rlhill@uiuc.edu, julien@wustl.edu, cxzhang@us.ibm.com)

Early computers were very large, occupying entire buildings, and the computer scientists that built and used them to develop some of the early breakthroughs in programming technologies and applications, worked literally inside the computer. In many respects, today's technology brings us back to live inside a computer. With the convergence of wired and wireless networking, handheld and embedded computer systems and the enormous amount of information collected everywhere via these and a large number of physical and virtual sensors, we live inside a huge, rapidly growing, intelligent information management system. This system can track all people and equipment in the building; record all the information produced in the building, whether speech, written text, or other media; can store this information indefinitely; can use powerful computers to analyze and organize it; and can provide an intelligent gateway to the rich content on the web. Unlike earlier technologies, the scale and complexity of ubiquitous computing introduces dependencies, feedback, and subtle control laws that govern the interaction between the physical, social and information worlds.

The desired and anticipated goals of living and interacting in a ubiquitous computing environment are still not within easy reach. Enhancing the collective experience of human beings in this environment, allowing them to intelligently access and exploit the available information, facilitating and enhancing their educational experience, supporting a productive and pleasant interaction with the information management system and, with other human beings, and augmenting the physical and cognitive capabilities of a community -- require a revolution in the capabilities of current software systems and in the way we presently develop them. On the other hand, the dangers of such systems to privacy, security and independence are all too clear. One needs to understand the social and legal implications of living inside an information management system and find the right compromises and approaches to make it socially desirable.

Additionally, before the various devices within the ubiquitous computing environment can be used by different kinds of systems, important challenges in the areas of managing, controlling, scheduling and accessing data from these devices have to be solved. The various devices within the environment have different interfaces, generate data in different formats, have different physical, virtual and logical domains of operations, perform different kinds of tasks, have different security and privacy implications, have different levels of reliability and fault-tolerance and are targeted towards different users.

During this panel, we will present some basic background information regarding ubiquitous computing environments. For example, we will present a taxonomy of ubiquitous computing environments that includes smart rooms or active spaces, super spaces and smart buildings. We will also discuss how middleware may be used to abstract away the complexity of discovering and interacting with the plethora of devices within a ubiquitous computing environment and how it presents a uniform interface for using and managing these devices. Panelists will also discuss how this middleware can be used to transform static spaces into reflective, context aware, active spaces. Additionally, we will discuss how these ubiquitous computing environments can be secured. The panelists will explore both reactive security techniques (i.e. intrusion detection, trace-back filtering) and proactive techniques (i.e. access control based filtering and

programmable secure overlays). Techniques for analyzing the security of the system will also be presented.

The main objectives of this panel is to further the discussion of techniques that may be used to facilitate the seamless integration of computing devices, manage and secure the resulting ubiquitous environments and analyze the effectiveness of the security mechanisms. The intended audience includes students and researchers who are interested in learning about ubiquitous computing environments and those who are currently involved in research within this area. The proposed length of this session is 90 minutes. Each panelist will present for 20 minutes on a related topic. Thirty minutes will be allotted for questions and moderated discussion with the panelists. There are no restrictions on the number that may attend this panel.

The moderator of this panel, Roy Campbell, is a Full Professor within the Department of Computer Science at the University of Illinois, Urbana-Champaign. Dr. Campbell and his students have developed a meta-operating system called Gaia OS that enables active spaces. Gaia OS supports the development and execution of portable applications for active spaces. Gaia is a distributed middleware infrastructure that coordinates software entities and heterogeneous networked devices contained in a physical space. Gaia exports services that allow applications to query and utilize existing resources, to access and use current context, and provides a framework to develop active space applications. Other current projects include authorization for sensor networks, simulations of network security, and the design of peer-to-peer distributed operating systems.

The panelists include Raquel Hill, Christine Julien and Xiaolan Zhang. Dr. Hill received the Ph.D. Degree in Computer Science from Harvard University in November 2002. Currently, she works with Dr. Campbell as a Post Doctoral Research Associate to develop a secure and survivable infrastructure for critical information systems, like smart buildings. Christine Julien will receive the D. Sc. Degree in Computer Science from Washington University in the Spring 2004. Her research focuses on the development of middleware for ad hoc mobile environments. Xiaolan Zhang received the Ph.D. Degree in Computer Science form Harvard University in November 2000. Currently, Dr. Zhang is a member of the Security Research Group at IBM Research where she has developed static analysis tools for evaluating the security of a system.