Virtual Walls: Protecting Digital Privacy in Pervasive Environments

As pervasive environments become more commonplace, the privacy of users is placed at an increased risk. The numerous and diverse sensors in these environments can record contextual information about users, leading to users unwittingly leaving "digital footprints." Users must therefore be allowed to control how their digital footprints are reported to third parties. While a significant amount of prior work has focused on location privacy, location is only one specific type of footprint, and we expect most users to be incapable of specifying fine-grained policies for a multitude of footprints. In this paper we present a policy language based on the metaphor of physical walls, and posit that users will find this to be an intuitive way to control access to their digital footprints. For example, users understand the physical privacy implications of conducting a meeting in a room enclosed by physical walls. By allowing users to deploy "virtual walls," they can control the privacy of their digital footprints much in the same way they control their privacy in the physical world. We present a policy framework and model for virtual walls with three levels of transparency that correspond to intuitive levels of privacy. We also describe the results of a user study (N = 23) that indicates that our model is easy to understand and use.

--- An Institute for Security Technology Studies project at Dartmouth College. This project is supported by Grant number 2005-DD-BX-1091 awarded by the Bureau of Justice Assistance. Points of view in this presentation are those of the author and do not necessarily represent the official position of the U.S. Department of Justice. ---

Bio:

David Kotz is a Professor of Computer Science at Dartmouth College in Hanover NH. He also serves as the Director of the Center for Mobile Computing, which focuses on wireless networks and mobile computing, and Executive Director of the Institute for Security Technology Studies, which is dedicated to interdisciplinary research and education in cyber security and trust. His research interests include security and privacy, pervasive computing, and wireless networks. He has published over 100 refereed journal and conference papers. After receiving his A.B. in Computer Science and Physics from Dartmouth in 1986, he completed his Ph.D in Computer Science from Duke University in 1991 and returned to Dartmouth to join the faculty. He is a Senior Member of the ACM and of the IEEE Computer Society, and a member of the USENIX Association, and of Computer Professionals for Social Responsibility. For more information see http://www.cs.dartmouth.edu/~dfk/.