A Location based security implementation in Smart Home

Manish T I

Department of Computer Science, MES College of Engineering,
Kerala, India
E-MAIL: manishti2004@yahoo.com

Abstract

Home networks and the interconnection of home appliances is a classical theme in pervasive computing research. Security is usually addressed through the use of encryption and authentication, but there is a lack of awareness of safety: preventing the computerized house from harming the inhabitants, even in a worst-case scenario where an unauthorized user gains remote control of the facilities. We address this safety issue at the programming language level by restricting the operations that can be performed on devices according to the physical location of the user initiating the request. Operations that pose a potential safety hazard can only be performed within a physical proximity that ensures the safety of the operation. And also study the performance of smart home hardware implementations

1. Introduction

The idea of a computerized smart home is an emerging trend of pervasive computing. The advantages of such a smart home include easing the household activities of the habitants, providing entertainment, and saving energy by intelligently controlling the house temperature and safety. We can use internet and mobile technology to control remotely. There is danger in giving computers control of the home, namely that operations that used to be carried out by a person aware of his environment now are invoked through a computer the user only has limited, if any, awareness of the consequences of his actions. Moreover, if security is compromised, a "virtual intruder" can gain remote control over all the functions of the home, including (perhaps) the central heating, the lock on the front door, or the cooking stove. The smart home can be protected by security measures like passwords and encryption. methods. The passwords may be unwarily reveal if using them in public. To avoid this safety fault, the smart homes are provided with an extra safety layer is needed. This layer will take care of basic safety rules are obeyed when controlling functions in the home from afar away. This extra safety layer not only applies to remotely controlling the home, but also to safety-critical functions that are controlled from within the home: turning on the cooking stove in the kitchen from the living room could for example be a potential safety hazard. The components are classified in terms of the maximal distance at which it can be controlled. For example, safety-critical components of appliances may only be controllable by people who are present in the same room since they would only then be fully aware of the consequences of their actions. Our aim is to develop a safety-enabled middleware for home networks.

2. Location-Based Capabilities:

978-0-7695-3352-0/08 $25.00 © 2008 IEEE
DOI 10.1109/HPCC.2008.174

We now present the principles behind our approach to safety in home networks, location-based capabilities. We first present a few considerations, and then describe the conceptual model. Then, we define simple language constructs for expressing safety restrictions, and show how to map them to our Java-based implementation which enforces the safety.

2.1 Considerations:

We consider a distributed system of devices programmed using software components. The software component model is language-independent, so the interfaces of the components are described using an IDL language similar to CORBA IDL. The operations implemented by the software components are activated by the users who operate the devices. Executing an operation may involve invoking operations defined by software components located in other devices of the system. Safety-critical operations should only be executed if the user who initiated the operation is located physically close to the device and how close depends on the specification of the operation. Determining the location of a user cannot in general be done in a completely reliable way, and hence the degree of safety offered by the system is limited by the technology used for determining the user location.

2.2 Conceptual model:

Conceptually, our system consists of a number of devices that are organized into hierarchically nested zones. Each device is a member of a zone. The zones are named according to their nesting level, e.g. all zones nested n levels deep from the root have the same name. Restricted operations on devices are marked with the zone level that can call them: to call an operation marked with a given zone name, the call must originate from within the same zone of that name. The origin of a call is an operation which has been marked as generating an origin in terms of the calling context (for example, the mapping of user input to action could be such an operation). Before executing a restricted operation, the capability is verified by querying the origin device to verify both that the call did indeed originate from it and that the device is currently at a location in the allowed area. How the origin is queried is implementation-specific, but it must be done in a way that does not compromise the safety guarantees provided by the implementation. Each device of the network is either considered trusted or untrusted. Untrusted devices can only be members of the root zone, and hence cannot invoke restricted operations. Trusted devices are assumed not to lie, so that the verification of the origin call can be trusted.

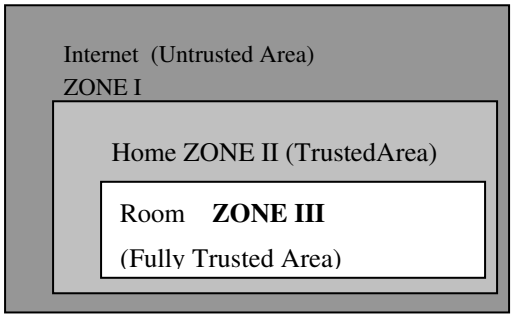

Figure 1: Location zones for the smart home

In our smart home network, we operate with three location zones:

Present (Fully Trusted Area)Close enough that the user is aware of the consequences of his action, which we define to be that the operation was initiated within the same room.

Local (Trusted Area)Close enough that the user can be trusted not to do damage to the home, which we define to be that the operation was initiated within the home.

Global (Un-trusted Area) Anywhere, which in practice means anywhere on the internet.

3. Location awareness technologies

We now check location awareness technologies, and evaluate their usefulness with regards to safety in home networks. Specifically, the technologies that can realistically be used in a home scenario to determine the location of the target device relative to the origin device, to be able to verify if they can interact via restricted operations.

Infrared. Infrared (IR) signals: tend to be diffused throughout an entire room, but do not traverse walls, which makes them useful for determining location at room granularity (given an IR receiver/sender in each room). IR signals can be transmitted through a window or from one room to another using a reflective surface, but requiring two-way IR communication limits the degree to which this can be done. Evaluation: medium degree of safety at room granularity.

Ultrasound: Ultrasound signals can give location information with sub-room precision, down to roughly 10cm, but require an extensive grid of precisely placed, ceiling-mounted sensors . However, each grid is linked to a room, and hence the distance between devices in different rooms cannot be computed. Evaluation: high degree of safety at sub-room granularity.

Bluetooth: Bluetooth uses a wireless communication protocol with a communication range of approximately 10m. Thus, simply detecting whether a device is within range provides location information, but triangulation using multiple devices is also possible].. Nonetheless, since it is a wireless medium that uses radio communication, signals can traverse walls. Evaluation: low degree of safety at room granularity.

WaveLAN: Standard IEEE 802.11b wireless networking can provide location information similarly to Bluetooth, very crudely but at long distances in terms of which basestation is used, and more precisely using multiple basestations. Evaluation: low degree of safety at room granularity, medium degree of safety at home granularity.

Local network: A local home network, for example based on IP, FireWire, or other home networking protocols, can trivially be used to verify physical presence (if it is connected to the network, it is in the home). However, restricted devices that have unrestricted access to the network can pose as other devices, and could therefore constitute a safety hazard. We note that unlike standard ethernet, FireWire devices cannot normally perform packet snooping , which facilitates constructing a safe communication mechanism. Evaluation: high degree of safety at home granularity, depending on the network type.

Physical contact: This is a very old-fashioned and secure way of establishing the presence of a person. Evaluation: high degree of safety at room and home granularity.

4. Smart Home hardware: IR and FireWire

The stationary device are connected using using IrDA standard for communication. All devices are equipped with IR senders and receivers based on the IrDA standard. Fire wire is considered as standard connection interface for audio and video component communication, which may present in homes. A gateway device bridges the FireWire network to the Internet.

5. Performance of Smart Home hardware implementations

IrDA infrared is secure as it is purposely limited at one meter line-of-sight and thirty degrees cone. Keeping in shorter distance, infrared uses very little power, which is an important factor to consider when it comes to handheld devices. "Diffused IR", although not being able to penetrate a solid object can avoid line-of-sight limitations and reach other infrared enabled devices at a distance. High power infrared beams

transfer high-speed data from 45Mbps to 10Gbps and are installed between buildings within a few miles for security protection or toll stations with high accuracy. FireWire, built from the ground up for speed, uses a "Peer-to-Peer" architecture in which the peripherals are intelligent and can negotiate bus conflicts to determine which device can best control a data transfer. Read and write test shows FireWire are faster than other implementations.

6. Conclusions and Future Work

Pervasive computing is an emerging trend not only in computer science but also in everyday life. The programming language support for central issues such as context awareness have not been widely explored, and little attention has thus far been devoted to basic concerns such as safety. We have presented a approach that expresses location awareness at the programming language level, and applied this approach to improving the safety of a home network for devices. This approach forces safety concerns to be considered as part of the design of the software interface of each device. Our current implementation, which is based on IR communication and FireWire, enforces basic safety concerns, in principle making it impossible for an intruder to compromise safety without physically entering the home. In terms of future work, we are primarily interested in further exploring software aspects of location awareness and implementing same kind of safety measures in a more critical application like reactors, chemical plants with modified features. In the case of the critical application the performance criteria should be given more importance.

7. References

[1]. Paramvir Bahl and Venkata N. Padmanabhan. RADAR: An in-building Rfbased user location and tracking system. In INFOCOM (2), pages 775–784, 2000.

[2]. Communication at internal meeting between B&O and the authors.

[3]. J.E. Bardram, R.E. Kjær, and M.Ø. Pedersen. Context-aware user authentication: Supporting proximity-based login in pervasive computing. In Proceedings of Ubicomp 2003: Ubiquitous Computing, volume 2864 of Lecture Notes in Computer Science, pages 107–123, Heidelberg, October 2003. Springer-Verlag.

[4]. F. Bennett, T. Richardson, and A. Harter. Teleporting — making applications mobile. In Proceedings of the IEEE Workshop on Mobile Computer Systems and applications, pages 82–84, Los Alamitos, CA, USA, 1994. IEEE CS Press.

[5]. J. Boyland, J. Noble, and W. Retert. Capabilities for sharing. In J.L. Knudsen, editor, Proceedings of the European Conference on Object-Oriented Programming(ECOOP'01), volume 2072 of Lecture Notes in Computer Science, pages 2–25, Budapest, Hungary, 2001.

[6]. B. Brumitt, B. aMeyers, J. Krumm, A. Kern, and S. Shafer. EasyLiving: Technologies for intelligent environments. In Proceedings of Handheld and Ubiquitous Computing, HUC 2000, volume 1927 of Lecture Notes in Computer Science, pages 12–29, Bristol, UK, 2000. Springer Verlag.

[7]. C. Chambers. Predicate classes. In Proceedings of the European Conferenceon Object-oriented Programming (ECOOP'93), volume 707 of Lecture Notes in Computer Science, pages 268–296, Kaiserstautern, Germany, July 1993.Springer-Verlag.

[8]. K. Crary, D. Walker, and G. Morrisett. Typed memory management in a calculus of capabilities. In ACM, editor, POPL '99. Proceedings of the 26th ACM SIGPLAN-SIGACT on Principles of programming languages, ACM SIGPLAN Notices, pages 262–275, Austin, Texas, USA, January 1999. ACM Press.

[9]. J.B. Dennis and E.C. Van Horn. Programming semantics for multiprogrammed computations. Communications of the ACM, 9:143–154, March 1966.

[10].Anind Dey, Gregory D. Abowd, and Daniel Salber. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Human-Computer Interaction, 16:97–166, 2001.

[11].Andy Harter, Andy Hopper, Pete Steggles, AndyWard, and PaulWebster. The anatomy of a

context-aware application. Wireless Networks, 8(2/3):187–197, 2002.

[12]. Jeffrey Hightower and Gaetano Borriella. Location systems for ubiquitous computing. IEEE Computer, 34(8):57–66, 2001.

[13]. Center for Pervasive Computing publication http://www.daimi.au.dk

[14]. IBM. Jikes Byte code Toolkit. URL: http://www.alphaworks.ibm.com/tech/jikesbt.

[15]. OSGI. http://www.osgi.org

[16]. UPnP. http://www.upnp.org

[17]. X10. http://www.x10.org

[18]. LonWorks. http://www.echelon.com

[19]. Pervasive Computing www.computer.org/pervasive

[20].http://www.itl.nist.gov/pervasivecomputing.html (NIST)

[21].Universal Designed Smart Homes for the 21st Century Book by: Charles Schwab Architect AIA,Member American Institute of Architects