An Application-led Approach for Security Research in Ubicomp

Philip Robinson
Telecooperation Office (TecO), University of Karlsruhe
Vincenz-Priessnitz-Strasse 1, 76131 Karlsruhe, Germany

Abstract. The difficulties of scoping security-related research within ubiquitous and pervasive computing are discussed. The paper provides a condensed background to this research domain, and shows how a generalized, application-oriented research methodology is being applied to a thesis on Intrusion Detection, such that a good balance of theory, technology and scenarios may be obtained.

1 Introduction

Application-led research encompasses theory, technology and scenarios. Nevertheless, problems arise when there is too much focus by researchers on a specific aspect of the research. Having both reviewed and contributed research in the area of security in Ubicomp[1] [9], it has often been observed that the content and focus of security-related research are either purely theoretical and hence not practically realizable, present too much technical details (e.g. equipment specification, cryptographic key-sizes, standards) and leave the reader without an explicit scientific conclusion, or describe scenarios/ stories that present very "special-case" problems with very limited solutions and outlandish assumptions. This paper offers a methodology for balancing these three aspects of research, using security as a case study. The particular area of security being considered is Intrusion Detection, as it is still relatively unexplored in UbiComp but has very clear analogies with real world social interactions and concerns.

Before proceeding to the central theme of the paper, it is necessary to have a clear understanding of some terminology. The first term that must be understood is that of "Application", as there tends to be a common misperception that an application is equivalent to a storyboard-like description or software. The description of "Application" being used in this paper is *the way in which processes, tasks and information are organized in order to optimally and consistently achieve specific objectives.* A scenario is a very specific instance of an application with very specific properties, assumptions and a storyline. Software and technology are tangible solutions for enhancing the way that the everyday objectives of people and organizations are met i.e. the application. Nevertheless, rapid deployment of technology into society and businesses often incurs problems for usability and management [10]. This is a particular concern for security, as new technologies and ideas may introduce new risks and opportunities for intrusion.

The paper proceeds by describing the proposed methodology, followed by section 3, where it is applied to a thesis on Intrusion Detection.

2 An Iterative Methodology for Application-Led Research

Application-led research should commence with clearly stated objectives and criteria by which the research will be evaluated. An approach of "iterative refinement" is suggested, as this allows a researcher to separate theory, technology and scenarios into different foci of research, and progressively refines the argumentation and results. Börger proposes strategies for iterative refinement of systems engineering using ASMs (Abstract State Machines) [5], from which similar principles are adopted for motivating iterative, objective-driven research. The resultant, iterative, four-step methodology proposal is described below:

Step 1: (Scope) Identify application domain and objectives to be realized, as well as the conditions under which the objectives are considered satisfied. Identify the *subjects* (entities with management roles in order to meet objectives), *utilities* (mechanisms employed by subjects) and *objects* (entities managed by subjects in order to meet objectives).

Step 2: (Theory) Postulate a ground model that proposes a conceptual strategy for meeting the application's objectives. Secondly, specify rules governing the interaction between subjects and objects based on how the objectives are decomposed.

[1] Ubicomp is used as a placeholder for both ubiquitous and pervasive computing. Despite the different origins of the two communities, there is no real distinction between the two today.

Step 3: (Technology) Propose the hardware and software that can either extend or newly implement mechanisms for meeting the objectives. Mechanisms are affiliated with functionality of subjects, utilities or objects.

Step 4: (Scenario) Evaluate the theory and technology proposals based on the objectives and constraints identified. This step is also useful as a "reality check", to validate claims made by the theory and technology with reference to enhancing the application needs of people and organizations. A good scenario should consider the target audience but make sure that the application objectives and scope specified in step 1 are maintained or qualified, without becoming superficial or overly imaginative.

The iterative property of the methodology suggests that an outcome of the scenario analysis (or feedback), may serve to refine the scope of the research, the theoretical assumptions and the technology considered. Furthermore, the scenario can be used to both make problems clear as well as present solutions.

3 Applying the Methodology to Intrusion Detection

In the well-known 1991 position paper of Weiser [12], he discussed the possibility of well-implemented ubiquitous computing systems offering enhancements to the way information privacy is traditionally handled, along with the observation that cryptographic techniques were already in existence for securing messages passed between computers. In a later paper [6] published in the 1999 "Pervasive Computing" edition of IBM Systems Journal, Weiser and the group at PARC issued another statement on the topic, identifying "the lack of control" as the principal problem for privacy, as it becomes increasingly harder to manage dynamic and complex interconnections, information flows, usages, failures and actions, characteristic of Ubicomp systems. Additionally, there have also been several theses and publications related to the usage of sensor-derived context information for the enhancement of security, such that security becomes more adaptive, representative of the circumstance of its subjects and based on a broader spectrum of attributes [3, 8]. The topic of Intrusion Detection has not been considerably addressed within Ubicomp, apart from what could be considered related work in the areas of mobile ad hoc networks [7] and wireless communications [1]. Nevertheless, the above citations provide a foundation for considering how Ubicomp can be applied to detecting and controlling intrusions, and why this is an important topic. An "Intrusion Detection System (IDS)" can be considered as an "Application", in that people and organizations often express the objective to protect their assets against theft or their privacy against intrusion. The proposed research methodology can therefore be applied as follows:

Step 1 (Scope): The *objects* of an IDS may include but are not limited to data, services, and physical items, as these are the ultimate goal of an intruder. The *subjects* of an IDS are therefore owners, administrators and users, while utilities are required for specifying rules and profiles, monitoring the success of these *rules*, and appropriately notifying and responding to intrusion alerts/ alarms that arise if a specified rule fails. This therefore describes the scope of the application being considered and already lends to developing a ground model.

Step 2 (Theory): The original papers on IDS were written by Dennings and Neumann in 1987 [4]. There is also a detailed and more recent taxonomy of IDS research available from Axelsson, from which the general properties of an IDS can be extracted [2]. These reliable citations were used to derive the requirements for an IDS, depicted as an ASM in figure 1.

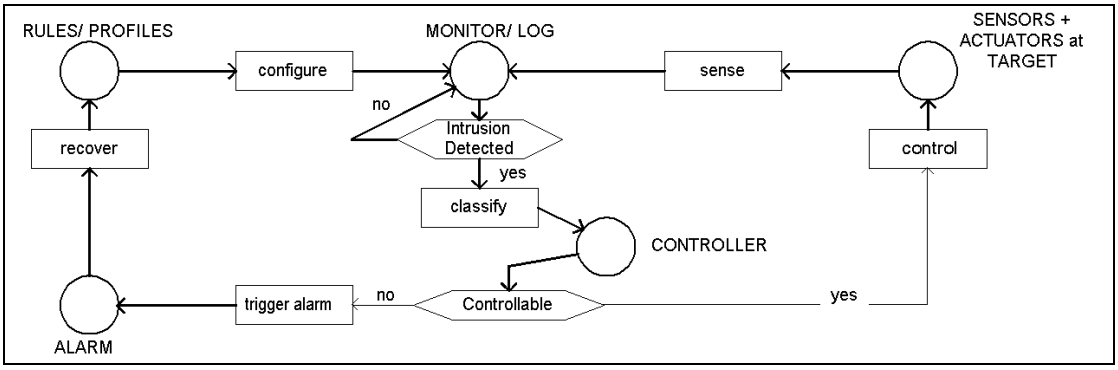

Figure 1: Proposed ASM ground model for an IDS

An intrusion detection system is bootstrapped with a definition of profiles of "normal or accepted" behaviour. The system then monitors in real-time or does inspections of system logs, with the goal of

classifying sensed activity data from the targets against the profiles. When an intrusion is detected, a controller is selected based on the classification of the intrusion. If there is no controller capable of controlling the intrusion, then an alarm is triggered until the system can be recovered (typically by a site security officer), which may entail an enhancement in the system's detection profiles.

Step 3 (Technology): What happens to the above theoretical model when Ubicomp is introduced? Kindberg and Fox have identified two key features of Ubicomp systems, namely, spontaneous interaction and physical integration [9], leading to the *volatility* and *boundary* principles respectively. Using these as refinement parameters of the model, the following requirements have been derived:

- *Configuration* – cannot assume central administration nor fixed detection profiles
- *Sensing and Classification* – the availability and validity of sensors and classification schemes change as the boundary changes.
- *Logging* – there is the issue of ownership of and access to logged data after the security boundary has been "dissolved" or modified
- *Controls and Alarms* – decisions about control and alarms need to be efficiently coordinated, in the case of shared ownership, to minimise false-positives and false-negatives
- *Recovery* – the feasibility and validity of a recovery plan has to be weighed based on the stability of the target and configuration of the security boundary

The working solution for the thesis suggests a model for selecting and reconfiguring specific roles in the IDS in response to changes in the security boundary and interactions.

Step 4 (Scenario): An area where Ubicomp technologies show commercial fortitude is that of shipping and logistics. Goods are transported between different points and are placed in intermediate holding areas along the way. Each holding area has different conditions and provides different services and appliances for the care of the goods. Different models could be applied to detecting and responding to intrusions, where an intruder is defined as someone or something whose presence or behaviour threatens the progress of the goods being delivered and intact. One model could be *localized*, where each item is responsible for detecting and responding to intrusions, but this would imply that each item would need to be very expensive in terms of communications, sensing and processing. A *centralized* model could be considered, where all processing is undertaken by one node, but this would result in complex detection logic at an overloaded and vulnerable central point of attack. Using scenarios to aid in understanding the problem, the proposed model follows progress in the area of "collaborative intrusion detection". However, the differentiating contribution of the thesis is the dynamic configuration and operation of a collaborative IDS.

4 Summary

This paper has provided a general methodology for performing application-oriented research primarily in Ubicomp. This methodology has been shown using the example of security, namely Intrusion Detection, which is a thesis under development by the author. By considering Intrusion Detection as an Application, based on the definition given above, it was possible to provide very clear research objectives and parameters by which the models and solutions could be evaluated. In addition, the theoretical, technological and scenario elements of the research complement each other, which, as stated at the beginning of the paper, should be the goal of application-led research.

References

[1] Adelstein F., Alla P., Joyce R., and Richard G. G., "Physically Locating Wireless Intruders" in Proceedings of IEEE 2004 IAS Conference, Las Vegas, Nevada, April 2004.

[2] Axelsson S., "Intrusion Detection Systems: A Survey and Taxonomy". Technical report 99-15, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, March 2000

[3] Covington M. et. al, "Securing Context-Aware Applications Using Environment Roles", SACMAT 2001

[4] Denning D.E., "An Intrusion Detection Model," IEEE Trans. Software Eng., vol. 13, no. 2, Feb. 1987, pp. 222–232.

[5] E. Börger, "The ASM Ground Model Method as a Foundation for Requirements Engineering." Verification: Theory and Practice 2003

[6] Kindberg T., Fox A., "System Software for Ubiquitous Computing",IEEE Pervasive Computing, 2002

[7] Parker J., Undercoffer J.L., Pinkston J. and Joshi A., "On Intrusion Detection in Mobile Ad Hoc Networks", IEEE Workshop on Information Assurance 2004

[8] Robinson P., Beigl M., "Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments". Springer, SPC 2003

[9] Robinson P., Vogt H., Wagealla W., "Privacy, Security and Trust within the Context of Pervasive Computing." ISBN: 0-387-23461-6, Kluwer 2005

[10] Smith S.W., Spafford E.H., "Grand Challenges in Information Security: Process and Output" IEEE Security & Privacy, 2004

[11] Weiser M., "How Computers Will Be Used Differently in the Next Twenty Years". IEEE Symposium on Security and Privacy 1999

[12] Weiser M., "The Computer for the Twenty-First Century. Scientific American". September 1991