

# Some security issues of wireless systems

Eduardo B. Fernandez<sup>1</sup>, Saeed Rajput<sup>1</sup>, Michael VanHilst<sup>1</sup>,  
and María M. Larrondo-Petrie<sup>1</sup>

<sup>1</sup> Dept. of Computer Science & Engineering, Florida Atlantic University,  
777 Glades Road, Boca Raton, FL 33431-0991  
{ed, saeed, mike, maria}@cse.fau.edu

**Abstract.** Wireless systems have found wide acceptance in many industries such as military and healthcare. These systems appear under a variety of architectures including fixed networks, cellular networks, and ad hoc networks. We survey some security problems, of interest to researchers, in wireless systems when used in these environments. Most studies of the security of these systems emphasize cryptographic aspects, we concentrate on other security aspects, such as operating systems, access control, web services, and location awareness.

## 1 Introduction

Wireless systems have found wide acceptance in many industries such as military, healthcare, business, manufacturing, retail, and transportation. These systems appear under a variety of architectures including fixed networks, cellular networks, and ad hoc networks. The challenges posed by the industries to each of these technologies are unique, especially for healthcare and military applications.

We survey some security problems in wireless systems. We do not attempt to be comprehensive but to give a general overview of some problems of interest to researchers. Most studies of the security of these systems emphasize cryptographic aspects. While important, they are not the only issues and we concentrate on other aspects. Background information about security aspects of wireless systems can be found in [1], [2], and [3], and about the structure of the networks and protocols in [4].

We start by discussing some general issues that define the context for our discussion. Then we consider the effects of the type of industry on application security. Next we talk about access control aspects and the effect of the operating system on security. We look then at web services and end with the effect of location awareness on security.

## 2 General issues

When compared to wired networks, there are four generic limitations of all wireless devices: 1) limited power, 2) limited communications bandwidth, 3) limited process-

ing power, and 4) relatively unreliable network connection. The bandwidth available to wireless systems is usually at least an order of magnitude less than that available to a wired device. The processing power is limited due to the limited space/cost of fixed wireless devices typically used for Wi-Fi networks, and is further limited due to power constraints in other wireless devices. The unreliability of the network connection is universal in all wireless networks. Protocols have been designed to take this lack of reliability into account and to try to improve it. However, in designing these protocols, choices have to be made about the size of the packets and frames to be used. Such decisions can have a profound impact on the effectiveness and efficiency of cryptographic protocols and other security measures. To this we add the fact that there is a large variety of devices using different architectures, several operating systems, and diverse functionality. On top of everything, security needs for wireless devices are greater than those of regular wired-network devices. This is due to the very nature of their use; they are mobile, they are on the edge of the network, their connections are unreliable, and they tend to get destroyed accidentally or maliciously. These devices can also be stolen, lost, or forgotten. Thus, we need more security processing. Security processing can easily overwhelm the processors in wireless devices. This challenge, which is unique to wireless devices, is sometimes referred to as the *security-processing gap*. Non-fixed wireless devices such as cellular handsets and ad hoc network devices such as sensors are severely handicapped due to their very low battery power. Even though significant advances are expected in computation and communication speed over the next decade, it is still expected that they will lag behind the power available to fixed computers due to the need for miniaturization. To make things worse, only modest improvements to battery power are expected. The battery limitation in mobile wireless devices is sometimes called *battery gap* and refers to the growing disparity between increasing energy requirements for high-end operations needed on such devices and slow improvements in battery technology.

Finally, ad hoc wireless networks have their own security challenges. Due to their extremely small device size (*smart dust* [5]), their battery life and processing power are further limited. However, security needs are even greater, since some security processing is needed just for the device to be able to function properly and be able to communicate in their routing protocols.

When it comes to the general service provider industry (internet and cell phone companies), they are mostly interested in providing cellular service and hotspot services. While the security issues of cellular networks are relatively well understood, those of Wi-Fi networks are not. Important issues are authentication of users on hotspots, wireless-hop security (the part of the ISP network that is wireless), and seamless security association transfer from one domain (e.g. the cellular network) to the other (e.g. the Wi-Fi network). An interesting direction here is authorization of devices once authenticated. This has to come from application semantics as we discuss below.

With the increase in functions, the typical problems found in larger systems are also appearing in portable devices. One of these problems is viruses [6]. The first portable virus to appear was Liberty, followed shortly by Phage. The WML (Wireless Markup Language), a script language used by WAP can also be a source of possible attacks [7] [8]. The devices do not distinguish between script code resident in the

phone from the one downloaded from potentially insecure sites, all of them execute with the same rights. An infected device can be used to launch denial of service attacks on other devices or the network. Similarly to wired systems, wireless systems need up-to-date antivirus programs. Companies such as Symantec, McAfee, and Trend Micro have specialized products for handheld devices. A problem here is that in some devices because of space and processing limitations, antivirus programs and other protection devices, such as firewalls and IDS, may not be feasible.

### **3 Applications and security**

For the healthcare industry both Wi-Fi and sensor networks are important. Issues in these networks are similar to the ones we discussed in the previous section in the context of service providers. The difference in this case is that the consequences of an error are severe, especially when it involves wireless bedside monitoring or a dispensing device communicating with the server. The area of sensor networks (biometric sensors) is still a research area. When we consider the collection of data from sensors, the issues of confidentiality, integrity, and non-interference also arise. HIPAA regulations have brought renewed concern about patient privacy and new models are being proposed [9]. A model defined at the application level, say using UML (Unified Modeling Language), must be mapped to the lower levels of the wireless networks; it is an open problem how to do this in a systematic way. The use of patterns, discussed in the last section, could provide a handle for this mapping.

The military has applications for all types of wireless devices. Their need for security in all areas is more rigorous. However, in their case, survivability of the network is very important, i.e. it is vital that theft or destruction of one device does not compromise the information stored on that device, or worse, the security of the entire system. In case of ad hoc networks, it is vital that removal of a few nodes does not affect the communication capabilities of the devices, which opens interesting research areas to develop authentication and security protocols that are friendly to such changes. The US Department of Defense recently issued Directive 8100.2 that requires encrypting all information sent in their networks according to the rules of the Federal Information Processing (FIP) standard [10]. The provision also calls for antivirus software. It is interesting to observe that their concern is mostly about message transmission and they don't seem to be worried about the other aspects of security, such as the ones discussed in this paper. This is also true for the NIST recommendations for wireless security in federal agencies. Apparently they were considering only simple applications; however, the increasing use of web services opens up many new possibilities for military uses, including battlefield communications, sensor networks, and soldier location and identification.

Another important application is mobile e-commerce. This includes mobile banking, wireless payment services, shopping, reservations, and many others. Many of the required functions can be secured using cryptography (see [11] for a survey), but access to specific services requires at least some type of Role-Based Access Control (RBAC), as discussed below.

## 4 Access control to sensitive information in or through the device

We should consider access control to:

- *Resources in the device.* The portable device may contain files that need to be restricted in access and it is the function of its operating system to perform this control. Control of types of access is important; for example, a user may play a song, but she should not copy it. This type of control can complement other types of digital rights management. The device may contain passwords to access networks, encryption keys, lists of people, etc.; all this data needs protection.
- *Resources provided by other mobile network devices.* This is the most interesting case for research. Because of the variety and unpredictability of potential users, access decisions must be based on attributes (roles, groups, qualifiers) and trust [12, 13]. For the same reasons and because of the variety of resources, rights must be created dynamically [14, 12]. In addition, it is not clear where the access rights should be kept because of the lack of a centralized repository for authorization rules (no device can hold large tables) [14].
- *Resources in wired networks.* When portable devices need to access application-related data from corporate databases some type of Role-Based Access Control (RBAC) may be necessary. Management and enforcement of application and institution constraints can be performed following PMI (Privilege Management Infrastructure) [15]. PMI is a standard of ITU X.509. There is some work on RBAC models that integrate the wireless access with access from the wired network users. One of these papers [16] uses a hierarchic role structure, which doesn't appear as very useful for practical situations because it is not easy to build meaningful hierarchies for complex applications. More flexible models are needed.

## 5 Operating systems

Portable devices have evolved from having ad hoc supervisors to standard operating systems. Some systems use the Java run-time system as supervisor. High-end cell phones run complete operating systems such as Palm OS (now being replaced by Cobalt), Microsoft Windows CE (renamed PocketPC), Symbian, or Linux; and provide IP networking capabilities for web browsing, email and instant messaging. Some typical security features include:

- *A unique device identifier* – this can be accessed by applications.
- *A kernel configuration with enhanced protection* – this allows the use of the protected kernel mode, instead of the full-kernel model.
- *Digital authentication in the dial-up boot loader* – the dial-up boot loader is a program in ROM used to upgrade the OS image file (NK.bin) using flash memory or a remote server. The OS image file should be signed using digital encryption to verify its integrity before it is downloaded.

In addition, these operating systems include support for the standard cryptographic protocols.

The security of the operating system is fundamental for any system because it controls all the resources and provides support for the execution of applications. There is an overemphasis on cryptography, while aspects such as memory protection and file authorization have been neglected in most products, although this is changing (Cobalt includes memory protection). Memory protection is important in the creation of compartments to stop the propagation of viruses, while as mentioned above, file authorization is necessary to protect cryptographic keys and to enforce digital rights management. Downloaded contents, such as music, wallpaper, and games need to be protected. Current devices have no protection or protection based on cryptographic means. The study of these aspects provides a potentially fruitful research direction, in particular protection of digital rights without resorting solely to cryptography.

## 6 Web services

A web service is a component or set of functions accessible through the web that can be incorporated into an application. Web services expose an XML interface, can be registered and located through a registry, communicate using XML messages, and support loosely-coupled connections between systems. Web services represent the latest approach to distribution and are considered an important technology for business integration and collaboration. Figure 1 shows the architectural layers of web services architectures. Each layer is regulated by a variety of security standards [17].

Wireless devices can access web services using SOAP (Simple Object Access Protocol) but web services still are not widely used in portable devices. The limited processing power of portable devices and the lack of network reliability are a serious obstacle for a full implementation. However, using appropriate gateway middleware, it is possible for portable devices to access web services. Most access to web services from mobile devices now goes through a WAP gateway and most of the use of web services for mobile systems is now between servers [18]. However, this situation is changing and predictions indicate that web services in cell phones will be arriving soon [19] [20] [21]. In fact, Nokia just announced a Service-Oriented Architecture for smart mobile phones [22]. Security will be an important issue for this generation of smart and complex devices.

The richness of web services brings along a new set of security problems [17]. All the attacks that are possible in wired systems are also possible in wireless systems using web services, e.g., viruses, buffer overflow attacks, message interception, denial of service, etc. Web services introduce several extra layers in the system architecture and we have to consider the unique security problems of these layers. Since these are layers that run on top of the platform layers, the security of the platforms is still fundamental for the security of the complete system. Wireless systems using web services have to face, in addition, the general vulnerabilities of wireless networks and may also add new security problems to these networks, although this aspect has not been explored in detail. There is also a variety of standards for web services security and a designer of wireless devices should follow at least the most important ones to be able to have a credibly secure system. On the other hand, the extra layers bring more flexibility and precision for security; for example, encryption can be applied at

the XML element level, authorization can be applied to specific operations in a web service interface. This greater security precision allows applying policies in a finer and more flexible way.

Web services make possible convenient implementations of location-based services, where information is pushed to the device depending on its location. We discuss below additional problems that may occur in that case.

## 7 Location awareness

Because mobile devices are usually connected to networks, it is possible to track their position. For example, the US Federal Communications Commission mandates that cell phones must be able to be located within 300 meters of their actual location. In some cases the user of the device may want others to know her whereabouts but in other cases she might not [23]. Even in the first case, only authorized persons should have access to location information. That means that we need to control access to location information. This is another aspect of access control, related to the discussion in Section 4. Ease of determining location also raises privacy concerns [24] [25].

Location can also be used to get access to physical resources; for example, doors in a building could be controlled depending on the location of an authorized user. In some cases nomadic users may want to access the resources provided by some physical devices, e.g., printers or storage devices. A device may establish its web presence through physical registration [26]. The position of the user is important to decide which resources would be more convenient for him to access.

Location can be absolute or relative. Examples of absolute location are geospatial representation (typically longitude and latitude) or civic (address, city, region, country). The position of the mobile entity with respect to other known locations is an example of a relative location.

Work on this area requires finding new models of access control based on location information, as well as standard characteristics such as roles, certificates, and identity. For example, access control to location information may need to be performed in a distributed way [27] [14]. An overview of access control situations is given in [28]. Another direction is finding ways to preserve privacy; for example, [14] proposes the use of logical borders and anonymous IDs, based on the concept of personal profiles and context-aware agents, and [29] considers preventing unnecessary information to be disclosed to third parties. Contexts are important for privacy and access control. A context is an evolving, structured, and shared information space [30].

## 8 Conclusions

There is serious concern about the vulnerabilities of wireless systems. The easy access to the medium by attackers is a negative aspect, compounded by the design errors in the early protocols [31] [32] [33]. It is true that Wi-Fi is becoming more secure and Bluetooth appears reasonably secure but they (and WAP) cover only some of the

security layers. A basic security principle indicates that security is an all-layer problem, securing one or more layers is not enough [34]. With some of the layers still insecure, it is not possible to have true security.

Third generation systems will have voice quality that is comparable to public switched telephone networks. Voice over IP over WiFi will bring its own set of security problems. In addition, the new systems will have higher data rates, symmetrical and asymmetrical data transmission rates, support for both packet and circuit switched data services, adaptive interface to the Internet to reflect common asymmetry between inbound and outbound traffic, more efficient use of available spectrum, support for wide variety of mobile equipment, and more flexibility. All of these are the potential sources of new security problems. The pervasiveness of mobile devices makes their users want them to work together. For example, a cellular phone extracting phone numbers from a PDA or a digital camera storing its pictures in a laptop. This will lead to new interoperable architectures [35], which in turn, will bring new security problems. The proliferation of small devices in all places leads to *ubiquitous computing*, security issues for that environment are discussed in [36]. Anonymity, traceability, and traffic analysis are aspects that will become more important in that environment and they are all related to the protection of the metadata of the wireless structure. Usability of the security interfaces is another possible problem due to the limited sizes of these interfaces [8].

We have indicated some aspects that offer promising avenues for future work. We are working on some of these issues but there are several areas that appear neglected and could be a good source of ideas for future research. A general approach that appears promising is the use of security patterns, which can help designers build secure systems [34]. Several patterns have been found in the Bluetooth architecture, including versions of the Broker, Layers, Lookup, and Bridge patterns [37]. Some patterns for ubiquitous computing have appeared [38]. However, no specific security patterns for wireless systems have been described. Patterns are part of the more general area of software architecture and the methods and approaches of that area should be more explored for possible use in security [39].

#### **Acknowledgements**

This work was supported by a grant from the Defense Information Systems Agency (DISA), administered by Pragmatics, Inc. Tami Sorgente, Alvaro Escobar, and Andrei Bretan provided valuable comments that helped improve this paper.

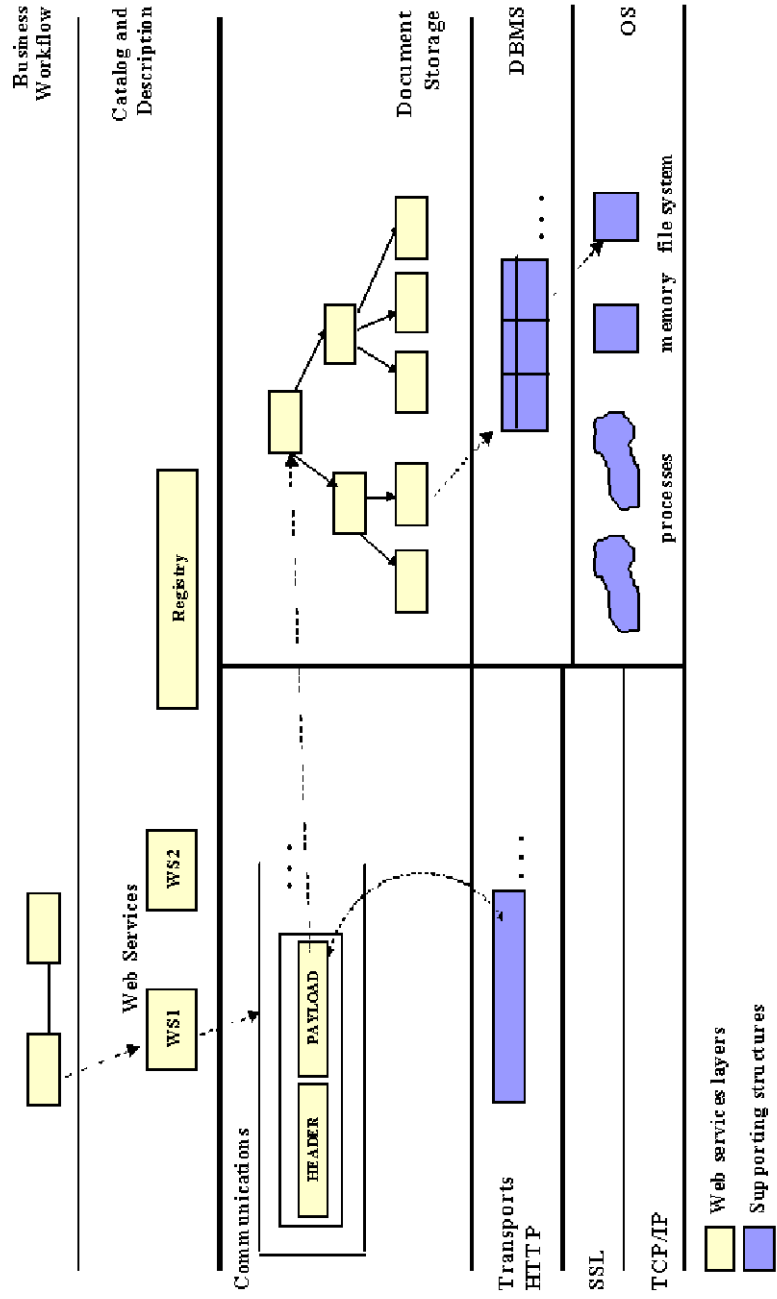


Figure 1. Web services architectural layers

## References

1. Fernandez, E. B., Jawhar, I., Larrondo-Petrie, M. M., and Van Hilst, M.: An overview of the security of wireless networks. In: Ilyas, M. (ed.): Handbook of Wireless LANs, CRC Press (2004)
2. Rajput, S.: Wireless security protocols. In: Ilyas, M. (ed.): Handbook of Wireless LANs, CRC Press (2004)
3. Elliot, G. and Phillips, N.: Mobile commerce and wireless computing systems, Addison-Wesley, 2004.
4. Stallings, W.: Wireless Communications and Networks, Prentice-Hall (2002)
5. Warneke, B., Last, M., Liebowitz, B. and Pister, K.S.J.: Smart dust: communicating with a cubic- millimeter computer. In: Computer, IEEE, January (2001)
6. Foley, S. and Dumigan, R.: Are handheld viruses a significant threat? In: Communications of the ACM, Vol. 44, No 1 (2000) 105-107
7. Ghosh, A.K. and Swaminatha, T.M.: Software security and privacy risks in mobile e-commerce. In: Communications of the ACM, Vol. 44, No. 2 (2001) 51-57
8. Josang, A., and Sanderud, G.: Security in mobile communications: Challenges and opportunities. In: Proceedings of the Australasian Information Security Workshop (2003)
9. Fernandez, E. B., Larrondo-Petrie, M. M., and Sorgente, T.: Security Models for Medical and Genetic Information. In: Proceedings of the IADIS International Conference (e-Society 2004), Avila, Spain, July 2004, (2004) 509-516
10. <http://www.dtic.mil/whs/directives/corres/html/81002.htm>
11. Thanh, D.V.: Security issues in mobile eCommerce. In: Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies (EC-Web 2000), Vol. 1875, Springer Verlag (2000) 467-476.
12. Kagal, L., Finin, T., and Joshi, A.: Trust-based security in pervasive computing environments. In: IEEE Computer, December 2001, (2001) 154-157.
13. Zhang, K., and Kindberg, T.: An authorization structure for nomadic computing. In: Proceedings of SACMAT'02, ACM (2002) 107-113.
14. Di Pietro, R. and Mancini, L.V.: Security and privacy issues of handheld and wearable wireless devices. In: Communications of the ACM, Vol. 46, No. 9 (2003) 75-79
15. Chadwick, D.W.: An X509 role-based PMI, (2001)  
[http://www.permis.org/files/article1\\_chadwick.pdf](http://www.permis.org/files/article1_chadwick.pdf)
16. Lee, Y.R. and Park, D.G.: The ET-RBAC-based privilege management infrastructure for wireless networks. In: Proceedings of EC-Web (2003) 84-93
17. Fernandez, E.B., Sorgente, T. and Larrondo-Petrie, M.M.: Web services security: Standards and research issues, in preparation.
18. Gralla, P.: Mobile web services: Theory vs. reality. <http://SearchWebServices.com>, 10 February 2004.
19. Pilioura, T., Tsalgatidou, A. and Hadjiefthymiades, S.: Scenarios of using web services in M-commerce. In: ACM SIGcomm Exchanges, Vol. 4, No 4, January 2003, 28-36
20. Yuan, M.J.: Access web services from wireless devices. In: Java World, August 2002, <http://www.javaworld.com/javaworld/jw-08-2002/jw-0823-wireless.html>
21. Yuan, M. J.: Securing wireless J2ME: Security challenges and solutions for mobile commerce applications. In: IBM DeveloperWorks, IBM, 1 June 2002  
<http://www-106.ibm.com/developerworks/wireless/library/wi-secj2me.html>
22. Yuan, M.J. SOA and web services go mobile, Nokia-style, 6 July 2004,  
<http://www.sys-con.com/story/?storyid=45531&DE=1>
23. Dogac, A. and Tumer, A.: Issues in mobile electronic commerce. In: Journal of Database Management, Jan.-March (2002) 36-42

24. Hong, J.I., and Landay, J.A.: An Architecture for privacy-sensitive ubiquitous computing. In: Berkeley EECS Annual Research Symposium, Berkeley, California, 24 February 2004; <http://www.eecs.berkeley.edu/BEARS/STARS.html>
25. Schilit, B. Hong, J. Gruteser, B. M.: Wireless Location Privacy Protection. In: IEEE Computer, December 2003
26. Barton, J., Kindberg, T., and Sadalgi, S.: Physical registration: Configuring electronic directories using handheld devices. In HPL-2001-119, Hewlett-Packard Co. (2001) <http://www.hpl.hp.com/techreports/2001/HPL-2001-119.pdf>
27. Hengartner, U. and Steenkiste, P.: Implementing access control to people location information. In Proceedings of SACMAT'04 (2004) 11-20
28. Larrondo-Petrie, M. M., VanHilst, M., Fernandez, E.B., Escobar, A., and Bretan, A.: Location-based access control, submitted for publication.
29. Gorlach A., Heinemann, A., and Terpstra, W.W.: Survey on location privacy in pervasive computing. In: Proceedings of 1<sup>st</sup> Workshop on Security and Privacy at the Conference on Pervasive Computing (SPPC), Vienna, April 2004.
30. Coutaz, J., Crowley, J.L., Dobson, S., and Garlan, D.: Context is key. In: Communications of the ACM, Vol. 48, No. 3, March 2005, (2005) 49-53.
31. Arbaugh, W.: Wireless security is different. In: Computer, IEEE, August 2003, 99-102.
32. Juul, N.C., and Jorgensen, N.: WAP may stumble over the gateway (security in WAP-based mobile commerce). <http://www.dat.ruc.dk/~nielsj/research/papers/wap-ssgr.pdf>
33. Saarinen, M.-J.: Attacks against the WAP WTLS protocol. In: Proceedings of Communications and Multimedia Security (1999) <http://www.jyu.fi/~mjjos/wtls.pdf>
34. Fernandez, E.B.: A methodology for secure software design. In: Proceedings of the 2004 International Conference on Software Engineering Research and Practice (SERP'04), Las Vegas, NV, 21-24 June 2004
35. Schilit, B.N., and Sengupta, U.: Device ensembles. In: IEEE Computer, December 2004, 56-64.
36. Stajano, F. and Anderson, R.: The resurrecting duckling: Security issues for ubiquitous computing. In: Security & Privacy 2002, Supplement to IEEE Computer, Vol. 35, No. 4, April 2002, (2002) 22-26. <http://www.computer.org/security/supplement1/sta/>
37. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, Boston, MA (1995).
38. Landay, J.A., and Borriello, G.: Design patterns for ubiquitous computing, In: Computer, IEEE, Vol. 36, No. 8, August 2003 (2003) 93-95.
39. Medvidovic, N., Mikic-Rakic, M., Mehta, N.R., and Malek, S.: Software architectural support for handheld computing. In: IEEE Computer, Vol. 36, No. 9, September 2003, (2003) 66-73.