# A THREE-DIMENSIONAL FRAMEWORK FOR SECURITY IMPLEMENTATION IN MOBILE ENVIRONMENTS

BETHUEL ROBERTO VINAJA
*Department of Computer Information Systems and Q.M., College of Business Administration, University of Texas Pan American, Email: vinajar@panam.edu*

Abstract: This paper describes a framework that can be used to identify security requirements for a specific mobile environment. The model includes three dimensions: mobile users, mobile hardware and mobile software. The analysis of the three dimensions can determine the characteristics of the specific implementation and needed security measures. Specific security measures for mobile hardware, mobile users and mobile software are also discussed.

Key words: Security, Mobility, Mobile Agents, Mobile Computers, Wireless

## 1. INTRODUCTION

The concept of mobility has become prevalent as the adoption of the Internet and wireless devices continues to grow. Strategy Analytic predicts that by 2004 there will be over one billion wireless device users and approximately 600 million wireless Internet subscribers. In this paper, we will examine the security aspects of mobility using a three-dimensional framework that analyses mobility in three aspects: mobile code, mobile hardware and mobile users. This framework distinguishes between three categories of mobility: hardware mobility, software mobility and user mobility.

## 2. MOBILE HARDWARE

Most transactions are still conducted at fixed locations using fixed personal computers and fixed terminals. Mobile devices provide users with convenient flexibility to conduct transactions and access information from multiple and varied locations, without being tied to any specific physical location. However, mobile devices have some limitations too. Most wireless networks and satellite-based systems have limited bandwidth. Cellular phone and satellite-based connections are generally more expensive than regular phone lines and ISDN. Given the bandwidth and cost challenges, it is very inefficient to handle long sessions and transfer large amount of data by using mobile devices (Wang et. al.1998). According to Chen (2000), the current network platforms have repeated shifts in both topology and network conditions. Such volatility in topology is attributed to:

1. Changes in the availability of various intermediate network hosts.
2. Mobility of mobile hosts such as laptops.
3. General shifts in network usage patterns that may affect bandwidth and host availability.

## 3. MOBILE USERS

Users are no longer accessing resources from a fixed location. Chen (2000) points out two possible scenarios:

- The user is relatively stationary towards a mobile device. A mobile user is one who accesses the Internet by using a laptop or portable computer.
- The user is mobile in relation to access devices. This user is called nomadic. A nomadic user accesses the Internet, but might move from one terminal to another.

The Internet open architecture allows resource sharing for both mobile and nomadic users. We can expect that as the Internet continues to spread out, more and more users will be classified as either mobile or nomadic. Both mobile and nomadic users need to transparently access resources either from a portable computer or any terminal connected to the Internet.

## 4. MOBILE SOFTWARE

Mobile computing has been already very successful, and mobile agents are now revealing that software can also be mobile. Mobile agent technology implies moving active code over spatially different places. An agent is a

software program that can autonomously perform a task on behalf of its user. Systems may combine static agents with mobile agents (Kearney 1998). The mobile agent paradigm encompasses three areas: Artificial Intelligence, networking, and operating systems. (Vogler et. al. 1998). From the Artificial Intelligence viewpoint, mobile agents are defined as autonomous software. From the operating system viewpoint, mobile agents are an evolution of code migration. Finally, from the networking viewpoint, mobile agents are an extension of client/server computing.

Mobile agents have several advantages. For example, mobile agents are relatively more efficient than traditional software programs and consume fewer network resources, because the agent moves the computation to the data, rather than the data to the computation. An additional characteristic is fault tolerance, that is mobile agents do not require a continuous network connection. An agent can start a job, disconnect, and later reconnect and get the results. Many mobile agents are implemented as Java applications. One of the advantages of Java applications is that they can be accessed from any terminal with Internet access. The requirements for executing an applet (Java application) are minimum; only a Java-enabled browser is required, and most popular browsers are Java-enabled. The following are some sample mobile agent applications.

One of the first mobile agent systems was Telescript, developed by General Magic, which by means of mobile agents, enables automated as well as interactive access to a network of computers.

D'Agents is a mobile agent designed at Dartmouth that supports mobile computers and disconnected operation. It is equipped with network-sensing tools and a docking system that allows the agent to transparently move between mobile computers, regardless of when the computers connect to a network (Brewington et. al. 1999).

Mobiware is an adaptive mobile networking environment based on distributed object technology. Built on CORBA and Java, it runs on mobile devices, wireless access points and mobile-capable switch/routers providing a set of open interfaces for adaptive mobile networking.

## 5. THE THREE-DIMENSIONAL FRAMEWORK

Dix et. al. 2000 have proposed a useful framework that can be used as a tool for the design of interactive mobile systems. The framework consists of taxonomies of location, mobility, population, and device awareness. The mobility dimension classifies levels of hardware mobility within the environment into three main categories:

—fixed: that is, the device is not mobile at all (e.g., a work station fixed in a particular place)
—mobile: may be moved by others (e.g., a PDA or computer that is carried around)
—autonomous: may move under its own control (e.g., a robot).

The taxonomy proposed by Dix, is very useful, but mobility is described using only one dimension, the hardware dimension. We can expand the analytical power of the framework by adding the software dimension and the user dimension. Our proposed framework is a three-dimensional matrix with three axis: mobile/static computers, mobile/static software and mobile/static users (Figure 1). Different applications can be differentiated in this basic classification matrix based on the criteria of computers, software and users. This framework can be used to categorise existing environments and even future developments. We can assign different scenarios to a three-dimensional space. Complete applications can be assigned to the areas of the matrix.

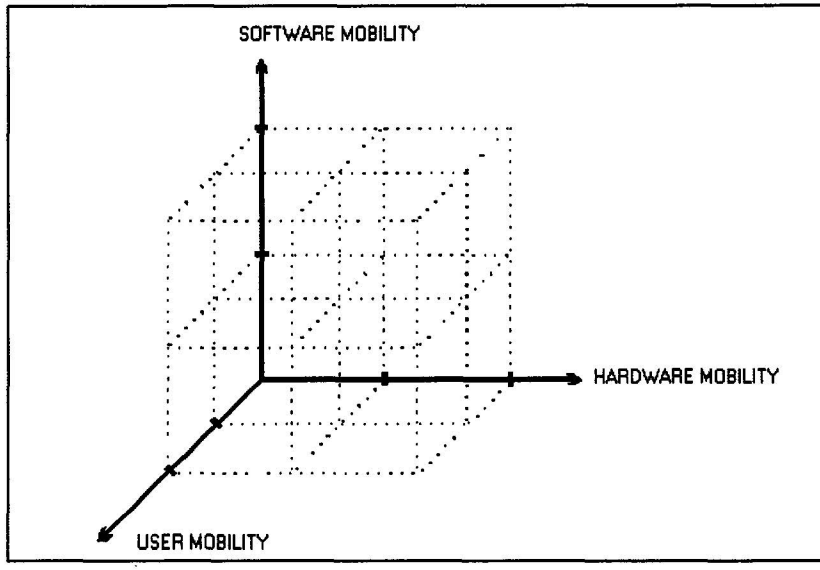


*Figure 1.* Three-dimensional framework

Personal computers, mainframes and computing centres are example of static computing environments. Laptops, PDAs, and cellular phones are examples of mobile environments. In a pure mobility environment all three dimensions (user, hardware and software) are mobile. This is represented as the upper front cube. The lower-back cube represents traditional fixed

environments. Other cubes include a mix of mobile and static characteristics. Table 1 describes sample scenarios combining the three dimensions.

*Table 1*. Sample environments

| Hardware | Software | User | Scenario |
|---|---|---|---|
| Static | Static | Static | A PC user at home. |
| Static | Static | Mobile | A user at the computer centre. |
| Static | Mobile | Static | A user launching Mobile agents at the computer centre |
| Static | Mobile | Mobile | A user launching agent from several static computers |
| Mobile | Static | Mobile | A salesperson using a laptop with office software. |
| Mobile | Mobile | Mobile | The optimum configuration |

Some of the quadrants in our three-dimensional space are difficult situations to define. In fact, the combination static user and mobile hardware is paradoxical, a static user, which always remains at the exact same location, would not get any value-added benefit from using a laptop or PDA. There may not be a real life situation that fits into some categories. However, these "empty" quadrants may present new opportunities to be discovered or new combinations of mobility dimensions.

The following is an example of the application of the framework to a specific scenario. The results are then interpreted and appropriate security measures are suggested. For example, a combination mobile hardware and mobile software for a mobile user would represent a pure mobile environment (Figure 2).

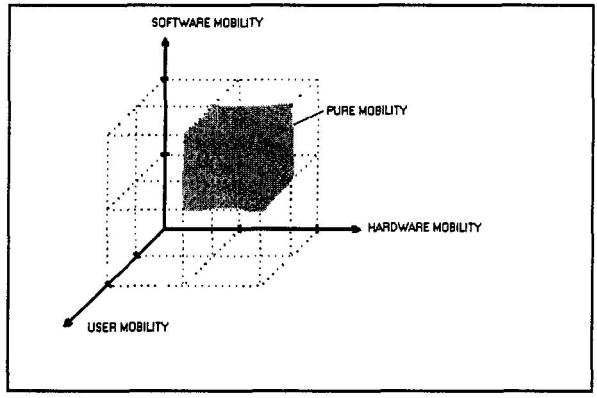


*Figure 2.* Pure mobility scenario

First, we analyse the hardware dimension. In our sample scenario a laptop is used. The laptop is more likely to get lost or stolen than a fixed computer because it is smaller and handy. If the laptop gets lost, the data on it gets lost too. If a third party steals or finds the laptop, that person might get unauthorised access to corporate resources. The proposed solution is the

user of strict authentication protocols so that the laptop can be used only by its owner, and not by anybody in possession of it.

Second, we analyse the software dimension. In our sample scenario, the user is launching mobile agent applications. The security implications are that the agent can be denied access by some server firewalls or filters. The solution to this problem can be to provide some cross-platform agent authentication mechanism so the server can verify the agent is coming from a trusted source. In those cases where the agent opens its code and data to the host server, there is the possibility for a malicious host server to modify this code and alter the agent behaviour. The solution to this security issue could be a partial or selective release of source code depending on the level of trust of the host server. Another solution could be to provide the agent with an "auto-disable" function in the event its source code is modified at the host server.

Finally, we analyse the user dimension. In our hypothetical case, the user is also mobile. A nomadic user, which is accessing the corporate network from multiple locations, requires some form of authentication in order to validate his/her identity. The main security concern in the user dimension is how to provide proper authentication. Passwords are the easier method of authentication, however mobile users might access the network from multiple locations and accidentally leave an open session. Another person might use the same computer and find the open session, and consequently an open door to confidential corporate data. A solution can be the use of other authentication methods based on smart cards or token authentication. However, the smart card can be lost too. A better solution can be the use of biometric authentication. Biometric methods can authenticate based on who the person is (unique characteristics), instead of what the person has (smart card method) or what the person knows (password method).

## 6. SECURITY IN A MOBILE ENVIRONMENT

Mobile devices and especially wireless devices require additional and more sophisticated security methods. Mobile devices are particularly exposed to specific risks not encountered in static environments. Mobile systems break assumptions that are implied in the design of fixed-location computer applications. Wireless devices always carry some level of uncertainty. Some of the potential risks include altered information, denial of access, interrupted transactions, transmission delays and power outages, (Davies 1994). In the case of a PDA used for electronic signatures, the user would need to always carry the PDA. If the device is left out of sight for

even a few moments, somebody might modify the signing program. The smart card could be stolen or modified too (Freudenthal et. al. 2000).

Mobile computers and wireless devices could also become the preferred tool for hackers given the difficulty to determine where an attack is coming from. Mobile devices are not linked to any specific geographic location, and the attacker can quickly get on-line or off-line, so it would be more difficult to determine the location of the hacker. As Chess (1998) states: "When a program attempts some action, we may be unable to identify a person to whom that action can be attributed, and it is not safe to assume that any particular person intends the action to be taken".

Malicious mobile scripts represent a significant risk for wireless devices. The potential damages of viruses, which are very well known in traditional fixed environments, can be even more malicious in a mobile environment. As one user moves from one cell area to the next, there is a security hole during the handing off process. It is during this lapse of time, that attackers can distribute malicious code and cause denial of service (Ghosh and Swaminatha 2000). In a traditional fixed environment, hackers break into a computer system; the attacker 'comes' to the targeted computer. In the case of wireless Internet access, the hacker can passively wait for its prey, which becomes an easy target as the user roams into the attacker's zone. The victim falls into the prepared 'trap'.

The authentication method used in mobile devices it is also an Achilles' heel. Many mobile devices authenticate only at initial connection. If connection is lost due to intermittent service failures and unreliable conditions (which is very usual with wireless devices,) the connection is re-established without re-authenticating. At this time, the reconnected session is not protected and a hacker can easily introduce viruses along with the transmitted data (Ghosh and Swaminatha 2000).

Users are commonly reluctant to transmit credit card information over the Internet, because they are concerned that their private information might be stolen or misused. This risk is even greater in the case of mobile Internet access. Lack of transaction security in mobile devices can be a major impediment for the adoption of M-Commerce. Ghosh and Swaminatha (2000) suggest the following security requirements to address the special risks of mobile computerd/devices:

- Memory protection for processes
- Protected kernel rings
- File access control
- Authentication of principals to resources
- Differentiated user and process privileges
- Sandboxes for untrusted code
- Biometric authentication.

Mobile devices or agents could be used for transferring controlled technologies and violate existing export regulations. Mobile agents and devices navigate from one location to another, making enforcement of export regulations more difficult (Bohm, Brown and Gladman 2000). Given all existing bamers on the export of intangibles, people may try to circumvent controls by using mobile devices agents, try to embedded encryption technology inside an intelligent agent, or as part of a mobile device.

## 7. FUTURE RESEARCH ISSUES

There are many opportunities for future research in the mobile security field. Current security protocols for mobile devices are alarmingly simple. A major limitation of mobile devices is its narrow bandwidth and capacity. This restraint forces designers to give up security and encryption to simplify the process and therefore improve on-line performance. Existing protocols for wireless devices are not as powerful as fixed-computer protocols. Clearly, there is a need for a protocol that is both efficient and powerful.

Future mobile applications might provide the ability to use e-cash stored on a phone's smartcard for purchases. The use of mobile devices for electronic payments can introduce additional security concerns. Malicious scripts might be able to off-load money from smartcards. The environment for conducting e-commerce transaction using a mobile device should support the following features (Van Thanh 2000):

- User authentication
- Merchant authentication
- Secure (encrypted) channel
- User friendly payment scheme supporting micropayments
- Receipt delivery
- Simple user interface.

Transaction security protocols such as SET are not suitable for wireless devices because of its complexity and resource requirements. More research is needed in the area of transaction security protocol for mobile devices.

## 8. CONCLUSION

This paper has described a proposed framework that can be used to identify security requirements for a specific mobile environment. The model includes three dimensions mobile users, mobile hardware and mobile software. Based on the combinations of these three dimensions we can determine the characteristics of the specific implementation and suggest

needed security measures. Mobile agent technologies and mobile computers will play an important role in the future, however many security issues need to be addressed before the technology can be fully implemented.

## 9. REFERENCES

Bohm, Nicholas, Brown, Ian and Gladman, Brian, "Strategic Export Controls: The Impact on Cryptography," *The Foundation for Information Policy Research,* Available online at: www.fipr.org

Brewington, Brian, Gray, Robert, Moizumi, Katsuhiro, Kotz, David, Cybenko, George and Rus, Daniela, "Mobile Agents for Distributed Information Retrieval," In Klusch, Mathias (Ed.): *Intelligent Information Agents,* Springer-Verlag, Germany, 1999, pp. 354-395

Chen, Larry T., "AgentOS: The Agent-based Distributed Operating System for Mobile Networks."

Davies, N., Blair, G., Cheverst, K., And Friday, A., "Supporting Adaptive Services in a Heterogeneous Mobile Environment," *In Proceedings of the Workshop on Mobile Computing Systems and Applications* (Mobile '94, Santa Cruz, CA, Dec.), IEEE, Los Alamitos, CA, 153–157.

Freudenthal, Margus, Heiberg, Sven and Willemson, Jan, "Personal Security Environment on Palm PDA," *IEEE,* 2000.

Ghosh, Anup K. and Swaminatha, Tara M., "Software Security and Privacy Risks in Mobile E-Commerce, *Communications Of The ACM,* February 2001, Vol.44, No.2.

Keamey, P., "Personal Agents: A Walk on the Client Side", In: Jennings, N.R. and Wooldridge, M.J., Agent Technology, Springer-Verlag, Germany, 1998, pp. 125-136.

Romao, Artur and Mira Da Silva, Miguel, "An Agent-Based Secure Internet Payment System for Mobile Computing," *Proceeding of Trends in Distributed Systems 1998: Electronic Commerce,* Hamburg, Germany, LNCS, Springer-Verlag, June 3-5, 1998.

Van Thanh, DO, "Security Issues in Mobile eCommerce," *IEEE,* 2000.

Vogler, Hartmut, Moschgath, Marie-Luise and Kunkelman, Thomas, "Enhancing Mobile Agents with Electronic Commerce Capabilities," In Klusch, Matthias and Weib, Gerhard, *Cooperative Information Agents II, Proceedings of the Second International Workshop, CIA 1998,* Paris France, July 1998, Springer-Verlag, Germany, pp. 148-159.

Wang, X.F., Lam, K.Y. and Yi, X., "Secure Agent-Mediated Mobile Payment," In Ishida, Toru (ed.) *Multiagent Platforms, First Pacific Rim International Workshop on Multi-Agents, PRIMA 98,* Singapore, November 1998, LNCS 1599, Springer-Verlag, Germany, pp.162-173.