Security Issues in a Mobile Computing Paradigm.

Mavridis I., Pangalos G.
Informatics Laboratory, Computers Division, Faculty of Technology
Aristotle University of Thessaloniki
Thessaloniki 540 06, Greece
Tel: +30-31-995965, Fax: +30-31-995949
Email: imavridi@athena.auth.gr, gip@eng.auth.gr

Abstract

In this paper, we discuss operational and security issues arising from the use of mobile components in distributed systems. We argue that mobile agents can be used to overcome intrinsic problems of wireless networking. We define the operational model of our mobile computing environment, where we plan to demonstrate our proposed solutions. We also discuss security problems and mechanisms that can be applied to each one of the three main components of our mobile computing model, which is intended to be implemented in a health care paradigm, where special conditions and emergency needs are imposing the use of services supported with mobile computing.

Keywords

Mobile computing, mobile computing security, distributed systems security, mobile agents security.

1 INTRODUCTION

The radical evolution of computers, especially in hardware (towards smaller size and weight, higher performance, lower power consumption, lower cost) and communications (wireless and satellite networks, cellular telephony, WANs, INTERNET), has introduced the idea of mobile computing (Imielinski and Badrinath, 1992). This means that users don't have to be tethered on expensive wired workstations in order to exchange data. All they need is mobile computers,

Communications and Multimedia Security Vol. 3 S. Katsikas (Ed.)

that is portable computers communicating via wireless networks. Mobile computer will be the 'communication car' for people of 21st century: the freedom to communicate in anyway, from everywhere and any time (Weiser, 1991),(Weiser, 1993). Mobile computing is tightly depending on available infrastructure of distributed systems. As a result, we can see it as an extension of distributed systems computing. Furthermore, the addition of ideas like mobile agents imposes mobility to a wide range of technological approaches towards future distributed information systems (Gray; Kotz; Nog; Rus and Cybenko, 1996).

The benefits of on-the-move network connectivity are obvious. However, there are serious networking and systems issues to be solved before the full benefits of mobile computing systems are realised in practice. One critical issue is security (Hardjono and Seberry, 1995).

This paper aims to discuss the security problems arising from today's technological approaches to mobile computing. In order to demonstrate our proposed solutions, we also introduce a technological model of implementation in a health care environment, where special conditions and emergency needs are imposing the use of services supported with mobile computing.

2 THE TECHNOLOGY INFRASTRUCTURE

Wireless information systems are computing systems that provide the ability to compute and communicate anywhere and anytime. A number of terms have been used in the literature to describe such systems, including wireless computing, ubiquitous computing, nomadic computing and decoupled computing.

Wireless networks communicate by modulating radio waves or pulsing infrared light. Wireless communication is linked to the wired network infrastructure by stationary transceivers. The area covered by an individual transceiver's signal is known as a *cell*. Cell sizes vary widely: for example, an infrared transceiver has a range of a few meters, and a satellite beam can cover an area more than 400 miles in diameter.

2.1 General architecture of wireless networks

The vision of mobile wireless computing requires ubiquitous wireless network connectivity, adequate wireless bandwidth and a small, portable computing platform with sufficient functionality. The necessary networking infrastructure (called *PCN*, for personal communication network) is still very much under debate, although it will most likely be based on the cellular networking architecture. The *cellular* (in future, microcellular and picocellular) architecture is capable of providing voice and data services to users with hand-held devices. Continuous coverage of cellular service is restricted to metropolitan regions. Wide-area moves require the user to inform the network of his new location. The available bandwidth is very low for most data intensive applications (Imielinski and Badrinath, 1992). *CDPD*, which stands for Cellular Digital Packet Data, is another emerging technology. It transmits packet-based data over existing analog networks for voice communications, using frequency hopping. The CDPD device listens to a channel. When it finds an adequate idle time in a call, it transmits the packets using the full bandwidth. If the channel is full, it hops to another channel and repeats the same process. The main advantage with CDPD is that it has low cost, while billing is based on amount of data rather than time. Finally, the so-called *PCS* (Personal Communication Services) technology can provide local area services such as voice, fax and data communication. The advantage of PCS over cellular networks is that it will offer a wider bandwidth.

Wireless LAN is a traditional LAN architecture extended with a wireless interface to service small low-powered portable terminals capable of wireless access. The wireless LAN is further connected to a more extensive fixed network such as LAN or WAN. Wireless LANs have limited range and are designed to be used only in local environments. There are two types of wireless LAN architectures: *ad-hoc* networks and *infrastructured* networks. The *Wide-Area Wireless Networks* are special mobile radio networks that provide wide coverage for low bandwidth data services. In *paging networks* the service is usually receive-only and has very low bandwidth. The initial applications for *satellite systems* are voice and paging. Additional services planned include messaging and fax transmission.

2.2 Operational problems

The essential properties of mobile computing are *wireless communication*, *mobility* and *portability* (Forman and Zahorian, 1994). Each one of these properties introduces, however, a number of problems.

Some of the problems that wireless communication introduces are:

- *Disconnection.* Wireless communications suffer from frequent disconnections due to a higher degree of noise and interference as well as the process of inter-cell hand-offs. Disconnections can be hidden by asynchronous operation.
- *Bandwidth and Interface Variability.* Bandwidth can shift one to four orders of magnitude, depending on whether the system is plugged in or using wireless access or switching interfaces, e.g. from infrared to radio when the user moves from indoors to outdoors. Mobile applications have to adapt their behaviour properly (Katz, 1994).
- *Heterogeneous network.* To achieve wireless communication a mobile host must get connected to different and heterogeneous networks. The general problem of heterogeneity can be addressed by exploiting emerging distributed systems standards such as the Object Management Group's Common Object Request Broker Architecture (OMG-CORBA), or the Open Software Foundations Distributed Computing Environment (OSF-DCE).
- *Security Risks.* Precisely because connection to a wireless link is so easy, the security of wireless communication can be compromised much more easily than that of wired communication.

Mobility also introduces a number of problems. For example:

- *Address Migration.* This a consequence of mobility and several techniques such as selective broadcast, central services, home bases and forwarding pointers may provide solutions (Forman and Zahorian, 1994).
- *Location-dependent Information.* Information needed to configure a computer, such as the local name server, available printers, time zone, etc., is location dependent. Mechanisms are needed for obtaining configuration data appropriate to each location.
- *Privacy.* Answering dynamic location queries requires knowing the location of other mobile users. Such information should be protected against misuse and this can be achieved by denying users the availability to know other users' location (Spreitzer and Theimer, 1993).
- *Inter-realm support.* Designing distributed services to support the mobile user. Providing authentication, accounting and management over a wide area and across organisations (Duchamp, 1992).

Finally, some of the problems that portability introduces are:

- *Low Power.* Power consumption is a very important design issue and affects portability.
- *Risks to transactions.* Disconnection of a user, during a transaction with his bank or the stock market might prove disastrous and a number of techniques and *policies* has been proposed.
- *Risks to data.* Making computers portable increases the risk of physical damage, unauthorised access, loss and theft. The security risks can be reduced by minimising the essential data kept on board.
- *Small user interface.* Solutions are virtual reality displays, handwriting recognition and voice recognition.
- *Small storage capacity.* To reduce the size of program code is to interpret script languages instead of executing compiled object codes.

3 SECURITY PROBLEMS IN MOBILE COMPUTING

Mobile computing, that is the ability of having computing and communication abilities on the move, depends on the existence of a suitable distributed systems infrastructure. So, security considerations of mobile computing can be seen as extensions to those of distributed computing. We will, therefore, examine the security issues in mobile computing on the basis of known security issues of information systems.

Current thinking of information systems security is that the issues centre on *confidentiality* (information that is stored on a system or transmitted over communication links, is only be disclosed to those users who are authorised to have access to it), *integrity* (information is modified only by those users who have the right to do so), *availability* (information and other IT resources can be accessed by authorised users when needed), *accountability* (system users are accountable for their actions) and *non-repudiation* (responsibility for actions cannot be denied) (Pangalos; Khair and Bozios, 1995),(Yialelis, 1996).

Security breaches in computer systems are related to the notions of exposures, vulnerabilities, threats and controls. *Exposure* includes disclosure of data, modifications of data, denial of legitimate access to computing. *Vulnerability* is a weakness in the security system that might be exploited to cause loss or harm. *Threat* to computing system is a circumstance that has the potential to cause loss or harm. *Control* is a protective measure that reduces a vulnerability (Russel, 1991),(Pfleeger, 1989). The major threats to the security of a computing system are interruption, modification, interception and fabrication. *Interruption* takes place when an asset of the system becomes lost or unavailable. *Modification* happens when some unauthorised party has gained not only access but tampers with an asset. *Interception* takes place when some unauthorised party has gained access to an asset. *Fabrication* happens when some unauthorised party fabricates objects for a computing system (Pangalos; Khair and Bozios, 1995).

3.1 Security of distributed systems

Security of distributed systems is a critical issue, as it is difficult to provide in such an environment physically secure communication and to co-ordinate multiple management policies. A distributed system is susceptible to a number of threats both from legitimate users of the system and from intruders. Two general types of security threats are the *host compromise* and the *communication compromise* (Yialelis, 1996),(Varadharajan, 1995).

Host compromise security threats refer to various degrees of subversion of individual hosts. Possible attack categories are the followings:

- *Masquerading*: when a user is masquerading as another to gain access to a system object to which he is not authorised.
- *Unauthorised use of resources*: when a user is accessing system object without having authorisation. This situation may lead to theft of computing resources or improper use of information.
- *Disclosure of information*: unauthorised reading of stored information.
- *Alteration of information*: unauthorised writing into stored information.
- *Denial of service*: the attacker acts to deny resources or services to entities which are authorised to use them, e.g. by locking a file.

The communication compromise security threats refer to threats associated with message communication. Possible attacks can be categorised as follows:

- *Masquerading*: when a user is deceiving about its real identity. Masquerading may lead to impersonation.
- *Unauthorised use of resources*: when a user is accessing a network component without have being authorised This situation may lead to theft or improper use of communication resources.

- *Interception*: The opponent gains access to the data transmitted over the communication link. Two types of interception are distinguished: *disclosure of information* (the opponent obtains information transmitted over the link), and *traffic analysis* (the opponent observes the message patterns and derives information about the identities and locations of the communicating parties, the message frequency and length, etc.).
- *Alteration of resources and information*: The opponent modifies the messages transmitted, alters their sequence or delays them. Unauthorised alteration of information may occur through active wire-tapping. This threat may also involve unauthorised introduction (removal) of resources into (from) a distributed system.
- *Fabrication*: The opponent inserts information into the communication link. A special type of this attack is replay of old messages in order to mislead the communicating parties.
- *Repudiation of actions*: This is a threat against accountability. A repudiation attack may occur whereby the sender (receiver) of a message denies having sent (received) it.
- *Denial of service/Interruption*: The attacker prevents the easy transmission of information.

Finally, the security functions and controls that can be used in distributed systems include (Yialelis, 1996):

- *Identification and Authentication*: Authentication information and mechanisms that involve trusted third parties (passwords, cryptographic techniques, challenge-response techniques).
- *Access control and Authorisation*: Access control information, access control rules, delegation.
- Information *confidentiality*: Confidentiality mechanisms (encryption) and attributes (secret keys, public and private keys).
- Information *integrity*: Integrity mechanisms that provide generation and verification of integrity checks.
- *Non-repudiation*: (e.g. through digital signatures).
- *Auditing* and *Accountability*.
- *Availability* and *Prevention of Denial of Service*.

3.2 Security in mobile unit extensions

When distributed systems include mobile parts, we face several additional security problems. Usually those that stream from distributed systems gain interest, for example delegation, while others, as for example authentication and encryption, must eliminate the system load they produce as a result of their completeness. Some properties of mobile computing systems that also affect security are broadcast base communications (ease accessible to eavesdroppers), crossing boundaries of administration domains with high heterogeneity, disconnections, physical constraints of mobile devices, high dependence on the infrastructure, highly distributed environment, etc.

Security and delegation

The security provisions used in mobile computers must operate in a dynamic and fluid communication environment. Furthermore, the subnetworks may be physically distributed and may not geographically overlap. Thus, a computer may have to switch communications between different kinds of subnetworks and it may become disconnected as it moves. The ability to *delegate* limited authority is essential to realise security in a ubiquitous computing environment. A *delegation* is a temporary permit issued by the delegator and given to the delegate who becomes limited authorised to act on the delegator's behalf (Campbell; Sturman and Tock, 1994).

Delegation is a well understood problem but there are special considerations for mobile systems that these existing approaches do not address. The usual requirements for a general delegation scheme include:

- *Revocation*: the delegator must have the ability to cancel delegations it has issued.
- *Cascading*: the delegate must have the option to create delegations on the delegator's behalf.
- *Restriction*: The delegator must be able to limit the rights granted by any delegation.

The delegation for mobile computers has, however, the following additional requirements:

- *Disconnected Delegates*: Since a client may disconnect after issuing a delegation, delegations must succeed even if the delegator is currently not attached.
- *Low Resource Usage*: It is crucial that bandwidth and host resource usage be minimised.
- *Frequent Creation and Revocation*: Delegations may be issued and revoked frequently as mobile hosts detach and reattach to the system.
- *Interoperability*: Delegation should be as independent of the underlying protocols and system software as possible to promote interoperability.

Security and mobility

In mobile computing it is sometimes difficult to achieve the required isolation and self-efficiency due to the relatively limited resources available to a mobile unit, which makes it necessary to communicate with the mobile support station. The mobility of users and data that they carry introduces, therefore, security problems from the point of view of the *location* of a user and the secrecy and authenticity of the data exchanged. A user on a mobile wireless network may choose, for example, to have the information concerning his existence treated as being confidential. That is a user may choose to remain *anonymous* to the majority of other users on the network, with the exception of a select number with whom the user often interacts.

Another potential security problem lies in the possibility of *information leakage*, through the inference made by an attacker *masquerading* as a mobile support station, who may issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user's profile containing the patterns and history of the user's movements.

Related to the management of these databases is the issue of *replication* of certain parameters and user profiles with the aim of replicating the environments surrounding the user. Thus, as the user roams across zones, the user must not experience a degradation in the access and latency times.

In general, as sensitive data is replicated across several sites, the security risks are also increased due to the multiplication of the *points of attack* (Hardjono and Seberry, 1995).

Security and disconnections

Differing levels of disconnection may be introduced, ranging from the normal connection to connections using low bandwidth channels. A crucial aspect of disconnection is the elective or non-elective nature of a disconnection (Imielinski and Badrinath, 1993). Security and integrity problems may occur in the case of frequent disconnections caused by *hand-offs* that occur when the mobile unit crosses zones (cells).

The transition from one level of disconnection to another may present an opportunity for an attacker to *masquerade* either the mobile unit or the mobile support station. An attacker should not be able to 'hi-jack' the communications of a mobile unit which is *stepping-down* its level of connection and then masquerading as the mobile unit. Similarly, an attacker must not masquerade as a mobile support station to a mobile unit that is about to *step-up* its level of connection.

4 SECURITY CONTROLS IN MOBILE COMPUTING SYSTEMS

Our work on the security of mobile computing aims to address the problems pertaining to the security of information within the following three sub-areas of the mobile environment:

1. The *security* of information residing in the *mobile units*, considering device constraints,
2. The *security* of information as it travels *'over the air'* between mobile units and mobile support stations. An important consideration in this area is the *power consumption* of the algorithms that implement this secure data transfer.
3. The *security* of information within the rest *network* (wired hosts). This includes the *security* of databases holding control data used for the operations and management of the mobile wireless network.

In the tables 1 and 2 below, we summarise for each of the above sub-areas the major security vulnerabilities and threats that a general mobile computing system is prone to.

Table 1 Security vulnerabilities of a general mobile computing system

	Mobile units	*Over the air*	*Wired hosts*
Physical vulnerabilities	small size and weight, portability, exposure in hostile places	random happenings that easy affect wireless communications	different locations
Natural vulnerabilities	exposure in outdoor environmental conditions	affected from weather situations, hand-offs between cells	unknown boundaries, many points to attack
H/W and S/W vulnerabilities	not enough hardware controls and resources		heterogeneity, shared use of resources
Communications vulnerabilities	dependence on the communication infrastructure	broadcasting	
Human vulnerabilities	away from technical support and management, lack of attention	unlimited capability for physical access	

Table 2 Security threats of a general mobile computing system

	Mobile units	*Over the air*	*Wired hosts*
Physical threats	theft, damage	physical disasters	physical disasters
Natural threats	problematic operation	interruptions, bad quality	
Intentional threats	denial of service, covert channels, used by third parties	interference, eavesdropping, denial of service, routing alterations	denial of service, faults in hardware and software
Unintentional threats		overloading	improper handling

Several proposals have been made for implementing security controls in the above three sub-areas of the mobile environment. Further work is, however, necessary to organise the various rules and practices towards a safe mobile computing environment.

4.1 Mobile user devices and security modules

According to (Pfitzmann; Pfitzmann; Schunter and Waidner, 1996), a *mobile user device* is any portable device that belongs to a specific user and has computing and storage capabilities. Mobile devices are designed to be small and lightweight, making them highly portable. They are vulnerable to: being misplaced, lost and theft, etc. Mobile devices can be protected by the use of passwords and smartcards. A *security module* is any device that is tamper-resistant.
The following types of trust in a mobile user device must be distinguished. As the device acts *on behalf of someone*, the analogy of agents is used:

- *Personal-agent trust*: User has to be able to trust that the device acts according to his wishes while he possesses it.
- *Captured-agent trust*: The legitimate user may want the mobile device to protect him even if it was lost or stolen or if he gave it away.
- *Undercover-agent trust*: Other parties may want a mobile user device to protect them from the legitimate user of that device.

4.2 Communication security services and mechanisms

According to (Katz, 1994), in a mobile computing environment, the security and accounting protocol will typically be invoked when a mobile unit and base station first set up communications. At this point, the base station and mobile unit authenticate each other, negotiate accounting terms, and set up a shared key for private communication. Efficient communication security services thus should have the following goals:

- *Authentication*: The mobile unit and the base station must be able to *mutually* authenticate each other.
- *Data Privacy*: The data transmitted over a communication channel must be protected from snooping, replay, or forgery.
- *Location Privacy*: It is desirable or critical not to compromise the location and identity of the mobile user.
- *Accounting*: The mobile unit must be charged for the services it uses.
- *Efficiency*: The security protocol should be efficient. Data security should be optional. Efficiency is critical since each hand-off requires an invocation of the above security services. Also, data encryption should be optional and differentiated between uplink and downlink communications on the basis of power consumption.

4.3 Security policies and domains

Security policy refers to the set of rules, laws and practices that regulate how an organisation manages, protects, and distributes sensitive information. A security policy must specify the security goals the system must meet and the threats it must resist. This implies that a security policy should determine the type of secure communication required for various transactions, the type of authentication, auditing procedures, recovering techniques and access control. One important part of security policy is access control. In general, the access control policy specifies who can access particular resources and what operations the accessor can perform on those resources (Yialelis, 1996).

The crossing of administrative (security) domains is of special interest, as the mobile unit moves, and appropriate functions needed. A security domain means a set of network entities on which a single security policy is employed by a single administrative authority (Vasquez-Gomez, 1994).

5 OUR SECURE MOBILE COMPUTING PARADIGM

In our secure mobile computing paradigm, we consider the case of a distributed health care information system which includes one or more mobile parts. As described in more detail below, the servers are stationary and users access takes place from mobile terminals (e.g. portable PCs).

As an example of such an environment, we consider a typical crisis management application during a physical disaster. The disaster has happened in a isolated area of the country and communications to the local health care information systems are out of proper work. Medical people are providing their services moving through the area and they are depending for their support on wireless connections. Doctors and nurses are using multimedia terminals that provide wireless communication and handle measurements of patients status data. They might need access to: (1) patient's history and special information to provide emergency treatment, (2) a list of local available medicines, (3) laboratory processing of patient's data and specialist's diagnosis and treatment support, (4) general purpose voice and data communications to other doctors, as well as other public service entities and (5) maps to plan the route from the care station to the patient.

Modern medicine places today a great reliance upon information technology. Health Care Environments (HCEs) contain a large number of systems processing many types of health data. These systems contain large amounts of information, much of it relating to individuals and of a sensitive nature. The issue is further complicated by the variety of information that may be held in databases, and the fact that several different levels of data sensitivity may exist. There is consequently an obvious need for data security and to retain a relationship of trust between patients and the HCE (Furnell, Pangalos, Sanders and Warren, 1993). The desired protection will depend upon several factors including the computer configuration, the operational environment and the information itself.

6 THE OPERATIONAL MODEL OF OUR MOBILE COMPUTING ENVIRONMENT

Our mobile computing model, which forms the basis of our research and experimentation, consists of (Bharghavan, 1994):

- *mobile units*: portable computers with multimedia and radio/infrared communication abilities, used by mobile users, that must have enough memory to cache efficient amount of data received or ready to transmit and enough ports to connect to various peripheral devices and instruments,
- *home stations:* stationary workstations on the backbone (wired) network which act as the repository of the mobile user's data, as well as docking machines (Gray; Kotz; Nog; Rus and Cybenko, 1996) for mobile agents transmission,
- *base stations:* machines (transceivers) connected to the backbone network which provide wireless networking connectivity to the mobile units in their cell and change when the mobile unit moves out of the cell.
- *a certifying authority:* a trusted authority which acts as a trusted third party and is useful to provide secure key dispositions.

All wireless communication is either *uplink* (mobile unit to base station) or *downlink* (base station to mobile unit). Consequences of this restriction are that mobile unit peer-to-peer communication (ad-hoc networks) is prohibited and only a base station is allowed to multicast packets in a cell (Katz, 1994).

6.1 System characteristics

Mobile units, in our model, may range from simple PDAs to powerful notebook computers. Wireless media are inherently less secure than wired. Wireless bandwidth is typically orders of magnitude lower than backbone bandwidth. Overhead of the security protocol (security messages) must be minimised. Mobile communications work in the presence of network partitions (Bharghavan, 1994).

The entities involved in an authentication (home station, base station, mobile unit, certifying authority) may be autonomously managed. The same mobile unit may be used by different users at different times. During the authentication process, the mobile unit generates the shared key, authentication information, and accounting information based on the user profile and identification key (Katz, 1994).

All objects residing on the backbone network are distributed, but stationary, and interact with each other through synchronous message-passing. This paradigm has to be enhanced with additional paradigms such as asynchronous message-passing, object mobility, and active objects (IBM Aglets).

6.2 Mobile agents

We use mobile agents to provide a paradigm for distributed object computing, encompassing synchrony and asynchrony, message-passing and object-passing, and stationary objects and mobile objects.

Along with mobility, agents have the following characteristics (Chang and Lange):

- *Object-passing.* When a mobile agent moves, the whole object is passed; that is, its code, data, execution state, and travel itinerary are passed together.
- *Autonomous.* The mobile agent contains sufficient information to decide what to do, where to go, and when to go.
- *Asynchronous.* The mobile agent has its own thread of execution and can execute asynchronously.
- *Local interaction.* The mobile agent interacts with other mobile agents or stationary objects locally.
- *Disconnected operation.* The mobile agent can perform its tasks whether the network connection is open or closed. If the network connection is closed and it needs to move, it can wait until the connection is reopened.
- *Parallel execution.* More than one mobile agent can be dispatched to different sites to perform tasks in parallel.

Mobile agents provide easy, efficient and transparent access to mission-critical data for mobile workers even when connections between mobile clients and stationary servers are problematic or not exist. We consider of an asynchronous, store-and-forward messaging architecture (ORACLE Mobile Agents).

7 IMPLEMENTATION

The experimental implementation's environment includes the AHEPA hospital as the main infrastructure that an isolated medical team is intended to use in the case of physical disaster conditions. The AHEPA university hospital is a general hospital, which is part of the Aristotelian University of Thessaloniki. The following figures describe briefly the hospital: 16 clinics including the reference and hospitalisation centre for AIDS patients from all Northern Greece; 40 laboratories; a radiological department including M.R.I., C.T., U.S., D.S.A., X-rays, etc.; a nuclear medicine department (SPECT, Gamma-Camera); 705 beds; 520 medical doctors including consultants; 762 nursing personnel; 466 personnel for financial and general support; 28,000 inpatients per year; 2,500 surgical procedures per year; 107,000 outpatients per year; 2,345,000 laboratory tests per year (1993). The backbone infrastructure consists of different networks that communicate with each other via INTERNET. To overcome heterogeneity problems we adopt the OMG/CORBA standards.

We consider different mobile station supports that a mobile unit can use, as it moves, to establish a communication link. Various kinds of disconnections, that are mainly due to hand-offs, are happening and different connection protocols are used. To cope with disconnections and bad communication conditions, we use mobile agents.

8 CONCLUSION

The use of mobile resources in distributed environments provides important benefits. Serious security problems are derived, however, from the essential attributes of mobile computing. Due to technological problems, especially in wireless communications, mobile agents are used to provide a reliable solution given the wide range of existent applications and distributed information systems. In this paper, we presented the general technological infrastructure, the mobile system model used for our experiments and the Health Care Environment where our work is in progress.

Future work includes a systematic definition of at least two different security policies that are used by different backbone networks. Mobile units and their delegates (mobile agents) are provoked to overcome those different situations and to complete their tasks. Further work also includes the implementation of special authentication and access control techniques.

9 REFERENCES

Bharghavan, V. (1994) A protocol for Authentication, Data and Location Privacy, and Accounting in Mobile Computing Environments. *Proceedings of the ACM Conference on Computers and Communications Security, Fairfax, Virginia.*

Campbell, R.; Sturman, D. and Tock, T. (1994) Mobile Computing, Security and Delegation. *International Workshop on Multi-Dimensional Mobile Communications, Japan.*

Chang, D.T. and Lange, D.B. Mobile Agents: A New Paradigm for Distributed Object Computing on the WWW. *Submitted to OOPSLA '96 Workshop Toward the Integration of WWW and Distributed Object Technology*, also available at URL http://www.trl.ibm.co.jp/aglets/ma.html.

Duchamp, D. (1992) Issues in Wireless Mobile Computing. *Proceedings Third Workshop on Workstation Operating Systems,* April 1992, 2-10.

Forman, G.H. and Zahorian, J. (1994) The Challenges of Mobile Computing. *IEEE Computer*, April 1994, 38-47.

Furnell, S.M.; Pangalos, G.; Sanders, P.W. and Warren, M.J. (1993) A Generic Methodology for Health Care Data Security. *Medical Informatics*, **19(3)**.

Gray, R.; Kotz, D.; Nog, S.; Rus, D. and Cybenko, G. (1996) Mobile agents for mobile computing, *Technical Report PCS-TR96-285, Department of Computer Science, Dartmouth College, Hanover,* available at URL ftp://ftp.cs.dartmouth.edu/TR/TR96-285.ps.Z.

Hardjono, T. and Seberry, J. (1995) Information Security Issues In Mobile Computing. *Information Security - the Next Decade, Proceedings of the IFIP TC11, Eleventh International Conference On Information Security, IFIP / Sec '95, Capetown, South Africa,* Chapman and Hall, London-Melbourne, 143-151.

IBM Aglets Workbench, http://www.ibm.co.jp/trl/aglets

Imielinski, T. and Badrinath, B.R. (1992) Mobile Wireless Computing: Solutions and Challenges in Data Management. *Technical Report DCS-TR-296, Department of Computer Science, Rutgers University, NJ.*

Imielinski, T. and Badrinath, B.R. (1993) Data management for mobile computing. *SIGMOD RECORD,* **22(1)**, 34-39.

Katz, R.H. (1994) Adaptation and Mobility in Wireless Information Systems. *IEEE Personal Communications, 1st Quarter, 6-17.*

ORACLE Mobile Agents, http://www.oracle.com

Pangalos, G.; Khair, M. and Bozios, L. (1995) An Integrated Secure Design of a Medical Database System. *MEDINFO '95, The 8th World Congress on Medical Informatics, Vancouver, Canada.*

Pfitzmann, A.; Pfitzmann, B.; Schunter, M. and Waidner, M. (1996) Mobile User Devices and Security Modules: Design for Trustworthiness. *IBM Technical Report RZ-2784.*

Pfleeger, C. (1989) Security in Computing. *Prentice-Hall International Editions.*

Russel, D. (1991) Computer Security Basics. *O'Reilly & Associates.*

Spreitzer, M. and Theimer, M. (1993) Scalable, Secure, Mobile Computing with Location Information. *Communications of the ACM,* July 1993, **36(7)**.

Vasquez-Gomez, J. (1994) Multidomain Security. *Computers and Security,* **13**.

Varadharajan, V. (1995) Distributed Object Systems Security. *Information Security - the Next Decade, Proceedings of the IFIP TC11, Eleventh International Conference On Information Security, IFIP / Sec '95, Capetown, South Africa,* Chapman and Hall, London-Melbourne, 305-321.

Weiser, M. (1991) The Computer for the Twenty-First Century. *Scientific American,* **265(3)**, 94-104.

Weiser, M. (1993) Some Computer Science Issues Related to Ubiquitous Computing. *Comm. ACM,* **36(7)**, 75-85.

Yialelis, N. (1996) Domain-Based Security for Distributed Object Systems. *Thesis, Imperial College of Science.*

10 BIOGRAPHY

IOANNIS MAVRIDIS obtained his Diploma in Computer Engineering and Informatics from the University of Patras, Greece in 1985. He holds experience in CIM (discrete manufacturing) obtained in ELBO, a vehicle industry, where he has worked as EDP-manager for six years. He is currently working towards his PHD in mobile computing security at the Aristotle University of Thessaloniki, Greece. His research interests include the areas of mobile computing security, medical information systems, distributed object systems and database security.

Prof. GEORGE PANGALOS has a B.Sc. degree in Mathematics from the University of Athens and a Master's (M.Sc.,1974) and a Doctor's (Ph.D., 1979) degree in computer science from the University of London, UK. He is a Professor of Informatics at the University of Thessaloniki. He has also taught informatics in the universities of Athens and of the Aegean. He is the current president of the northern-Greece branch of the Greek Computer Society. He is also the current vice-president of the Greek Medical Informatics Society. He has also been president of the Confederation of European Computer Users Association (CECUA). His research interests include the areas of database technology, database security, medical information systems and information systems security. He has been the author of several books on I.T. and has published over 70 papers in the above areas.