# Security Issues for Mobile Government

**L. Ertaul[1], B. S. Chelivendri[2], and G. Saldamli[3]**
[1]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[2]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[3]MIS, Bogazici, Istanbul, TURKEY

**Abstract** - *Mobile and Wireless systems offer new services for public administration that cannot be served by customary wired systems. The wireless mobile system is a solution for some problems that exist in traditional wired systems but they also initiate new security issues. Although the security concerns of wireless mobile systems cannot be completely eliminated with today's available standards and techniques, it can be moderate some of the problems by a proper integration of standards, technologies, management, policies and service environments. This paper will address the wireless and mobile security issues and challenges faced in the development and implementation of mGovernment Systems and we will also discuss the cases and lessons learned, and future of security solutions, as they relate to mGovernment.*

**Keywords**: Security issues in mGovernment, Network Security, Wireless Security**.**

## 1 Introduction

Use of mobile technologies to enhance government activities leading ways for mobile government (mGovernment), and applications and services involved are becoming increasingly popular. While governments seem to be very effective in providing better or more significant services through these new technologies, the value of mGovernment comes from the capabilities of applications supporting mobility of the citizens, businesses and internal operations of the governments [1]. mGovernment is inevitable. The number of people having access to mobile phones and mobile Internet connection is increasing rapidly. The mobile access - anywhere any time – is becoming a natural part of daily life, and the governments will have to transform their activities according to this demand of convenience and efficiency of interactions for all parties [1]. The goal of this paper is to present the security issues for mGovernment. In the system security architecture we will discuss major areas where we need to concentrate to maintain mGovernment security issues.

## 2 System Security Architecture

In this section, we will see what kind of attacks is possible in mGovernment environment? And what are some of the topics, which include in the security issues of mGovernment?

Basically there are two types of security attacks to a wireless system Passive attack and the Active attack. Passive attack is an attack in which an unauthorized party gains access to an asset and does not modify its content. On the other hand Active attack is an attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable.

Major mGovernment security issues include [2].

1) Security for the Wireless Networks
2) Wireless sensor networks (WSNs).
3) Mobile communication security.
4) Cyber Security.
5) Information, Database, and Access Control Security
6) User and Service Authentication Techniques
7) Homeland Security Preparedness.
8) Information Privacy

Next we will discuss each of the above issues.

### 2.1 Security for the Wireless Networks

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices [3]. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders. However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new [3]. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot [3]. An overview of the attack of the wireless technology is explained in Fig.1 [3]. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks [3].

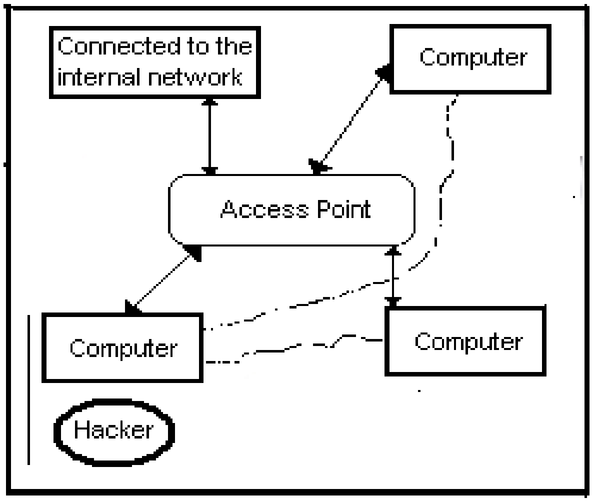

Figure 1: An overview of an attack for a wireless technology

Here are some of the remedies for the security issues.

1) Maintaining a full understanding of the topology of the wireless network.

2) Labeling and keeping inventories of the fielded wireless and handheld devices.

3) Creating backups of data frequently.

4) Performing periodic security testing and assessment of the wireless network.

5) Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.

6) Applying patches and security enhancements.

7) Monitoring the wireless industry for changes to standards that enhance security features and for the release of new products.

8) Vigilantly monitoring wireless technology for new threats and vulnerabilities.

## 2.2 Wireless Sensor Networks (WSNs)

WSNs are usually built with a large number of small, inexpensive, battery-powered devices that have limited residual energy, computation, memory, and communication capacities. Small low-cost sensor devices with limited resources are being used widely to build a self-organizing wireless network for various applications, such as situation monitoring and asset surveillance [4]. Making such a sensor network secure is crucial to their intended applications, yet challenging due to the severe resource constraints in each sensor device. We present a *lightweight security protocol* (LiSP) that makes a tradeoff between security and resource consumption via efficient re-keying [4],[5]. The heart of the protocol is the novel rekeying mechanism that offers

1) efficient key broadcast without requiring retransmission/ACKs,

2) authentication for each key-disclosure without incurring additional overhead,

3) the ability of detecting/recovering lost keys,

4) seamless key refreshment without disrupting ongoing data encryption/decryption, and

5) robustness to inter-node clock skews.

Furthermore, these benefits are preserved in conventional contention-based medium access control protocols that do not support reliable broadcast. Refer to figure2 for more about the key hierarchy for Lisp [4].

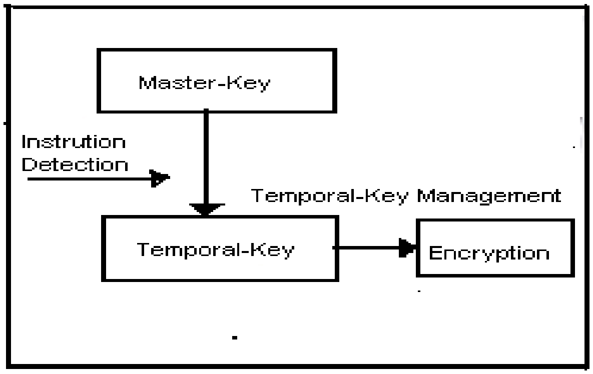

Figure 2: The key hierarchy for LiSP.

Some of the security issues of the WSNs are [4], [5]:

1) Jamming that interferes with the operating radio frequencies.

2) Collisions that are induced on ongoing packet transmissions.

3) Exhaustion that forces the link layer to repeat packet retransmission.

4) Vulnerabilities of existing protocols.

Lisp achieves the following goals in protecting security-critical information from attackers [4] [5].

1) *Confidentiality*: keeps data from being eavesdropped, and ensures that an attacker will not acquire any information about the plaintext, even if it sees multiple encrypted versions of the same plaintext.

2) *Data integrity*: prevents tampering with the transmitted data.

3) *Access control*: protects and controls access to the network.

4) *Availability*: protects the network from interruptions in service.

5) *Key renews ability and revocability*: protects the network from compromised nodes, if any.

## 2.3 Mobile Communications Security

Wireless communications are being driven by the need for providing network access to mobile or nomadic computing devices. The need for wireless access to a network is evident in current work environments. A number of new protocols have been recently published with the goal of providing both privacy of data and authentication of users for mobile systems [6], [7]. Cryptographic protocols are used to achieve secure communication over insecure networks. Weaknesses in such protocols are hard to identify, as they can be the result of subtle design flaws. Formal verification techniques provide rigid and thorough means to evaluate security protocols [6]. Such protocols can employ private-key and/or public key cryptographic algorithms. Publickey algorithms hold the promise of simplifying the network infrastructure required to provide security services such as: privacy, authentication and non-repudiation, while symmetric algorithms require less processing power on the mobile device. In addition to the security requirements for fixed network such as; identity authentication, data confidentiality and non-repudiation, mobile systems have a number of additional requirements due to the nature of the mobile environment. These include [6], [7]:

1) Communications path: The communications path contains many parts, one of which, the radio link is particularly vulnerable to attack.

2) Location Privacy: Since mobiles roam freely it may be advantageous to keep its location a secret.

3) Computational constraints: Most mobile devices are computationally and/or power limited, therefore it is necessary to limit the computational complexity of any security algorithm used. A wireless communication security protocol was given by both second-generation and third-generation protocols. The primary difference between second-generation protocols and third generation protocols is the requirement of the mobile device/phone to handle information transfer to and from Internet sites as WEB active components. While second generation systems can supply the necessary security for data transfer, the ability to setup initialization of payment for valued added services, or supply non-repudiation services is not readily provided. These services are an essential requirement for third generation mobile systems where e-commerce applications will take a central role [6], [7].

## 2.4 Cyber Security

It seems that everything relies on computers and the Internet now — communication (email, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system [8]? Cyber security involves protecting that information by preventing, detecting, and responding to security attacks. To meet federal guidelines for protecting national security and to address internal business requirements for online security, cyber systems must be able to share data securely, ensure the continuous availability of critical services, interoperate across federal, state, and local systems, and comply with federal consumer-privacy regulations. Some of the regulation is described below [8]:

1) **Data Security**: As government agencies and departments open their networks and databases to share sensitive information with employees and partners in other agencies, the opportunities for unauthorized access, data tampering, and fraud increase. To safeguard mission-critical information and facilitate compliance with recent regulations regarding consumer privacy, data availability, and record keeping, government agencies must implement reliable mechanisms for user authentication, authorization, data privacy, and nonrepudiation. These mechanisms must protect not only human-initiated data exchanges but also machine-to machine communications [8]. A reliable public-key infrastructure (PKI) is the first pillar of a trusted network, in which all people and all devices are strongly authenticated in an open, interoperable environment. In this environment, information can be securely shared and identities can be trusted across independent partners. The PKI enables information to be secured by digital-certificate-based services, including authentication, authorization, encryption, digital signing, and non repudiation.

2) **Continuity of Government**: Continuous availability of systems, services, and information is as important as protecting the privacy and integrity of data. Whether it’s a natural disaster, such as a hurricane, or a disaster caused by terrorism, a hacker, or human error, government agencies face a variety of potential causes for disruption in operations [8]. The quantitative losses associated with service disruption and system downtime can be expressed in terms of diminished productivity or lost revenues. However, the qualitative tolls related to service unavailability or impaired communications may ultimately present the greater risk to government agencies and the citizens they support. At their gravest, these costs could potentially be measured in lives lost or saved. To maximize the availability and effectiveness of

government services, agencies must maximize uptime and effectiveness of the security infrastructure [8]. If the firewall itself is down, or if the intrusion-detection system (IDS) is not in operation, the entire network is open to security attacks. Uptime alone is not sufficient for network-security infrastructure; systems must also be effective. Networks need to be actively monitored and managed to prevent malicious attacks on the enterprise network and application infrastructure. According to the Government Technology magazine article “Tech Trends 2002”, researchers at MIT report, “The average machine is connected to the Internet for less than five minutes before an automated attack program scans it [8]. Once a system is compromised, it can be used as a jumping-off point for deeper attacks, as into [government] infrastructure and connected systems. In considering continuity of services, agencies must also attend to the DNS infrastructure. Preventing a single point of failure caused by an attack on the DNS infrastructure has been largely overlooked as a critical component of network continuity. However, when the DNS server goes down, enterprise Web sites and email services are inaccessible, and online transactions and communications cannot be conducted—an unacceptable condition in handling emergencies or conducting business in real time. To ensure that critical services are not disrupted and to enable rapid identification of and response to system attacks, government agencies must develop and implement business continuity plans for all major aspects of IT infrastructure, including applications, data storage, facilities, and networks. They must protect the core infrastructure of the IT system, including the servers, routers, and other components that move traffic back and forth [8]. Systems must be able to quickly and reliably detect intrusions and protect against denial of- service attacks and other assaults. In addition, they must be engineered to scale during a crisis and must have built-in redundancies so that services and information are available even if one part of a network, system, or infrastructure fails.

3) **Regulatory Compliance**: Though not a direct requirement of the new cyber security strategy, regulatory compliance is a key issue whenever data is shared online. As government agencies open their networks to share information with other agencies and with the private sector, compliance with new consumer-privacy regulations becomes part of any cyberspace initiative [8]. To ensure compliance, agency managers must establish administrative, technological, and physical safeguards to protect the confidentiality and integrity of customer records, ensure the 24/7 availability of specific information, and enable auditing.

## 2.5 Information, Database and Access Control Security

All Information security builds on computer security and cryptography, but also reaches out to other branches of the information sciences [9]. Information security is an important aspect of protecting the information from a wide variety of threats like [9]

1) System security - intrusion detection, secure end systems, secure operating systems, database security, security infrastructures, security evaluation.

2) Network security - Internet security, firewalls, mobile security, security agents, protocols, anti-virus and anti-hacker measures.

3) Content protection - watermarking, software protection, tamper resistant software.

4) Applications - electronic commerce, electronic government, health, telecommunications, mobility

5) Foundations - privacy, access control, authentication, identification, cryptography, steganography, formal methods in information security.

## 2.6 User and Service Authentication Techniques

All Authentication, access control, and audit together provide the foundation for information and system security [10], [11]

1) Authentication establishes the identity of one party to another. Most commonly authentication establishes the identity of a user to some part of the system, typically by means of a password. More generally, authentication can be computer- to-computer or process-to-process and mutual in both directions.

2) Access control determines what one party will allow another to do with respect to resources and objects mediated by the former. Access control usually requires authentication as a prerequisite [10], [11].

3) The audit process gathers data about activity in the system and analyzes it to discover security violations or diagnose their cause. Analysis can occur offline after the fact or online in real time. In the latter case, the process is usually called intrusion detection [10], [11].

## 2.7 Homeland Security Preparedness

Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. When a terrorist attack occurs, emergency response organizations and agencies at the federal, state, and Local levels must quickly collaborate to assess the nature, severity, and effects of the attack, as well as to plan and coordinate their response actions [12]. Figure 3 explains clearly about the roles and responsibilities of the homeland security [12]. The strategic objectives of homeland security in order of priority are to [13]:

• Prevent terrorist attacks within the United States;

• Reduce America’s vulnerability to terrorism; and

• Minimize the damage and recover from attacks that do occur.

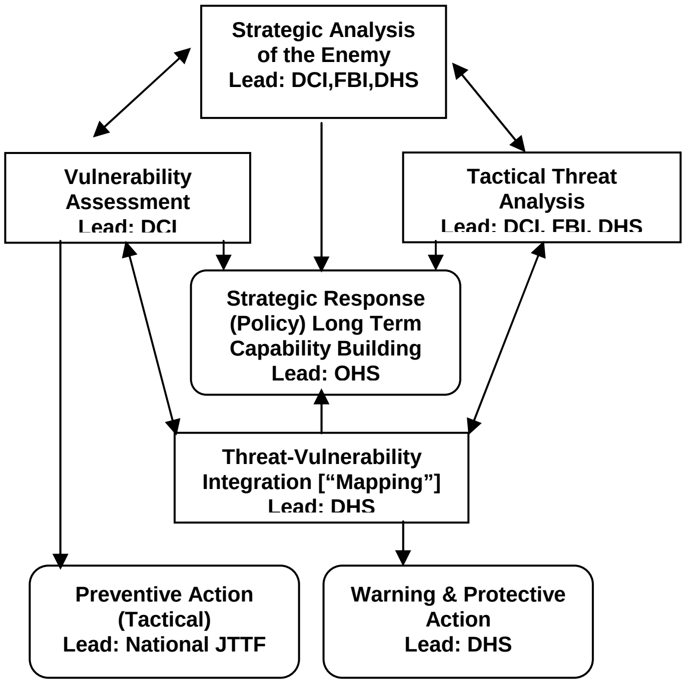
Strategic Analysis of the Enemy Lead: DCI,FBI,DHS
Vulnerability Assessment Lead: DCI
Tactical Threat Analysis Lead: DCI, FBI, DHS
Strategic Response (Policy) Long Term Capability Building Lead: OHS
Threat-Vulnerability Integration [“Mapping”] Lead: DHS
Preventive Action (Tactical) Lead: National JTTF
Warning & Protective Action Lead: DHS

Figure 3: Roles & Responsibilities of Homeland Security Intelligence and Information Analysis.

Measure preparedness [13], [14]:The National Strategy for Homeland Security demands accountability from every government body responsible for homeland security Initiatives. Every department or agency will create benchmarks and other performance measures by which we can evaluate our progress and allocate future resources.

Critical Infrastructure Sectors [13],[14]: Agriculture, Food, Water, Public health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy Transportation Banking, Finance, Chemical Industry and Postal and Shipping.

Emergency preparedness [13], [14]: We must prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. Past experience has shown that preparedness efforts are the key to provide an effective response to major terrorist incidents and natural disasters. Therefore, we need a comprehensive national system to bring together and command all necessary response assets quickly and effectively. We must equip, train, and exercise many different response units to mobilize for any emergency without warning.

## 2.8 Information Privacy

As information privacy concerns assume a greater role, more laws are enacted, and enforcement increases, information technology professionals are well advised to become familiar with the international and national laws governing data privacy. This knowledge is essential to both the design and operation of databases, which are often the first line of defense in maintaining compliance. Non-compliance can have severe consequences for a company legally, and offensive of inept data collection and privacy policies can damage customer trust and undermine business [15], [16] Consequently, instruction in the legal and philosophical basis for information privacy, in the laws enacted to defend it, and in the design of accommodating databases, is an essential part.

The Need for Information Privacy Awareness: Inept or insensitive information policies can literally be bad for business. One study revealed that 80% of internet shoppers routinely abandon their shopping carts upon encountering the repurchase demand for personal information. Consumer data of increasing detail and specificity drives forecasting, marketing, and product development [15]. And technological capability has forged ahead of privacy policies. While a higher percentage of purely internet companies post privacy policies than do the more traditional mixed net, brick and mortar companies, a substantial percentage of companies overall have yet to develop information privacy policies. Those policies that do exist are often offensively paternalistic and one-sided. An individuals associated with personal data are best qualified to determine what constitutes their own benefit regarding the sharing and use of their data, rather than having this function preempted by commerce. Yet examples of that preemption abound in the privacy policies of even the most prominent companies. For example, the privacy policy displayed on Ford Motor Company’s site states [15] that there are instances where Ford Motor Company requests personally identifiable information to provide site visitors with a service. “This information, such as name, mailing address, email address, and type of request, is collected and stored in a manner appropriate to the nature of the request as determined by Ford Motor Company, to fulfill your needs. When other information is collected from you, such as your name and e-mail address, we generally let you know at the time of collection how we will use your personal information. Usually, we use the personal information you provide only to respond to your inquiry or to process your request (such as to receive electronic annual reports or to be added to our supplier diversity database.) This information may be shared with other GE business, but only if necessary to fulfill your request or for related purposes.”

Information Privacy Principles under the Privacy Act:

1) Manner and purpose of collection of personal information. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless: (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and (b) The collection of the information is necessary for or directly related to that purpose. Personal information shall not be collected by a collector by unlawful or unfair means [16].

2) Solicitation of personal information from individual concerned (a) a collector collects personal information for inclusion in a record or in a generally available publication; and (b) the information is solicited by the collector from the individual concerned; the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:(c) the purpose for which the information is being collected;(d) if the collection of the information is authorized or required by or under law - the fact that the collection of the information is so authorized or required; and (e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information [16].

3) Solicitation of personal information generally (a) a collector collects personal information for inclusion in a record or in a generally available publication; and (b) the information is solicited by the collector: the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected: (c) the information collected is relevant to that purpose and is up to date and complete; and (d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned [15].

4) Storage and security of personal information: A record-keeper who has possession or control of a record that contains personal information shall ensure: (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorized access, use, modification or disclosure, and against other misuse; and (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorized use or disclosure of information contained in the record. Limits on use of personal information [15], [16], [17].

5) Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use [16].

6) Limits on disclosure of personal information: A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless: (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency; (b) the individual concerned has consented to the disclosure (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person; (d) the disclosure is required or authorized by or under law; or (e) the disclosure is reasonably necessary for the enforcement *of* the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency [15], [16], [17].

## 3 Conclusions

This absolute security is unattainable. However, it is possible to obtain effective results by changing some of our beliefs and working in the development of comprehensive security systems, which starts with the conversation about the business processes involved in the application to identify key control points on the application [18]. The success of the initiative involves good management, enforced procedures, and the adequate technical tools, with an appropriate policy framework. Security policies should not only consider the control of computer systems and networks, but physical security, administrative, legal and organizational controls too. In addition, the adequate balance of information policy values embedded in a security system for any mGovernment application is an *ad hoc* social and political decision.

## 4 References

[1] NECCC research group “M-Government: The Convergence of WirelessTechnologies and e-Government”. Year 2001.

[2] L.Ertaul, “M-Security: Security Issues for Mobile Government” (call for papers) Euro mGov 2005.

[3] T. Karygiannins and L. Owens "Wireless Network Security 802.11, Bluetooth and handheld Devices," Rel. C v1.0, November 2002.

[4] Taejoon Park and Kang G. Shin "A Lightweight Security Protocol for Wireless Sensor Networks", ACM transition on Embedded Computing Systems, Vol. 3, No. 3, August 2004.

[5] Chris Karlof and David Wagner "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Jan. 1999.

[6] Chii-Hwa Lee, Min-Shiang Hwang and Wei-Pang Yang "Enhanced privacy and authentication for the global system for mobile communications," May 1996.

[7] Audun Josang, Gunnar Sanderud "Security in Mobile Communications: Challenges and Opportunities Distributed System Technology Centre Vol. 21, Nov 2003.

[8] White Paper Verisign "Verisign CyberSecurity" http://www.verisign.com/static/005567.pdf Vol 17 May 2005

[9] D. Gollmann; J. Lopez; C.A. Meadows; E. Okamoto "International Journal of Information Security", ISSN: 1615-5262

[10] Ravi Sandhu George Mason University. "Authentication, Access Control, and Audit" ACM Computing Surverys, Vol. 28, No. 1, March 1996.

[11]Ian Christofis "User Authentication Issues for online Government" electronic trading concepts July 1999.

[12]John Yen." Emerging Technologies for Homeland Securities" Communications of the ACM /Vol 47.No 3, March 2004.

[13]The National strategy for Home Land Security "ExecutiveSummary"http://www.whitehouse.gov/homeland/book/sect1.pdf

[14] U.S Department of Commerce Bureau of Industry & Security Annual Report for 2002.Chapter 7 Critical Infrastructure Protection year 2002 http://www.bxa.doc.gov/news/2003/AnnualReport/chapter7p.pdf

[15] Sushil Jajodia "Managing security and privacy of information" Vol 28 May 1996

[16] Legislative Drafting Act 119"Information Privacy Principles under Privacy act 1988" , Apr 2004. http://www.privacy.gov.au/publications/ipps.html

[17]Robert F. Dacey "Information Sharing responsibilities Challenges, and Key Management Issues". Sep 2003

[18]Ibrahim Kushchu mGovLab, Minami Uonuma-gun "A Mobility Response Model for government" Apr 2004

[19]Ai-Mei Chang "Preparing for wireless and mobile Technologies in Government" management National Defense University. Oct 2002

[20]Adrian Perrig, Robert Szewczyk,J.D.Tygar, Victor Wen and David E. Culler "SPINS:Security Protocols for Sensor Networks" Aug 2002.

[21]Sandra J. Milberg, Sandra J. Burk, H. Jeff Smith, and Ernest A. Kallman. "Values Personal Information Privacy, and regulatory Approaches" Communication of the ACM December 1195/Vol. 38, No.12

[22] Wade Williamson "Wireless Security in the Government Environment" An AirMagnet Technical White Paper.2004.