


Security Issues in mGovernment

View metadata, citation and similar papers at core.ac.uk

brought to you by  CORE

provided by ePrints@Bangalore University

¹ Lecturer, MCA Department, M. S. Ramaiah Institute of Technology,
MSR Nagar, Bangalore-560054 Karnataka, India

manishkumarjsr@yahoo.com

² Dept. of Computer Science and Applications, Central College Campus, Bangalore University,
Bangalore -560 001 Karnataka, India

hanu6572@hotmail.com

³ Director – MCA, Garden City College, 16th KM, Virgo Nagar,
Old Madras Road, Bangalore-49, India

mailreddy99@yahoo.com

Abstract. E-government is one of the most rapidly evolving service domains in the contemporary information society. Many governments have already developed and provided e-government services to businesses and citizens. Nowadays actors in the government domain attempt to take the next step and exploit the latest wireless technologies in order to provide ubiquitous services for mobile users. However, this approach involves some hidden risks mainly due to the inherent insecurity of the air medium and the vulnerabilities of the wireless systems. Thus, in this paper we investigate the security gaps and considerations which should be taken into account for an m-government system. Finally, we provide a list of security guidelines and policies, which the users of the system should be aware of and follow in order to avoid security attacks.

Keywords: m-government, mobile security, security architectures, security policies.

1 Introduction

Electronic government (e-government) is a very promising challenge for national governments and governmental agencies of any level. E-government refers to the use of information and communication technologies for transforming the interactions among governments (G2G), governments and businesses (G2B), governments and citizens (G2C) and governments and their employees (G2E). E-government can contribute to the improvement of government services delivery to citizens, the facilitation of interactions with businesses and the empowerment of citizens through the access to information and services. Resulting benefits include less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (The World Bank, 2004). The potential advantages of e-government impel governments around the world to strongly support it. Many of them have already invested greatly on their e-government agenda. In the race for achieving full transformation of governmental services, governments are making efforts to provide more services in alternative

channels, in this way increasing variety and quality of services as well as citizen participation. In this context, the explosion of use of wireless devices is forcing governments to shift from e-government to mobile government (m-Government).

M-government can be considered as a strategy, the implementation of which involves the use of all kinds of wireless and mobile technologies, applications and devices for improving service delivery to the parties involved in e-government including citizens, businesses and all government units. Similarly to e-government, m-government operates on four different levels represented by the following interactions: (a) m-government to government (mG2G) referring to inter-agency relationships and the interaction between governmental agencies; (b) m-government to business (mG2B) describing the interaction of government with businesses; (c) m-government to employee (mG2E) concerning the government and its employees; and (d) m-government to citizen (mG2C), which refers to the interaction between government and citizens. The main advantages of m-government services are ubiquity, namely providing information and services anywhere and at any-time, personalization, ease of use, time and cost saving and location-based services. Many countries are offering m-government services, such as the USA, the UK, Singapore, Malaysia and Australia. Also, there are various examples concerning each type of interaction regarding different sectors of society, such as education, public safety, justice and employment. It should be noted that m-government services require radically different approach for service design, development, operation and interaction model.

Nevertheless, the provision of such services alone does not insure that citizens and businesses will use them. The emergence of e-government and m-government services has raised various issues, among which security is of great importance. In order to fully exploit the benefits of e-government, there is a number of special security requirements which are dictated by the sensitive nature of the data transmitted during e-government transactions. These data may include personal data, such as identity and contact details, government data, such as record / registration numbers and certificates, as well as financial data, such as credit card and bank account numbers. Therefore, it is imperative that in an e-government transaction the involved parties are mutually and securely authenticated, and the information is transmitted with confidentiality and integrity. These security requirements have become even more crucial with the advent of m-government. The main reason is that the wireless interfaces have some proven security deficiencies in comparison with wired ones. Furthermore, the constantly increasing storage and processing capabilities of mobile devices have attracted the attention of malicious programmers.

Hence, this paper aims at investigating the various methods for securing an m-government system. More specifically, we analyze some known security gaps of the most widely deployed mobile networks and we present an overview of the security mechanisms deployed in handheld devices.

2 Mobile Security Gap Analysis

During the last decade, wireless network technologies have greatly evolved and have been able to provide cost-effective solutions for voice and/or data mobile services. Their main advantages over wired networks are that they avoid expensive cabling infrastructure and they support user mobility and effective broadcasting. As a result, wireless networks managed to take over a large percentage of the “voice” market, as

the Global System for Mobile Communication (GSM) technology promoted the worldwide expansion of mobile telephony. Furthermore, nowadays the Internet has become a necessity for many individual users and businesses and the main challenge is to find cost-effective solutions for the provision of wireless services. Hence, a large research community has been involved in designing and implementing standards for wireless data networks and there are some technologies, such as Wi-Fi and General Packet Radio Service (GPRS), which have already been widely adopted. In the years to come, more and more of our voice samples and data packets will be transmitted over wireless links and therefore it becomes imperative that these data are secured from malicious eavesdroppers and hackers. Especially in application domains such as m-government, it is of crucial importance to prevent the revelation of sensitive data to non-authorized persons or the submission of unauthorized data. Therefore, the main objectives of this section are to investigate the available security mechanisms of handheld devices and to analyze the security gaps of wireless protocols.

2.1 Security Principles

Wireless network security is the scientific field dealing with the risks related to wireless computer networks. In order to clearly identify the kind of protection a security system or algorithm provides, the security goals are categorized as follows:

- *Confidentiality*: ensures that information is not disclosed to unauthorized users.
- *Integrity*: ensures that the information cannot be corrupted or altered in any way.
- *Accountability / Non-repudiation*: guarantees for the identity of the sending and receiving party in an information transmission.
- *Availability*: ensures that the services implemented in a system are available and function properly.
- *Access control*: ensures that only authenticated / authorized entities are able to access services and data. More specifically, the access control security goal can be further categorized in the following sub-goals:
 - *Authentication*: confirms the claimed user identity.
 - *Authorization*: controls the access rights granted to authenticated users.

2.2 Handheld Devices

Handheld devices (e.g mobile phones, smart phones, Personal Digital Assistants-PDAs) have gained popularity because of the technological advancements of the last decade. Longer battery life, larger storage capacity and faster processing capabilities have promoted handheld devices to a worthy substitute of the personal computers when users go “mobile”. However, along with great power comes great responsibility. In this case, the responsibility is to devise and apply security standards for handheld devices, which are equivalent to these of the personal computers. In this context, the security requirements for the handheld devices are affected by two main deficiencies with respect to personal desktop computers: firstly, the handheld devices are much more vulnerable to loss or theft due to their mobility and their small dimensions. Secondly and more importantly, they mainly use the air medium to gain access

to networks, which is inherently more insecure and prone to eavesdropping than traditional wired lines.

In order for the device to be secured against loss or theft, it has to incorporate sufficient access control mechanisms to protect stored data and functionality. Unfortunately, there seems to be no widely accepted standard for access control services in handheld devices and there seems to be no consensus over standard access control routines in the various mobile device operating systems. The main security goals that need to be achieved with respect to device security are authentication and authorization. In the domain of authentication, the following mechanisms are utilized for handheld devices:

- *Password protection*: A private value known only by authorised users in order to authenticate them. It is often synonymous with the concept of Personal Identification Number (PIN) code.
- *Biometrics*: A hardware based solution that examines a physical attribute of an authorized user in order to authenticate him (e.g. fingerprint reader, voice/handwriting recognition).
- *Auto Logout*: The authenticated user is automatically logged off after a predefined time interval or inactivity period.

In the domain of authorization, the following mechanisms are utilized:

- *File Masking*: The system prevents certain protected records from being viewed without user authentication.
- *Access Control Lists*: Permissions for a particular object are associated with users in the form of a matrix.
- *Role-based Access Control*: Permissions are associated with roles and users get associated with roles. Users therefore inherit the permissions of the roles they are assigned to.

In most of the cases, handheld devices do not incorporate all of the aforementioned mechanisms. Password or PIN protection is the most common mechanism, although biometric mechanisms, such as fingerprint readers have made their appearance. The authentication of the user to the handheld device takes in most cases- place through a password challenge or a biometric measure and after successful completion full access is granted to the device's applications and data. In other words, in the majority of the cases handheld devices incorporate no authorization mechanisms at all. This is mainly due to the fact that since the handheld device is typically a personal device, authentication is equivalent to authorization. Nevertheless, this is not the case when the device belongs to an employee of a corporation, because the device's data are actually owned by the corporation and the disclosure of sensitive data could cause serious financial damage to the business.

2.3 Mobile Networks

As mentioned before, the second main security deficiency of handheld devices is that they use the air interface to gain access to networks, which is inherently more

insecure and prone to eavesdropping than traditional wired lines. This is mainly because any transceiver in the radio coverage of the mobile device can capture transmitted traffic or inject its own data in the communication link. Therefore, wireless links facilitate passive as well as active attacks (e.g. replay, man-in-the-middle, DoS attacks). This fact has led to the exposure of security vulnerabilities in the air interface protocols of some well-known wireless protocols:

- **Bluetooth – IEEE 802.15 :-**

There are three types of potential vulnerabilities with respect to the Bluetooth standard, version 1.0B. The first vulnerability opens up the system to an attack in which an adversary under certain circumstances is able to determine the key exchanged by two victim devices, making eavesdropping and impersonation possible. The second vulnerability makes possible an attack in which an attacker is able to identify and determine the geographic location of victim devices. Finally, the third vulnerability concerns deficiencies of the security cipher itself. Furthermore, in August 2004 an experiment (Trifinite, 2004) proved that the range of Bluetooth radios could be extended to 1.78 km with high-gain directional antennas. This technique which is also known as Bluetooth sniping poses a potential security threat since it allows attackers to access vulnerable Bluetooth devices from a safe position far away from the victim. In addition, a group of security researchers from Cambridge University (Wong et al., 2005) have presented an actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, which confirmed that the Bluetooth's symmetric key establishment method is vulnerable. Finally, Shaked & Wool (2005) have demonstrated both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof if he was present at the time of initial pairing. The active method utilizes a special message which prompts the master and slave devices to repeat the pairing process. After that, the first method may be used to crack the PIN. The aforementioned vulnerabilities pose a serious question on the security of Bluetooth links and about their ability to carry sensitive data. Although the Bluetooth security specifications have been revised quite a few times in the past, a large number of older version Bluetooth devices is still utilized and suffers from the aforementioned security risks.

- **Wi-Fi – IEEE 802.11**

The first encryption standard used for Wi-Fi was Wired Equivalent Privacy (WEP). Unfortunately, WEP has been proved to be breakable on many publications (Borisov et al., 2001) even when correctly configured. This is because of a vulnerability of the RC4 cryptographic algorithm of WEP, which utilizes the RC4 initialization vectors improperly (Stubblefield et al., 2002). Although most new wireless products support the much improved Wi-Fi Protected Access (WPA) protocol, most of the first generation access points, which are widely deployed, cannot be upgraded and have to be replaced in order to support the improved standard. The security standard published by the IEEE802.11i group (aka WPA2) in June 2004 offers a still further improved security scheme, which is gradually becoming available on the latest equipment. Due

to these vulnerabilities, many Wi-Fi providers deploy additional layers of encryption (such as Virtual Private Networks-VPNs) to enhance the wireless security.

- **GPRS - GSM**

GSM was designed with a moderate level of security. The system is designed to authenticate the subscriber to the network using shared-secret cryptography. Nevertheless, GSM has no provision for authenticating the network, namely the base station to the subscriber's terminal. Furthermore, communication between the subscriber and the base station can be encrypted, using temporary keys assigned with respect to the terminal's identification code. Therefore, the security model offers confidentiality and authentication, but limited authorization capabilities and no non-repudiation. GSM uses several cryptographic algorithms for securing the communication link. The A5/1 and A5/2 stream ciphers are utilized to encrypt the voice channels over the air interface. A5/1 was first developed and is a stronger algorithm used within Europe and the United States. A5/2 is weaker and used in other countries. Serious vulnerabilities (Biham & Dunkelmann, 2000; Biryukov et al., 2000) have been found in both algorithms, and it is possible to break A5/2 in real-time in a ciphertext-only attack (Barkan et al., 2003). Fortunately, GSM does not specify a single algorithm but it supports multiple algorithms so operators may replace that cipher with a stronger one.

3 Security Mechanisms

In the literature, there are several available security protocols architectures that can be applied on the different Open System Interconnection (OSI) layers. The purpose of these layer security approaches is the implementation of VPNs which can provide secure communication over unsecured networks. A formal definition of a VPN is the following: "A VPN is a logical computer network with restricted usage that is constructed from the system resources of a relatively public physical network (such as the Internet) with encryption of the used and tunneling links created by the virtual network across the public network" (Schafer, 2003). More specifically, in the link layer there are a couple of security protocols such as PPTP (Hamzeh et al., 1999) and L2TP (Townsend et al., 1999) that can secure the transmission of the information independently of the air interface. In the network layer, a popular approach is to implement IPSec (Kent & Atkinson, 1998) in combination with mobile IP (Perkins, 1996). More specifically, IPSec is meant to provide the secure transmission of IP packets, whereas mobile IP aims at providing transparency to the transport layer by hiding the change of IP address when the user roams between different networks.

However, security solutions in the link and network layer have the following disadvantages. Firstly, the specification of the link layer significantly varies in different kind of technologies, such as cellular technologies (e.g. GSM) compared to mobile broadband technologies (e.g. Wi-Fi). This fact increases the complexity and the cost of adopting a link layer security solution. The aforementioned disadvantage is not an issue in the case of the network layer, since its purpose is actually to present a uniform and homogeneous network structure to the upper layers. In the majority of the modern packet-based data networks, the main protocol used in the network layer is IP.

Nevertheless, network layer security has also some serious shortcomings, since the system should rely on the network operator in order to utilize the security protocols.

Moreover, different points of access in wireless telecommunications networks have different capabilities and restrictions in the kind of traffic that they allow. Therefore, network layer security is not able to guarantee smooth operation in every case. A preferable solution in the case of mobile-government is the session layer security. In the session layer, the following security protocols are available: Secure Socket Layer (SSL) / Transport Layer Security (TLS) and Secure Shell (SSH). Although these protocols are often referred to as transport layer security protocols, they actually belong to the session layer within the meaning of the OSI model (Schafer, 2003). The main advantage of session layer security protocols is that they preserve their transparency with respect to the application and at the same time they can survive transport connection failures caused by TCP.

These characteristics make session security protocols appropriate for securing wireless data communications, since they can be implemented end-to-end directly from the client to the server without interfering with the lower layers. Furthermore, the majority of operating systems available for handheld devices (e.g. Windows Mobile, SymbianOS, PalmOS) either inherently support SSL/TLS functionality in their browsers or they can incorporate these functionalities through a third-party plug-in. The last candidate is application layer security, which actually implements the security services (e.g. authentication, data confidentiality and integrity) as part of the application. This approach could be appropriate for our scenario, but it was abandoned in favour of the session layer security since it significantly increases the complexity of the application development. Thus, the final decision was to deploy end-to-end session security over wireless links.

4 Policy Implications

Even the most secure system in the world has a serious flaw, namely the human factor. In other words, security architectures are not of much use, unless people start realizing the risks involved in the information society. Information systems can greatly facilitate the everyday activities of our society, but at the same time they create new kind of security gaps which could attract malicious users. However, most of the times these security breaches are due to human error or negligence rather than system deficiency.

Hence, we present a concise list of policies, which should be adopted by the users of m-government:

- *The user should ensure that the handheld device supports SSL/TLS session layer security and possibly VPN software.* The SSL/TLS session layer security is utilized to access the https secure web pages of the portal and it is supported by the majority of the modern mobile web browsers. The VPN software is usually utilized to establish a tunnel between the mobile and the network access point, so that all traffic can pass securely through that tunnel. However, the availability and the provision of this service depend on the network operator and it cannot be considered as an integrated solution especially if the users roam through different networks.

- *The registered users of the system should change their authentication credentials frequently.* This is a common practice in web portals where security is of great concern (e.g. e-banking systems). Moreover, passwords are configured to expire after a predetermined time period in order to enforce this policy. This mechanism prevents users from storing the password in the web browsers, thus enhancing the authentication security of the portal. Furthermore, password-checking mechanisms can be utilized in order to ensure that the user has not selected a common easy-to-guess password. This is usually achieved by forcing the user to select a password, which is at least eight characters long and it contains numbers, letters and symbols.
- *Storing sensitive information in the handheld device or in storage cards is not allowed unless it is encrypted.* In this case sensitive information includes authentication credentials, completed m-government forms etc. This information could be exposed to malicious users in case of device theft or loss. Thus, the users are advised to encrypt files which contain sensitive information. This can be achieved quite easily, since most modern mobile operating systems (e.g. Symbian, Windows Mobile, PalmOS) either inherently support encryption routines or they can incorporate encryption functionalities through third-party software.
- *The user should empower the access control of the handheld device when possible.* Every mobile device has different capabilities as far as access control is concerned. The users are advised to enable the two common mechanisms which can be found in the majority of handheld devices, namely password protection and auto logout. If more advanced access control mechanisms such as biometrics and smartcards, are available, users are advised to utilize them in combination with password protection in order to achieve two-factor authentication.
- *Untrusted wireless network access points should be avoided.* The users should configure the handheld device, so that it may not access unknown or untrusted wireless networks, e.g. rogue access points, open/unsecured networks. These networks may not have all the security mechanism enabled and properly configured, thus exposing m-government traffic to security threats.
- *Antivirus / firewall software and latest security patches should be installed in handheld devices.* Antivirus software can protect the device from malicious code, whereas firewall software can prevent network attacks. The aim of security patches is to repair newly-discovered exploits of the mobile Operating system. All these measures are meant to prevent malicious programmers from gaining remote access to the handheld device.

5 Conclusions

Nowadays, wireless technologies are becoming more and more popular in all ranges of network access, i.e. personal, local, metropolitan and wide. Such technologies have been widely acknowledged as complementary channels for two-way transactions between governments, citizens and businesses. As the mobile devices, networks and application evolve m-government services will have to be provided through flexible

and adjustable systems which can support different kinds of connections and terminals. Past implementations of wireless protocols have presented a number of security vulnerabilities, but latest protocols such as 3G and WiMAX seem to have the requisite maturity for secure deployment and utilization. However, the majority of wireless equipment utilized today has been manufactured based on older versions of wireless protocols and it is still exposed to security threats. Thus, additional security measures and policies have to be taken into account while deploying sensitive mobile services, such as m-government services.

In this paper, we have discussed about the security deficiencies of wireless networks and we have presented an analysis of the available security protocols. We have described a list of policies which should be adopted by the operator and the users of the m-government system, so that security awareness can be increased and attacks can be avoided. These measures and policies produce a large overhead for both service providers and users, but new alternative technologies and systems emerge, such as PKI (Public Key Infrastructure) SIM, which seem more promising. PKI SIM is an enhanced SIM card, which incorporates a digital certificate (Siltanen, 2000). This certificate is used to authenticate the user, so no username/password credentials are needed. Furthermore, it can be utilized as a digital signature for document signing and email signing. Since wireless technologies are constantly evolving, our future work has to include technologies such as PKI SIM, which seems promising for unraveling security issues.

References

1. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Technical Report CS-2003-05, Technion - Israel Institute of Technology (2003)
2. Bassara, A., Wiśniewski, M., Żebrowski, P.: USE-ME.GOV - Usability-driven open platform for mobile government. In: Proc. of Business Information Systems (BIS) 2005, Poznań, Poland, pp. 193–202 (2005a)
3. Bassara, A., Wiśniewski, M., Żebrowski, P.: USE-ME.GOV – A Requirements-driven Approach for M-Gov Services Provisioning. In: Proc. of Business Information Systems (BIS) 2005, Poznań, Poland, pp. 203–214 (2005b)
4. Beynon-Davies, P.: Constructing electronic government: the case of the UK inland revenue. *International Journal of Information Management* 25, 3–20 (2005)
5. Biham, E., Dunkelman, O.: Cryptanalysis of the A5/1 GSM Stream Cipher. In: Proc. of the First International Conference on Progress in Cryptology, pp. 43–51 (2000)
6. Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: The insecurity of 802.11. In: Proc. of the 7th annual International Conference on Mobile computing and networking, Rome, Italy, pp. 180–189 (2001)
7. Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G.: Point-to-Point Tunneling Protocol (PPTP), RFC 2637 (1999)
8. Jakobsson, M., Wetzel, S.: Security weaknesses in Bluetooth. In: Proc. of RSA Security Conference- Cryptographer's Track. LNCS. Springer, Heidelberg (2002)
9. Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998)