Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MOBILE SECURITY: SECURITY MECHANISMS AND PROTECTION OF MOBILE APPLICATIONS

[1]NAJIM AMMARI, [2]MOHAMED GHALLALI, [3]ANAS ABOU EL KALAM, [4]NORELISLAM EL HAMI, [5]ABDELLAH AIT OUAHMAN, [6]BOUABID EL OUAHIDI

[1]PhD student Cady Ayyad University, National School of Applied Sciences, OSCARS Laboratory Marrakech, Morocco
[2]PhD holder Faculty of Sciences, Mohammed-V AGDAL University, Information Research Laboratory Rabat, Morocco
[3]ISER - Director of the IPI research laboratory, France
[4]PH - Ibn Toufail University, National School of Applied Sciences, ENSA Kenitra, Morocco
[5] PES - Cady Ayyad University, National School of Applied Sciences, OSCARS Laboratory Marrakech, Morocco
[6]PES - Faculty of Sciences, Mohammed-V AGDAL University, Information Research Laboratory Rabat, Morocco
E-mail: [1]najim.ammari@gmail.com, [2]ghallali2001@yahoo.fr, [3]elkalam@hotmail.fr, [4]norelislam@outlook.com, [5]aitouahman@yahoo.fr, [6]ouahidi@fsr.ac.ma

ABSTRACT

The main objective of this paper is to propose security policies and mechanisms for mobile phones that better meet the expectations of users, either at the level of mobile networks, or mobile applications.At the mobile networks level: The study focuses on limiting the spread of malware via SMS / MMS and emails. It describes the steps involved in identifying, analyzing and securing traffic in mobile networks. For this purpose, a Framework MPSS (**M**obile **P**hone **S**ecurity **S**cheme) is used as part of the mobile network of operator Telecom. MPSS aims to increase the level of information security through the network of the telecom operator and solve problems related to limited resources on mobile devices and reduce the risk of loss of data users (individuals, companies). Basically, this study proposes a new model of mobile security applications consisting of several levels and layers. Each layer of this model is responsible for the security of its components, and nothing more. The upper levels of the model are based on all lower levels to ensure that their components are safe in an appropriate manner. This model based on abstraction allows the design of a particular mobile security mechanism to focus on one area of concern without spending resources to analyze all layers that support its current position in the model.
Keywords: *Mobile security, Framework Mobile Phone Security Scheme (MPSS), Spread of mobile malwares, The Security Model for Mobile Applications* (*SMMA), Mobile Network Operator.*

1. INTRODUCTION

The evolution of mobile phones that can be used anywhere as well as, the growing trend of their features and performances have triggered new serious security issues. The number of Android malware has increased 400% from June 2010 to January 2011 [1].

Unfortunately, most of the deployed security mechanisms are not adapted to these contexts mainly due to the limited hardware resources (CPU, RAM and battery) and the particularities of mobile threats. Moreover, attacks targeting mobile devices have increased by 614 % in one year and the number of malware has increased from 38 689 to 276 259 in a year.

The main objective of this work is to:

1. Control and protect mobile devices and mobile applications.
2. Limit the spread of malicious applications via SMS / MMS or email.
3. Implement strategies and best practices dedicated to data protection.

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. Identify potential vulnerabilities in developed or downloaded mobile applications.
5. Enable the company to secure its business activities, given the widespread use of mobile devices in the workplace.

Allow the mobile operator (being the default gateway for all users sharing via SMS / MMS or email) to provide a security service to its users and thus to improve its attractiveness.

This work also aims to develop a new Framework to limit the spread of malware via SMS / MMS to mobile cloud computing of the private mobile operator. This framework will include the following:

- Mobile strategy and security policy
- The safety of mobile phones and the integrity check;
- Periodic audit carried out by the operator through scans and vulnerability tests;
- The warning and prevention system against the risks associated with the existence of malware.

In a second step this work aims to design a new multilevel model for mobile application security SMMA (The Security Model for Mobile Applications) to define a strategy and architecture dedicated to mobile security to minimize the risks associated with development and deployment of mobile applications, and to identify potential defects in mobile applications. Basically, this model consists of four security levels:

- Physical Level
- Hardware Level
- Operating System Level
- Application Level

Each one of these levels defines a separate section of the security model of a mobile phone.

Our contribution could also be applied in the context of the Mobile Cloud Computing (MCC) of the private telecom operator to avoid the risk of loss of personal and business data.

Our approach is divided into four parts:

The first part describes the state of the art of the mobile and specifically issues related to the spread of malware art solutions. The second will be devoted to the study of the MPSS Framework and its implementation in the local network operator mobile network, the third part will be dedicated to the study and design of a new security model for mobile applications SMMA, and finally the last part is devoted to the design of a test model to validate our MPSS Framework.

2. STATE OF THE ART TECHNIQUES OF MOBILE MALWARE PROPAGATION

The number of mobile phones has increased dramatically in recent years due to improved memory, processor and also the small size of mobile devices and their sophisticated features (3G or 4G, WiFi, Bluetooth, wired to a PC, …) (Figure 1).

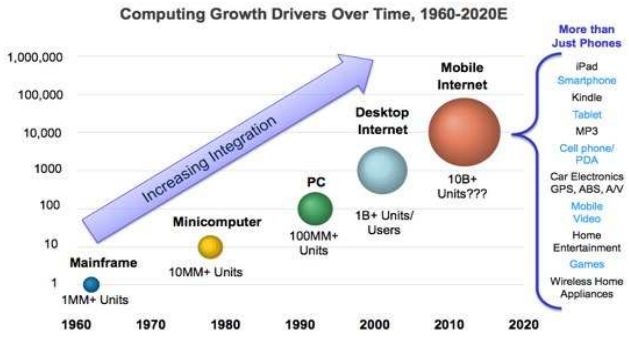

Figure 1: The growth of smartphones and tablets [1]

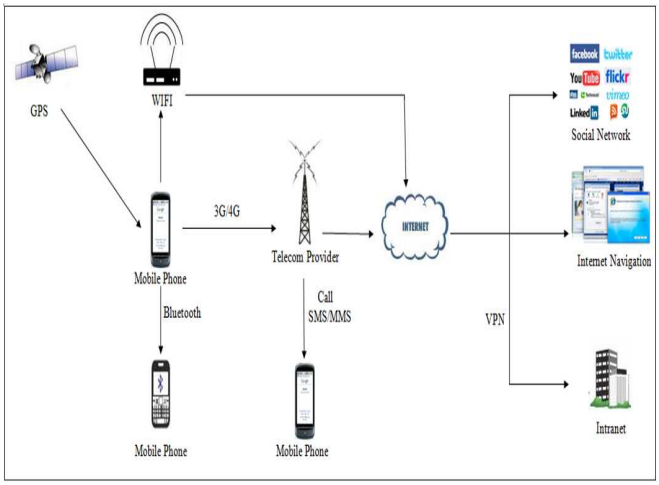

Figure 2: Types of communication mobile phones

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

These mobile devices are more convenient to use in our daily lives: using a mobile, we can surf the Internet and exchange data.

Therefore, due to the development of the mobile phone such as adding new features (4G), the number of mobile phone users Internet users exceed that standard users by the end of 2013 [2].(Figure 2).

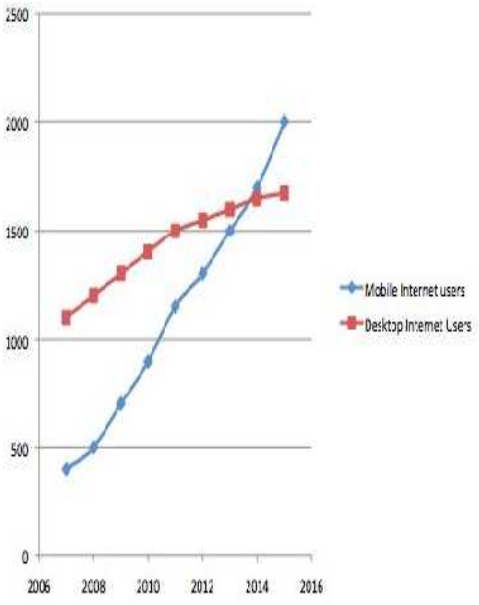

Figure 3: Comparison between the number of Internet users and mobile voice telephony [2]

This will contribute significantly to the spread of malware in mobile phones. This software, as Commwarrior [3], Flexispy [3], Cabir [3] Inqtana [3] use the hidden operating and spread in networks unsecured wireless systems vulnerabilities.

2.1. Spread Malware

Mobile phones have multiple communication interfaces [4] (USB, GPRS, 3G/4G, WiFi, ...) to sync with the computer, data storage on memory cards, media sharing via Bluetooth Wifi, etc. in a social network, malicious software tries to use these interfaces to propagate using services such as MMS and Bluetooth. Using the most malware centralized methods implemented in the network operator [5] to existing distributed.

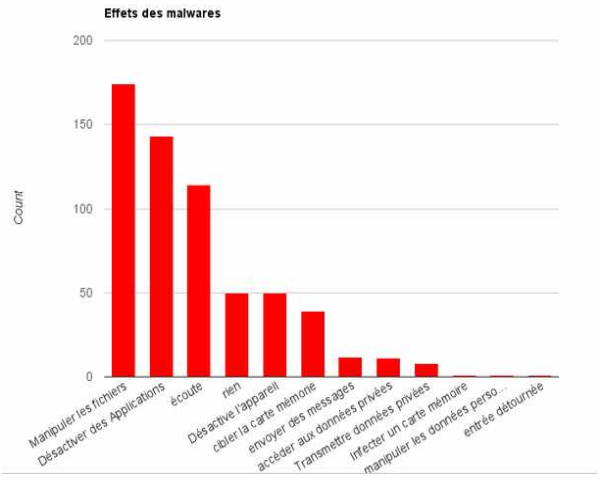

Figure 4: Effects of malware [6]

When a node is infected, it launches attempts to spread malware via MMS, it behaves as e-mail viruses on the Internet. It usually starts with sending MMS messages to the contacts found in the telephone directory or generate combinations of numbers that belong to a telecom operator or a known region. [7] This fake message is very lucky to be open and active. The environment enables mobile networks to spread malicious programs by direct contact via Bluetooth or Wi-Fi connection between nodes in the case of a limited geographical area (LAN) and by indirect contact with SMS or MMS for large geographical areas (WAN).

Both methods of hostile programs that broadcast on a large scale are the origins of the need for adequate solutions to limit the dangers of malware on the confidentiality, integrity and availability of data.

2.2. Solutions Against The Spread Of Malware

The traditional way to detect malware based on the digital signature is becoming a recent approach that aims to prevent and mitigate the threat posed by mobile malware.

According to the survey on the prevention of measuring the integrity malware based on [8, 9] which applies a mandatory access control to prevent the hostile behavior of programs, the major challenge is to determine automatically the sound rules, without any human intervention.

Otherwise, the review [10,11] of the anomalous variation of the electric power of the mobile phone which detects malware by observing the extra energy caused by a hostile consumer behavior. The major drawback of this technique is the lack of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

precision and accuracy in modeling energy consumption for multitasking mobile platforms.

Other industrial efforts against malware mainly focuses on two mechanisms:

1. Access control at different level: application, network, operating system (Android, Symbian and Microsoft Windows).

2. Antivirus (Kaspersky, McAfee, Norton ...), who works at the base attack signatures (detection of execution traces) [12]

A threat example via MMS: Malware can spread to mobile devices with a copy of itself to an SMS / MMS that is sent from the infected machine. Commwarrior is an example of a worm that can spread via MMS [12]. The worm is able to analyze the phone book and send MMS to contacts found thus infecting these devices once the MMS is opened.

Example of protection: network servers adopt this strategy for the automatic filtering of messages generated by spammers. For example, we take the module security policy to ensure the Qtopia Linux-based voice mail; Qtopia offers a number of applications integrated messaging (eg SMS, MMS and e-mail client). The rules can be defined for other applications of this module and other modules.

A threat example via Bluetooth: infection via Bluetooth depends on the physical proximity of the attacker to the infected machine. It requires that the Bluetooth phone is switched on, sufficient signal strength and the phone is in discoverable mode. Because there is no intermediary between the infected machine and a potential victim, it is difficult to remotely monitor the route of infection. Cabir is a worm known Bluetooth works on SymbianSeries 60 and spread among devices that are Bluetooth enabled discovery mode. [13]

Example of protection: defense strategy against the spread via Bluetooth architecture is summarized hereafter blue-Guard; this strategy can detect the spread of Bluetooth Worms in public areas.

Blue watchdog consists of two basic elements:

1. Bluetooth watches.
2. The center of Bluetooth detection.

Bluetooth monitors [14] are used to collect the number of times people search, which is essential for the distribution of the Bluetooth technology. However, the number of packets of the investigation is not a good signal to detect the worm, as packets of the survey are used to discover neighbors can be used for normal operations monitoring.

Bluetooth worm [15] is designed to spread rapidly and aggressively explore new victims in the coverage area.

The detection technique is time, Bluetooth detection by analyzing time series that has been collected: Watchdog uses a blue dot on the detection of exchange sequences, whose goal is to find the point of exchange, if it product in time series by checking if it is a continuous process. The worm can increase the overall average significantly paging.

After presenting some security threats and solutions in the context of mobile phones, let us now present our solution.

For distribution via MMS: To ensure the privacy of its subscribers, the Telecom supplier is invited to implement an audit program / automatic disinfection in all versions of operating systems, all mobile phones, SMS distinguish the actual program / MMS hostile and limit its spread in the future (Figure 4).

The program itself should not afflict the performance of the mobile device by using resources (CPU, RAM, battery power).

For distribution via Bluetooth: Telecom operators can integrate new solutions with access to strong and powerful identification using the IP address or MAC (Bluetooth Access List) address filtering in their mobile devices marketed to allow access for known and trusted mobile phones only. With this solution, only authenticated and authorized users can share resources through a Bluetooth network.

In addition, to prevent the spread of malware through a wireless network, 3G or 4G, we propose a solution based on the telecom provider [16].

More resources than one mobile can help to offer a new service to detect and eliminate viruses messaging and Internet virus to all its subscribers.

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

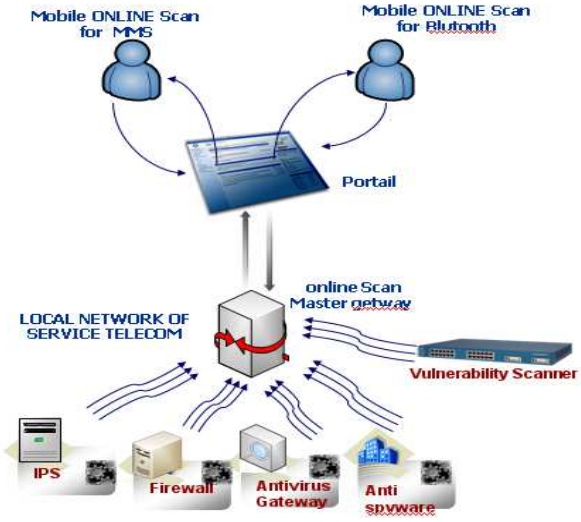

Figure 5: Scan / disinfection mobile phones via the online services of the telecom operator

These solutions, once installed in the local network provider Telecom (Figure 5), stop the spread of malicious program over the network, which is a focal point of interconnection of all mobile devices and a gateway to interconnection from other providers of telecommunications with a complete security solution (gateway antivirus, firewall, intrusion detection, vulnerability testing and filter SMS / MMS..).
In this step, we need a comprehensive and central Framework [17, 19, 21, 22] that meets the following objectives:

- Application Security Policy,
- Knowledge of mobile security [18],
- Implement best practices for mobile security,
- Establish a monitoring system at several levels: (Layer2, layer 3, and the application-level data),
- Automatic update security patches,
- Integration of a warning system in real time by SMS [20],
- Application tests of the security status of the mobile system through a periodic audit or scan for vulnerabilities.

To meet these security requirements that must be provided by the telecom operator, we present our new Framework in the next Section.

3. THE MPSS FRAMEWORK

For better security against the risk of data loss due to malware, and to address the challenges mentioned above, we present the MPSS Framework (Mobile Phone Security Scheme) [23].

This Framework Consists of four modules, these modules will be shown as follows:

Module 1: Strategy and policies

This module will generate all mobile security policies and implement security policies to be applied in the gateways of the telecom operator (for all mobile phones). Following standards and best practices, this module aims to reduce the risk of attacks via malicious programs that spread via SMS / MMS or email.

Module 2: Security of mobile telephony and the integrity check

This module is the heart of the MPSS Framework, it consists of four parts:

1. Access Security: This module deals with the safety applied in the step of accessing, using level 2 (MAC address filtering) and level 3 (IP Access List) filters to allow access to only trusted mobile phone.

2. Data security: it allows encryption of critical data during transfer between two devices on the same Telecom operator (encryption of data), plus a backup / restore of critical data of mobile and personal contacts.

3. Application Security: This module is the most interesting; it can detect and eliminate, in real time, the spread of malware of all mobile phones. This can be done at the telecom operator using an application firewall to filter incoming and outgoing traffic.
Access from mobile phones will be via a secure VPN tunnel (client-to-site) on the transfer of confidential user data.

In addition, authentication and authorization systems allow limited to the mobile device via a strong password access. It also provides automatic disconnection in case of non-use (timeout).

Antivirus / Antispam control and vulnerability analysis are used in this module to allow access to legitimate data. The illegitimate access in this module will be dropped, and an alert will be sent to the alert system (Figure 6).

4. Log and Report: Function traceability of all activities (analysis and disinfection) allows the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mobile user to know the level of security of their mobile devices. This is done through private and reserved space of the web portal operator.

Each user can access via the internet portal periodic reports after a suitable authentication.

This feature will enable the telecom operator to better understand the nature and frequency of malware by region and period.

Module 3: Security Audit

This module will be based on an audit periodically generated security report: the telecom operator performs a quick scan of each cell phone during the phase of battery charging.

This control module is supported by a vulnerability testing manually by the subscriber via a secure VPN. This vulnerability testing is performed by a security guard integrated into the mobile phone operating system at the time of purchase.

Module 4: Warning system

This module is the last module of the MPSS Framework.

The telephone company should notify the customer of the risks related to the existence of malware. The owner of the mobile device should then initiate a manual scan from their mobile phone.

In this module, the user will be informed in real time of the security status of their mobile device.

SMS or e-mail will be sent directly by the telecom operator to the subscriber when a security issue has been detected.

Finally, the overall pattern of MPSS Framework which includes four modules mentioned above.

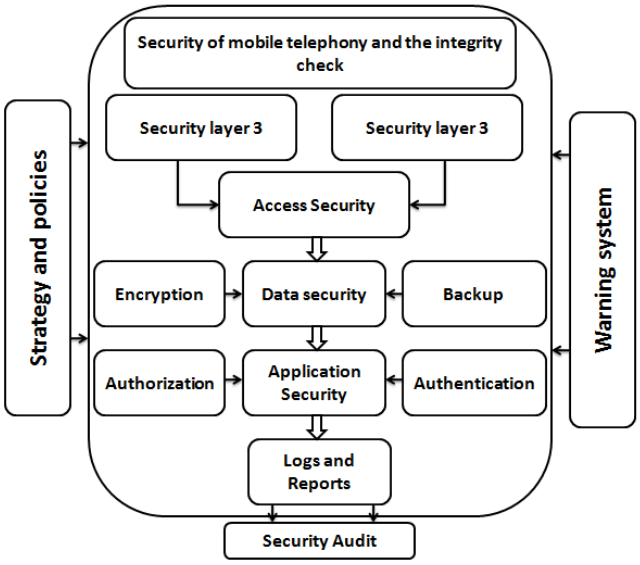

Figure 6: Our MPSS Framework [23]

The use of this plant-based solution provider of security services contributes to a range of telecommunications usage and optimum protection for users of mobile devices with a reasonable cost and effort. The users of these mobile devices will not be required to install security programs in their handsets.

With this centralized solution, a user is not supposed to:

• Have too much knowledge on mobile security,

• Download updates of antivirus signatures or IPS signatures periodically.

• Pay the purchase price mobile security programs (program firewall or antivirus for mobile).

• Consume the resources of his mobile phone, CPU, RAM, hard disk space for installation and battery power.

This security analysis will in fact be performed by the service provider to all subscribers within two ways:

• A manual analysis requested by a user using an ISP service online [24].

• An automatic scan / disinfection using centralized security solution based on LAN.

org E-ISSN: 1817-3195

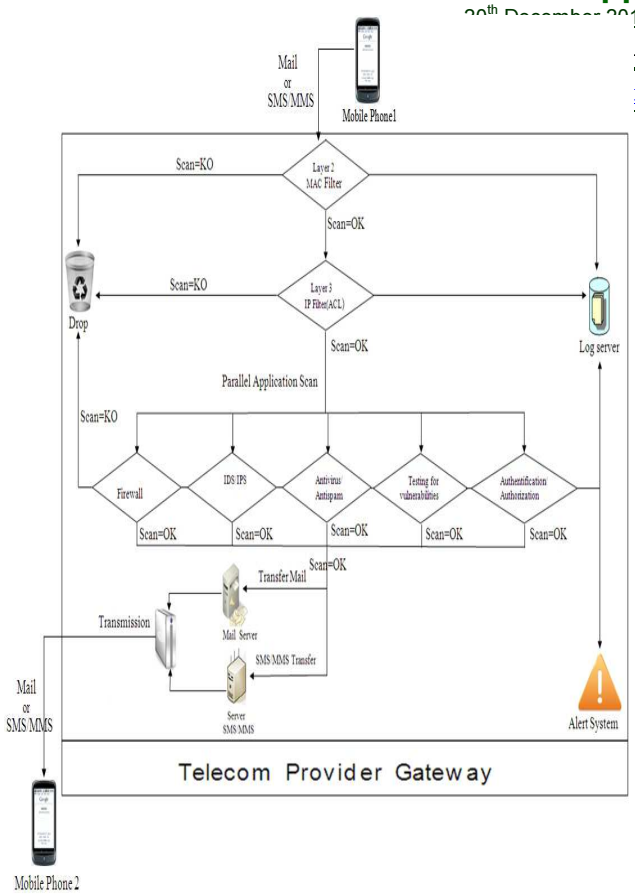

Figure 7: Implementation of our MPSS Framework

the model based on all lower levels to ensure that their components are safe in an appropriate manner. This model based on abstraction allows the design of a particular mobile security mechanism to focus on one area of concern without spending resources to analyze all layers that support its current position in the model.

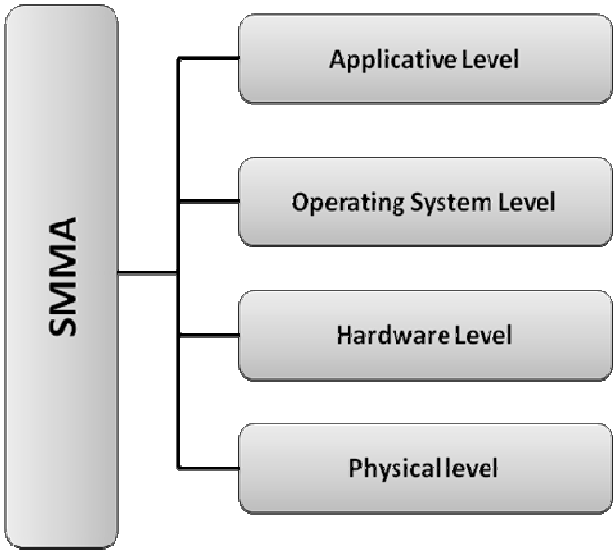

Figure 8: Levels of SMMA

4. THE SECURITY MODEL FOR MOBILE APPLICATIONS (SMMA)

The increased adoption rate of mobile phones coupled with the rapid growth of the number of mobile applications has created a situation in which private and sensitive information are pushed new boundaries of the device at an alarming rate. The mobile device is quickly becoming ubiquitous. Although there is much overlap with common models of the operating system, the security model code of the mobile device has some distinct points of differentiation.

The security model for mobile applications is composed of four distinct levels. The lowest level of the model is the physical level and then upwardly by the hardware, the operating system level and the application level. These levels of security model each define a separate section of the security model of a mobile phone.

Each layer in the security model for mobile applications is responsible for the security of its components, and nothing more. The upper levels of

4.1. Physical Level

The physical level is the first level of the model and the lowest and therefore the most suitable security model for mobile applications. This level is the foundation that supports all other levels of the model. The majority of functional components at this level are owned and operated by a mobile operator or provider of physical infrastructure, data is transmitted from this level up, can carry cellular voice data, and manage infrastructure that carries all the data and voice communications from one point to the end point.

La sécurité des composants à ce niveau englobe généralement les protocoles utilisés par les opérateurs et les fournisseurs d'infrastructures physiques elles-mêmes. Des exemples de tels protocoles comprennent le protocole d'accès multiple par répartition en code (CDMA), global system for mobile communications (GSM), les systèmes de géo-localisation (GPS), les systèmes des messages courts (SMS) et les systèmes de messagerie multimédia (MMS).Les anomalies ou les vulnérabilités découvertes à ce niveau

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

réussissent généralement sur de multiples plateformes, plusieurs transporteurs, et de multiples fournisseurs de jeux de téléphones portables.

4.2. Hardware Level

Then we introduce the second level security model for mobile applications, we enter the realm of a physical unit which is usually under the direct control of an end user. The material can be identified by the equipment installed at the end user, usually in the form of a smart phone or mobile device section of the tablet. The hardware is available to the operating system that allows a direct control of the physical components of the unit.

This material is usually called the "firmware" and updated by the physical handset manufacturer and sometimes comes vicariously through phone support. Security flaws or vulnerabilities discovered at this level generally affect all end users who use a particular material or an individual hardware component. If a material defect is discovered in the device from one manufacturer, it is likely that all hardware revisions using the similar design and / or chip will be made as well.

4.3. Operating System Level

The third level in the security model of mobile applications is the operating system layer. This level corresponds to the software running on a device that allows communication between the hardware and the application level. The operating system is periodically updated with feature enhancements, fixes, and security patches that may not coincide with the firmware fixes made by the manufacturer of the physical handset. The operating system provides access to its resources through program interfaces and applications. These resources are available to be consumed by the application level and it is the only top-level model to the operating system. The operating system communicates simultaneously with the hardware and firmware to perform process and transmit data to and from the device.

The flaws in the operating system are a very common type of anomalies and now tend to be the prime target for hackers who want to have a strong impact. If a malfunction is detected, the entire installed base operating system of this particular will likely is vulnerable. On this layer, where the software is the primary mechanism for application security. Specifically because the invoked software, operating system and the application layer above, are the most common security vulnerabilities that are discovered.

4.4. Applicative Level

The applicative level lies in the model's head of mobile security. It is the direct interface with the end user. The application layer process can be identified by running the interface using programs and applications provided by the operating system layer as the entry point to the rest of the model.

Security breaches the application layer typically reside in the cracks of applications delivered or installed on a mobile device. These defects are classes that are similar to the area of IT. Buffer overflows, insecure storage of sensitive data, inappropriate cryptographic algorithms, words of hardcoded passwords and backdoors applications are a set of samples of abnormal application layer categories. Operating income security vulnerabilities of the application layer can vary the elevated operating system to the exfiltration of sensitive data.

When analyzing the safety of an individual, it is appropriate to consider each level security model for mobile applications and determine the effectiveness of security mechanisms in place bet. At each level determine what, if any, security mechanisms and mitigation measures that the manufacturer has put in place and whether these mechanisms are adequate for the type of data you plan to store and access the device.

5. IMPLEMENTATION OF THE MPSS FRAMEWORK

To validate our MPSS Framework, we will proceed with the design of a model test in light of the elements presented in the module: "Security of mobile telephony and the integrity check" of our MPSS Framework.

The design of this model will involve the connection support, the choice of routers and switches, the location of servers and elements of security, redundancy and load sharing at different areas of the model, in addition to the open source tools required to perform the test, and finally, the addressing plan that will be proposed in the overall scheme of the model.

The objective of the design of this model is:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. The control validation of the MAC address of mobile 1 at the wireless router of the model.
2. The control validation by IP address (ACL) of mobile 2 at the firewall 1 or the firewall 2.
3. Performing tests of disinfecting email viruses sent by the wireless network from mobile 1 (Samsung S4) to another mobile device 2 (Iphone 4) using a professional antivirus solution, and stopping the spread of this virus between them.
4. Validation of the traceability at the log server of the model.

This model was fully realized at the LAN of the Moroccan Ministry of Finance, using real equipment items (servers, wireless routers, switches and routers) and based on open source tools.

5.1. Construction Of The Network Architecture Of The Model

5.1.1. Location of equipment and servers

The location of equipment and servers at the network architecture of the test model is an important task.

The architecture of the model must allow achieving the Access Control Level 2 (by MAC address) and Level 3 (by IP address), in addition to scan/disinfection of email virus sent by a mobile 1 to another mobile 2.

The main components of the architecture of the model are:

Router 1: allows the connection between the model and the public network.

Router 2: provides redundancy of router 1, running in load sharing.

Firewall: the firewalls (1 and 2) will be deployed in series architecture (back-to-back), to prevent direct connectivity to the model.

Public servers: These are Web, FTP and mail servers. These servers, accessible from the outside via the Internet, will be accommodated in the public area.

Database servers: servers containing the necessary data for different applications.

In our case, it would be interesting to implement a database solution composed of two DBMS servers the most used in the market, i.e.: Oracle and SQL Server, with a backup solution (redundant) for all personal and professional data.

The principle of this model is to separate servers communicating with the outside of the other machines. The filter is designed such that only the Internet/DMZ communication is authorized for the mobile users.

In addition, the servers are placed in different areas according to their roles and the security level desired.

Improvements in the architecture of the model (security, redundancy, addressing) will be presented in the following pages to get to the final schema of the model (Figure ---).

a. At the perimeter level

The following technologies provide security at the network perimeter:

- Firewall: as we have seen in the architecture of the overall model, we have proposed an architecture with two firewalls: the first one is external and the other is internal. The external firewall is placed at the input of the model. It thus provides a single access point for mobile users, who connect to the public network through a 3G/4G mobile connection.
- The internal firewall is used to prevent unauthorized access to the model by mobile 1 or mobile 2, the implementation of the filtering policies is highly recommended to ensure that only legitimate mobile users can access to the resources of this test model.

b. At the network levl

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To monitor mobile traffic flowing in the model, we have chosen to implement network-oriented sensors (IDS) at different locations.

Upstream of the firewall: This architecture allows the sensor to detect all potential attacks from the Internet.

Downstream of the firewall: the sensor is less vulnerable to attacks which specifically target it.

We will place IDS upstream of the firewall to get visibility on inbound traffic. This allows identifying attempts of mobile attacks even if these attacks will be rejected by the firewall.

The use of the IDS in the DMZ has a huge advantage because the network flow through this area will be validated and well defined. We can thus set up a very specific NIDS configuration, which ensures a very good relevance of the alerts.

Architecture with many DMZ requires the implementation of as many sensors as necessary: one sensor by area (IDS1, IDS2, IDS3, IDS4 and IDS5).

➔ See global schema of the model (Figure 11).

c. At the server level

To ensure the correct operation of the servers, we will put in place mechanisms to protect them and monitor their activities:

- IDS for machines (HIDS): are inserted between the application and the core of the operating system to protect applications or critical servers.
- Antiviral models: A key element to ensure proper functioning of our antivirus scan test is the deployment of a complete and updated antivirus solution.

d. At the access level

For this part, we will implement:

- Basic filtering at routers: most routers integrate the functions of filtering through access control lists (ACL). To avoid burdening treatments at routers and ACLs that will be implemented, we realize only some basic filtering.
- Authentication (WPA2/AES) at the wireless connection with access control at the firewall level will help to identify authorized mobiles to access to the model and the services they can use (SMTP in our test).

The following figure shows the architecture of the model taking into account the implementation of the IDS, the antiviral gateway and the authentication server:

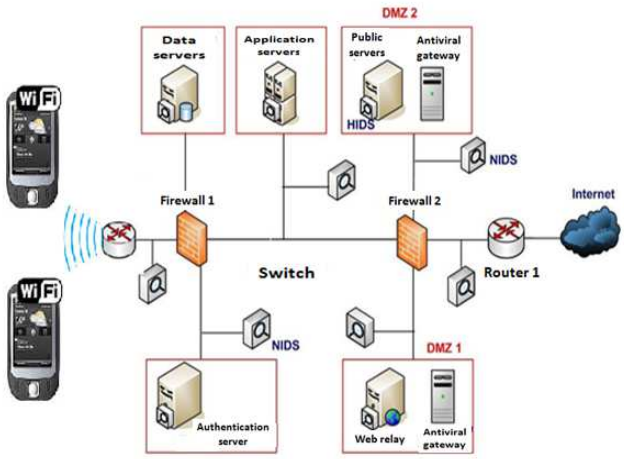

Figure 9: The initial architecture of the model

The two firewalls are the core of the architecture of the model. They protect the three types of servers: public, applications and databases. The architecture of the proposed model consists of two DMZ:

DMZ 1: zone containing an email relay (antivirus server) that redirects the mail requests to the SMTP server. This will allow control SMTP stream before sending them to the destination mail server.

DMZ 2: zone containing the different public servers and a second antiviral solution for double protection against viruses and spam. It is recommended to use different software manufacturers to ensure optimum protection.

5.1.2. Implementing total redundancy of the architecture of the model

Redundancy is to repeat, with variations, some elements of the model in order to make it open,

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

intuitive and always available to respond to increasing requests of mobile users.

To properly protect the MPSS model in case of malfunction (failure or saturation), it is necessary to implement a redundant system in the model. This results in two ways:

a. Link redundancy

Internet links must be duplicated to ensure their full redundancy and to ensure the dependence vis-à-vis a single ISP, it is strongly recommended to order them to two different telecom operators.

Each of the two operators provide two Internet links from two different locations; in case of failure of one of their sites (or even the two connections of an operator), the model will remain connected to the Internet with degradation in debit and response time of these services.

This operation aims to ensure a constant debit for the services of the model to protect them from a network congestion caused by increased network resource requests.

b. Equipment redundancy

For an optimal functioning of the MPSS model, it is important to implement a fully redundant solution in terms of equipment and servers of this model; because any unavailability of an equipment (due to a physical failure or attack...) can make some or the entire model off.

- In case of an equipment failure or after an attack, all or part of the architecture of the model can be found in a state of denial of service.
- In case of saturation of an interconnection equipment, a rapid decline in performance will be noted.

To properly use the different redundant equipment, and return on investment, it is essential to use a load sharing solution (active-active).

Hereinafter, we will present these different aspects of performance that will be integrated into the overall schema of the model.

The implementation of this redundancy will be done in the following elements:

- ✓ **Internet access routers** (Cisco 2611) and **wireless routers** will be duplicated to ensure a reliable network connection and continuity of services of the model: 24/24 and 7/7.

Firewalls will be redundant (1 ⇒ 2 and 3 ⇒ 4) to improve fault tolerance and to distribute the load.

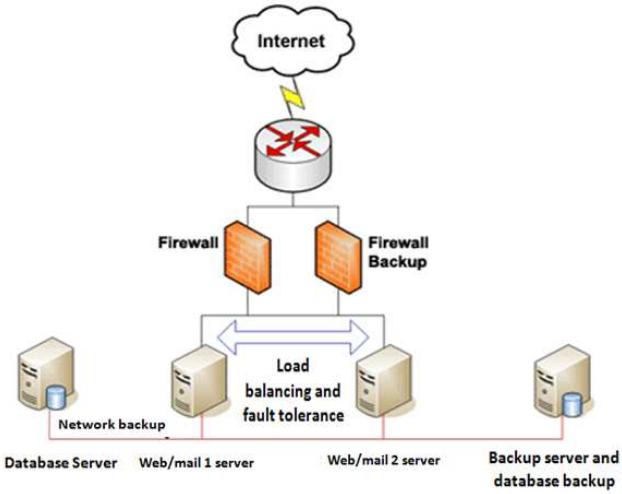

Figure 10: Example of implementation of the redundancy of the model

- ✓ **The switches of zones** will be redundant to ensure high availability in different zones of the model.
- ✓ **The unifying Switch** Cisco Catalyst 6509 is fully redundant at the stage of construction at the factory and only requires a redundant power supply from two different sources.

In addition, these devices (routers and switches) are configured to automatically share the traffic between different devices.

- ✓ **The DNS server** is a fundamental component in a network since it performs the step of resolving a name to an IP address. If the DNS server becomes inaccessible, the entire network becomes inoperable. This is why it is essential to have multiple servers: a master server on which we configure the files of the zone and one or more slave servers on which

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

we simply set up synchronization with the master server.

- ✓ **The Web server** is the interface to access the services of the model; its strategic role requires duplication to one or two web servers whose configuration and contents are identical.

Redundancy is achieved at the level of configuration of relay web server that automatically shares the user queries between real web servers of the model.

- ✓ **Database Servers** (Oracle, SQL Server and MySQL) will be redundant to ensure reliability and performance of data. The data is striped across multiple DBMS located at the model.

In addition to the redundancy of these servers, a backup solution will be installed at the model with the option to backup to a distant site.

- ✓ **The Mail servers** are also redundant, load sharing between the two mail servers of the model (Mail1 and Mail2) will occur at the configuration of mail relays, which are two servers antivirus/anti-spam: each email once scanned will be redirected alternately on the Mail1 or Mail2 server.
- ✓ **Authentication servers** are also redundant; the redundancy configuration will be in the firewalls 1 and 2.

The test model is made redundant by the implementation of a total duplication of these links and components.

5.1.3. Management of high availability for central routers

HSRP (Hot Standby Routing Protocol) is a protocol for high availability derived from the standardized redundancy protocol RSVP. The items to be set are:

- The Master router
- The Standby router
- The interface to monitor.

In the case of our test model, both routers Router_1_model and Router_2_model have as logical address 172.26.1.4.

The router Router_1_model is the master HSRP router because its priority is the default priority 150 (the master router has the highest priority). The priority of the router Router_2_model is 90, which assigns to it the role of standby router.

When the interface FastEthernet0/0 of the router Router_1_model fails, the interface FastEthernet0/0 of the router Router_2_model takes over. Once the router Router_1_model restores, its initial priority will be substituted (standby preempt) and it becomes HSRP Master.

The HSRP configuration performed for the routers of the model is:

For Router 1:

```
hostname Router_1_model
interface FastEthernet0/0
ip address 172.26.1.1 255.255.255.0
no ip mroute-cache
speed 100
full-duplex
standby use-bia
standby ip 172.26.1.4 (logical address)
standby preempt (Substituting the role of HSRP Master)
```

For Router 2:

```
hostname Router_2_model
interface FastEthernet0/0
ip address 172.26.1.2 255.255.255.0
speed 100
full-duplex
standby use-bia
standby ip 172.26.1.4 (logical address)
standby priority 90 (it assumes the role of backup because its priority is 90 < the default priority 150)
standby pre-empt
```

We have configured one logical address 172.26.1.4 for the two central routers of the model.

With this configuration, high availability and load sharing are guaranteed between the two the routers of the model: Standby IP 172.26.1.4.

5.2. Presentation Of The Global Schema Of The Model MPSS

Following the work of choosing the connection support, creating the DMZ zones (zones

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1, 2, 3, 4 and 5) and locating the servers in the model, an overall summary is presented in the following figure which shows the final architecture of the model after integration of the security, addressing and redundancy elements:

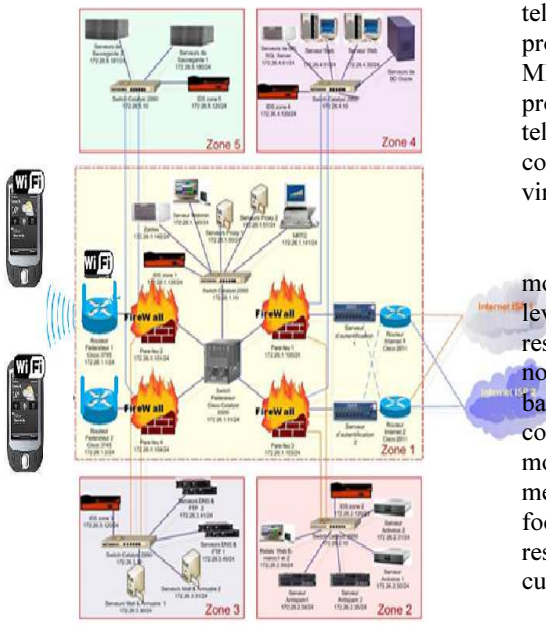

Figure 11: Global schema of the Model

This architecture can thus withstand a series of multiple failures, while balancing the load and the bandwidth.

: The test was successfully completed; we could use this model to block the spread of viruses sent from mobile1 to mobile2 through wireless connectivity, with strong authentication for the mobile device (WPA2/AES) and control at layers 2 and 3 of the OSI model.

Also, this test allowed us to:

- Validate the control of the MAC address of the mobile 1 at the WIFI router,
- Validate the control of the IP address (ACL) of the mobile 2 at the firewall 1 or at the firewall 2,
- Disinfect the email virus test sent from mobile 1 to mobile 2 using two different antivirus solutions,

In addition, the traceability function provided by the log system of the firewall and the antivirus solution 1 and 2 has been validated.

6. CONCLUSION

Our work is centralized around the study of security mechanisms and the mobile protection in wireless network traffic and in mobile applications.

We have proposed an approach based on telecommunications providers offer architecture to provide solutions to security problems SMS / MMS. A new framework (MPSS) has been proposed and implemented in the gateway provider telecommunications provider and enveloping a comprehensive analysis against all malware: viruses, spam and DOS attacks.

This work has proposed a new model of mobile security applications, consisting of several levels and layers. Each layer of this model is responsible for the security of its components, and nothing more. The upper levels of the model are based on all lower levels to ensure that their components are safe in an appropriate manner. This model based on the abstraction can design a special mechanism mobile security; the principle is to focus on an area of concern without spending resources to analyze all the layers that support its current position in the model.

The MPSS framework does not protect the privacy of users and companies, in case of loss or theft of the device. This limitation, in addition to the traditional limitations of a mobile system (internal storage capacity, processing power and battery life), will be the subject of our future work in which we are aiming to improve the framework (MPSS) to support more security features based on private Mobile Cloud Computing (MCC) of the mobile operator.

REFERENCES:

[1] Rapport de la société d'investissement KPCB : "*Top 10 Mobile Internet Trends*": http://www.terminauxalternatifs.fr/, 2011.

[2] Morgan Stanley Research: "*The mobile internet report setup. Smart phone security*".December 2009.

[3] Retrieved on March, 2012 from:

http://f-secure.com/v-descs/commwarrior.shtml,

http://www.f-secure.com/v-descs/flexispy_a.shtml

http://f-secure.com/v-descs/cabir.shtml

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

http://f-secure.com/v-descs/inqtana_a.shtml

[4] Aubrey-Derrick Schmidt and Sahin Albayrak 2008. "*Malicious Software for Smartphone*". Berlin 2011.

[5] Feng Li, Yinying Yang, Jie Wu. CPMC: "*an efficient proximity Malwares Coping Scheme in Smartphone-based Mobile Networks*",2010.

[6] (en) Aubrey-Derrick Schmidt, Hans-Gunther Schmidt, Leonid Batyuk, Jan Hendrik Clausen, Seyit Ahmet Camtepe et Sahin Albayrak, "*Smartphone Malware Evolution Revisited: Android Next Target*", 4th International Conference on Malicious and Unwanted Software ,april 2009.

[7] RadmiloRacic, Denys Ma, Hao Chen. 2006. "*Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery*".CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm), Baltimore, MD, August 2006.

[8] Muthukumaran, Sawani, Schiffman, Jung, Jaeger "*Measuring integrity on mobile phone systems*",2008.

[9] Zhang, X., Aciicmez, O., Seifert, J.P, "*Building efficient integrity measurement and attestation for mobile phone platforms*",2009.

[10] Liu, L., Yan, G., Zhang, X., Chen, S. "*Virus meter: Preventing your cell phone from spies*".2009.

[11] Kim, H., Smith, J., Shin, K.G "*Detecting energy-greedy anomalies and mobile malware variants*", 2008.

[12] *F-Secure Labs,*" *Worm: SymbOS/ Commwarrior, Accessed*" *26th February 2011*

[13] *F-Secure Labs,* "*Bluetooth-Worm: SymbOS/ Cabir, Accessed*" *26th, February 2011,* http://www.f-secure.com/v-descs/cabir.shtml

[14] Guanhua Yan Leticia Cuellar Stephan Eidenbenz Nicolas Hengartner, "*Blue-Watchdog: Detecting Bluetooth Worm Propagation in Public Area*",2009.

[15] IosifAndroulidakis, "*Mobile Phone Security and Forensics*", Springer 2012.

[16] Mohamed Ghallali, "*Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods*". Proceedings of the 9th International Conference on Advances in Mobile Computing and MultimediaShin-MingMoMM 2011: p256-259.

[17] Martin Abadi and CédricFournet, "*Mobile values, new names, and secure communication".* In Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on Principles of programming languages, pages 104–115. ACM Press, 2001.

[18] Kingpin and Mudge, "*Analysis of Potable Devices and Their, Weaknesses Against Malicious Code Threats*", RSA Conference, San Francisco, CA, April 11, 2001.

[19] UpkarVarshney and Ron Vetter, "*A Framework for the Emerging Mobile Commerce Applications*", Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[20] Lars Bollen , Sabrina Eimler , H. Ulrich Hoppe, "*SMS-based Discussions - Technology Enhanced Collaboration for a Literature Course*", Proceedings of the 2nd IEEE International Workshop on Wireless and Mobile Technologies in Education, p.209, March 23-25, 2004 .

[21] Ross, S. J. *et al.* "*A Composable Framework for Secure Multi-Modal Access to Internet Services from Post- PC Devices*" Third IEEE Workshop on Mobile Computing Systems and Applications, 2000.

[22] Luvai F. Motiwalla, "*Mobile learning: A framework and evaluation*", journal Computers & Education archive Volume 49 Issue 3, November, 2007.

[23] Mohamed Ghallali&Bouabid El ouahidi *"DESIGNING A NEW FRAMEWORK IN ORDER TO LIMIT THE SPREAD OF MALWARE IN MOBILE PHONE"* International Journal of Engineering, Computer Science and Technology , v0102, 01 - 08 ISSN : 2277 – 9337, 2012 - ijecst.com2012

[24] Wayne Jansen, Tom Karygiannis, "*Mobile Agent Security*", NationalInstitute of Standards and Technology Computer Security Division Gaithersburg, MD20899