Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

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

MOBILE SECURITY: DESIGNING A NEW FRAMEWORK LIMITING MALWARE SPREAD IN THE MOBILE CLOUD COMPUTING

[1]MOHAMED GHALLALI, [2]ABIR EL MIR, [3]BOUABID EL OUAHIDI , [4]BOUCHAIB BOUNABAT, [5]NORELISLAM EL HAMI, [6]BADR ELMIR,

[1,3]Faculty of Science, Mohammed-V AGDAL University, Information Research Laboratory Rabat, Morocco

[2,4,6]ENSIAS, Al Qualsadi R&D Team, Mohamed-V Souissi University, Madinat Al Irfane, BP 713, Agdal-Rabat, Morocco

[5] EMI, Mohammed-V AGDAL University Avenue Ibn Sinae, BP 765, Agdal-Rabat, Morocco

[1]ghallali2001@yahoo.fr, [2]elmir.abir@gmail.com, [3]ouahidi@fsr.ac.ma, [4]bounabat@ensias.ma, [5]norelislam @outlook.com, [6]b.elmir@daag.finances.gov.ma,

ABSTRACT

Our study is primarily interested in limiting the spread of malwares via SMS/MMS, and Emails. It describes the steps leading to identify, analyze and secure traffic in mobile networks. For this purpose, a Framework MPSS has been used to be part of the network of the mobile network operator. MPSS aims to increase the level of information security across the telecom provider network in order to resolve the problems of the limited hardware and software resources on those mobiles devices. Finally, a new study based on MPSS Framework limitations, has driven a designing of a new Framework called MPSS2 based in the private Mobile Cloud Computing of the ISP. In addition, with the approach of MCC, the proposed security takes the form of a service provided by the mobile network operator (SaaS: Security as a Service). Therefore MPSS2 has the main objective to limit the risk of losses of personal and professional user's data.

Keywords: *Mobile Security, Framework, Spread of Mobile Malwares, Mobile Cloud Computing, Mobile Network Operator.*

1. INTRODUCTION

Recent years have seen a rapid increase in the number of mobile devices in addition to a growing trend of functionality and performance. In the almost total absence of mechanisms and security solutions in the majority of these facilities and meet the limitations of hardware resources (CPU, RAM and battery power) and software (operating systems weaknesses and security issues mobile applications), the equipment is exposed to new threats related to increased risk in a world where the mobile device becomes an easy target for various attacks: threats and attacks targeting mobile devices increased 614% in a year and the number of malware increased from 38 689 to 276 259 in one year [1].

Faced with these challenges, many efforts have been devoted to the security of these mobile devices because of the complexity of security problems and their importance in the business world.

The aim of this work is to find solutions to these problems of mobile security as a four-part, to:

1. Limit the spread of malware via SMS / MMS or email.
2. Allow a single user access to their data in a reliable and secure manner, without being a target of a mobile attack.
3. Enable the company to secure its information assets, 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 improve its attractiveness.

As a contribution, this work aims at the development of a new Framework for limiting the spread of malware via SMS / MMS at the Private Cloud Computing Mobile Operator Mobile. This framework will include the following components:

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

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

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

Our contribution is interested in the use of 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 three parts:The first part describes the state of the art mobile and the problems associated with the spread of malware solutions, the second will be devoted to the study of the MPSS Framework and its implementation in the local network of mobile network operator, Finally, the third part will concern the design and the implementation of the new Framework MPSS2 in the mobile cloud telecom's operator.

2. STATE OF THE ART TECHNIQUES OF MOBILE MALWARE PROPAGATION:

The number of mobile phones has increased dramatically in recent years (Figure 2) due to improved memory, processor and also the small size of mobile devices and their sophisticated features (3G or 4G, WiFi, Bluetooth,).

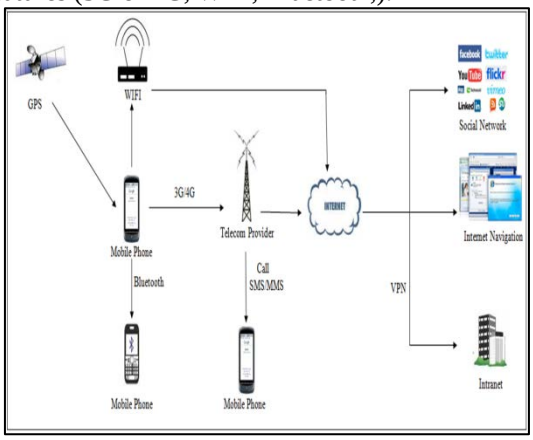

Figure 1 :Types Of Communication Mobile Phones

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

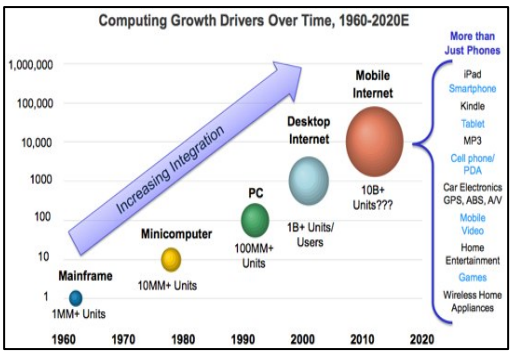

Figure 2 : The Growth Of Smartphones And Tablets [1]

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).

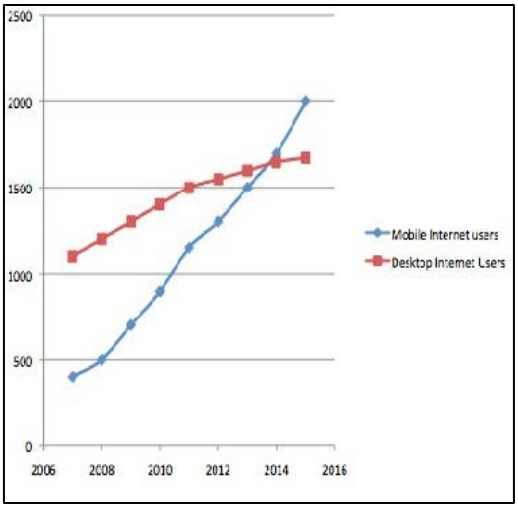

Figure3: Comparison Between The Number Of Internet Users And Mobile Voice Telephony [2]

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 of 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.

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

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 numbers found in the telephone directory or generate combinations of numbers that belong to a telecom operator or a known region. [7] This false 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 precision and accuracy in modeling energy consumption for multitasking mobile platforms.

Other industrial efforts against malware result primarily from two sources:

1. The operating system (Android, Symbian and Microsoft Windows) based on the privileges and access control.

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

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.

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 voicemail, 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.

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 Symbian Series 60 and spread among devices that are Bluetooth enabled discovery [14] mode.

Defense strategy against the spread via Bluetooth architecture is summarized hereafter blue-Guard, this strategy allows to detect the spread of Bluetooth Worms in public areas.

Bluewatchdog consists of two basic elements:

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

Bluetooth [15] monitors 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 [16] 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 this description of the solutions against infection and the spread of malware via Bluetooth and SMS / MMS, we will outline the proposed solution.

The challenge: the strong growth in the use of mobile devices to access private and business data

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

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

(email, intranet, databases) rapidly increased security risks.

The number of Android malware has increased 400% from June 2010 to January 2011 [17], This can also lead to legal liability in case of theft or alteration of confidential business data (corporate email, intranet..), the main question is how we can protect our mobile phones against the spread of malware.

To reduce the impact of malware propagation in SMS / MMS and data transfer mail, we propose a solution that consists of two actions. This solution is based on the network operator Telecom.

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.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 [18].

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.

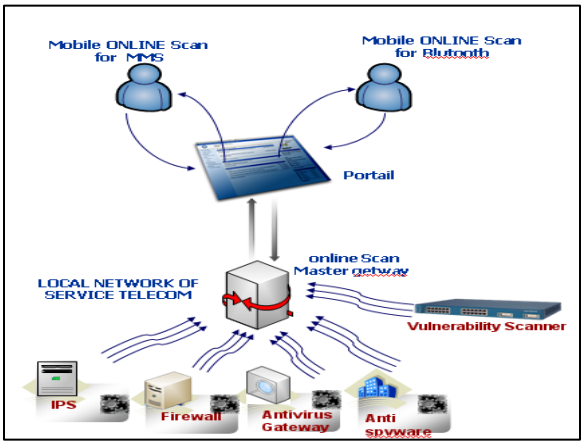

Figure 4: Scan/ Disinfect Mobile Phones Via The Online Services Of The Telecom Operator

These solutions, once installed in the local network provider Telecom (Figure 7), 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 [19, 21, 23, 24] that meets the following objectives:

- Application Security Policy,
- Knowledge of mobile security [20],
- Implement best practices for mobile security,
- Establishing 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 [22] or e,
- 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.

3. RESEARCH FRAMEWORK MPSS:

For better security against the risk of data loss due to malware, and to address the challenges mentioned above, we will study the MPSS Framework [27] Mobile Phone Security Scheme.

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 Framework MPSS, it consists of four parts:

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

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

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 5).

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

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 report periodically generated security: 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 Framework MPSS.

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.

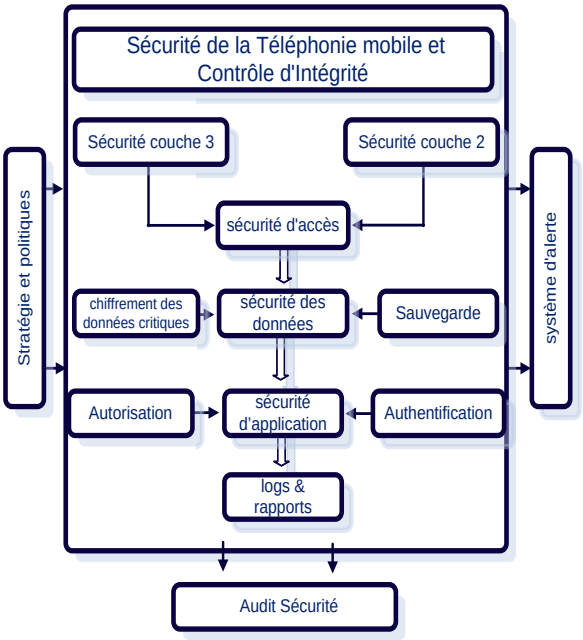

Figure 5 : The Framework MPSS [27]

The use of this plant-based solution provider of security services provides a range of telecommunications usage and optimum protection for users of mobile devices without providing a great effort and a great investment. 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 (firewall program or antivirus).
- Consume the resources of his mobile phone, CPU, RAM, hard disk space for installation and battery power.

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

- A manual analysis requested by a user using a service online ISP [25].
- An automatic scan / disinfection using centralized security solution based on LAN.

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

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

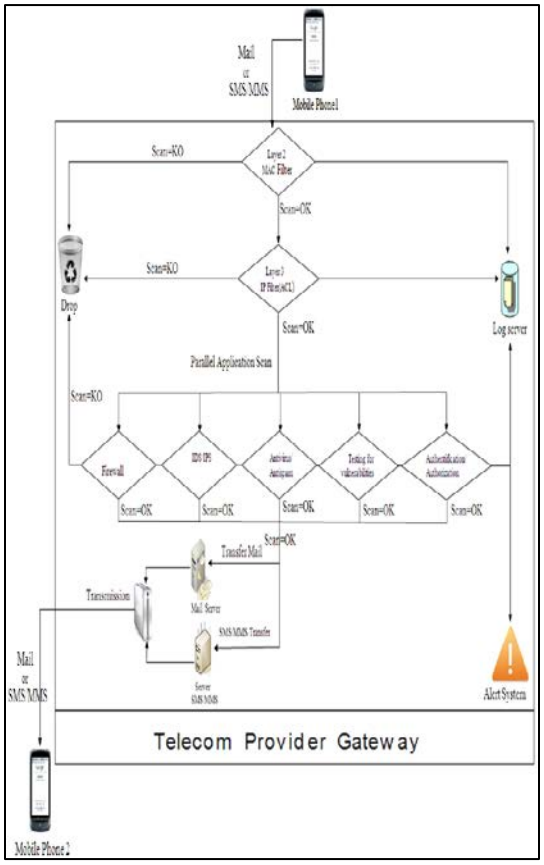

Figure 6 : Implementation of the Framework MPSS[28]

4. LIMITATIONS OF THE FRAMEWORK MPSS

The Framework MPSS is designed with a view to limiting the spread of malware in mobile devices, based on the infrastructure of the telecom operator.

The MPSS may limit the spread of malware for any transfer (SMS / MMS or Email) at the same operator or between different operators [27], but it does not protect the privacy of the user or the company, 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), we have pushed to improve this Framework (MPSS) to support more security features based on MCC private mobile operator.

To give a description of the new modules MPSS2 Framework and its use, we will start by defining the main characteristics of the security at the MCC.

5. SECURITY NEEDS IN MOBILE CLOUD COMPUTING.

To better understand the mobile cloud computing, it is necessary to have a complete idea about cloud computing in general.

Cloud computing can be defined as a way to provide recent and use the provisions proposed by the localized computer systems based on the Clouds. Indeed, the cloud comprises both more equipment (machinery, equipment, network) and a set of programs supported by a dedicated provider, making these services available to the consumer demand for its free Internet.

The cloud computing proposes a new computer model to provide information technology as services on the Internet, the goal of this new computing model is to increase the capacity and speed of execution without the need invest in new infrastructure or new software licenses or train new recruits. Guests can use services through the Internal cloud computing. These services may include: Infrastructure as a Service (IaaS), data storage as a service (DaaS), Communication as a Service (CaaS), as security service (SecaaS) Hardware as a Service (AHA), Software as a Service (SaaS), Business as a Service (BAAS) and Platform as a Service (PaaS).

The combination of cloud computing and mobile networks can bring many benefits for mobile users, network operators and providers of cloud computing. This provides an opportunity for a new computer model called Mobile Cloud Computing (MCC). Mobile devices are powered by batteries, which limits the processing power, in addition to the low storage capacity, less security, and unpredictable Internet connectivity.

The limitations mentioned above mobile devices are still obstacles for demanding applications computationally intensive and more storage space on a mobile.

To increase the capacity of work, demanding more time from the battery of mobile devices and computationally intensive in addition to a high storage capacity, this work must be moved to a cloud [97,98].

Based on the foregoing, the MCC can be defined as following:

Strict planning is necessary before delegating tasks on a cloud server, taking into account network conditions to a beneficial unloading for mobile users [99]. The architecture of the MCC is shown in the following figure.

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

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

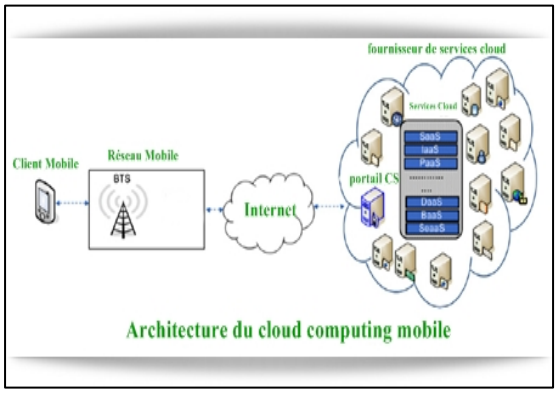

Figure 7 : Mcc Architecture

In the field of MCC there are many challenges, including data replication, limited unreliable scalability, low resource availability in the cloud, portability, trust, security and privacy [100].

The challenges mentioned above have become obstacles to the rapid growth of MCC subscribers. According to the survey [101,102], 74% of IT managers and senior executives of information are not ready to adopt services Cloud Computing because of the risks related to security and privacy.

To attract potential consumers, service providers must target the Cloud Computing all safety issues to provide a totally secure environment. Research organizations and universities have started a lot of work to ensure an environment of Cloud Computing.

Nevertheless, some aspects of security must be addressed, such as security and confidentiality of data stored on a server (s) for the cloud security threats, caused by virtual machines and intrusion detection. MCC is based on the Cloud Computing all security issues are inherited from the MCC with the additional limitation of resource constraints for mobile devices.

Due to the limitation of resources, the algorithms proposed for the security environment Cloud Computing can not be directly executed on a mobile device.

This requires a light Framework, which provides secure data security and access with minimal processing on mobile devices.

Security and protection services of privacy can be achieved using the secure cloud application services. These can provide secure user management, key management, encryption request, intrusion detection, authentication, and authorization services for mobile users.

It will eventually need a secure channel between the mobile device and cloud communication channel. Secure routing protocols can be used to protect the communication channel between the mobile device and cloud. Virtualization improves resource utilization in cloud, but introduces new security challenges due to the lack of complete isolation of virtual machines hosted on a server.

Security issues imposed by virtualization can be addressed to some extent with the help of a secure virtual machine monitor. To provide a transparent cloud environment, mobile users should be able to check the security of hosted services.

The audit can be done using a monitor cloud service. The Service Monitor examines the level of security and the flow of the execution environment. The security level must meet the safety requirements of users and the flow of the execution environment must be normal. The verification of the security of downloaded data on a cloud can be made using a verification service for safe storage.

The physical security of the data center plays a very important role in ensuring the safety and protection of privacy. To ensure the physical safety must be taken to avoid physical access for unauthorized to the cloud service provider .

This physical security can be achieved with security guards, CCTV, sensors and alarms. In this context, work has addressed this need for security at the MCC [103-104] to provide a secure environment and high performance. However, we will also need the security Frameworks energy efficient for mobile devices to have security and privacy in a CMC environment [105].

In what follows, we will try to provide an improved Framework to address some of these security needs Liesa these mobile devices based on the offer of MCC mobile operator.

CONTRIBUTION:

Our contribution is summarized in the conception of a new Framework that will have as main objective limiting and mitigating Malware attacks using the MCC services.

6. THE DESIGN OF A NEW FRAMEWORK MPSS2:

The security of personal and business data is a major challenge for businesses and individuals. Hence the need to develop another Framework, based on Mobile Cloud Computing related to private telecom operator.

To minimize security risks of mobile devices, the telephone or mobile operator, through its private MCC may provide a security service to its clients, which meet the following requirements:

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

- accessibility and availability of resources: the operator must offer a new service for storing data reliable and durable, with guaranteed 24/7 availability through system redundancy and fault tolerance;
- pooling of data that can be shared;
- data storage with a cloud service provider (mobile operator in this case) rather than on the mobile device, storage is a reliable and continuous manner, with an uptime guarantee;
- use of a combination of control techniques:
  - ✓ asymmetric key encryption based on a single certification authority certified and accredited;
  - ✓ authentication account creation (a name and password) for legitimate users;
  - ✓ authorization clients are allowed to access to information stored on the private MCC.
- access to the secure network, fast and reliable;
- standardized access regardless of the brand and the operating system of device;
- decentralization and redundancy systems to minimize bottlenecks and single points of failure.

Components Framework MPSS2 :

To meet some security requirements listed in the previous section, we will propose the Framework MPSS2. The MPSS2 is an improvement on the previous version of the MPSS, based on the concept of MCC secure telecom operator.

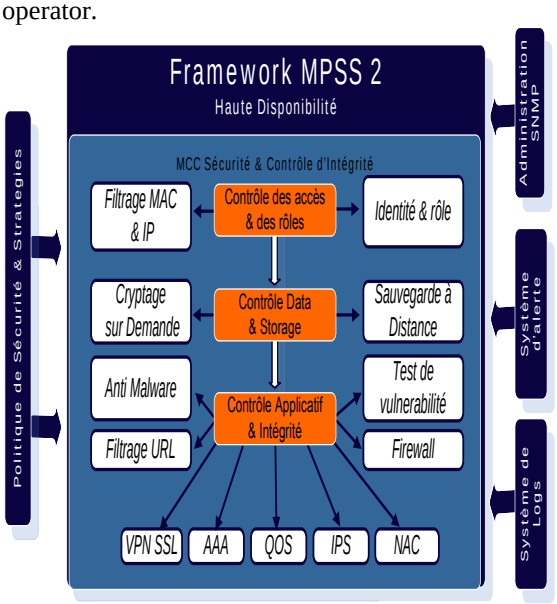

Figure 8 : Proposed Framework MPSS2

Module 1: MCC security and access control

This is the central part of the Framework, it will treat the part of physical and logical access (Packet Inspection, and IP Filtering Mac) in addition to the backup of the user data at the MCC platform this module will consist of three parts:

a) Access Control and roles:

This is the part that is the first security control based on MAC or IP address, in addition to the rights of users of MCC, this module will be divided into two parts, in the following table:

Tableau 1 : MPSS2 Module access control and roles

Security module	Its Role in the MCC
MAC filtering IP filtering	An access control based on the MAC address of the mobile device (filter at the level of data link layer) . Access control based on the IP address of the mobile device (Access-List IP) .
Identity and Roles	A mechanism to verify the identity of a user (ID of SIM card) and the services as are accèsess IP-List).

It must be possible to define the identity, roles, rights and other attributes of the users of MCC and services in a consistent, readable way to properly implement access control and enforce policy security MCC.

b) Control and data backup

Once validated by the first control, the user moves to the second level which offers the possibility of encryption and backup according to the need and rights of users, this control module and data backup is itself divided into both sides:

Tableau 2 : MPSS2 Control module and data backup

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

Security Module	Its Role in the MCC
Encryption on request	Through this infrastructure, we can use asymmetric cryptographic functions between the mobile device and the platform sleep MCC mobile operator. The user has the option to choose this option to encrypt your critical data.
Remote Backup	It must be possible to store personal or business data in clear or encrypted format in the network MCC and not on the mobile device. Some users will need their data to be stored separately from data of other users for privacy reasons.

c) Application and integrity control:

The most interesting control takes place in the MCC part is based on the features of this module, which provides a set of security mechanisms. These new mechanisms are described in the following table:

Tableau 3 : MPSS2 Application control module

Security Module	Its Role in the MCC
IPS	Intrusion Prevention System is a tool to detect and block attacks on the mobile in a MCC environment.
Anti-Malware	Protects the mobile device against malware programs such as viruses, trojan.
Firewall	Application filtering system for filtering incoming and outgoing packets between the MCC and the mobile device.
VPN SSL	Virtual Private network: tunnel between the mobile device and the network operator, based on the new generation of VPN: VPN SSL.
Test vulnerabilities	Element that allows to do a scan (external) on known vulnerabilities on the mobile device : to correct them.
NAC : Network Access Control	System for verification and validation of prerequisites before authorizing access to a mobile device.
AAA: Authentication, Authorization, Accounting	System that ensures strong authentication for users by group and domain: with different rights and privileges for each user.
URL filtering	System to allow or to prohibit access to websites by category.
QOS : Quality Of Service	System used to assign a different priority for each service: SMS, MMS, Mail, Backup ...

Module 2:Security policy and management strategies

In MCC, it is very useful to define policies, set and enforce security policies to support access control, resource allocation and other decisions in a consistent, readable machine. The method of defining policies should be clear enough; SLAs and licenses can be applied automatically.

It must be possible to configure, deploy and manage services in accordance with defined security policies and contracts with customer's mobile operator that manages the platform MCC.

Module 3:Delivery system platform MCC

This system must be able to handle all the hardware, and networks (physical or virtual) under s infrastructure that make up the mobile cloud computing, it must in particular be able to account for any physical or access based on network a mobile equipment for verification and compliance.

Module 4:Warning systems

Consumers should be able to access data on events that occur in the cloud, in particular system failures and security breaches. Access to events includes the ability to learn from past events and reports of new events as they occur.

The following diagram describes several use cases and security requirements for each.

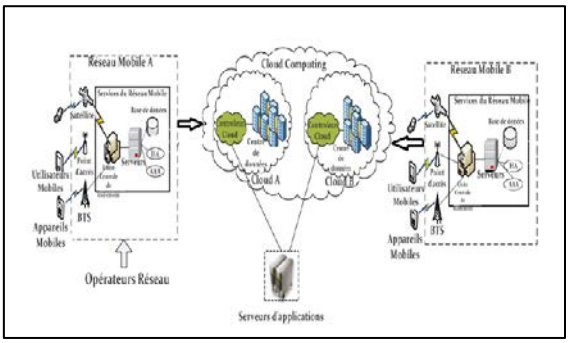

Figure 9: Pool supply MCC service for two mobile operators

7. FRAMEWORK MPSS2 WORKING:

Although there are various tools and techniques available to detect malware attacks and to protect mobile devices, it is important that users are aware of the dangers of these threats and their impact on privacy and the professional world company: Most security attacks on mobile phones can be caused by the negligence of an unwary user.

The best practices for a secure use of mobile devices:

In this section, we offer some good practices to protect mobile devices, focusing on the responsibility of the user who is the critical link in the security of their mobile device.

To contribute to the overall security of personal and business data, the user is prompted to:

- install only the applications of mobile security offered by their mobile provider, as well as the implementation of necessary corrective operating

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

system of the mobile device and locally installed applications, as well as monitoring of alert messages sent by the supplier mobile;

- Ensure to download the official mobile applications and trust MCC only, avoiding downloading other unreliable sources: the verification of the source download is the main eliminating the spread of malware installed unintentionally key with pirated or considerate applications from untrusted sources;
- disable various communication channels of the mobile device (Wi-Fi, Bluetooth, 3G/4G) in case of non-use, in addition to disabling all non-secure sharing and use of tunnels as secure connections SSL or VPN;
- encrypt all sensitive data when it is stored in the mobile device;
- use in possible password for confidential files and business applications: the use of strong passwords is strongly recommended in this section;
- monitor, continuously, the life of the battery, SMS / SMS sent or received: to detect and block any unusual behavior by focusing first on the newly installed applications: there is a higher possibility of infection by a virus or trojan because of an insecure installation;
- Finally, in case of loss or theft of their mobile device, the user must delete all the applications, contacts and confidential data remotely. In parallel to the lock using their mobile device through its unique ID (IMEI).

8. BID SECURITY OF THE MOBILE OPERATOR :

8.1 Offer for Subscriber

The telecom operator, in addition to the basic service (telephony and internet access 3G/4G) can offer its customers an additional security service based on its private or shared with another MCC operator.

This offer contains all the security services needed for optimal and safe operation, namely:

Backup / restore personal data (photos, videos, SMS, MMS, Contacts, Calendar, installed on the mobile device applications, favorites GPS and websites visited), in addition to business data (confidential and professional documents, Mail, list of professional contacts..) ;

Automatic disinfection or upon request of all malware propagating via SMS / MMS or E-Mail;

The ability to encrypt the request, all data from the mobile device;

Access to the MCC resources through a secure connection: SSL VPN, through a secure web access (HTTPS) eg;

The detection and prevention against intrusions and attacks on their mobile device;

The authentication and authorization system and management of access rights depending on the type of user;

Periodic vulnerability testing of the mobile device with proposals updates necessary patches mobile operating system (IOS, Android ...) and various applications installed;

The applications firewall is used for an external access to the mobile device control.

For mobile applications, the processing and storage of data will be moved from the mobile device to a powerful platform and centralized MCC located in the private operator. These centralized applications are accessible through secure connection mechanisms.

Thus the private mobile operator MCC integrates cloud computing in the mobile environment and overcome obstacles and challenges to performance (the life of the battery, the storage volume and flow bandwidth), the environment (heterogeneity, scalability and availability) and safety (reliability and confidentiality) and access personal and professional user data.

8.2 Offer for Business

This offer will affect the entire mobile fleet of the company / organization will outsource the management of mobile security part to its phone service provider and the Internet, through a contract SLA (Service Layer Agreement) Service.

Thus, the company / organization will delegate this task to the ISP, and it will use its private MCC (or shared with another ISP) for the treatment of its confidential and critical data, this offer may contain:

Secure access to business applications via an SSL VPN tunnel;

A customizable system after validation of the company;

Suppression of critical business data and confidential, in case of loss or theft of the mobile device;

Strong encryption of highly sensitive data;

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

A remote backup center: This backup can be scheduled automatically or on demand and system administrator, network administrator, database administrator and security administrator of the company.

The company may seek to keep some of its information assets in its local network, plus the ISP will sign a contract of confidentiality.

9. INTEROPERABILITY AND SECURITY ISSUES IN THE MCC

The use of the MCC involves services integration between mobile operator and Cloud provider in order to ensure operations management: customer management, access methods management and installation fees and licenses payment. Mobile Cloud Computing infrastructure encloses a collection of resources to secure. These resources require to interact and to exchange information and services between them.

With the use of the mobile operator platform, interoperability becomes an important issue while end users need to interact and communicate with the MCC elements. The interconnection involves measurement impact of shared platforms use and pooled on the security of users private data and the supplied quality service. A service convergence of several entities could be considered in cases where a single cloud can meet all the demands of the mobile user: a new system is needed to allow the use of two or more cloud on a unified, permanent and reliable way.

Therefore, Quality assurance in this context is very important. There is a need to have adequate assessment tools for context-dependent quality. Such measurement activity has to take into account conceptual, organizational and technical considerations and gives importance to architectural elements. RatQual model [30] is an example of tool to use in order to characterize information system external qualities influenced by environmental parameters such interoperability and security. RatQual considers internal, external and in use aspects. It combines à priori evaluation elements within the design phase of interconnection setup and à posteriori evaluation aspects considering the performance degree of collaboration.

Joint interoperability and security monitoring using the “Quality monitoring tool” (QMT) [30] helps to track periodically the evolution of security and interoperability degrees over time.

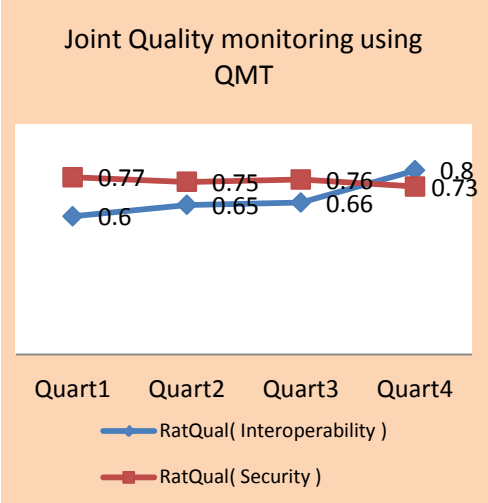

Figure 10 :Security And Interoperability Joint Monitoring Using QMT

Security is to be enhanced while taking into consideration other information system quality characteristics including functionality, adaptability and evolution ones. Interoperability and security are to be jointly prepared, planned and analyzed in this context. Focusing on interoperability and openness to the ecosystem may expose the MCC to more security vulnerabilities. On the same time, giving only importance to security may hinder interoperation capacity.

CONCLUSION:

As part of this work, we studied the MPSS Framework based on the network of the telecom operator whose principal role is to limit the spread of malware via SMS / MMS or via email.

Subsequently, we tried to improve and adapt the first Framework (MPSS), which had limitations for the use of the mobile device in a professional environment, to provide the new Framework MPSS2.

The new Framework will be designed for the private Mobile Cloud Computing to improve the security access and data, based on a unique offering that brings the two actors: the users and the company, through a service security in the Cloud Mobile (Security As a Service) for all subscribers and all mobile companies.

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

REFERENCES:

[1] The KPCB Report: "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

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, SeyitAhmetCamtepe et SahinAlbayrak, "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"26thFebruary 2011

[13] Qiang Yan, Robert H. Deng, Yingjiu Li, and Tieyan Li. "Onthe potential of limitation oriented Malwareetectionand Prevention Techniques on Mobile Phones", International Journal of Security and Its Applications, 2010.

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

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

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

[17] JuniperNetworks"Malicious Mobile Threats Report"2010/2011, May 2011.

[18] 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.

[19] 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.

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

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

[22] 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 .

[23] 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.

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

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

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

[26] Sebastian Nanz, Chris Hankin, "A framework for security analysis of mobile wireless networks", Theoretical Computer Science, Volume 367, Issues 1–2, 24 November 2006, Pages 203–227.

[27] 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

[28] Haji, R., Mohamed Ghallali., Hasbi, A., Bouabid El ouahidi."Designing an adaptive QOS-oriented and secure Framework for wireless sensor networks in emergency situation"Journal of Theoretical and Applied Information Technology, 15 August 2012. Vol. 42 No.1 ISSN: 1992-8645, pp. 59. 2012

[29] "Gartner press release: "Gartner Says worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 billion units by 2013"; full report: Carolina Milanesi, Lillian Tay, Roberta Cozza, RanjitAtwal, Tuonghuy Nguyen, Tracy Tsai, Annette Zimmerman, CkLu; March 28, 2013. http://www.gartner.com/newsroom/id/2408515

[30] ELMIR Abir, ELMIR Badr, BOUNABAT Bouchaib, "Towards an Assessment-oriented Model for External Information System Quality Characterization", International Journal of Computer Science Issues (IJCSI), Volume 10, Issue 4, July 2013.