SCITECH
RESEARCH ORGANISATION|

Volume 2, Issue 2
February 28, 2015|

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

# Adaptive Security Mechanism: a study on the different approaches to mobile devices

Cláudio Aroucha [1], ZairAbdelouahab [2], Denivaldo Lopes [3], Jonathan Santos [4], Willian Ribeiro [5], Higo Pires [6]

[1]UFMA, DEINF, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& cmp.aroucha@gmail.com
[2]UFMA, DEEE, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& zair@dee.ufma.br
[3]UFMA, DEEE, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& dlopes@dee.ufma.br
[4]UFMA, DEINF, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& darkjontex@gmail.com
[5]UFMA, DEINF, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& willfribeiro@gmail.com
[6]UFMA, DEINF, Avenida dos Portugueses, s/n, Campus Universitário do Bacanga, CEP 65085-580,
São Luís, Maranhão, Brasil.& higofelipe@gmail.com

## Abstract

In this paper, provides an overview of some major works that focus on the use of adaptive security for mobile computing to protect information and data traffic. The limited resources on the mobile device makes security mechanisms implementations very expensive. However, these devises are very attractive to attack and exploit their weaknesses, launch scanning attacks, and man-in-the-middle attacks to have access to private data of mobile users. To provide security for users of mobile devices, security mechanism with the ability to adapt to various state sand situations maybe applied such as encryption to increase confidentiality, authentication so that only authorized users or systems have access to its data, and prioritizes ergonomics of the mobile device. For this purpose, mobile features such as CPU, memory, battery, and the environment in which it is connected must be operated by the adaptive security mechanism.

**Keywords:** Adaptive Security; Mobile Computing; Cryptography; Authentication.

## 1. Introduction

The emergence of mobile devices(e.g., PDAs and smart phones) and its wide acceptance and search by the population, increased the need to develop applications which fulfill the necessities of their users with a wide variety of mobile computing technologies, network and security [5]. However, resources are limited in mobile devices such as power processing, memory, and battery storage limit[1]. Security mechanisms, such as encryption and authentication are needed to protect data traffic between mobile devices and the internet. Encryption provides privacy in communication between two entities without the participation of unauthorized entities[2]. Authentication is a service that performs the mutual identification between two entities to understand each other[3]. Because of limited resources in mobile devices, reducing their consumption without harming their safety is required. One possible solution is to use dynamic security adapters to perform resource savings in situations where there is no need for a level of security that requires many resources, since in most cases the higher security complexity requires greater expenditure of funds to achieve it[4]. To create security controls and policies dynamically, context-aware security levels, context aware of mobile devices and the environment that surrounds may be employed[14].

In this paper, we discuss the different solutions of security mechanisms for mobile devices, security techniques employed in such solutions, analyzing possible strengths and limitations.

This paper is organized as follows: section 2 and 3 present a review of the main adaptive security and mobile computing concepts. Section 4shows the work done in the area of adaptive security mechanisms for mobile computing. Finally, in section 5, we present the conclusion with a report of possible working improvements that can contribute to a better protection of the mobile device data.

## 2. Mobile Computing

Mobile Computing has become real through the convergence of two technologies: the emergence of powerful portable computers and the development of wireless, fast and reliable networks [16], making it possible for users to access information and collaborate with other users as they move [6].

Mobile devices and mobile computing have several characteristics. In particular, mobile computing has the following characteristics [8]:

- Portability: it becomes easy to move to different locations.
- Connectivity: it can connect to the internet through various technologies like3G, 4GandWi-Fi.
- Interactivity: it is critical for mobile device with little computing power.
- Individuality: mobile devices, tablets and smartphones are designed for individuals and become useful for people in many aspects of their lives.

According to [7], mobile devices are growing and will continue to evolve more and more; Android surpasses one billion users on all devices yet. Table Is how`s that Android is the operating system of choice for mobile devices.

Table I

Worldwide Device Shipments by Operating System (Thousands of Units)

| Operating System | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|
| Android | 503,690 | 877,885 | 1,102,572 | 1,254,367 |
| Windows | 346,272 | 327,956 | 359,855 | 422,726 |
| iOS/Mac OS | 213,690 | 266,769 | 344,206 | 397,234 |
| RIM | 34,581 | 24,019 | 15,416 | 10,597 |
| Chrome | 185 | 1,841 | 4,793 | 8,000 |
| Others | 1,117,905 | 801,932 | 647,572 | 528,755 |
| Total | 2,216,322 | 2,300,402 | 2,474,414 | 2,621,678 |
| The values are given in ref. [7]. | | | | |

## 3. Adaptive Security

Security is a way to ensure that the information traffic in computer networks is not read or modified; its essential features are the provision of integrity, confidentiality and authentication [15]. Software adaptation concerns changes made to a system according to its needs or state in order to optimize it. [16] Providing security to mobile devices can be very exhausting to their resources. To solve this problem, adaptive security may be used. Security functions can be added to mobile devices based on decisions made considering information context on the device resources.

## 4. Adaptive Security Mechanisms for Mobile Devices

Mobile devices have limited resources and it is still a major challenge optimize and provide security simultaneously. In the literature there are several ways to provide security to applications and data of mobile devices [9], [10], [11], [12] and [13]. Some related works are listed below.

### 4.2. Prometheus: An Adaptive Security Service

The work proposed by [9] provides two features of dynamic adaptation of security controls and their own security policies. The differential of this work is the adaptation at run-time of these two features during the execution of ubiquitous applications on mobile devices, ensuring the availability, confidentiality and integrity of these applications. Figure 1 shows the adaptive security service that has as the main components of Prometheus, the adaptive security manager, connections manager and resource manager.

- Adaptive security manager: is the main component responsible for determining the policy and security controls dynamically. Using 3 levels of security for adaptation: weak (DES), medium (3DES) and high (AES).
- Connection Manager: ensures the confidentiality and integrity of information traffic, and creates security channels using most suitable encryption algorithms to the environment in which the device is located.
- Resource Manager: responsible for managing device features. For example, when a device has little battery level, it may reduce the transmission power to save the battery resource.

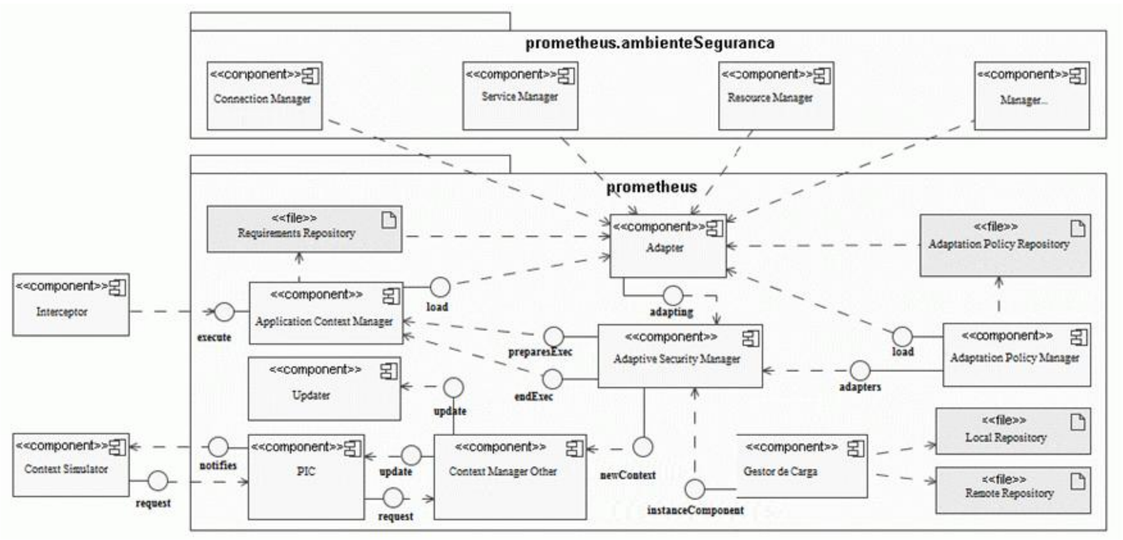
prometheus.ambienteSeguranca
<<component>> Connection Manager
<<component>> Service Manager
<<component>> Resource Manager
<<component>> Manager...
prometheus
<<file>> Requirements Repository
<<component>> Adapter
<<file>> Adaptation Policy Repository
<<component>> Interceptor
<<component>> Application Context Manager
load
adapting
execute
preparesExec
<<component>> Adaptive Security Manager
load
<<component>> Adaptation Policy Manager
<<component>> Updater
endExec
update
adapters
<<file>> Local Repository
<<component>> Context Simulator
notifies
<<component>> PIC
update
<<component>> Context Manager Other
newContext
<<component>> Gestor de Carga
<<file>> Remote Repository
request
request
instanceComponent

Figure 1- Component Diagram of Prometheus adapted from [9].

### 4.3. Context-aware Dynamic Security Configuration for Mobile Communication Device

The scheme proposed in [10], has the objective of maximizing the performance of mobile devices in terms of computational resources without degrading security level based on context awareness by providing users with high convenience and device resources economy. This scheme does not deal with adaptation to various cryptographic algorithms and security automation in the evaluation phase, but it is proposed as a future work. The implementation of this scheme is carried out on a platform of a personal computer Linux Ubuntu XPX DELL M1710to maintain protection of firewall security features, IDS, virus scanner, access control, battery monitor and protection against data leakage.

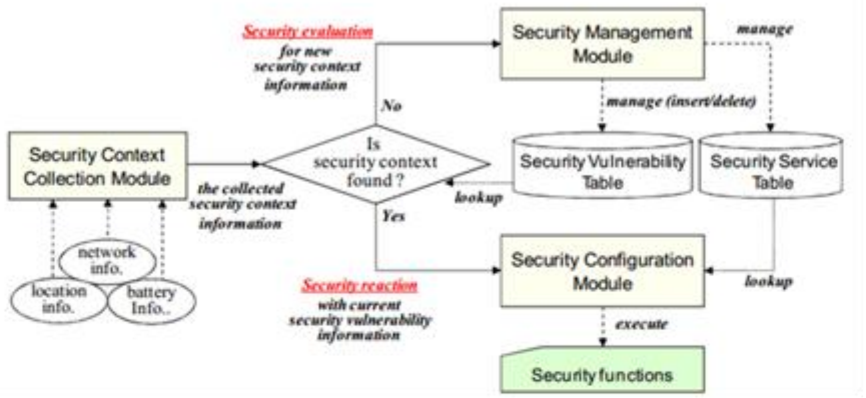
Security evaluation
for new security context information
Security Management Module
manage
No
manage (insert/delete)
Security Context Collection Module
Is security context found ?
Security Vulnerability Table
Security Service Table
the collected security context information
lookup
Yes
network info.
location info.
battery Info..
Security reaction
with current security vulnerability information
Security Configuration Module
lookup
execute
Security functions

Figure 2 – Architecture of context-aware security configuration [10].

This architecture is divided into three modules and two tables:

- Security Context Collection Module: it is used to collect mobile device context information.
- Security Management Module: it manages the tables of safety and security service vulnerabilities.
- Security Configuration module: it provides the best security service according to the context of the mobile device.
- Security vulnerability table: it indicates which attack a mobile is vulnerable.
- Security service table: it stores the capabilities and security features.

### 4.4. A Security Mechanism with Dynamic Run-time Adaptation for Mobile Devices

The mechanism presented by [11] proposes an adaptive security of confidentiality for data traffic in mobile devices based on context and efficient use of resources. The selection and use of a better cryptographic algorithm is made based on the context of the mobile device and where the algorithm has been previously evaluated taking into account the expenditure of resources such as CPU, memory and battery.

All user interactions of users with the application are relevant context information, such as passwords and credit card numbers. An example of resource saving is a mobile device connected to a secure-network environment in which case it does not need require strong encryption since the latter consumes a lot of computational resources; thus choosing an algorithm that uses less resources can lead to lifetime device increases.

### 4.5. Context-Aware Security model for Social Network Service

The work proposed by [12] is a security model for social networking services for smartphones. Smartphones are increasingly used, not only providing voice phone function, but also as computers with email functions, internet, etc.

This work suggests a context aware access control and authentication system via scenarios where the smartphone is found. It first collects information from the device and then uses a fuzzy algorithm to determine a security level of the device based on information context. Then, the proposed system provides context-aware security service via optimized authentication, access control, and process control service.

### 4.6. Security Service for Context-aware Authentication for Mobile Devices in Cloud Computing paradigm (SSACC)

The proposed work by [13] aims to provide a secure channel service for transferring files between the mobile device and a server using SSL with different cryptographic processes. Authentication is performed by means of public key cryptography. The integrity and confidentiality are provided by means of private key encryption and digital signatures. Aiming to provide authentication security, in relation an encryption algorithm is selected based on the network security level, the amount of available battery and the processing power of the mobile device.

The contribution of this work is to create a dynamic and adaptive security service, which takes the decision on which encryption algorithm is sufficiently safe for device authentication from the environment where it is connected. Figure 3 shows the SSACC application using the stack of protocols SSL to create a secure channel of communication with the computing environment.

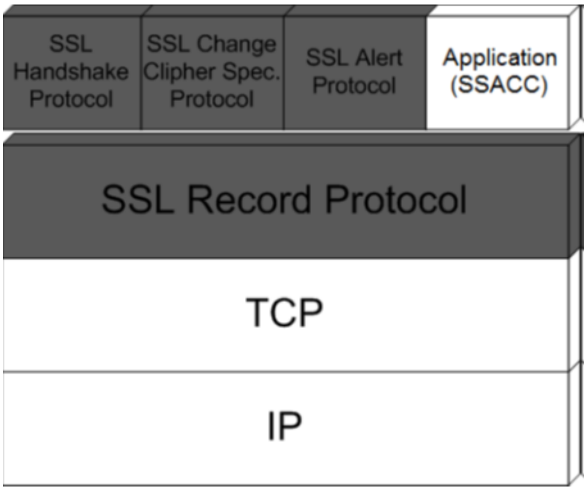

Figure 3 – Diagram of SSACC layers arranged with SSL [14].

## 5. Analyzes and Comparisons

The solution proposed by [9] does not maintain security in certain situations of the mobile device since some packets may be intercepted. Context information which are collected in the works [9], [10], [11] and [13] are not determined by Fuzzy algorithms as in [12] which uses a quantitative estimation and unambiguous way of its interpretation. The use of SSL proposed by [13] is a standardized technology that ensures the integrity, confidentiality, authenticity and non-repudiation when set up correctly. In work [11], it provides an adequate level of security that depends on the degree of cryptographic confidentiality of the algorithm and the mobile device behavior, since the resources are very important for ergonomics and device security. The scheme [10] learns from the vulnerabilities that surrounds it and it has a table that is feedback to each new situation, and it is associated with the most appropriate safety function.

Table II shows a comparison between the adaptive security mechanisms for mobile devices presented in section 4. This comparison takes into account the time of adaptation, the use of security levels, collecting of context information, the context of representation through Fuzzy algorithms, evaluation of the encryption algorithm and the use of SSL

Table II
Adaptive security mechanisms for mobile computing

| Approaches Proposed | Dynamic adaptation at runtime | Security level | Collecting context information | Fuzzy | Evaluator of cryptographic algorithms | SSL use |
|---|---|---|---|---|---|---|
| [9] | x | x | x | | | x |
| [10] | x | | x | | | |
| [11] | x | x | x | | x | |
| [12] | x | x | x | x | | |
| [13] | x | x | x | | x | x |

## 6. Conclusion

In this paper we present some of the major existing works on adaptive security mechanisms for mobile computing. The main advantage of using adaptive mechanisms in mobile computing is to save resources of mobile devices providing security to information through integrity authentication and confidentiality and thus preventing changes and unauthorized access to user data.

A possible extension to the above work is to integrate the best solutions in a single facility. To achieve this goal, we can provide a component that implements the standardized SSL technology to provide a secure channel of communication, a Fuzzy context analyzer to set the state of the mobile device and the environment that is connected, and an evaluation system of cryptographic algorithms appropriate to the context of decision making.

## Acknowledgments

Financial support of CAPES and FAPEMA are gratefully acknowledged.

## References

[1] Satyanarayanan, M. (2001). Pervasive computing: Vision and challenges. *Personal Communications, IEEE*, *8*(4), 10-17.

[2] Leeuwen, J. (1990). *Handbook of theoretical computer science: algorithms and complexity* (Vol. 1). Elsevier.

[3] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[4] Jiang, W., Guo, Z., Ma, Y., & Sang, N. (2013). Measurement-based research on cryptographic algorithms for embedded real-time systems. *Journal of Systems Architecture*, *59*(10), 1394-1404.

[5] Qi, H., & Gani, A. (2012, May). Research on mobile cloud computing: Review, trend and perspectives. In *Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on* (pp. 195-202). ieee.

[6] Gupta, S. K. S., & Srimani, P. K. (2000). Experience in teaching a graduate course in mobile computing. In *Frontiers in Education Conference, 2000. FIE 2000. 30th Annual* (Vol. 2, pp. S1C-6). IEEE.

[7] Gartner. "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014".

[8] Alliance, C. (2012). Security Guidance for Critical Areas of Mobile Computing, V1.0. *Cloud Security Alliance*.

[9] Pirmez, M., Pirmez, L., da Costa Carmo, L. F. R., Delicato, F. C., Pires, P. F., & de Sousa, E. B. (2008). Prometheus: Um Serviço de Segurança Adaptativa. *SBSEG2008, Gramado, RS (to appear)*.

[10] An, G., Bae, G., Kim, K., & Seo, D. (2009, December). Context-aware dynamic security configuration for mobile communication device. In *New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on* (pp. 1-5). IEEE.

[11] Cirqueira, A. C., Andrade, R. M., & de Castro, M. F. (2011). Um mecanismo de segurança com adaptação dinâmica em tempo de execução para dispositivos móveis. *Seminário Integrado de Software e Hardware*, 1337-1351.

[12] Lee, H., & Chung, M. (2011, October). Context-Aware Security model for Social Network Service. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*(pp. 144-151). IEEE.

[13] Moraes, R. U. M. (2014). *Ssacc - serviço de segurança para autenticação ciente do contexto: para dispositivos móveis no paradigma da computação em nuvem*. Master's thesis, UNIVERSIDADE FEDERAL DO MARANHÃO.

[14] Elgamal, T., & Hickman, K. E. (1998). *U.S. Patent No. 5,825,890*. Washington, DC: U.S. Patent and Trademark Office.

[15] Kurose , J. F., Ross, K. W., & Marques, A. S. (2003). *Redes de Computadores e a Internet: Uma nova abordagem*, volume 1. Addison Wesley.

[16] Oreizy, P., Medvidovic, N., & Taylor, R. N. (2008, May). Runtime software adaptation: framework, approaches, and styles. In *Companion of the 30th international conference on Software engineering* (pp. 899-910). ACM.

## Authors' Biography:

**CláudioManoel Pereira Aroucha** received the B.S. degree in Computer Science from Federal University of Maranhão (UFMA) in 2012. He is now coursing the MSc degree in Computer Science, at the Federal University of Maranhão. His research interests is Network Security.

**Zair Abdelouahab** received his BSc, MSc and Ph.D degrees in Computer Science from University of Setif (Algeria in 1985), Glasgow University (UK in 1988) and Leeds University (UK in 1993) respectively. He is now a professor of Computer Science at the Federal University of Maranhão (UFMA) in Brazil. His research interests include distributed systems, Security Networks, and requirement and software Engineering.