Extended Abstract: an Adoptable Multi-Level Security based on different Algorithms Key Sizes for Mobile Devices

Abdullah Almuhaideb, Phu Dung Le, and Bala Srinivasan

Faculty of Information Technology, Monash University, Australia
Amalm3@student.monash.edu.au,{Phu.Dung.Le, Bala.Srinivasan}@infotech.monash.edu.au

Abstract

The limitations of mobile devices (MD) increase the gap between security and performance and this gap increases with the growing heterogeneity of the computing environment. The aim of this paper is to identify research challenges in MD security and to propose a practical solution to maintain the balance between security and performance to secure mobile communication. We propose an Adaptable Algorithm-Key Size (AAKS) architecture that adds more flexibility to security protocols; hence it can better satisfy diverse security requirements in different application scenarios, especially for emerging mobile applications.

Keywords: security architecture, security protocols, selective security, sensitive information, mobile security.

1 Introduction

Motivation. The development of mobile devices (MD) has grown significantly over the last decade from a simple mobile phone to a pocket size computing device with the capability to access the Internet via various wireless systems such as Wi-Fi and 3.5G networks. The increase in MD capability (processing power, memory, storage) as well as the introduction of wireless systems (Bluetooth, Wi-Fi, WiMAX, 3.5G) open new opportunities for the next generation of mobile services such as mobile Internet, m-commerce and m-government. Furthermore, the future wireless system 4G network carries more promises for a WWWW (World Wide Wireless Web) with a fully IP-based integrated system at a higher data rate (Frattasi, Fathi, Fitzek, Prasad, & Katz, 2006; Kim & Prasad, 2006). However, the security of MD still involves a lot of concerns and issues that need to be addressed in order to speed up the development of mobile services.

Problem Statement. Most of the problems in mobile security relate to applying the same security techniques of the fixed environment without taking into account the mobile environment limitations. This paper attempts to address two drawbacks in security protocols that should be considered in order to achieve a better security performance in general and for mobile computing in particular. First limitation is the lack of providing sufficient capability information during the negotiation phase. Hence, some security protocols do not take the MD capabilities and other important factors into account in making decisions for the appropriate cipher suites(Song, Beznosov, & Leung, 2006). MD performance capabilities differ significantly from desktop PCs in terms of power supply, computational ability, memory capacity and other features introducing new challenges between these heterogenic devices. The battery capacity is considered the most critical issue that limits the development of MD as it is growing far slower than that of the CPU (Hirani, 2003; Potlapally, Ravi, Raghunathan, & Jha, 2003). Thus, there should be careful consideration in applying additional security processing as it can have a significant impact on MD battery life. Another issue under this category is the low processing and memory capability of MD compared to the security processing requirements (Daswani & Boneh, 1999; Gupta & Gupta, 2002). For instance, a PalmIIIx phone takes 3.4 minutes to complete 512-bit RSA key generation, 7 seconds to complete digital signature generation and can complete (single) DES encryption at only 13 kbps even if the CPU is entirely dedicated to security processing (Daswani & Boneh, 1999). A number of efforts have been made to improve MD security performance by either making the wireless security protocols and their adopted cryptographic algorithms lightweight, or by enhancing the security processing capability of the MD processor

(Ravi, Raghunathan, & Potlapally, 2002). The next issue is the network heterogeneity which is related to the increasing number of wire and wireless access network technologies (e.g. Ethernet, Gigabit Ethernet, UMTS, WiMAX, Wi-Fi, and Bluetooth). These heterogeneous networks vary greatly in terms of coverage, data rate, latency and rate loss (Frattasi, et al., 2006).

The second limitation is the lack of selective security consuming the limited resources of mobile devices. The popular security protocols such as IPSec and SSL do not support different levels of security according to a degree of information sensitivity(Portmann & Seneviratne, 2001). They either provide strong information security or none at all. In practice not all information is confidential. However when applying security, it is still encrypted with the same level of confidentiality using single cipher suite such as the case in an SSL session(Song, et al., 2006). For example, a web page for online banking contains confidential information including account numbers and balances; however, other parts of the web page, including HTML tags, JavaScript/Java code, images and advertisements are not confidential. A further examination of the previous example found (Song, et al., 2006) that only around 4% of the data needing both integrity and confidentiality protection while the rest requires just integrity. As the experiment shows, CPU savings could be up to 37% in a case when 96% of non-confidential data is provided with only data integrity and the remaining 4% of confidential data encrypted with adequate integrity and confidentiality protection leading to a battery-life saving (Song, et al., 2006). As a result, there should be support for selective multi level protection to provide better security performance.

Related Work and Our Contributions. In previous research there are a number of approaches to address security protocols problems (Portmann & Seneviratne, 2001; Song, et al., 2006; Sung Woo Tak, 2003). However, none of these approaches addresses the MD security protocols issues adequately either because they have not taken the network and device capability into account or they are restricted to specific protocol such as SSL.

The main contribution of our work is the possible solution of maintaining the balance between security and performance to secure mobile communication. The proposed AAKS architecture provides a support for security protocols in selecting the appropriate algorithm key sizes based on various levels of performance and security. Our approach can be integrated to security protocols to provide an efficient and secure mobile communication. The process of selecting the suitable key size is based on two main classifications. The first classification is based on four information security levels which support diverse security levels according to a degree of information sensitivity. Every information sensitivity level is defined by the approach policy indicating the type of information and the range of security tolerated.

The second classification is based on MD capability performance. This classification is divided into three independent attributes of performance, namely processing-memory capacity, power supply and communication system. The result of this process is the selection of the appropriate algorithm key size for every information security level taking in to account the available MD and network resources. The proposed technique meets strong security requirements for more sensitive information while trading off security for better performance for less critical information.

2 The Proposed Technique

In this section the proposed Adaptable Algorithm-Key Size (AAKS) architecture and its components will be described. The Architecture covers general concepts, security requirements, definitions and mechanisms defining AAKS approach. As the figure below shows (Fig.1), the AAKS architecture consists of two main blocks. The first block is the approach operation engine which contains two core components, namely Capability Performance Levels and Message Security Levels. The second block is the customisation and maintenance engine which contains two components - Policy and Key Management.

In the AAKS architecture, the first block supports the selection of the suitable algorithm which is based on the availability of the algorithm on both sides. The decision of the most appropriate algorithms and their key size is based on capability performance level and the degree of information sensitivity level. While the second block supports the first block through both policy management (which customises the approach and defines its configuration) and key management, which deals with storing keys and maintaining them. Our approach is thus particularly effective to achieve a flexible selection of the appropriate algorithms key size to meet the objective of a balance between efficiency and protection.

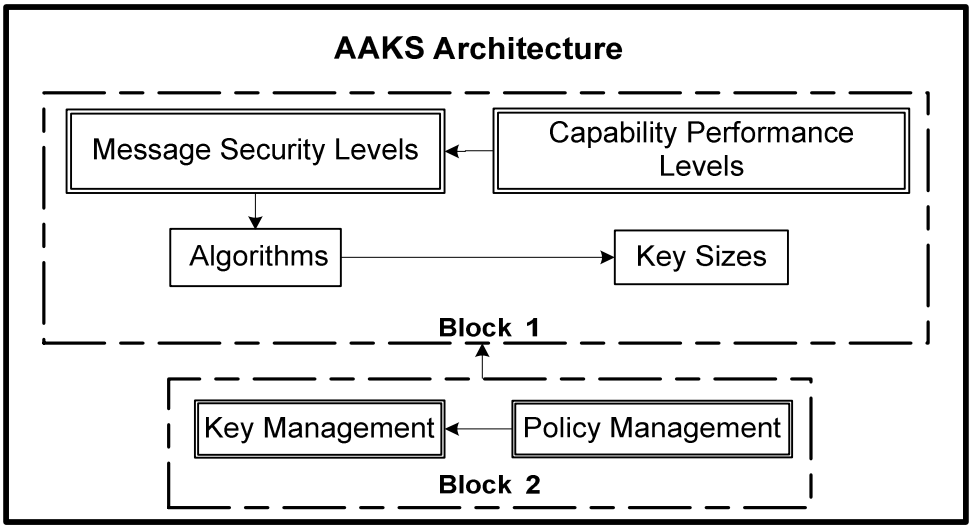

Fig. 1. Adaptable Algorithm-Key Size (AAKS) architecture.

2.1 Capability performance levels

The device and network capability performance levels are defined and customised by a set of policies. The goal of this component is to provide a flexible security system with a variety of performance levels that can deal with different MD and network capabilities. The figure below (Fig.2) illustrates how the capability performance level mechanism operates in order to select the key size based on seven performance levels (0-6). The system is based on three main categories called CPU-RAM, Power Supply and Communication system which have been used for capability classification. Under every main category there are three classification levels called High, Medium and Low with a weight of two, one and zero respectively. Calculating the performance level by adding up the three capability weights gives the performance level of the MD which can be used to select the appropriate key size. The seven Performance levels is in a scale of zero to six, where zero represents the lowest and six the highest performance. These capabilities will be described in more details below.

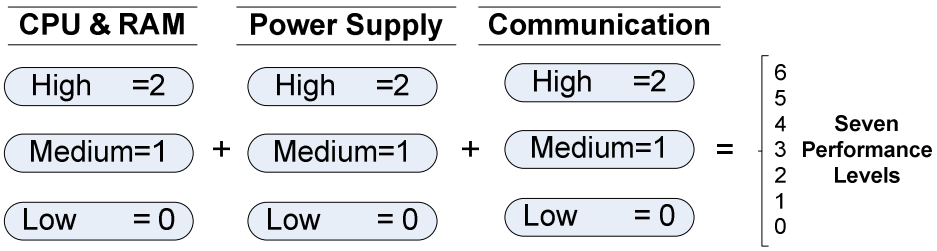

Fig. 2. Device and Network Capability performance levels classification.

Category 1: Processing Power and Memory Capacity. One of the MD challenges is the processing power and memory capacity gap, classifying MD based on their processing speed gives more control of the gap and a better choice for the suitable key size for that device.

Category 2: Power Supply. In terms of battery gap challenge, the power supply of an MD will be classified in three categories based on the amount of power left in the device. For instance, the maximum power supply is when the device is recharging while the least is when there is less than one hour left for talk time.

Category 3: Communication System. To address the mobile network challenge using different wireless systems such as WLAN and GSM, the communication medium can be categorized on three levels based on data rate, latency and error rate. For example, the faster one such as WiMAX will be at the high performance level. While the slower one (3G) will be in the Low performance level.

In summary, for every device capability there are three category levels. Knowing these levels will result in knowing the performance level of the MD which leads to the appropriate key size for that device. This classification can be applied to various mobile handset applications.

2.2 Message security levels

This section defines four message security levels, named none critical, least critical, critical and most critical. The most critical level represents the highest sensitive information; while none critical level contains the least significant information to the system security. At the application layer, the decision can be made as to what message is sensitive and what is not. Every information security level has to select the security degree out of seven security levels based on MD capabilities. In these security levels, they define the appropriate algorithm key sizes based on the range of security tolerated. In our approach, the significance of the information in the message is linked to key size. Therefore, when the message security level increases the key size increases also to provide an efficient assurance to the information and the system. The table below summarizes these levels.

Security Level	Description
Most Critical	Highest level of sensitivity. Strong security should take place to stop loss of money or information. Strong authentication, confidentiality and integrity required.
Critical	Moderate level of information sensitivity. Medium level of authentication, confidentiality and integrity required
Least Critical	Very low, but still requiring some protection. Low level of authentication, confidentiality and integrity is needed.
None Critical	Information in this level is not critical to the system and will not cause loss of money or data in case of active of passive attacks. Therefore, only information integrity is needed.

Table 1. Message (Information) security levels classification.

This mechanisem will result in distinctive keys in various sizes providing appropriate security for different information sensitivity levels without overprotecting some information or underprotecting others with a balance between security and performance (Fig.3).

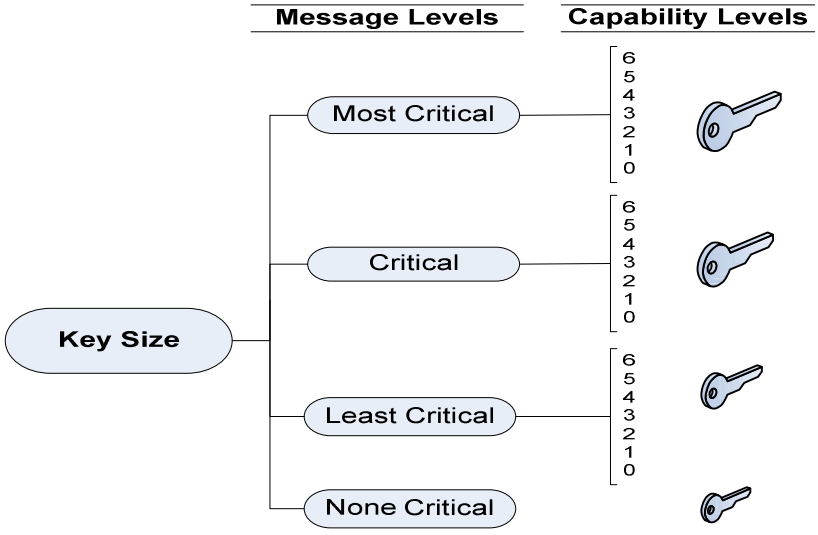

Fig. 3. Different Keys Sizes for different messages and capability levels.

3 Conclusion

We argued in this paper the need to adopt flexible, multi-level security based on different algorithm key sizes, tied specifically to the information sensitivity and capability status in a mobile environment. We proposed the AAKS approach as a practical solution to maintain the balance between protection and efficiency to secure mobile communication. As the information sensitivity levels are different, the security of this information should be different too. The AAKS architecture provides different levels of performance and security to adapt the MD heterogeneous environment. Our future work includes further research on AAKS to increase its security and usability.

References

Daswani, N, & Boneh, D (1999). Experimenting with Electronic Commerce on the PalmPilot. *Lecture Notes in Computer Science, 1648/1999*, 1-16.

Frattasi, S, Fathi, H, Fitzek, FHP, Prasad, R, & Katz, MD (2006). Defining 4G technology from the user's perspective. *Network, IEEE, 20*(1), 35-41.

Gupta, V, & Gupta, S (2002). *Experiments in wireless Internet security.* Paper presented at the IEEE Wireless Communications and Networking Conference, 2002. WCNC2002. , Orlando, FL, USA.

Hirani, SA (2003). *Energy Consumption of Encryption Schemes in Wireless Devices.* University of Pittsburgh, Pittsburgh, Pennsylvania, USA.

Kim, Young Kyun, & Prasad, Ramjee (2006). *4G roadmap and emerging communication technologies*. Boston, MA: Artech House.

Portmann, M., & Seneviratne, A. (2001). *Selective security for TLS.* Paper presented at the Ninth IEEE International Conference on Networks (ICON'01), Bangkok, Thailand.

Potlapally, Nachiketh R., Ravi, Srivaths, Raghunathan, Anand, & Jha, Niraj K. (2003). *Analyzing the energy consumption of security protocols*. Paper presented at the Proceedings of the 2003 international symposium on Low power electronics and design.

Ravi, S, Raghunathan, A, & Potlapally, N (2002). *Securing wireless data: System architecture challenges*.

Song, Yong, Beznosov, K, & Leung, VCM (2006). Multiple-channel security architecture and its implementation over SSL. *EURASIP Journal on Wireless Communications and Networking, 2006*(2), 1–14.

Sung Woo Tak, Eun Kyo Park (2003). Adaptive secure software architecture for electronic commerce. *Software: Practice and Experience, 33*(14), 1343-1357.