Journal of Network and Computer Applications 33 (2010) 569–587

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Adaptive security protocol selection for mobile computing☆

Bruno P.S. Rocha [a,b], Daniel N.O. Costa [b], Rande A. Moreira [b], Cristiano G. Rezende [b,c], Antonio A.F. Loureiro [b,*], Azzedine Boukerche [c]

[a] *Eindhoven University of Technology, The Netherlands*
[b] *Federal University of Minas Gerais, Brazil*
[c] *PARADISE Research Laboratory, University of Ottawa, Canada*

ARTICLE INFO

Article history:
Received 14 November 2009
Received in revised form
13 March 2010
Accepted 25 March 2010

Keywords:
Mobile computing
Autonomous computing
Adaptive computing
Security
Data semantics

ABSTRACT

The mobile computing paradigm has introduced new problems for application developers. Challenges include heterogeneity of hardware, software, and communication protocols, variability of resource limitations and varying wireless channel quality. In this scenario, security becomes a major concern for mobile users and applications. Security requirements for each application are different, as well as the hardware capabilities of each device. To make things worse, wireless medium conditions may change dramatically with time, incurring great impact on performance and QoS guarantees for the application. Currently, most of the security solutions for mobile devices use a static set of algorithms and protocols for services such as cryptography and hashes.

In this work we propose a security service, which works as a middleware, with the ability to dynamically change the security protocols used between two peers. These changes can occur based on variations on wireless medium parameters and system resource usage, available hardware resources, application-defined QoS metrics, and desired data "security levels". We compare our solution to some widespread static security protocols, demonstrate how our middleware is able to adapt itself over different conditions of medium and system, and how it can provide a performance gain in the execution of cryptographic primitives, through the use of data semantics.

1. Introduction

The tremendous advances in wireless data communication and mobile computing have created a new computing paradigm that promises to provide services anytime and anywhere for everyone. Such an environment enables users to access a wide range of services and applications using a large variety of mobile and ubiquitous devices. Voice and video streaming, file transfers, notification and localization are some examples of applications developed for this environment.

In this diverse, dynamic and complex scenario, it is not appropriate to create static specifications for ubiquitous applications. Designers and developers should consider, for instance, hardware limitations, data communication properties, QoS requirements, and security demands when designing services for pervasive environments. Unfortunately, all this information is not promptly available beforehand what leads to a very difficult and challenging design. In any wireless technology, risks are inherent. Some of them are similar to those of wired networks, some are more severe due to the wireless communication, whereas others are new. Probably the most important source of risks in wireless networks is the data communication medium, which is easily accessible to intruders. The loss of confidentiality and integrity, and the threat of denial of service (DoS) attacks are risks common to wireless communications. Unauthorized users may gain access to the system and information, corrupt data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use legitimate resources to launch attacks on other networks.

Given all these potential problems, the specification of security protocols becomes a major concern. From the system point-of-view, each application may not only have different security needs, but also different QoS demands. Furthermore the application may be running on a hardware platform with different capabilities and communication protocols. Some of the current protocols for wireless networks, such as IEEE 802.11 and Bluetooth, propose solutions which are either incomplete or flawed (Karygiannis and Owens, 2002), besides been focused only on the link layer of the network stack. Even though updates have been made to improve native security of these protocols, in

☆Funded by BZG.

* Corresponding author.
E-mail address: loureiro@dcc.ufmg.br (A.A. Loureiro).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.028

practice there is a great heterogeneity on which of these mechanisms are actually used, easily allowing misconfiguration. For instance, even the flawed WEP can still be found in operation (RSA Security, 2007).[1]

A common solution to this problem is the adoption of application-level security mechanisms originally developed for desktop computers and Internet applications. This approach is not always successful, as the challenges posed by mobile devices often create a "gap" between requirements and hardware capacities (Ravi et al., 2002). Besides, security mechanisms designed for typical Internet applications usually do not consider the distinct properties of the wireless medium, which are important information sources regarding the local environment (Li et al., 2006).

In order to overcome problems related to heterogeneity of hardware, software, and communication, it has become common the development of a mobile computing middleware. A middleware is a software layer that intermediates the interactions between applications and lower-level system directives, such as data communication. Its role is to provide the application with directives for transparent interaction with the underlying distributed system (Capra et al., 2001; Rocha et al., 2007).

In this work, we propose a context-aware security middleware that dynamically changes the security protocols used between a pair of peer-entities according to a set of variables. Our service, named **ASecMid**, monitors some parameters related to the wireless medium conditions, system resource usage, hardware capabilities, application-defined QoS metrics, and desired security services. Our solution transparently chooses the best security protocol for each transmission, from a large collection of protocols, according to the parameters monitored. The application accesses the middleware as a standard network socket, unaware of security protocols being applied. Besides, the application can supply a semantic description of the data to be transmitted, so that the sensitivity of each piece of data can be determined individually. The main purpose of this work is to bridge the gap between underlying network information, protocols, and primitives and the high-level service oriented software. The idea is not to develop new security algorithms, but use existing and consolidated protocols as efficiently as possible, based on the "Adequate Protection Principle" (Pfleeger and Pfleeger, 2006), which states that adequate security should be applied to each data type and context, independently. Our results show the effectiveness of our solution.

The main motivations for this work are as follows. First, there is an important aspect related to mobile computing security: the tradeoff between providing security and maintaining communication quality and system performance. Our service has the goal of working with this tradeoff, keeping the balance between security and performance according to the specifications defined by the supporting application. Second, the development of the service in the form of a middleware presents a benefit in providing a single security layer for different contexts of hardware, software and communication. Third, the characteristics of the medium where a device is inserted often are powerful sources of information (Li et al., 2006). With that, the utilization of parameters from different sources (e.g., application requirements, data semantics, wireless medium, system resources) is an interesting approach to create an adaptive and context-aware mechanism. Finally, the possibility of using data semantics to determine different sensibility levels of the data being transmitted can be interesting due to the fact that strong security mechanisms can be employed only where they are actually needed, providing an expected performance gain over utilizing the same mechanism for the whole data.

The main contributions of this work are:

- Formal definition of the problem of selecting security protocols based on security (cryptographic strength) and resource-usage (e.g., processing, memory and network overhead) metrics.
- Proposal of a methodology for treating the problem, divided in stages and also with the goal of not incurring considerable system overhead.
- Development of a reference implementation of the proposed mechanism, in the form of a middleware, ready to be executed on Linux environments and with portable source code.
- Evaluation of the solution concerning its adaptability regarding changes of the execution context (system resources and wireless medium conditions).
- Evaluation of the solution concerning its performance gain when a semantic description of the data being transferred is made available.

This paper is organized as follows. In Section 2, we present the related work. In Section 3, we discuss the environment model we considered, as well as definitions used throughout this paper, including a formal definition of the problem to be treated. We discuss how to represent and deal with semantic data definitions in Section 4. The solution itself is presented in Section 5, including the system design and architecture, and the decision algorithms. Our experimental results are discussed in Section 6. Finally, in Section 7 we present our conclusions and future work.

2. Related work

Standard security mechanisms for wireless networks have been broadly studied, with its flaws discussed in literature. Patiyoot and Shepherd (1999) discuss the main cryptographic techniques for wireless networks, including IEEE 802.11, wireless ATM, GSM, UMTS and others. Karygiannis and Owens (2002) present a detailed study of the flaws and vulnerabilities of the native security services provided by IEEE 802.11 and Bluetooth. Bhagyavati et al. (2004) analyze security techniques for the IEE 802.11 protocol and its variations (802.11i and 802.1X family). Denko et al. (2009) discuss, among other aspects, security issues in the design of a middleware for mobile ad hoc networks, and TalebiFard et al. (2010) discuss security and privacy in next generation IP-based networks, including wireless networks.

Some studies found in the literature have identified special approaches to promote security on wireless environments, pointing out challenges to achieve them. Some of these challenges include the problem of restricted processing capacity of mobile devices, as pointed out by Ravi et al. (2002) and Botha et al. (2009). Specific challenges regarding the IEEE 802.11 protocol are discussed by Arbaugh (2003) and Potter (2006), the latter focusing on hotspots.

Proposals have been made to provide security considering mobile and wireless properties. Soliman and Omari (2005) propose a cryptographic system aimed to the mobile domain, using flow cipher algorithms. Li et al. (2006) propose a system that uses radio signal properties for authentication and confidentiality on the physical layer of the network stack, outlining the necessity to work with cross-layer design in this scenario. Dong et al. (2009) propose two general frameworks that

[1] For an example, as of October 2009, US-based Verizon FiOS internet provider installs home-based internet routers with WEP security by default.