Chapter IV
Policy-Based Security for M-Commerce Networks

Wassim Itani
American University of Beirut, Lebanon

Ayman Kayssi
American University of Beirut, Lebanon

Ali Chehab
American University of Beirut, Lebanon

ABSTRACT

In this chapter we present an overview of a general policy-based security architecture for securing the confidentiality, authenticity, and integrity of enterprise mobile commerce (m-commerce) data. A policy-based architecture protects data based on content and sensitivity and highly surpasses the performance of bulk encryption protocols such as secure sockets layer (SSL) and transport layer security (TLS) by utilizing a customizable, policy-driven approach. This approach makes use of the structure of enterprise data objects (Web pages, relational database entities, directory hierarchies, log files, etc…) to provide flexible, multi-level, and fine-grained encryption and hashing methodologies. This makes policy-based security protocols a very efficient choice for operation in wireless m-commerce environments characterized by low-bandwidth networks and supporting limited-resource devices with low memory, battery, and processing power.

INTRODUCTION

With the emergence of the wireless application protocol (WAP Forum, 2000) in 1998, which provided users of mobile devices with an optimized wireless protocol to access the Internet and to browse specific Web content, and with the introduction of specialized wireless programming models such as Java 2 Mobile Edition (J2ME) (Lawton, 2002), the .Net Compact Framework (Neable, 2002), and the Binary Runtime Environment for Wireless (QUALCOMM Incorp., 2004), businesses started accepting a new set of clients represented in cell phones, two-way pagers, PDAs,

and palmtops. Enterprise application software is witnessing a rapid proliferation and an increased user base supported by the ubiquity, accessibility, and flexibility provided by wireless networking and mobile computing and communication (Shim, Varshney, Dekleva, & Knoerzer, 2006).

New m-commerce applications are becoming possible (Smith, 2006) and many existing e-commerce applications can be modified to fit into the mobile environment. M-commerce offers several advantages for today's businesses by allowing them to reach existing and new clients through new and extended channels, such as mobile communications and wireless channels. It also allows companies to offer new and enhanced applications and services that are unique to the wireless world. Using a mobile device, the user can interact with m-commerce applications in real time, anywhere and at any time, without being bound to one location. In the same sense, m-commerce vendors and application service providers can access their users through location or positioning systems, such as global positioning systems (GPS), which could lead to a suite of valuable location-based applications and services. In addition and due to the fact that mobile devices are not usually shared among users, huge opportunities exist for developing personalized applications and services that can be offered by application providers to individual users.

Although the adoption of m-commerce services is showing some acceleration, great concerns are raised about the security of the sensitive data over the wireless links where confidentiality, authenticity, and integrity are potentially compromised by unauthorized access. Mobile applications have special and unique requirements compared to Internet applications. Usually, mobile applications operate over low bandwidth networks with high latency and frequent disconnections using devices that vary greatly in capabilities and resources. For these reasons, the protocols used in securing mobile enterprise applications have to be designed specifically for operation in wireless environments and must address the needs and requirements of a large variety of devices which are, in their majority, severely constrained in terms of processor speed, memory resources, storage capacity, and battery power. This diversity makes the implementation of a unique security standard that encompasses the whole device range infeasible. A least-common denominator security standard that targets devices with limited memory and slow processors would be unfair for powerful devices and would not meet their security requirements, and in the same sense, a security standard that addresses high-end devices would neither fit nor perform efficiently on limited-resource devices. What is needed is a security protocol that can be customized and configured to perform the security operations flexibly, taking into consideration the memory capabilities and the processing power of the device, the wireless network latency, and the specific requirements of the enterprise application. This ensures the efficient operation of the same application on a wide range of devices and wireless networks. Moreover, this protocol must be extensible, scalable, and capable of evolving to meet new challenges and to adapt to new application requirements.

In this chapter we present an overview of a general, policy-based security architecture for securing the confidentiality, authenticity, and integrity of enterprise m-commerce data. A policy-based architecture protects data based on content and sensitivity and highly surpasses the performance of bulk encryption protocols such as the SSL protocol (Freier, Karlton, & Kocher, 1996) and the TLS protocol (Dierks & Allen, 1997) by utilizing a customizable, policy-driven approach. This approach makes use of the structure of enterprise data objects (Web pages, relational database entities, directory hierarchies, log files, etc…) to provide flexible, multi-level, and fine-grained encryption and hashing methodologies. This makes policy-based security protocols a