IGI PUBLISHING **ITB14875**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao © 2007, IGI Global**

Chapter V

A Survey of Key Generation for Secure Multicast Communication Protocols

Win Aye, Multimedia University, Malaysia

Mohammad Umar Siddiqi, International Islamic University Malaysia, Malaysia

Abstract

Multicast communication demands scalable security solutions for group communication infrastructure. Secure multicast is one such solution that achieves the efficiency of multicast data delivery. Key generation plays an important role in enforcing secure and efficient key distribution. This chapter addresses the issues focused on the area of key generation on key management cryptographic algorithms that support security requirements in multicast group communications. These issues are of importance to application developers wishing to implement security services for their multicast applications. The three main classes, centralized, decentralized, and distributed architectures, are investigated and analyzed here and an insight given to their features and goals. The area of group key generation is then surveyed and proposed solutions are classified according to the efficiency of the cryptographic algorithms and multicast security requirements. We also outline the open problems in this area.

Introduction

Today, e-business applications provide critical links among businesses, customers, and business partners. Web services are rapidly becoming the enabling technology of today's e-business and e-commerce systems, and will soon transform the Web as it is now into a distributed computation and application framework. Web services security is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of security models and encryption technologies. Web services security is flexible and is designed to be used as the basis for the construction of a wide variety of security models including public key infrastructure (PKI).

Companies are turning to unify IP networks to connect employees, customers, vendors, strategic partners, and even competitors. They are creating a digital Web that redefines both business-to-business (B2B) and business-to-customer (B2C) relationships. The emphasis is on real time because the enterprise with the timeliest information has a competitive edge. It can be more responsive to customers, bring products to market faster, and create a value chain that works at Internet speeds.

Specifically, today's enterprises are looking for delivery of real-time information to customers and partners over the Internet, intranets, and extranets. The primary real-time infrastructure products that provide all these required services are publish/subscribe products. Leading publish/subscribe products are looking for most demanding real-time multicast applications such as stock exchanges, financial market data, multimedia content streaming, live news, distance learning, and software distribution.

Key generation is one of the important roles for secure key distribution of content distribution in multicast communication. Group communication can benefit from IP multicast to achieve scalable exchange of messages. Multicast communication as defined in Deering (1989) and Parkhurst (1999) is an efficient means of distributing data to a group of participants depicted in Figure 1. Efficiency is achieved because data packets need to be transmitted once and they traverse any link between two nodes only once, hence saving bandwidth. This contrasts with unicast-based group communications where the sender has to transmit *n copies* of the same packet.

Figure 1. Example of multicast transmission