Chapter 9
Identity-Based Encryption Protocol for Privacy and Authentication in Wireless Networks

Clifton Mulkey
Texas A&M University – Corpus Christi, USA

Dulal C. Kar
Texas A&M University – Corpus Christi, USA

ABSTRACT

Wireless networks are inherently insecure due to the fact that information on the network can be passively retrieved by an eavesdropper using off-the-shelf network hardware and free software applications. The most common solution for this vulnerability is the Wireless Protected Access (WPA) protocol. This protocol provides data encryption and access control for wireless networks. However, the WPA protocol contains drawbacks in its authentication mechanisms that can cause inconveniences for end users and performance degradation for the network. Furthermore, many of the authentication methods used with WPA are not friendly to small and resource-constrained wireless devices. This chapter presents the design of a new wireless security protocol for privacy and authentication using efficient Identity-Based Encryption (IBE) techniques. This protocol can be used to eliminate the need for a central authentication server for enterprise networks, as well as to provide the new feature of privacy without authentication for public wireless networks. This work also puts forth an analysis and validation of the new protocol, including security strength, storage overhead, communication overhead, and computational efficiency.

DOI: 10.4018/978-1-4666-4789-3.ch009
1. INTRODUCTION

From large corporations to street-corner coffee shops, wireless networks provide an important means of connectivity in today’s world. However, security in wireless communications is hindered by the fact that wireless media is by nature a broadcast media. Since wireless signals are carried on radio waves, any receiver within range can potentially intercept a message passed between a wireless access point and a client. In fact, free tools exist that allow users to listen to traffic in promiscuous mode, capturing any data that happens to come to the wireless network card (“Wireshark,” n.d.). Furthermore, this type of network sniffing is passive, and cannot be detected by intrusion detection systems that may be operating on the network.

Without encryption, a wireless eavesdropper can capture potentially sensitive information from other clients on the wireless network. Although some traffic is protected using application or session layer security protocols, there are still many plaintext messages that are sent across the wireless media. For example, email, instant message programs, and HTTP often send messages in plain text which can be captured easily. This inherent security risk on wireless networks is often mitigated today by using the Wireless Protected Access (WPA) protocol (Eaton, n.d.). WPA and its second revision, WPA2, both operate in the same manner, but with a different security strength (MacMichael, n.d.). The WPA protocol includes two authentication modes, WPA Pre-Shared Key (WPA-PSK) and WPA Extensible Authentication Protocol (WPA-EAP). Using WPA-PSK, a pre-shared key is required to gain access to the network, so that only authenticated users can connect to the access point. Though WPA-PSK has greatly improved wireless security, it still may not be a good solution for all scenarios. Since the WPA-PSK key is a symmetric key, it must be distributed to all users of the network. This may be infeasible for very large wireless networks. In addition, this creates a problem for networks that expect to have a large number of temporary users. Furthermore, any user that obtains the WPA-PSK network key may still be able to sniff traffic from other users on the network (MacMichael, n.d.). WPA-EAP provides a much stronger authentication method and does not require a pre-shared key among the access point and all clients. However, WPA-EAP requires a central authentication server and a persistent database with all authorized user credentials (MacMichael, n.d.). For this reason, it may not be suitable for small or single access point wireless networks. The reliance on a central server can also create a bottleneck or single point of failure for the network. In addition, WPA-EAP uses higher level public key protocols that may require certificate storage and exchange, as well as expensive encryption. Finally, for some wireless networks, such as in a coffee shop or airport, it may be desirable to have traffic confidentiality but not client authentication.

To address the issues with the WPA protocol, a novel protocol using a form of asymmetric cryptography known as Identity Based Encryption (IBE) is proposed. Asymmetric cryptography is needed to avoid the requirement for shared keys. More specifically, IBE is used because it eliminates the need for public key storage and certificate infrastructure. IBE can be used to securely share symmetric keys, which can later be used by AES symmetric encryption to establish secure channels. IBE key exchange methods can also be formulated in such a way to authenticate both the access point and the client. IBE uses Elliptic Curve Cryptography (ECC), which provides high cryptographic strength with a smaller amount of computation and smaller key size in comparison to traditional public key methods (Anoop, 2012; Kar, Ngo, & Mulkey, 2011). This provides for a