Chapter XLIV
Access Control in Wireless Local Area Networks:
Fast Authentication Schemes

Jahan Hassan
The University of Sydney, Australia

Björn Landfeldt
The University of Sydney, Australia

Albert Y. Zomaya
The University of Sydney, Australia

ABSTRACT

Wireless local area networks (WLAN) are rapidly becoming a core part of network access. Supporting user mobility, more specifically session continuation in changing network access points, is becoming an integral part of wireless network services. This is because of the popularity of emerging real-time streaming applications that can be commonly used when the user is mobile, such as voice-over-IP and Internet radio. However, mobility introduces a new set of problems in wireless environments because of handoffs between network access points (APs). The IEEE 802.11i security standard imposes an authentication delay long enough to hamper real-time applications. This chapter will provide a comprehensive study on fast authentication solutions found in the literature as well as the industry that address this problem. These proposals focus on solving the mentioned problem for intradomain handoff scenarios where the access points belong to the same administrative domain or provider. Interdomain roaming is also becoming common-place for wireless access. We need fast authentication solutions for these environments that are managed by independent administrative authorities. We detail such a solution that explores the use of local trust relationships to foster fast authentication.

INTRODUCTION

Wireless local area networks (WLAN) are rapidly becoming a core part of enterprise network access. The IEEE 802.11 standardization has lead to vendor interoperability and rapidly plummeting prices, making wireless access an economically tantalizing alternative to wired access. Currently, enterprise deployment incorporates support for mobility between access points (AP) as well as security and monitoring solutions. Mobility introduces a new set of problems, not present in a wired infrastructure, due to handoffs between network access points. The implications of frequent handoffs to different APs is that for communication security, the IEEE 802.11 standard requires that the mobile node (MN) has to undergo a full authentication process each time it wants to connect to a new AP. The recent security ratifications from the IEEE task group i (TGi) (IEEE 802.11i, 2004) defined several security remedies for WLANs in the standard IEEE802.11i. According to this standard, the complete (full) authentication process involves the use of 802.1X port-based access control architecture, and provides mechanisms for key management (IEEE 802.1X, 2001). An AAA server such as RADIUS (Rigney, Willats, Rubens, & Simpson, 2000; Rigney, Willats, & Calhoun, 2000) is to be used for authentication and key derivation. Following a successful authentication, the MN and the AP are to undertake a four-way handshake protocol for deriving various encryption keying material. Keying material derived in this way then is used in the encrypted (secure) communication sessions between an AP and the MN. Thus the four-way handshake, which does not involve the AAA server, is a *must* in each secure association of an MN to the AP and cannot be avoided.

However, the authentication process, suggested in the 802.11i ratifications using extensible authentication protocol (EAP) over transport layer security (TLS) can introduce significant handoff delays because it involves the exchange of a round of messages between the MN and the AAA server via the AP. It has been shown that a full EAP-TLS authentication (i.e., the full authentication) can take as long as *1.1* seconds (Mishra, Shin, & Arbaugh, 2004). The delay can only increase when the AAA server is located at the ISP's site, topologically far from the AP site. The longer the delay in handoffs, the longer the outage time experienced by applications. While this kind of delay is acceptable for applications with flexible response time requirements, emerging real-time applications, such as wireless voice-over-IP, have stringent delay requirements (Cisco IP phone). Thus, this kind of network delay and outages are detrimental for real-time applications, especially in frequent handoff scenarios, which hinders the success of wireless local networks to support such popular applications.

The aim of this chapter is, therefore, to provide readers with state-of-the-art knowledge on this significant issue, and solutions as found in the industry and literature. The mentioned issue arises from two directions: (1) intradomain handoffs and (2) interdomain handoffs. Thus solutions are needed for both. While various solutions have been mostly proposed for the first direction, we will show that interdomain, or interprovider handoffs are becoming a common place and need specific solutions that are different from the intradomain solutions because of the involvement of more than one administrative authority in the latter cases.

To reduce the handoff delays due to the exchanges of authentication messages when a MN hands off to a new AP (nAP), there have been several proposals from the industry and the research community. These solutions are targeted for providing fast access when changing APs belong to the same administrative network domain.

However, handoffs within a single domain might not always be the case. There are possible scenarios where different service providers need to collaborate to provide continuous connectivity to roaming users for supporting seamless services. In addition, IEEE 802.11 has lead to price levels suitable for the mass consumer market and small operators. This has caused an explosive trend in the deployment of residential gateways (RG) for home networking and wireless hotspots at city areas by various business owners and hotspot providers.

The capacity offered by these APs and residential gateways (RGs) at various sites may not