Chapter XLVI
Security and Privacy Approaches for Wireless Local and Metropolitan Area Networks (LANs & MANs)

Giorgos Kostopoulos
University of Patras, Greece

Nicolas Sklavos
Technological Educational Institute of Mesolonghi, Greece

Odysseas Koufopavlou
University of Patras, Greece

ABSTRACT

Wireless communications are becoming ubiquitous in homes, offices, and enterprises with the popular IEEE 802.11 wireless local area network (LAN) technology and the up-and-coming IEEE 802.16 wireless metropolitan area networks (MAN) technology. The wireless nature of communications defined in these standards makes it possible for an attacker to snoop on confidential communications or modify them to gain access to home or enterprise networks much more easily than with wired networks. Wireless devices generally try to reduce computation overhead to conserve power and communication overhead to conserve spectrum and battery power. Due to these considerations, the original security designs in wireless LANs and MANs used smaller keys, weak message integrity protocols, weak or one-way authentication protocols, and so forth. As wireless networks became popular, the security threats were also highlighted to caution users. A security protocol redesign followed first in wireless LANs and then in wireless MANs. This chapter discusses the security threats and requirements in wireless LANs and wireless MANs, with a discussion on what the original designs missed and how they were corrected in the new protocols. It highlights the features of the current wireless LAN and MAN security protocols and explains the caveats and discusses open issues. Our aim is to provide the reader with a single source of information on security threats and requirements, authentication technologies, security encapsulation, and key management protocols relevant to wireless LANs and MANs.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The topic of this chapter is the security of 802.11 wireless local area networks (WLANs) and of 802.16 wireless metropolitan area networks (WMANs). These networks are based on the IEEE standards belonging to the 802 family, which include the much-beloved Ethernet (802.3) that is common today in homes and offices. Although the development of the 802.11 technology and standards have been ongoing sine the late 1990s, grassroots adoption of "wireless Ethernet" only began in the 2000-2001 timeframe when access point (AP) devices became cheap enough for the home user to obtain.

The convenience of having wireless access to the IP Internet is self-evident. The value proposition in terms of employee productivity has been so compelling that many enterprises began also to introduce the technology into their corporate networks. This enterprise adoption, however, was prematurely halted when security flaws in the wired equivalency privacy (WEP) algorithm were discovered and published. Various temporary patches were then suggested in order to support existing enterprise investments in WLAN equipment, with the IPsec-VPN (e.g., over the wireless segment) as the most common approach. The IEEE standards community completed the revision of the security-related components of 802.11 in 2004, with conforming products scheduled to be shipped in 2005.

This chapter is not a user guide to specific WLAN or WMAN products, and intentionally avoids specific references to such products. It is also not a thesis on the various engineering solutions that could have been applied to solve the Wi-Fi security problem. Instead, the chapter attempts to explain what current approaches and solutions have been adopted, and why these were chosen.

The contents of the chapter are arranged in four parts, where each part groups together topics and issues that are closely related. These parts roughly cover the topics of WLAN authentication and authorization, WLAN security algorithms and protocols, security in WLAN roaming, and security in WMANs. These are described in more detail next.

BACKGROUND

Traditionally, the term *authentication* in the context of computer and network security concerns the ability of a verifier (or prover) entity to ascertain the correct *identity* of another entity claiming to be that identity. Thus, the aim of authentication is for one entity to prove its identity to another based on some *credentials* possessed by that first entity. Examples of credentials include passwords, digital certificates, or even physical keys. The outcome of an authentication process is typically binary, namely success or fail. The process is typically defined and implemented as one or more *protocols*.

The term *authorization* pertains to the rights, privileges, or permissions given to an authenticated entity in relation to some set of resources. In practice, authorization for an entity to take actions (e.g., access network, read files) is preconditioned on a successful authentication. The functions of authentication and authorization are often accompanied by *accounting* (or auditing), with the three loosely referred to as *AAA*.

The level of authorization assigned to an entity when it seeks access to resources is often tied to the type and strength of the authentication protocol used and the type of credential possessed by the authenticated entity. Hence, differing levels of assurance or certainty regarding the outcome of an authentication process can be gained by using different credentials and authentication protocols.

For example, when a password (as a credential) is used with a weak protocol (e.g., plaintext challenge-response), then a low or weak level assurance is obtained as both the credential and the authentication protocol are weak. In contrast, a strong credential such as a digital certificate when combined with a strong authentication protocol, such as SSL or transport layer security (TLS), achieves a higher level of assurance regarding the identity of the authenticated entity.

In today's complex computer and network systems, multiple credentials might be needed for an entity to access multiple resources, each access instance of which may be governed by separate sets of privileges. Thus, often the term *layer* (of

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-privacy-approaches-wireless-local/22081

Related Content

The Need for Multi-Disciplinary Approaches and Multi-Level Knowledge for Cybersecurity Professionals

Eleni Berki, Juri Valtanen, Sunil Chaudharyand Linfeng Li (2018). *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals (pp. 72-94).*

www.irma-international.org/chapter/the-need-for-multi-disciplinary-approaches-and-multi-level-knowledge-for-cybersecurity-professionals/198252

Detecting the Risk of Online Harms on People With Social Orientation Impairments: The Role of Automated Affective Content Screening of Neuro-Response Plasticity

Jonathan Bishopand Darren Bellenger (2021). *Handbook of Research on Cyber Crime and Information Privacy (pp. 739-753).*

www.irma-international.org/chapter/detecting-the-risk-of-online-harms-on-people-with-social-orientation-impairments/261753

Privacy-Preserving Transactions Protocol Using Mobile Agents with Mutual Authentication

Song Han, Vidyasagar Potdar, Elizabeth Changand Tharam Dillon (2007). *International Journal of Information Security and Privacy (pp. 35-46).*

www.irma-international.org/article/privacy-preserving-transactions-protocol-using/2455

Paradise to Peril: Humanistic Uncertainty during Hurricanes Isaac and Katrina

Scheljert Denas (2013). *International Journal of Risk and Contingency Management (pp. 67-70).*

www.irma-international.org/article/paradise-peril-humanistic-uncertainty-during/76658

Deep Learning-Based Cryptanalysis of a Simplified AES Cipher

Hicham Grari, Khalid Zine-Dine, Khalid Zine-Dine, Ahmed Azouaouiand Siham Lamzabi (2022). *International Journal of Information Security and Privacy (pp. 1-16).*

www.irma-international.org/article/deep-learning-based-cryptanalysis-of-a-simplified-aes-cipher/300325