CROSS-DOMAIN MOBILITY-ADAPTIVE AUTHENTICATION

Hahnsang Kim
INRIA, Sophia Antipolis, France
E-mail: hahnsang.kim@inria.fr

Kang G. Shin
Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, U.S.A.
E-mail: kgshin@eecs.umich.edu

When mobile users with on-going sessions cross the domain boundary, their re-authentication affects significantly the inter-domain handoff latency as each inter-domain handoff requires remote contact with the home authentication server across domains, making it difficult to employ existing authentication protocols as they are. This chapter focuses on cross-domain authentication over wireless local area networks (WLANs) that minimizes the need for remote contact/access. We analyze the security requirements suggested by the IEEE 802.11i authentication standard, and consider additional requirements to help reduce the authentication latency without compromising the level of security. We propose an enhanced protocol called the Mobility-adjusted Authentication Protocol (MAP) that performs mutual authentication and hierarchical key derivation with minimal handshakes, relying on symmetric cryptographic functions. We also introduce security context routers (SCRs) that handle security context in conjunction with MAP, eliminating the need for continual remote contact with the home authentication server. In contrast to Kerberos that favors inter-domain authentication, MAP achieves a 26% reduction of authentication latency without degrading the level of security.

1. INTRODUCTION

Time-sensitive applications, such as Voice over IP (VoIP) or video streaming, are now possible over wireless local area networks (WLANs), such as those based on the IEEE 802.11 Standard [4], thanks to their high bandwidth. WLAN technologies also allow
the mobiles to roam within public/corporate buildings or university campuses. Furthermore, we anticipate that mobile users might cross the domain boundary without their on-going application sessions disrupted. However, VoIP requires a handoff to be completed in less than 50 ms for acceptable Quality-of-Service (QoS) [33], including the execution of the IEEE 802.11i authentication [6] as part of a secure handoff mechanism.

Minimizing the number of messages to be exchanged is important as cross-domain authentication needs to contact the remote home server. Moreover, the authentication latency increases in proportion to the round-trip time between two points involved in inter-domain message exchanges. Optimization of the authentication protocol is of utmost importance since an existing redundant combination of authentication and key negotiation functions incurs more rounds of message exchange than necessary.

We propose an enhanced protocol for cross-domain authentication, Mobility-adjusted Authentication Protocol (MAP) that relies on far less costly symmetric cryptography. (1) MAP reduces the cross-domain authentication latency by reducing the number of message exchanges. MAP requires less message exchanges without degrading security or the re-authentication mechanism, reducing the authentication latency significantly. (2) MAP replaces the 4-way handshake of the IEEE 802.11i authentication. In coordination with the authenticator within an access point, MAP defines hierarchical key derivation and generates consecutive keys during authentication operations. This leads to optimizing the 802.11i authentication mechanism by removing the need for the 4-way handshake. (3) MAP leverages the concept of security context to mostly avoid remote contact. With the mobile moving along, its security context is transferred via security context routers (SCRs) we present in this chapter. An SCR also plays a role of an authentication server in a foreign domain; it provides security context for MAP operating as if in the home server. Via a prototype implementation, our evaluation results show that the cross-domain authentication latency of MAP accounts for 74% and 85% that of Kerberos [17] and Needham-Schroeder symmetric-key protocol (NS) [26, 27], respectively. It makes up to 53% improvement in the authentication latency which is proportional to the end-to-end domain distance until the round-trip time counts up to 100 ms.

The remainder of this chapter is organized as follows. Section 2 gives an overview of the 802.11i authentication scheme and protocols applicable to the cross-domain authentication, and then describe the design requirements of authentication protocols. Finally, we explore prerequisites to BAN logic.

2. OVERVIEW OF AUTHENTICATION MECHANISM AND REQUIREMENTS

In this section, we first introduce the 802.11i authentication scheme and protocols applicable to the cross-domain authentication, and then describe the design requirements of authentication protocols. Finally, we explore prerequisites to BAN logic.