Chapter 2
Cryptography-Based Authentication for Protecting Cyber Systems

Xunhua Wang
James Madison University, USA

Hua Lin
University of Virginia, USA

ABSTRACT

Entity authentication is a fundamental building block for system security and has been widely used to protect cyber systems. Nonetheless, the role of cryptography in entity authentication is not very clear, although cryptography is known for providing confidentiality, integrity, and non-repudiation. This chapter studies the roles of cryptography in three entity authentication categories: knowledge-based authentication, token-based authentication, and biometric authentication. For these three authentication categories, we discuss (1) the roles of cryptography in the generation of password verification data, in password-based challenge/response authentication protocol, and in password-authenticated key exchange protocols; (2) the roles of cryptography in both symmetric key-based and private key-based token authentications; (3) cryptographic fuzzy extractors, which can be used to enhance the security and privacy of biometric authentication. This systematic study of the roles of cryptography in entity authentication will deepen our understanding of both cryptography and entity authentication and can help us better protect cyber systems.

INTRODUCTION

Entity authentication studies how to verify the identity of an entity (either a human being or a computer) and it is a fundamental issue in protecting cyber systems, including web services and web applications.

DOI: 10.4018/978-1-61520-783-1.ch002

Four factors can be used to authenticate an entity, namely, *what you know*, *what you have*, *who you are*, and *where you are*. A what-you-know authentication verifies an entity through the proof of memorable knowledge, such as a password, a PIN number, or the answer to a specific question. Password authentication is the most commonly seen *knowledge-based authentication*. A what-you-have authentication verifies

an entity through the proof of possession of a hardware *token*, which stores a strong secret that most human beings have difficulty to remember. Example hardware tokens include a USB token, a smartcard, and a Radio Frequency Identification (RFID). A who-you-are authentication verifies a *human being user* through his/her biological or behavioral characteristics and hence is also called *biometric authentication*. Example biological characteristics include fingerprints, voices, faces, iris and DNA; example behavioral characteristics include handwritten signature and keystrokes. A where-you-are authentication verifies an entity through its geographical location, for example, through the global positioning system (GPS).

What roles does cryptography play in these entity authentication categories? This question turns out to be surprisingly elusive. This is in sharp contrast to the fact that cryptography is widely known for providing *data confidentiality* through encryption (including symmetric-key encryption and public-key encryption), *data integrity* through message authentication code (MAC, such as cipher-based MAC and hash-based MAC), and *non-repudiation* through digital signatures.

This book chapter is to fill this gap and provide a comprehensive view on the important roles of cryptography in the first three authentication factors for protecting cyber systems. First, in the what-you-know authentication category, we will focus on three significant roles of cryptography in password authentication: (1) the application of cryptographic hash functions in the generation of password verification data (PVD) to protect against malicious server administrator and server compromise-based network attacks; (2) the use of cryptographic algorithms in the password-based challenge/response protocol, which has been used by Microsoft Windows authentication and HTTP digest authentication; (3) the marriage of password authentication with cryptographic key exchange protocols, resulting in password-authenticated key exchange (PAKE) protocols that offer password-based *mutual* authentication.

Second, in the token-based what-you-have authentication category, we will study the cases where a token stores either a symmetric key or the private key of a public/private key pair. For symmetric key-based authentication, we focus on the symmetric key-based challenge/response authentication paradigm and its applications. For private key-based authentication, we shall focus on the authenticated key exchange paradigm, which has been used in IP Security (IPsec) Internet Key Exchange (IKE), Secure Socket Layer (SSL), and Secure Shell (SSH).

Third, in the biometric-based who-you-are authentication category, we will study *fuzzy extractor*, a new cryptographic primitive that can be used to enhance the security and privacy of biometric authentication through protecting biometric reference templates.

This chapter is organized around cryptography's roles in these authentication categories. Before going into these details, we shall first review some basic authentication concepts in next section.

BACKGROUND

Network-Based Entity Authentication

Some network applications are designed to serve certain users, not the public. Example applications of this type include online banking, web email, and online payment services. To access such a service, an entity has to authenticate itself first. In this authentication scenario, the entity to be authenticated is called *the client* and the service provider is called *the server*. The authentication of the client to the server is called *client-side authentication*; the authentication of the server to the client is called *server-side authentication*. When used alone, client-side authentication is a *one-way authentication*; so is server-side authentication. When the client and the server are authenticated together, the authentication is *mutual*.