Chapter 7
Public Key Infrastructure

Reed H. Petty
University of Arkansas at Little Rock, USA

Jiang Bian
University of Arkansas at Little Rock, USA

Remzi Seker
University of Arkansas at Little Rock, USA

ABSTRACT

Electronic forms of communications are becoming increasingly pervasive. The Internet links not only senders and receivers of e-mail, but also consumers to suppliers, businesses to businesses, citizens to governments, and so forth. The potential for communications to be intercepted, hijacked, emulated, or otherwise manipulated for nefarious purposes is an area of grave concern. The security of message traffic relies heavily upon encryption. Encryption relies upon keys. Public key infrastructure (PKI) addresses keys – how they are used, how they are exchanged, and how they are validated. Furthermore, public key cryptography provides confidentiality, integrity, authentication, and non-repudiation. In general, PKI is a broad subject matter and is constantly evolving to meet the rapid growth in today's information world. This chapter is intended to reveal the mystery, and perhaps misconceptions, of the PKI as well as offering readers a broad high-level view of the PKI.

INTRODUCTION: WHY ARE WE HERE?

Just after midnight on December 7, 1941, on a tiny island situated between Seattle and Bremerton Washington, radio technicians snagged a message flying through the ether. Monitoring of message traffic flowing between Washington DC and Tokyo had become routine. The intended recipient was the Japanese Embassy. The transmission began at 1:28 a.m. and was complete by 1:37 a.m. At 7:58 a.m. an alert was raised, "Air Raid, Pearl Harbor. This is Not a Drill!" A few hours later, the American Pacific Fleet lay decimated (Kahn, 1967).

American code breakers, having gained technical skill while working in programs with distinctive code names, such as "Magic" and "Purple", were aware of the message content well before the bombs fell. What do we learn from this story?

DOI: 10.4018/978-1-4666-2919-6.ch007

1. Codes can be broken. The Japanese government was stunned to learn that the Americans had been "reading their mail" for months.
2. Obtaining a technical advantage by exploiting a weakness in a crypto system does not necessarily translate into a strategic advantage. The officials in Washington DC had opportunity to respond and reduce the impact at Pearl Harbor but failed to do so.

In cryptography, it is helpful to assign names to the roles assumed by various players. Traditionally "Alice" and "Bob" refer to parties having a need to communicate with each other. "Eve the Eavesdropper" hopes to read Alice and Bob's secrets. "Mallory the Malevolent" hopes to modify or disrupt the messages sent by Alice to Bob.

In the case of the Pearl Harbor embassy message, Alice was an official located in Tokyo. Bob was the Japanese embassy in Washington, and Eve was the naval intercept station located near Seattle. Mallory was not yet active.

More than 50 years has passed since the events described above occurred at Pearl Harbor. Communication and computer technology have progressed at an astonishing rate. The risk that communications may be compromised now reaches directly into the lives of billions of people. This chapter explores technology intended to manage and, hopefully, reduce such risk.

THE THREE-FOLD MISSION OF ENCRYPTION

Encryption systems serve a three-fold mission: (1) protect the message content, (2) authenticate sender and receiver, and (3) prevent the repudiation after transmission. Alice, Bob, and Eve are active players. Their roles will be explored as we explore each area.

Privacy

The Greek word *kryptos* means "secret, hidden". The first and most fundamental objective of cryptography is the keeping of secrets secret. Alice and Bob are strongly motivated to prevent Eve from learning of the message content. Alice and Bob also are strongly motivated to protect against Mallory's desire to tweak individual words, or entire paragraphs, within their messages. Alice and Bob consider their message to be a private matter not to be read by others, and certainly not to be altered by others. Alice and Bob may be generals in a military campaign, captains in an industry, a lawyer and a client, a doctor and a patient, a political candidate and a campaign chairman, and so forth.

Authentication

The industry refers to the process of verifying player identities as authentication. Assume for a moment that you, the reader, have a need to withdraw cash from your local automatic teller machine. Let us, for the moment, designate the teller machine as Alice. The bank to which Alice communicates we will designate here as "Bob the Banker".

For this discussion, we will designate Alice with a title, "Alice the ATM" to help us remember her role in the current scenario. Before Alice the ATM hands you your cash, she checks with Bob the Banker to ensure that your account exists, has sufficient cash to cover your withdrawal, and so forth. Both Alice and Bob are strongly motivated to ensure that each is who they say they are. Furthermore, both Alice and Bob are interested in ensuring that "you are who you are you are". Both Alice and Bob believe that you would be unhappy if "Mallory the Malevolent" were to withdraw some or all of your cash. Similarly, both you and Bob would be unhappy if Mallory were