IGI PUBLISHING **ITB14884**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao**

Chapter XIV

Subtle Interactions: Security Protocols and Cipher Modes of Operation

Raphael C.-W. Phan, Swinburne University of Technology, Malaysia

Bok-Min Goi, Multimedia University, Malaysia

Abstract

In this chapter, we show how security protocols can be attacked by exploiting the underlying block cipher modes of operation. We first *present a comprehensive treatment of the properties and weaknesses of standard modes of operation. We* then *show why all modes of operation should not be used with public-key ciphers in public-key security protocols. This includes the cipher block chaining (CBC) mode when there is no integrity protection of the initialisation vector (*IV*). In particular, we show that it is possible in such instances to replace a block at the beginning, middle, or end of a CBC-encrypted message. We* further *demonstrate that the security of single-block encryptions can be reduced to the security of the electronic codebook (ECB) mode, and show that in the absence of integrity, one could exploit this to aid in known- and chosen-*IV *attacks.* Finally, *we present chosen-*IV *slide attacks on counter (CTR) and output feedback (OFB) modes of operation. Our results show that protocol implementers should carefully select modes of operation, be aware of the pitfalls in each of these modes, and incorporate countermeasures in their protocols to overcome them. It is also important to realize that modes of operation only provide confidentiality, and that when used in the context of security protocols, these modes should be combined with authentication and integrity protection techniques.*

Introduction

It is necessary in a distributed computer system that two agents can be assured of each other's identity. They would really wish to talk to each other rather than to a third-party impostor. This is achieved with an *authentication protocol* (Boyd, 1997; Boyd & Park, 1998; Lowe, 1995, 1996; Mao & Boyd, 1993, 1994, 1994a, 1995, 1995a; Park, Boyd, & Dawson, 2000). Often, they also need to exchange a shared secret key to guarantee the confidentiality of the messages that they communicate. This is achieved with a *key-exchange protocol* (Boyd & Mathuria, 1997).

In this chapter, we consider how the security of authentication and key exchange protocols can be compromised by exploiting the underlying modes of operation.[1] Reminders have been made in the past as to the careful use of the underlying modes of operation, and that they should be used in conjunction with integrity protection (Bellovin, 1996; Bellovin & Blaze 2001). We strive to strengthen this by further presenting new attacks on security protocols based on the exploitation of the modes of operation used. Our first main contribution is in showing why even the popular CBC mode is insecure when used in the absence of *IV* integrity protection in public-key security protocols. Our second contribution is to reduce the security of single-block encryptions to that of the ECB mode, and further presenting chosen *IV* slide attacks on the two stream cipher modes of operation.

This chapter is organized as follows: In Section 2, we describe the five standard modes of operation, and then in Section 3, comprehensively treat the properties and weaknesses of these modes. In Section 4, we show why modes of operation should not be used with public-key protocols, concentrating particularly on the CBC mode. In Section 5, we relate the security of single-block encryptions to the ECB mode security, and hence show that single-block encryptions cause known and chosen-*IV* attacks to be practical. Finally, we show that by abusing the *IV*s, one could mount chosen-*IV* slide attacks on the CTR and OFB modes. We conclude in Section 6.

Modes of Operation

We will briefly describe, in this section, the standard modes of operation used when encrypting messages longer than the block size of a block cipher. One main observation is that though the term "block cipher" is often taken to mean secret-key block ciphers, there are also public-key block cipher versions. The most popular example is the public-key RSA cipher, which encrypts messages one block at a time.

When plaintext, P, to be encrypted by a block cipher is longer than the block size, n, the plaintext is divided into several n-bit blocks, P_i, and each one is encrypted at a time using a block cipher mode of operation that could either be the electronic code book (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB) or counter (CTR) modes.