MODIFIED FORMS OF CIPHER BLOCK CHAINING

Chris J. Mitchell

Computer Science Department
Royal Holloway and Bedford New College
Egham Hill
Egham
Surrey TW20 0EX
England

Vijay Varadharajan

Hewlett-Packard Laboratories
Filton Road
Stoke Gifford
Bristol BS12 6QZ
England

17th May 1990

Abstract

A long-standing proposal for modifying cipher block chaining to prevent data expansion is shown to be insecure in some circumstances. Different modifications are then presented which appear secure.

1. Introduction

A block cipher algorithm can be used in a number of different ways to encrypt data; four such 'modes of operation' are described in ISO Standard 8372, [1]. One well-used such mode is Cipher Block Chaining (CBC). Before describing this mode we introduce some notation.

Suppose the block cipher transforms *n*-bit blocks of plaintext into *n*-bit blocks of ciphertext. If P denotes such a block of plaintext, denote by $e_K(P)$ the ciphertext obtained from P by encryption under the control of the key K.

To perform Cipher Block Chaining it is first necessary to divide the plaintext to be encrypted into a series of *n*-bit blocks,

$$P_1, P_2, \ldots, P_s$$

where, if necessary, the last block is padded out with extra bits. The ciphertext is then computed as

$$C_1, C_2, \ldots, C_s$$

where

$$C_i = e_K(P_i + C_{i-1}) \quad (1 \le i \le s)$$

and + denotes bit-wise exclusive-or of blocks. Note also that C_0 = SV, a 'Starting Variable', which needs to be known to both the sender and recipient of the encrypted plaintext.

This mode has one disadvantage, namely the data expansion caused by the need to 'pad' the last block to a full *n* bits. In many cases this would not be significant, especially as *n*

would typically be 64 and in many applications data comes naturally in blocks of length a multiple of 64. However, in certain special situations data expansion becomes a major problem, and it would therefore be desirable to have a way of using CBC which does not have this characteristic.

As a result, the latest Draft International Standard concerned with Modes of Operation, DIS 10116, [2], contains a modified form of CBC. This modified CBC is of long standing, see, for example, p.272 of Konheim, [3], p.94 of Davies and Price, [4] or p.76 of Meyer and Matyas, [5]. It is designed to prevent data expansion in the case where plaintext messages are not a multiple of n bits in length. The modification only affects the encryption of the last block of the data.

It operates as follows. Suppose the last block of plaintext is P_s, of $j < n$ bits. Suppose also that the penultimate block of ciphertext is C_{s-1}. Then C_s, the encrypted form of P_s, is computed as:

$$C_s = P_s + (e_K(C_{s-1})|_j)$$

where $|_j$ denotes the left-most j bits of a block.

2. Cryptanalysis

Unfortunately, the modified form of CBC described above is, in some circumstances, subject to a chosen-plaintext attack which will reveal the last plaintext block P_s. We now describe the attack. Note that we assume that the party responsible for encrypting the data will be prepared to encrypt a set of plaintext supplied by the cryptanalyst - this is the meaning of the term 'chosen-plaintext' attack. Note also that a much weaker version of the attacks described below is outlined on p.79 of Meyer and Matyas, [5].

We consider two different scenarios in which a chosen plaintext attack can be successfully launched. The success of the attacks depends on the way in which the Starting Variable

is used. In both cases it is assumed that a plaintext of s blocks is encrypted such that the last block is processed as above. It is also supposed that the resulting ciphertext has been obtained by a cryptanalyst who wishes to decrypt the last ciphertext block C_s to recover the corresponding plaintext P_s.

3. Scenario A

First suppose that the SV, although changing for every data set to be encrypted, changes in a predictable way, for example being based on a counter which is incremented every time a data set is encrypted. In some circumstances this would mean that the SV would not need to be sent or stored with the ciphertext, an advantage if communications band-width or storage space is at a premium; see, for example, p.97 of Davies and Price, [4].

Suppose the cryptanalyst knows that the next message to be encrypted will have X as its SV. The cryptanalyst now constructs a message

$$P_1, P_2, \ldots$$

with the property that

$$X + P_1 = C_{s-1}$$

and offers it for encryption. The first block of the resulting ciphertext, D_1 say, will satisfy

$$D_1 = e_K(X + P_1).$$

It is now straightforward to see that the simple computation

$$(D_1|_j) + C_s$$

will reveal P_s, and the attack is complete.

Before proceeding note that a similar attack is possible in the case where the cryptanalyst is capable of choosing the SV as well as the plaintext. In this case the first block of plaintext P_1 can be chosen arbitrarily by the cryptanalyst.

4. Scenario B

Suppose next that the same SV is used repeatedly for different plaintexts (e.g. SVs are secret and treated as part of the key). The cryptanalyst constructs an arbitrary data set

$$P_1, P_2, \ldots$$

and has it encrypted as

$$D_1, D_2, \ldots$$

where

$$D_1 = e_K(P_1 + SV).$$

(note that the cryptanalyst does not need to know SV).

The cryptanalyst now constructs a second data set

$$Q_1, Q_2, \ldots$$

with the property that

$$Q_1 = P_1 \quad \text{and} \quad Q_2 = D_1 + C_{s-1}$$

and has it encrypted as

$$E_1, E_2, \ldots$$

where

$$E_1 = e_K(Q_1 + SV) \quad \text{and} \quad E_2 = e_K(Q_2 + E_1)$$

and hence

$$E_1 = D_1$$

and so

$$E_2 = e_K(C_{s-1}).$$

The simple computation

$$(E_2|_j) + C_s$$

will reveal P_s, and the attack is complete.

5. Secure modifications to CBC

It should be apparent that the above attacks would not work if the SV was changed for every data set in an unpredictable way. In this circumstance the above described modified form of CBC remains secure. However, it is not always practical to use the SV in this way. Therefore we conclude this short paper by suggesting two different modifications to the CBC computation, (one of them apparently novel), neither of which have the same problems. However, both modifications retain the desirable property of avoiding plaintext expansion.

The first modification also only affects the encryption of the last block of plaintext. Suppose the last block of plaintext is P_s, of $j < n$ bits. Suppose also that the penultimate block of ciphertext is C_{s-1}. Then C_s, the encrypted form of P_s, is computed as:

$$C_s = P_s + (d_K(C_{s-1} + X)|_j)$$

where X is a fixed (public) block which is not all zeros, and where d_K denotes block cipher decryption using the key K.

The second modification, previously described as *ciphertext-stealing* in Ref. [5], affects the encryption of the last two blocks of plaintext. Suppose that the last two blocks of plaintext are

$$P_{s-1}, P_s$$

where P_s is of $j < n$ bits, and let C_{s-1} be the ciphertext block derived from P_{s-1} using 'regular' CBC. Then set:

$$C_s = e_K(P_s ; C_{s-1}|^{n-j})$$

where X;Y denotes the concatenation of data blocks X and Y, and where $|^k$ denotes the right-most k bits of a block. The last two ciphertext blocks are then $C_{s-1}|_j$ and C_s. When decrypting, C_s needs to be decrypted before $C_{s-1}|_j$ in order to first recover the right-most $n-j$ bits of C_{s-1}.

Both these modifications appears to resist all types of chosen

plaintext attack, although it would seem prudent to subject them to further careful analysis before adoption.

References

[1] ISO 8372, 'Information processing - Modes of operation for a 64-bit block cipher algorithm' (International Organization for Standardization, 1987).

[2] DIS 10116, 'Information processing - Modes of operation for an *n*-bit block cipher algorithm' (International Organization for Standardization, 1989).

[3] KONHEIM, A.G., 'Cryptography: A primer' (John Wiley and Sons, New York, 1981).

[4] DAVIES, D.W. and PRICE, W.L., 'Security for computer networks' (John Wiley and Sons, Chichester, 1984).

[5] MEYER, C.H. and MATYAS, S.M., 'Cryptography: A new dimension in computer data security' (John Wiley and Sons, New York, 1982).