Journal of Craptology, Vol 0, No 0

Deletion Cryptanalysis

Lars R. Knudsen and Fauzan Mirza

November 19, 1998

Abstract

In this paper the deletion cryptanalysis is considered. The method deletes certain parts of a cryptosystem before cryptanalysis. All cryptosystems are susceptible to this attack. It is shown why the one-time pad and the DES are very weak under this attack.

Keywords. Craptology.

1 Introduction

In this paper, the *deletion cryptanalysis* of secret-key systems is considered. By enabling an attacker to selectively delete crucial operators or functions in a particular cryptosystem, it is usually possible to break the system much more efficiently than usual. Even cryptosystems which obtain what Shannon called *perfect secrecy* are trivially broken with this new attack.

Two examples of deletion cryptanalysis as applied to the one-time pad and the DES block cipher are given.

2 The One-time Pad minus 1 XOR

One-time pad encryption is described by

$$C = P \oplus K,$$

where the ciphertext C, plaintext P and key K are the same length.

A deletion attack completely demolishes the security of the one-time pad. By deleting an XOR from the cipher, notice that

$$C = P.$$

The attacker can easily read the plaintext, without knowledge of any part of the original key. To protect against this devastating attack, one should always ensure that the key is in fact XORed to the plaintext. Alternatively, the deletion of the key could be done by the sender himself, in which case an attacker can never retrieve the secret key.

3 The DES minus 3 XORs

DES is a 16-round iterated cipher, based on the Feistel network. Let the plaintext be denoted by $P = (L_0, R_0)$, the ciphertext by $C = (R_{16}, L_{16})$, and the round subkeys by K_i, for $i = 1..16$. The round function is

$$L_{i+1} = R_i, \qquad R_{i+1} = L_i \oplus P(S(E(R_i) \oplus K_i)),$$

where P, E are bitwise permutations and S is composed of eight nonlinear S-boxes S_i operating in parallel. The differential attack by Biham-Shamir breaks the DES using a 13-round characteristic with probability 2^{-47} and 2^{47} chosen plaintexts. If in the rounds 3, 5, and 7, the first XORs in the above round description are removed, the probability of the characteristic increases to $2^{-23.5}$ and the differential attack requires only about 2^{24} chosen plaintexts.

4 Conclusion

This paper has demonstrated the effectiveness of deletion cryptanalysis when applied to two well-known cryptosystems. It is shown that deletion cryptanalysis can sometimes break systems as efficiently as the chosen-key attacks (where the attacker can choose the key to be used and, optionally, any plaintexts that they would like to be encrypted).

We expect that many public-key systems can also be broken by selective deletion of crucial operations or functions and feel that it is our duty to warn the craptologic community of the threat of deletion attacks.