Cryptanalyse et sécurité des algorithmes à clé secrète*

[Thèse de doctorat, École Nationale Supérieure des Télécommunications, Paris, Octobre 1999.**]

Helena Handschuh[1,2]

[1] École Nationale Supérieure des Télécommunications
46 rue Barrault, 75013 Paris, France
handschu@enst.fr
[2] Gemplus Card International, Cryptography Department
34 rue Guynemer, 92447 Issy-les-Moulineaux, France
helena.handschuh@gemplus.com

Résumé. La sécurité des algorithmes à clé secrète est un sujet qui intéresse de près la communauté scientifique ainsi que les industriels. Depuis la découverte de la cryptanalyse différentielle et linéaire, d'innombrables nouvelles attaques ont été publiées.
Dans ce mémoire, nous développons tout d'abord les attaques génériques qui ne nécessitent pas la connaissance de la structure interne de l'algorithme, mais permettent néanmoins d'extraire les clés d'un grand nombre de modes multiples ou bien de constructions visant à doubler la taille d'un bloc. Ces attaques s'appliquent à divers schémas à base de DES.
Nous montrons ensuite comment la moindre faiblesse permettant de distinguer une situation du cas aléatoire permet d'extraire de l'information, voire même la clé secrète de divers types d'algorithmes, y compris SEAL et RC6. Ces attaques appartiennent à une classe beaucoup plus large comprenant toutes les approches spécifiques à un algorithme donné.
Enfin, un nouveau type d'approche s'est intensifié ces deux dernières années. Au-delà des attaques théoriques que l'on peut mener sur tout algorithme, il faut également prendre en compte l'environnement dans lequel celui-ci est utilisé. Il existe souvent un canal caché qui permet d'obtenir des données de type temps d'exécution, courant consommé, valeur d'un bit à un instant donné. Comme le montrent les exemples du DES et de RC5, il s'avère que ces fuites d'information sont la plupart du temps fatales à la sécurité de l'algorithme.

Abstract. The security of secret-key algorithms is a subject which addresses both the cryptographic community and industry. Ever since differential and linear cryptanalysis were discovered, multiple new attacks have been published.

* Cryptanalysis and Security of Secret-Key Algorithms.

** PhD Thesis, École Nationale Supérieure des Télécommunications, Paris, October 1999.

In this thesis, we first address generic attacks which do not require the knowledge of the internal structure of the algorithm, but nevertheless enable to extract the secret keys of different multiple modes or constructions that achieve double bloc length encryption. These attacks apply to several DES-based schemes.
Next, we show how the slightest weakness which distinguishes a situation from the random case may enable an attacker to extract information about the secret key or even to recover it from different kinds of algorithms including SEAL and RC6. These attacks belong to a much larger class of attacks, namely those which make use of the details of a given algorithm.
Finally, a new approach has received increasing attention lately. Besides all the theorical attacks that can be applied to any algorithm, one also has to take into account in which environment the latter is being used. Often information leaks through side-channels such as execution time, power consumption, or bit probing on tamper-resitant devices. As shown for DES and RC5, the information leaked generally compromises the security of the whole algorithm.