Whitebox

David Wong Jacques Monin Hugo Bonin

March 26, 2014

1 Introduction

1.1 DRM

1.2 Problmes

l'attaquant accs la mmoire et donc il peut facilement rcuprer la clef en analysant l'excution du programme.
De base il peut aussi choisir ce qu'il envoit au programme et voir comment le programme l'encrypte ou le dcrypte (chosen plaintext attack) (cas d'une blackbox)
Whitebox: l'attaquant a encore plus de possibilit puisqu'il controle l'environement: accs la mmoire, trace, breakpoints,...

1.3 Solution

but : Rendre l'extraction de la clef impossible

2 DES

2.1 Pourquoi DES?

3 Concepts

3.1 Look up tables

4 Notre implmentation

4.1 Les fonctions de base