

Analyse automatisée d'une bibliothèque cryptographique



Détection de failles par canal auxiliaire par analyse statique et symbolique

Duzés Florian

Introduction



Introduction

1996 : Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.

Introduction

1996 : Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.

2003 : BRUMLEY et BONEH *Remote Timing Attacks Are Practical*

Introduction

1996 : Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.

2003 : BRUMLEY et BONEH *Remote Timing Attacks Are Practical*

2011 : BRUMLEY et TUVERI *Remote Timing Attacks are Still Practical*



Introduction

- QR1** Est-il possible de propager les garanties de sécurité pendant la compilation ?
- QR2** Est-il possible d'automatiser la détection de ces failles sur des fichiers compilés ?
- QR3** Est-il possible d'appliquer ces mécanismes pour assurer la vérification d'une bibliothèque cryptographique ?

Sommaire