РЕФЕРАТ

Обсяг роботи 71 сторінок, 7 ілюстрацій, 8 таблиць, 31 джерело літератури.

Об’єктом дослідження є генератори псевдовипадкових чисел операційних систем Android та iOS. Предметом дослідження є особливості структури генераторів псевдовипадкових чисел операційних систем Android та iOS, та їх криптографічні властивості за умов низького рівня ентропії. В роботі з теоретичної точки зору досліджувалась структура генераторів Android та iOS та їх властивості і особливості. Для Android запропоновано суттєві модифікації існуючих атак. Також був проведений емпіричний експеримент на Android, що дав змогу оцінити кількість ентропії в генераторі, її розподіл за джерелами надходження і за шляхами споживання. Для iOS підтверджено атаку на генератор псевдовипадкових чисел. В результаті роботи досліджені структура генератора, методи отримання ентропії, методи її передачі всередині генератора, та шляхи її споживання для генератора Android. В результаті експерименту встановлено, що наявної ентропії в генераторі недостатньо. Також виявлено, що генератор використовує модифікацію виткового регістру зсуву з лінійним зворотним зв’язком, що не є дослідженою, і ставить під сумнів стійкість цього об’єкту. Також використовуючи особливості оцінювача ентропії та способів її передачі всередині генератора модифіковано існуючі атаки. З огляду на отримані результати, в більшості випадків, генератори як в Android так і iOS можна розглядати як звичайний генератор псевдовипадкових чисел без джерел ентропії, що дає змогу будувати на нього відповідні атаки.

ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ, ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ, ANDROID, IOS, ЕНТРОПІЯ, ДЖЕРЕЛО ЕНТРОПІЇ, ЛІНІЙНИЙ РЕГІСТР ЗСУВУ.