УРАЗЛИВІСТЬ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

Рисований О.М., Вінокуров А.І.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

При дослідженні генераторів випадкових чисел виявлено критичну вразливість, яка впливає на шифрування інформації. Така вразливість присутня у функції змішування ентропії генератора псевдовипадкових чисел. Вразливість дозволяє передбачити такі *n*-біт послідовності.

Збої в роботі генератора випадкових чисел можуть відбуватися з ряду причин, але найпоширенішою (і найчастіше використовуваною) є нестача джерел ентропії.

Генератори псевдовипадкових чисел є підкласом генераторів випадкових чисел. Для псевдовипадкових генераторів розроблено серйозний математичний апарат. Однак, псевдовипадкова послідовність має недоліки, які впливають на критичність їх використання.

Атака на генератор псевдовипадкових чисел спрямована на розкриття параметрів генератора псевдовипадкових чисел з метою подальшого передбачення псевдовипадкових чисел.

Успішна атака на такий генератор може розкрити багато криптографічних систем незалежно від того, наскільки ретельно вони були спроектовані. Деякі системи використовують погано спроектовані генератори.

У роботі розглянуто типи атак: пряма криптоаналітична атака; атаки, що базуються на вхідних даних; атаки, засновані на розтині внутрішнього стану.

Типи атак, що базуються на вхідних даних:

- атаки з відомими вхідними даними;
- атаки з відтворюваними вхідними даними;
- атаки на обрані вхідні дані.

Атаки, засновані на розтині внутрішнього стану:

- атака зі зворотним прокручуванням;
- перманентне компрометування стану;
- атака ітеративним вгадуванням;
- зустріч посередині.

В роботі показано, що і псевдовипадкові послідовності можуть мати дуже високу стійкість. А при застосуванні різних типів генераторів з різними властивостями можна стверджувати, що виявити вразливість у таких схемах майже неможливо.