Омельченко Віктор

Side-Channel Attacks

Отримання данних, не пов'язаних напряму з інформацією, яку потрібну отримати, але аналіз яких дає можливість визначити захищені персональні данні назівається атакою по побічним каналам ( каналам втрат ).

Використання побічних каналів втрати данних в класичному предснавленні, такі як аналіз енергетичних або електромагнітних данних зазвичай потребують дорогого обладнання та великіх потужностей, для дешифровки отриманих данних.

З урахуванням розповсюдженості мобільних пристроїв, а також збільшення їх функціоналу, в тому числі пов'язаного з обробкою, отриманням та відправленням персональної інформації, з'являється можливість використовувати додаткові канали втрат. Так, наприклад для корректної роботи більшості мобільних пристроїв постійно використовуються данні з гіроскопа та акселерометра, віконуються заміри температури екрану, та внутрішньої температури, збираються данні системи GPS та виконується запис звуку.

Задача программіста, котрий займається розробкою ПО, для атак по каналам втрат - проаналізувати массив отриманих данних, виділити подібні елементи ( ознаки ), та за їх аналізом побудувати ПО, що зможе з певною точністю визначити подібність тій чи іншій ознаці. ( Наприклад з допомогою використання методу - к-найближчих сусідів, як самого простого ), а також зібрати певну базу статистики, щоб виявити ознаки.