

Device Security

يتضمن:

Physical Device security - 1

Firmware/OS security - 2

Application Security - 3

Physical Device security

تندرج تحتها الـ Side channel Attacks

Side channel Attacks:

- تعتبر نوع من أنواع الـ reverse engineering
- هذا النوع من الهجمات يستغل الأجزاء الـ hardware في الجهاز حتى يحصل المهاجم على المفتاح الذي تم استخدامه في عملية التشفير أو يقوم بفك النص المشفّر، بدلاً من محاولة كسر خوارزمية التشفير نفسها.
- المهاجم قد يراقب الموارد التي يستهلكها الجهاز خلال عملية التشفير للحصول على أي معلومة قد تساعد في فك النص المُشفّر أو الحصول على المفتاح الذي تم استخدامه في عملية التشفير.
- يوجد عدة طرق مختلفة لشن هذا الهجوم، مثل:
 - Cache attack
 - Timing attack
 - Power monitoring attack