Physical Device security

المخاطر/ أنواع البرامج الخبيثة التي قد نواجهها هنا:

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، بدلًا من محاولة كسر خوارزمية التشفير نفسها.
- المهاجم قد يراقب الموارد التي يستهلكها الجهاز **خلال عملية التشفير** للحصول على أي معلومة قد تساعده في فك النص المُشفّر او الحصول على المفتاح الذي تم استخدامه في عملية التشفير.
- يوجد عدة طرق مختلفة لشن هذا الهجوم، مثل:
  - Cache attack
  - Timing attack
  - Power monitoring attack

Firmware/OS security

Rootkit:

- نوع من أنواع البرامج الخبيثة ، تعمل على طبقة الـ Kernel mode بالتالي يكون لها صلاحيات مثل صلاحيات الـ operating system ، يوجد عدة أنواع منها مثل:
  - Kernel rootkit : تستبدل الـ kernel الخاصة بالجهاز، بالتالي الـ rootkit هذا يعمل بشكل اوتوماتيكي عندما يتم تحميل نظام التشغيل
    - نظام التشغيل يتم تحميله من قبل الـ bootloader
  - Firmware rootkit : هذا النوع يستبدل الـ firmware الخاص بالجهاز
  - Driver rootkit : هذا النوع يستبدل أي من الـ drivers الموجودة في الجهاز
    - الـ Drivers : عادةِ تساعدنا في التواصل مع الـ Hardware الخاصة بالجهاز
- كيف نحد من مخاطر الـ rootkit ؟

1- Secure Boot:

is a technology where the system firmware checks that the system boot loader is signed with a cryptographic key authorized by a database contained in the firmware. Secure Boot helps prevent malware from running before the OS

- هي تقنية حماية تعمل عندما يتم بدء تشغيل الجهاز، حيث يقوم الـ firmware الخاص بالجهاز بالتحقق من أن الـ bootloader الخاص بالجهاز موثوق (موقّع بمفتاح)، يتم التأكد عن طريق المقارنة بقاعدة بيانات تحتوي على قيمة هذا المفتاح.
- في نظام Windows الـ secure boot جزء من عملية كاملة تسمى الـ Trusted Boot

2- Trusted Boot:

هذه ملاحظات تمت كتابتها خلال "مرحلة دراسية"، المعلومات الوارد ذكرها قد تحتمل الخطأ، لذلك التأكد من كل ما ورد هنا يقع تحت مسؤوليتك (اطلع على خانة المراجع)

مراجع:

- https://docs.fedoraproject.org/en-US/Fedora/18/html/UEFI_Secure_Boot_Guide/chap-UEFI_Secure_Boot_Guide-What_is_Secure_Boot.html
- https://blogs.msdn.microsoft.com/olivnie/2013/01/09/windows-8-trusted-/boot-secure-boot-measured-boot
- https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot