TPAS Project 2021/2022

Security Tokens Guide

Phase 1 - Getting started

Study about security tokens and tools:

- USB generic analysis:
  https://wiki.wireshark.org/CaptureSetup/USB
  https://github.com/desowin/usbpcap
- Smartcards:
  https://www.youtube.com/watch?v=YM5I8yR7yCw
  Smart Card APDU Analysis
- NFC cards:
  Take a look at the slides of the NFC talk by Pedro Carbal @ Oposec
  https://www.youtube.com/watch?v=eVIq3--O8bM
- 2FA keys:
  https://portswigger.net/daily-swig/this-nxp-side-channel-attack-can-clone-google-titan-2fa-keys (including the paper)

Phase 2 - Setup

Install necessary tools to interact with your target. You should research for available middleware and tools. Examples:

- Generic USB: wireshark, USB sniffing and decoding tools.
- Smartcards and SIM cards: pcsc-tools, globalplatform, apdu, middleware example for PT national card, sim-tools.

- NFC cards: configure and install the Proxmark device and software: proxmark3, mobile apps such as MifareClassicTool, NFC tools.

If you have questions, please ask the professor or schedule meetings via email.

Phase 2 - Picking a target

Security tokens are anything you can have to increase security, authorization, and authentication. You can pick smartcards, SIM cards, NFC cards or other access cards, transportation tickets, QR codes, 2FA keys, or any other token. If you need help choosing, please ask the professor.

Phase 3 - Analysis

Interact with the token and explore tools to retrieve information about the technology, e.g. card type. Try to sniff the communication channel, read, write and tamper data.

Here are a few questions you can explore: Can you reverse engineer APDUs and understand their content (bytes)? Can you bypass PIN verifications? Can you bypass authentication and authorization? Can you retrieve private keys? Are there any vulnerabilities?

Phase 5 - Final report

You must submit a final report describing your work and perform a presentation in class (dates TBD). Suggested sections are: Introduction, Learning Process, Analysis, (Vulnerabilities), Final Remarks.