2021
Advanced Information
Security Summer School

教育部資訊安全人才培育計畫

# 110年度新型態資安暑期課程

Advanced Information Security Summer School

# Hacking OT by Bluetooth Attack

AIS3

# Wireless Communication Attack

- Denial of Service(DOS)
- Replay
- Masquerade
- Traffic Analysis
- Eavesdropping
- Message Modification
- Man-in-the-middle Attack

# What Protocol Can Hacker Do Wireless Communication Attack

- WIFI
- **Bluetooth**
- Zigbee/Z-wave
- Sigfox
- another Proprietary protocol

# Bluetooth Attack

- BlueSmacking
- BlueJacking
- BlueSnarfing
- BlueBugging

# What Do Attackers Thinking? And The Risk Of OT?

- Attackers can intercept the sensitive information that operators didn’t encrypt. Including authentication material passed over the network.
- Attackers also can use the sensitive information which intercept by MIMA. And start another attack, Including APT, Malware attack or break the HMI/PLC.

# Tools  Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi
- Software
  1. Statistical Test Suite
  2. Adafruit_BLESniffer_Python

# Tools Needs To  Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi
- Software
  1. Statistical Test Suite
  2. Adafruit_BLESniffer_Python

# Tools Needs To  Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi
- Software
  1. Statistical Test Suite
  2. Adafruit_BLESniffer_Python

# Tools Needs To  Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi
- Software
  1. Statistical Test Suite
  2. Adafruit_BLESniffer_Python

# Tools Needs To  Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi
- Software
  1. Statistical Test Suite
  2. Adafruit_BLESniffer_Python