Insights from Waves

Forensic Insights from IoT with Electromagnetic Side-Channel Analysis

Asanka Sayakkara, Mark Scanlon, Nhien-An Le-Khac

DFRWS EU 2020

UCD Forensics and
Security Research Group

Outline

- Electromagnetic Side-Channel Analysis for Digital Forensics - 1 hour

  coffee break - 15 mins

- Introduction to EMvidence Framework - 1 hour and 15 mins

Introduction to EMvidence Framework

(Duration: 1 hour & 15 mins)

Asanka Sayakkara, Mark Scanlon, Nhien-An Le-Khac

UCD DUBLIN

DFRWS EU 2020

UCD Forensics and
Security Research Group

The need for a tool...

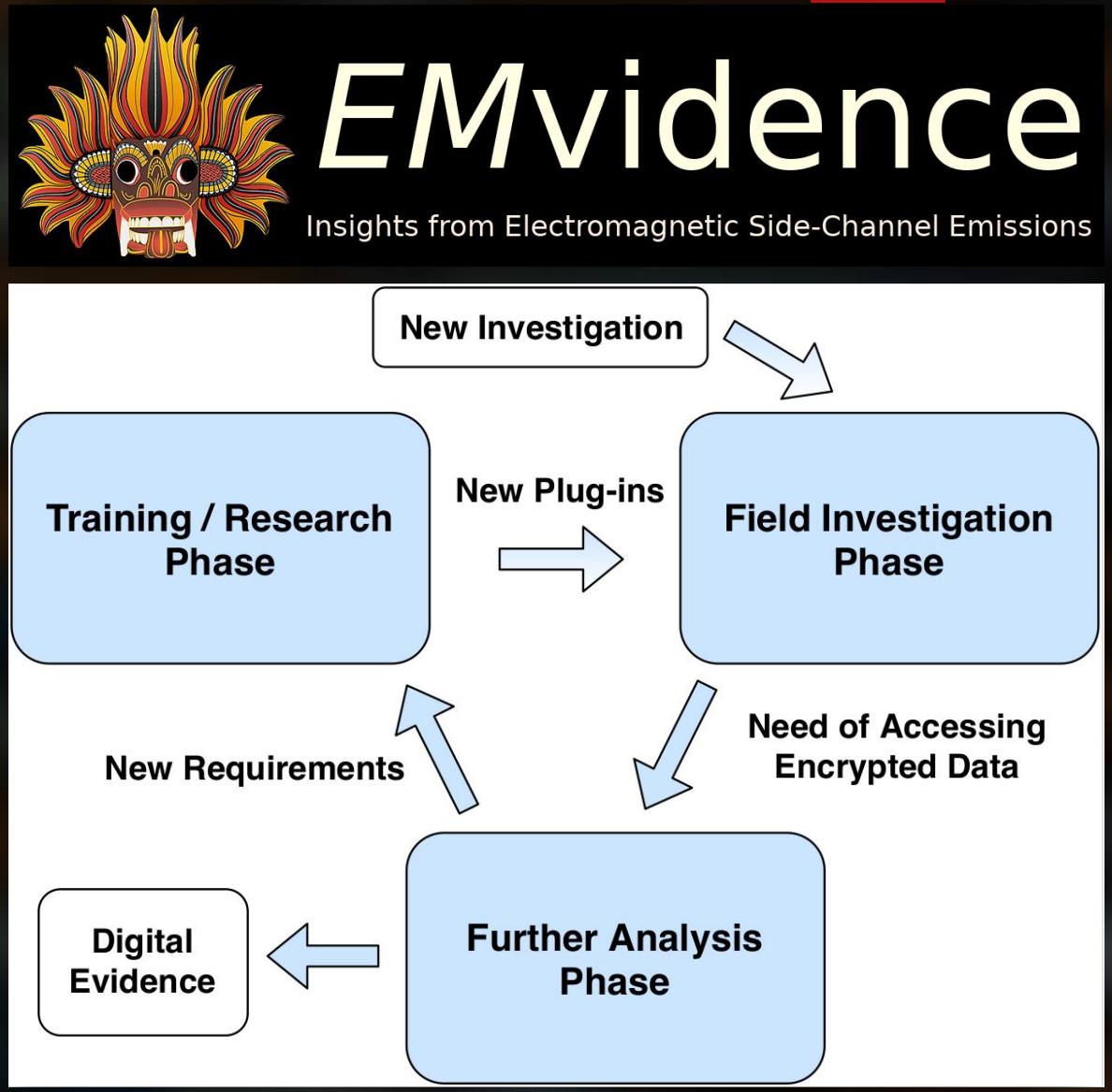
- EM-SCA demands investigators to have technical expertise on the domain.
- A large variety of devices exists - new IoT devices and firmware are emerging day-by-day.
- Research community can individually build EM-SCA methods targeting specific IoT devices or specific scenarios, but how to share all these with investigators?

We need a software tool that facilitate this!

EMvidence Framework

- A free & open-source software framework that facilitates EM-SCA for forensics.
- Capable of capturing and storing EM traces using SDR devices.
- Facilitates the community to insert their EM-SCA method implementations, trained ML models, etc. into the tool as third-party modules.
- Users can analyse EM data with the help of modules and gain useful insights.

Let's checkout the basic features!



EMvidence Framework

- Start EMvidence.
- Generate an EM trace with “cosine-generator” (if you have either RTL-SDR or HackRF, use that instead).
- Upload the EM trace “data-upload-test.cfile” to EMvidence.
- Upload “mod-visualizer” module that is available as a zip file into EMvidence.
- Analyse the two EM traces separately and generate two reports.

Modules for EMvidence

- A module for EMvidence does a specific task using given EM trace data and produce results.
- The module we tried, “mod-visualizer” simply visualize the EM data using graphs.
- We can use most of its source code as a skeleton to build other modules.
- Let’s have a look at mod-visualizer module source code.
- Then, let’s edit it slightly to be a different module with a different name.
  a. Module name should be mod-[your name], e.g., mod-asanka
  b. Text output should be a little description of yourself.
  c. Leave the graphical output as it is.

Processing EM Data

- In order to build useful modules for EMvidence, we need to know how to process EM data.
- Let's explore data processing in the following Jupyter-Notebooks
  a. Pre-processing EM data - "Preprocessing-EM-data.ipynb"
  b. Machine learning for EM data classification - "Machine-Learning-For-Signal-Classification.ipynb"
  c. Arduino program classification - "Arduino-Program-Classification.ipynb"

An ML Module for EMvidence

- We know how to process EM data and build classifiers to identify known EM signals.
- Let's build a module for EMvidence that can distinguish between two known EM emission signals.

Conclusion

- Now you have some hands-on experience into handling EM data and how to analyse them.
- Though EM-SCA for digital forensics appears to be a very narrow area of research, in fact, there is large number of unexplored avenues that awaits research attention.
- We need more people to work in this area.
- EMvidence is still in its early stage of development. We have a long way to go.
- You can help the development of EMvidence.

https://github.com/asanka-code/EMvidence

ASANKA.SAYAKKARA@UCDCONNECT.IE

HTTPS://ASAYAKKARA.ORG/

WWW.FORENSICSANDSECURITY.COM

@ASAYAKKARA

@FORSECRESEARCH

UCD Forensics and
Security Research Group