Electromagnetic Side-Channel Analysis for Obfuscated Malware classification

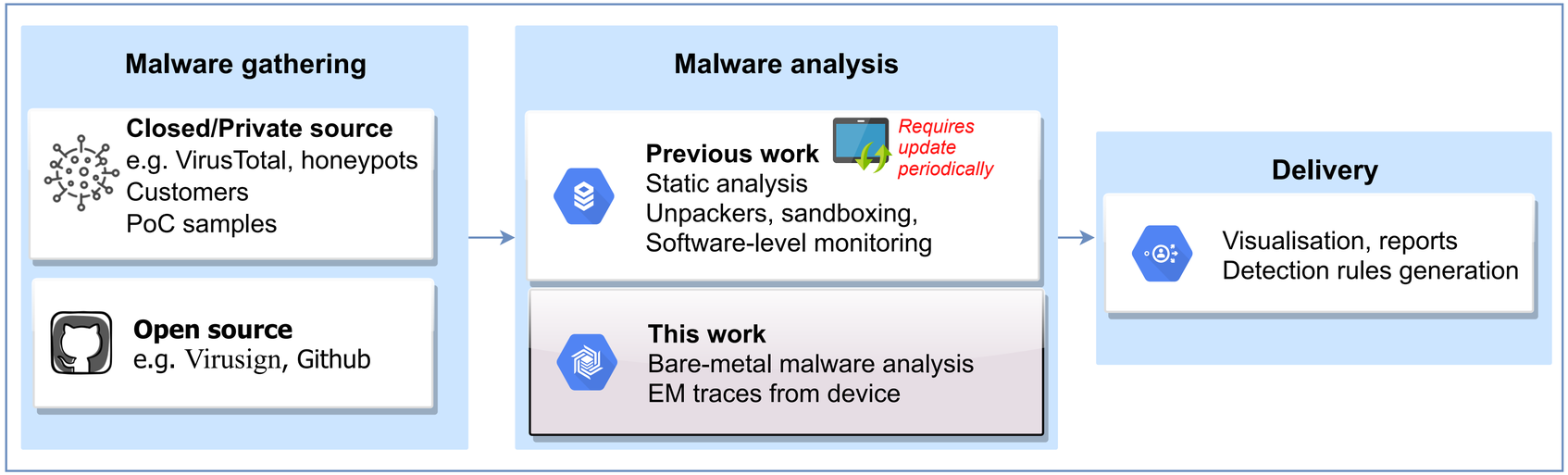
Duy-Phuc Pham
CAPSULE team, IRISA, Rennes, France
Supervisor: Dr. Annelie Heuser
ICHSA 2021. 1st June 2021.

phd_phuc
duy-phuc.pham@inria.fr

Malware analysis workflow

- (Noisy) EM traces
- Embedded devices & background processes

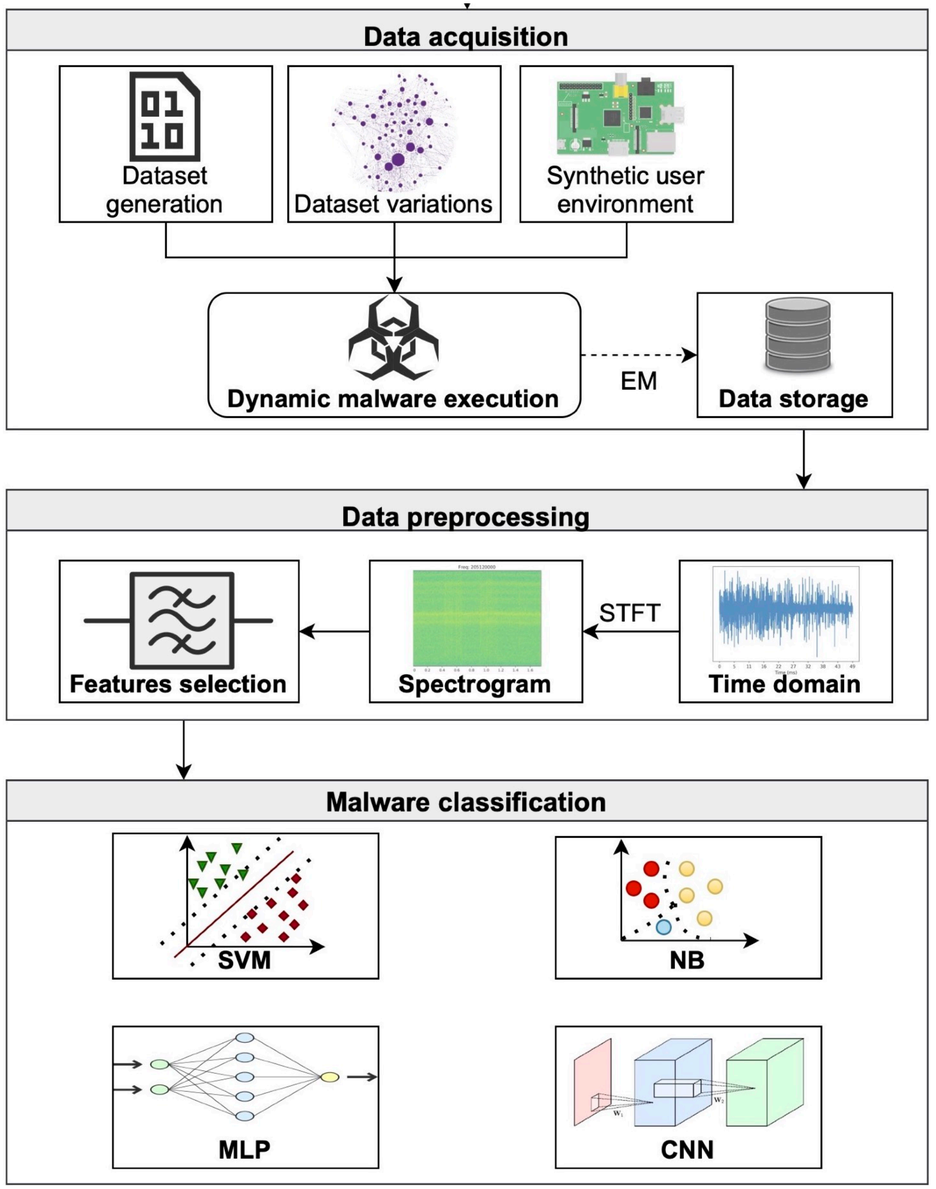
- Real-world malware
- Packed & Obfuscation: UPX, Tigress, LLVM



Type	Family
DDoS	*Mirai, Bashlite*
Ransomware	*Gonnacry*
Rootkit	Keysniffer, MaK_It
Benign	Linux binaries

Proposed framework

- Real-world malware analysis environment
- Spectrogram as preprocessing
- Bandwidth-feature selection
- ML&DL classification



Results

- 96000 traces: obfuscated malicious and benign.
- Numerous classification scenarios:
  * Types(99.92%), families(99.33%)
  * Virtualization (95.95%), packer (90.84%), obfuscation (81.85%)
- Mostly CNN models are more accurate

Further work

- Rootkit detection
- More target devices (e.g MIPS)
- SDR traces

Q&A

Thank you!

phd_phuc
duy-phuc.pham@inria.fr