Obfuscation defeated: Leveraging electromagnetic signals for malware classification with Deep learning

September 24, 2021

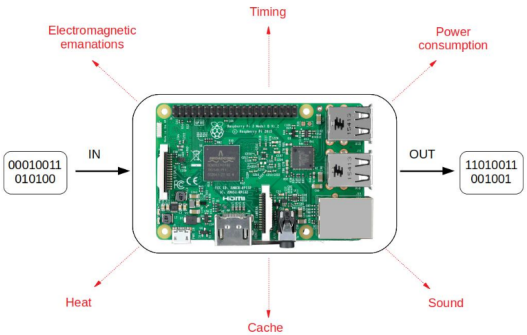
Duy-Phuc PHAM

Introduction

- Trending of attacks on embedded devices.
- Malware analysis and bypasses: difficulties such as malware evasion techniques, packed and obfuscated samples.
- Limited resources of embedded devices, diversity of architectures.

Proposed solutions

- Black-box monitor
- Side channel information
  - Power consumption, heat & EM
  - Sound (freq.)
  - Cache, HPC (software)



EMSEC embedded security & cryptography

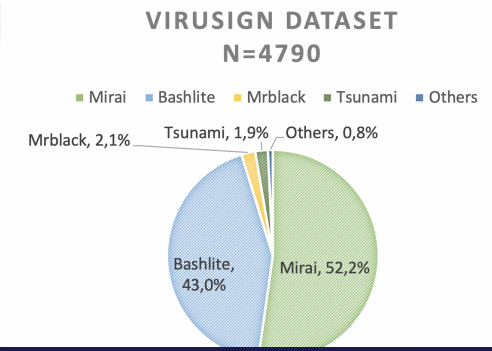
UMR IRISA

Outline

- Generate datasets: Malware insights
- AHMAM framework: Automatically record EM emanations using oscilloscopes.
- Data processing
- Machine Learning & Deep Learning classification

Dataset: Understanding of IoT malware epidemiology

- AVClass to classify malware labels



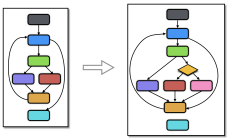
Dataset: Understanding of IoT malware insights

- AVClass to classify malware labels
- Code reviews and reverse engineering

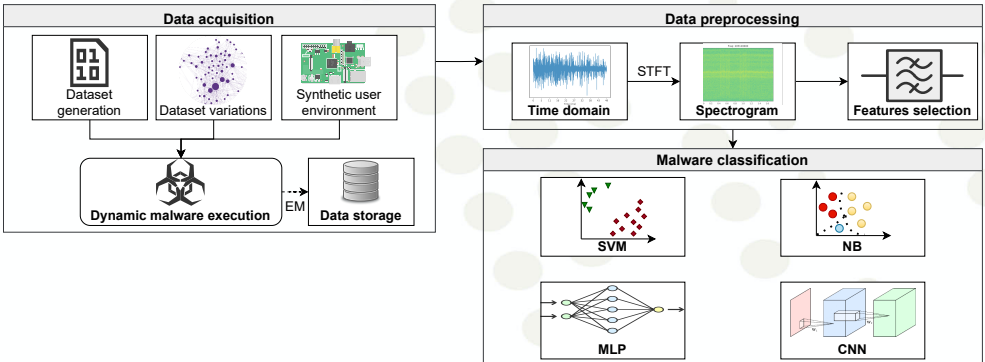
DDoS	Ransomware	Rootkits
Mirai	GonnaCry	KeySniffer
Bashlite	(AES, Blowfish)	MaK_It

Dataset: Variations

- AVClass to classify malware labels
- Code reviews and reverse engineering
- Obfuscations
  - UPX, Tigress, O-LLVM
  - Opaque predicates, bogus control flow, instructions substitution, control-flow flattening; packer and code virtualization



Proposed framework (Open source)



EMSEC embedded security & cryptography

UMR IRISA

Target device

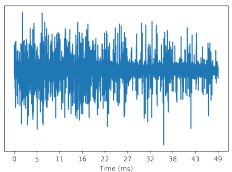
Requirements

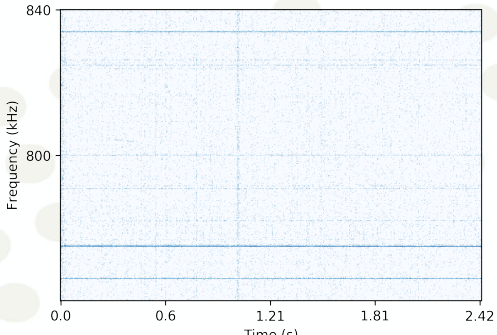
- Multi-purpose embedded device.
- Prominent architecture (ARM).
- Vulnerable to EM side-channel attack.

→ Raspberry Pi 2B

Data processing

- 100k(traces) * 2(MSs) * 2.5(s)
- Short-time Fourier transform
- Band-pass filter

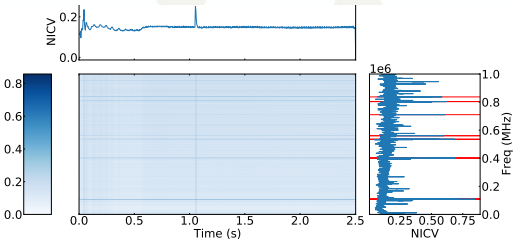




Features selection

$$\mathrm{NICV}(X, Y) = \frac{\mathrm{Var}[\mathbb{E}[X|Y]]}{\mathrm{Var}[X]}$$

$$F_{\text{extract}} = \{\mathrm{argmax}_{\epsilon}(\frac{1}{D}\sum_{d=0}^{D-1}[(\mathrm{NICV}(X, Y))_d^F]\}$$



EMSEC embedded security & cryptography

UMR IRISA

Machine Learning & Deep Learning models

- Naive Bayes (NB)
- Support vector machine (SVM)
- Multi-Layer Perceptron (MLP)
- Convolutional Neural Network (CNN)

Malware classification results

Scenarios	#	MLP	CNN	LDA+NB	LDA+SVM
Type	4	99.75	**99.82**	97.97	98.07
Family	6	98.57	**99.61**	97.19	97.27
Novelty	5	88.41	**98.85**	98.25	98.61
Virtualization	2	95.60	**95.83**	91.29	91.25
Packer	2	93.39	**94.96**	83.62	83.58
Obfuscation	7	73.79	**82.70**	64.29	64.47
Executables	31	73.56	**82.28**	70.92	71.84

Table 1. Accuracy obtained with MLP, CNN, LDA + NB and LDA + SVM applied on several scenarios.

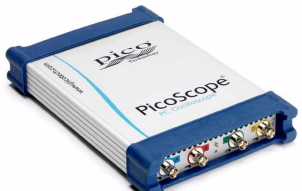
Conclusion

- Published work: Duy-Phuc Pham, Damien Marion, Mathieu Mastio, and Annelie Heuser. ACSAC 2021. *Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification.*
- Open source: https://github.com/ahma-hub/
- Future work
  - Implement research on Software Defined Radio.
  - Extend to side-channel rootkits detection.

Thank you!

Monitor device(s)

- Picoscope 6000
- Keysight Infiniium
- Nooelec Smart SDR

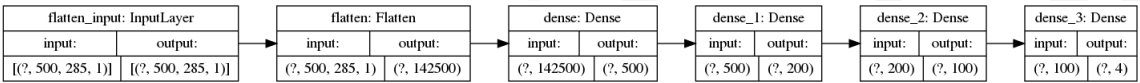


EMSEC
embedded security & cryptography

UMR IRISA

Deep Learning models

- Multi-Layer Perceptron (MLP)
- Convolutional Neural Network (CNN)



EMSEC embedded security & cryptography

UMR IRISA

Deep Learning models (MLP)

Layer	Size	Filter	Activation
Flatten	spectrogram_size	_	LeakyReLU
Dense	500	_	LeakyReLU
Dense	200	_	LeakyReLU
Dense	100	_	LeakyReLU
Dense	nb_labels	_	softmax

Deep Learning models (CNN)

Layer	Size	Filter	Activation
Convolution	64	7×7	relu
Max Pooling	64	2×2	_
Convolution	128	3×3	relu
Convolution	128	3×3	relu
Max Pooling	128	2×2	_
Convolution	256	3×3	relu
Convolution	256	3×3	relu
Max Pooling	256	2×2	_
Dense	128	_	relu
Dense	64	_	relu
Dense	nb_labels	_	softmax