Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification

ACSAC, December 10th, 2021
Introduction

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

→ Malware analysis through side-channel signals.
Introduction (2)

- Side channel information
  - Power consumption, heat
  - Electromagnetic
  - Sound
  - Cache, HPC (software)
- Black-box dynamic execution
State of the art

- Anomaly detection using power consumption and EM.
- Lack of research on in-the-wild malware side-channel detection.
- No variations regarding obfuscation and packers.
- Our contributions:
  - Malware classification
  - Real-world malware
  - Malware variants
Dataset: Understanding of IoT malware epidemiology

AVClass to classify malware labels
Dataset: Malware through code reviews and reverse engineering

<table>
<thead>
<tr>
<th>DDoS</th>
<th>Ransomware</th>
<th>Rootkits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirai</td>
<td>GonnaCry</td>
<td>KeySniffer</td>
</tr>
<tr>
<td>Bashlite</td>
<td>(AES, Blowfish, DES)</td>
<td>MaK_It</td>
</tr>
</tbody>
</table>
Dataset: Variations through Obfuscations

- UPX, Tigress, O-LLVM
- Opaque predicates, bogus control flow, instructions substitution, control-flow flattening; packer and code virtualization
Proposed framework (Open source)

- **Data acquisition**
  - Dataset generation
  - Dataset variations
  - Synthetic user environment
  - Dynamic malware execution

- **Data preprocessing**
  - Time domain
    - STFT
  - Spectrogram
  - Features selection

- **Malware classification**
  - SVM
  - NB
  - MLP
  - CNN
Target device

Requirements

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

→ Raspberry Pi 2B
Data and pre-processing

- **Raw traces:**
  106k(traces) × 2(MS/s) × 2.5(s) [1.2To]

- **Time-frequency representation:**
  Short-time Fourier transform
  
  \[
  \begin{align*}
  \text{windows} &= 8192 \\
  \text{overlap} &= 4096 
  \end{align*}
  \]
Features selection

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

\[ F_{\text{extract}} = \arg\max_{\epsilon} \left( \max \left[ \text{NICV}(X, Y)^{D_f} \right] \right)_{f < F} \]
### Machine Learning & Deep Learning models

- Linear Discriminant Analysis (LDA) + Naive Bayes (NB)
- Linear Discriminant Analysis (LDA) + Support vector machine (SVM)
- Multi-Layer Perceptron (MLP)
- Convolutional Neural Network (CNN)
Malware classification results

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>#</th>
<th>MLP</th>
<th>CNN</th>
<th>LDA+NB</th>
<th>LDA+SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obfuscation</td>
<td>7</td>
<td>73.79[28]</td>
<td>82.70[24]</td>
<td>64.29[10]</td>
<td>64.47[10]</td>
</tr>
</tbody>
</table>

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

- Classify various malware samples in multiple in-the-wild scenarios.
- Obfuscation technique can be distinguished.
- Evaluation of both DL/ML.
- Evaluated Artifacts:
  - Code: https://github.com/ahma-hub/analysis/wiki
  - Data: https://zenodo.org/record/5414107
Thank you!