Acceleration of AI for Implementation Security Testing

Stjepan Picek

OPTIMIST, April 17, 2025

Outline

1 Introduction

2 Implementation Attacks

3 Conclusions

Outline

1 Introduction

2 Implementation Attacks

3 Conclusions

Artificial Intelligence

AI is the new electricity. (Andrew Ng)

- Computer vision.
- Healthcare.
- Speech recognition.
- Natural Language Processing.
- Robotics.
- Security.
- ...

Artificial Intelligence

- Powerful hardware.
- Big data.
- Novel applications.

Outline

1 Introduction

2 Implementation Attacks

3 Conclusions

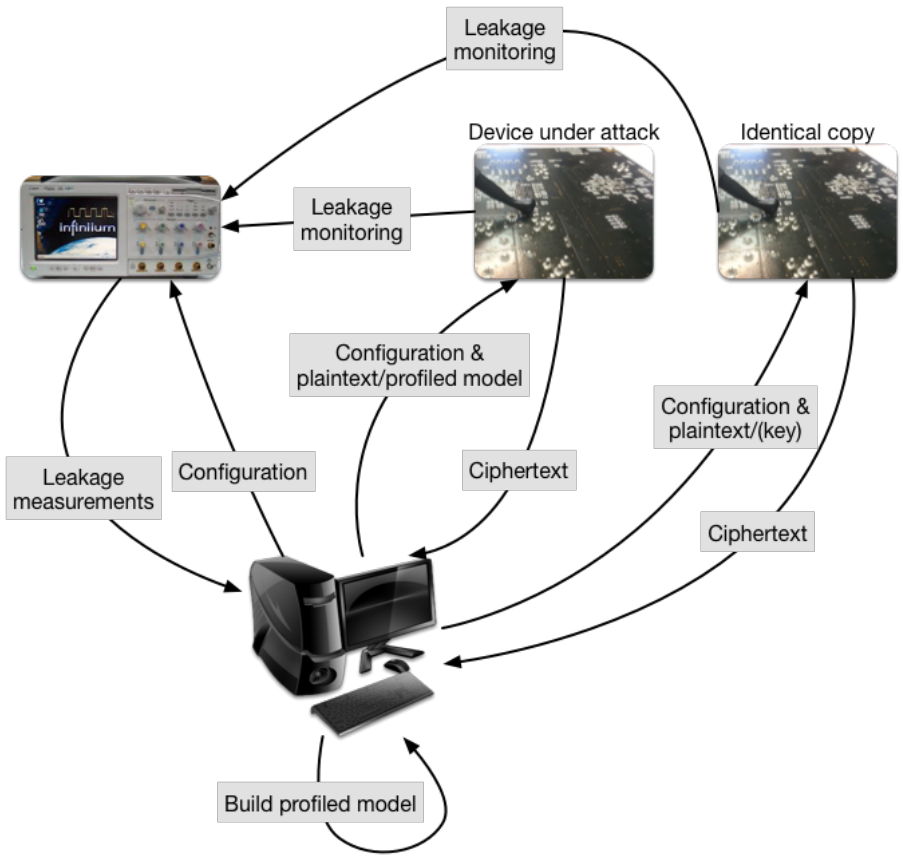
Implementation Attack Categories

- **Side-channel attacks**.
- Fault injection attacks.

Profiling Attacks

- Profiling attacks have a prominent place as the most powerful among side-channel attacks.
- Within profiling phase the adversary estimates leakage models for targeted intermediate computations, which are then exploited to extract secret information in the actual attack phase.
- Machine (deep) learning now extensively used here.

Profiling Attacks



- Profiling attacks are more complicated than the direct attacks.
- The attacker must have a copy of the device to be attacked.

Standard Architectures

- Hyperparameter tuning is extremely important.
- General design principles.
- Methodologies.
- Random search.
- Grid search.
- Advanced techniques.
- Can we even hope to have standard architectures? Do we need them?

Standard Interfaces and Libraries

- We already have several publicly available tools.
- Unfortunately, it seems there is little acceptance.
- Reasons? Many techniques/papers, constantly being out of date, relative ease to make something from scratch, etc.
- `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_AI_guide.pdf?__blob=publicationFile&v=7`

Standard Datasets

- We must be able to attack relevant targets.
- ASCAD was a good start but with better attacks, we need new datasets.
- Portability.
- Stronger masking.
- Different ciphers.
- Hardware targets.

Outline

1 Introduction

2 Implementation Attacks

3 Conclusions

Conclusions

- Deep learning is efficient and powerful option for SCA.
- Current results are very promising as we can break protected targets even with very small architectures.
- If we do not need big(er) architectures, how difficult is tuning?
- If tuning is not difficult, do we need standard architectures?
- Doing the attacks/evaluations is only half of the picture!

- AI is also very useful for fault injection!

Questions?

Thank you for your attention!

stjepan.picek@ru.nl