Machine Learning(ML) based Side-Channel Analysis on AES Cryptosystem Through Power Consumption Data

Sourin Manna
CrS2218

April 2024

1 Introduction

In the world of cybersecurity, protecting sensitive information is a constant challenge. The Advanced Encryption Standard (AES) is a strong encryption method widely trusted for keeping data safe. However, hackers are always looking for new ways to break into systems. One method they use is called side-channel attacks, where they watch how much power a device uses during encryption to figure out the secret key. We are working with a power consumption dataset comprising 20,000 rows, representing the power consumption during the encryption of 20,000 plaintexts using AES, and 17,000 columns, signifying 17,000 features. These features are gathered by measuring power consumption every nanosecond.

2 Background

2.1 Side-Channel Analysis

One method of attacking cryptographic algorithms by attempting to exploit hardware vulnerabilities is side-channel analysis (SCA), which involves analyzing device information associated with the internal workings of an algorithm. More specifically, side channel analysis entails learning information

about a system by analyzing things like device power consumption, electromagnetic radiation, timing, and sound, and in doing so attempting to reveal information that was intended to remain unknown to unauthorized parties.

2.2 Machine Learning

Machine learning is an area of computer science a subset of Artificial Intelligence(AI) that uses algorithms to learn from data to build computer systems that can learn and improve on their own. In our project, we used different types of machine-learning classification algorithms:

- Random Forest: Random Forest employs an ensemble of decision trees for classification and regression tasks.
- Naive Bayes: Naive Bayes is a probabilistic classifier based on Bayes' theorem, assuming independence among features.
- Artificial Neural Network(ANN): Artificial Neural Network (ANN) mimics the human brain's neural network structure to learn complex patterns.
- K-nearest neighbor: K-nearest neighbor assigns a class to an unlabeled example based on the majority class of its k nearest neighbors.
- XGBoost: XGBoost employs gradient boosting to iteratively build a series of decision trees for predictive modeling.

2.3 Advanced Encryption Standard (AES-128)

AES, or the Advanced Encryption Standard is a symmetric encryption algorithm and a block cipher and is one of the most widely used symmetric-key algorithms today.AES can operate with 128, 192, or 256-bit keys, which is a significant step up from what is commonly regarded as its predecessor. Here we work with 128-bit AES.

3 Methodology

First, we collect our data where the data is a power consumption of AES encryption. where dataset We are working comprising 20,000 rows, representing

the power consumption during the encryption of 20,000 plaintexts using AES, and 17,000 columns, signifying 17,000 features. These features are gathered by measuring power consumption every nanosecond. Here 20,000x17,000 of our independent data now we find our dependent data. where the dependent feature is the Hamming weight of the 1st 8-bit of cipher text obtained after performing XOR between the plaintext and key, followed by passing through the S-box. Since we find dependent data(Hamming weight) we apply several multi-class machine learning models to predict Hamming weight.

4 Results

Through our internship project, we explored the vulnerabilities of the Advanced Encryption Standard (AES) cryptosystem to side-channel attacks using power consumption data. By applying various machine learning models, our final goal is to predict the 128-bit encryption key through a multiclass classification approach. Specifically, we first, focused on predicting the hamming weight of the first 8 bits of the cipher text after XOR with the key and S-box transformation.
After rigorous experimentation, we achieved promising results for predicting hamming weight. Utilizing XgBoost, we attained a significant accuracy rate of 63.9% in predicting the hamming weight, outperforming Logistic Regression (44.2%), Random Forest (47.9%), and ANN (43.95%). This success underscores the potential of machine learning in identifying vulnerabilities in AES encryption systems and highlights avenues for further research and development in enhancing encryption security.

5 Discussion and further works

Next, we try to find a 128-bit secure key using the hamming weight of 1st 8-bit cipher test. we build several multiclass classification machine learning models to predict 128-bit secure keys.

Reference

[1]Machine Learning-Based Side-Channel Analysis on the Advanced Encryption Standard, Jack Edmonds, Tyler Moon.