Лабораторная работа № 1

Изучение криптографических атак с помощью машинного обучения на физически неклонируемые функции

Физически неклонируемые функции (ФНФ) часто используются в качестве криптографических примитивов при реализации протоколов аутентификации.

Рассмотрим простейший из них, основанный на на запросах и ответах (challenge response). Схема данного типа протокола приведена на рис. 1.

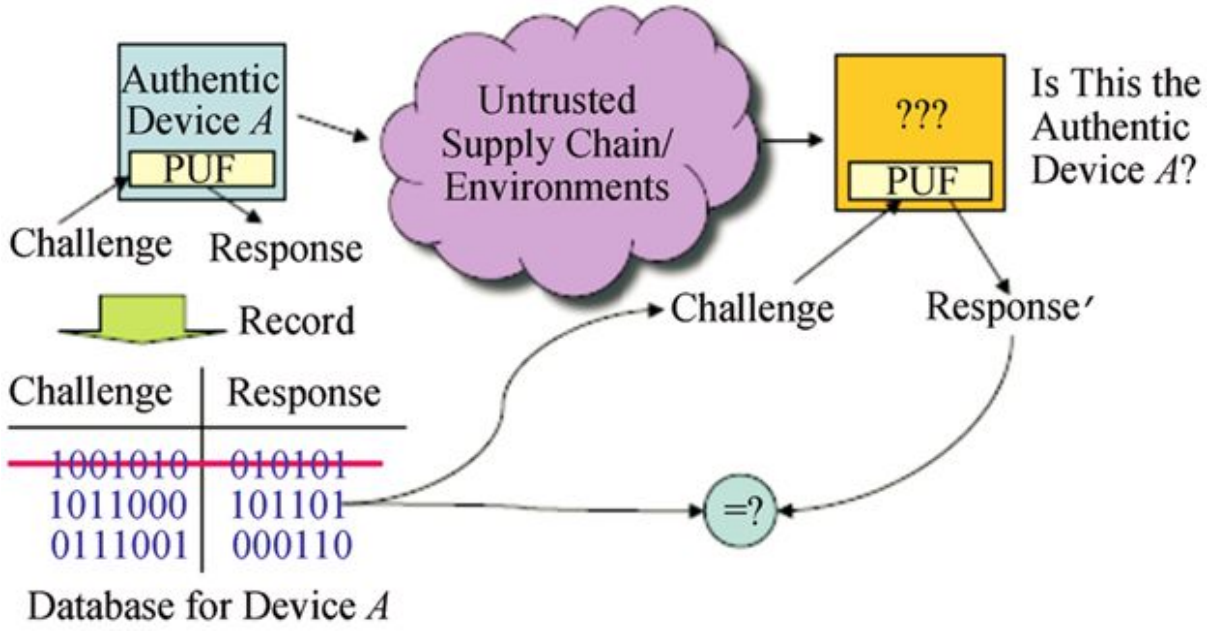

Рисунок 1. Протокол аутентификации, основанный на ФНФ.

Более подробно о физически неклонируемых функциях можно прочесть:

1. https://habr.com/post/343386/
2. https://www.researchgate.net/profile/Alexander_Ivaniuk/publication/322077869_Proektirovanie_vstraivaemyh_cifrovyh_ustrojstv_i_sistem/links/5a43724caca272d2945a0464/Proektirovanie-vstraivaemyh-cifrovyh-ustrojstv-i-sistem.pdf (глава 5, раздел 4)

Задание

1. Изучите классическую работу У. Рурмаира о криптографических атаках с помощью машинного обучения на ФНФ.

U. Ruhrmair et al., “Modeling attacks on physical unclonable functions,” in Proc. ACM Conf. on Comp. and Comm. Secur. (CCS’10), Oct. 2010, pp. 237–249.
https://eprint.iacr.org/2010/251.pdf

2. Сформулируйте задачу в терминах машинного обучения.
3. Предложите возможные методы решения.
4. Какой объем обучающей выборки необходим?
5. Развернутые ответы на вопросы оформите в виде отчета.

Лабораторная работа № 2

Реализация криптографических атак с помощью машинного обучения на физически неклонируемые функции

Дан набор данных следующего вида:

1. *N*-битное двоичное число (запрос);
2. Ответ ФНФ на данный запрос (0 или 1);
3. *N* изменяется от 8 до 128 с шагом 8.

Данные хранятся в архивах Base8.zip, Base16.zip, …, Base128.zip.

Задание

1. Обучите модель, которая могла бы предсказывать ответы по запросам, которых нет в обучающей выборке.
2. Применить как минимум 3 различных алгоритма (например, метод опорных векторов, логистическая регрессия и градиентный бустинг).
3. Какая метрика наиболее подходит для оценки качества алгоритма?
4. Какой наибольшей доли правильных ответов (Accuracy) удалось достич?
5. Какой размер обучающей выборки необходим, чтобы достигнуть доли правильных ответов минимум 0.95?
6. Как зависит доля правильных ответов от *N*?
7. Ответы на вопросы представьте в виде графиков.
8. Оформите отчет.

Лабораторная работа № 3

Реализация криптографических атак с помощью машинного обучения на модифицированные физически неклонируемые функции

Дан набор данных следующего вида:

1. *N*-битное двоичное число (запрос);
2. Ответ ФНФ на данный запрос (0 или 1);
3. *N* изменяется от 8 до 128 с шагом 8.

Данные хранятся в архивах Base8.zip, Base16.zip, …, Base128.zip.

Предположим, что значения запросов были обработаны криптографически стойкой хеш-функцией (SHA-256). В связи с этим атака с помощью методов машинного обучения против модели «черного ящика» не годится. В данном случае применим метод Эволюционной стратегии адаптации ковариационных матриц (Covariance Matrix Adaptation Evolution Strategy, CMA-ES).

Статья Г. Бекера показывает применимость данного метода в описанной выше ситуации.

G. T. Becker, “On the pitfalls of using arbiter-PUFs as building blocks,” IEEE Trans. on Comp.-Aided Des. of Integr. Circ. and Syst., vol. 34, no. 8, pp. 1295–1307, Apr. 2015.

https://eprint.iacr.org/2014/532.pdf

Задание

1. Обучите модель на модифицированных с помощью SHA-256 запросах.
2. Какой максимальной доли правильных классификаций удалось достичь?
3. Изучите алгоритм CMA-ES, приведите краткие теоретические сведения о нем.
4. Какой доли правильных классификаций удалось добиться с помощью алгоритма CMA-ES?
5. Оформите отчет.