Side Channel Analysis

Problem badawczy

Czy techniki uczenia maszynowego są w stanie przełamać zabezpieczenie typu *masking* w **SCA**?

SCA (*Side Channel Analysis*) to klasa ataków kryptoanalitycznych, która ignoruje matematyczną siłę algorytmu, a zamiast tego atakuje jego fizyczną implementację.

Dane

W projekcie wykorzystuję zbiór danych ASCAD v1 variable key, zawierający próbki pochodzące z mikrokontrolera ATMega8515 wykonującego szyfrowanie algorytmem AES.

Cel

Celem jest pozyskanie klucza, którego kontroler używa do szyfrowania danych, na podstawie zmierzonych wartości poboru mocy. Teoretycznie jest to możliwe - pobór mocy mikrokontrolera jest skorelowaneyz wagą Hamminga przetwarzanych danych.

Zadanie to jest klasyfikacją szeregów czasowych, o tyle specyficzną, że poszczególne timestampy możemy traktować również jako cechy, ponieważ ślady są ze sobą zsynchronizowane.

Akumulacja wiarygodności

Problemem w SCA jest bardzo duże zaszumienie danych, przez co ciężko uzyskać pewny model. Jak przeglądałem literaturę związaną z tym zagadnieniem, zauważyłem, że model jest tu traktowany jako swojego rodzaju weak learner, a cała siła ataku tkwi w akumulacji wiarygodności na przestrzeni ataku. Co to znaczy? Załóżmy, że mamy N próbek walidacyjnych T pochodzących z szyfrowania tym samym kluczem. Ostateczne prawdopodobieństwo, że dany kandydat na etykietę $\hat{z}$ jest poprawny to:

$$log(P(\hat{z}|T)) = \sum_{i=0}^{N} log(P(\hat{z}|T_i))$$

Ewaluacja

Metryka Perceived Information mierzy ile średnio bitów klucza model odzyskuje na próbkę.

$$PI(k, X^{(k)}) = H + \frac{1}{N} \sum_{i=0}^{N} log(P(k|X_i^{(k)}))$$

$X^{(k)}$ - ślady dla danego klucza k.

S-box

Funkcja S-box to pierwsza nieliniowa operacja w algorytmie AES. Polega ona na podmianie bajtu tekstu jawnego d zmieszanego z bajtem klucza k przy użyciu tabeli podstawień:

$$z = \text{Sbox}(d \oplus k)$$

Operacja S-box jest wrażliwa, bo jest to punkt, w którym klucz jest po raz pierwszy bezpośrednio mieszany z danymi wejściowymi. Nieliniowość tej operacji ułatwia statystyczne odróżnienie poprawnego klucza od błędnego.