Side Channel Analysis Contest 2022			
6. BNN			
학교	국민대학교	이름	이현호

1. BNN의 가중치 복구를 위한 논리 요약

본 라이트 업에서는 주어진 CTF-6-BNN-input.bin 파일에서 한 입력 노드는 1 또는 0 값을 가지므로 입력 노드 8개를 하나의 8비트 값으로 놓고 연산한다. 예를 들어 8개의 입력 노드 [0 0 0 1 1 1 1 1]는 0b00011111 이며 이는 십진수로 31이다. 가중치들은 1 또는 -1의 값을 가지지만 -1을 0으로 생각한다면 입력값에 가중치를 곱하여 누적하는 연산을 특정 비트 연산들로 대체 할 수 있다. 이를 활용하여 첫 번째 [8 × 8] 가중치를 8개의 8비트 값으로 변환해 가중치를 구할 수 있다. 마찬가지로 두 번째 가중치 또한 같은 논리로 구할 수 있다.

2. 가중치 복구

본 라이트업에서 사용할 기호와 그에 대한 정의는 [표 1]과 같다. ($Sign(X)$는 계단 함수를 나타냄)

기호	정의
$XNOR$	exclusive-NOR 연산
$Popcount(X)$	X의 비트 stream에서 1의 갯수
$N(X)$	X의 총 비트 길이
$Sign(X)$	$+1,\ \text{if}\ \ X \geq 0$ $-1,\ \ else$
in_n	입력 노드 n개를 하나의 n비트 값으로 나타낸 것
$weight_n$	[1 × n] 가중치에서 -1을 0으로 둔 하나의 n비트 값
•	Dot product

[표 1] 기호 및 정의

입력 노드 8개를 [8 × 1]인 $\overrightarrow{in}$ 로 표현하고 [1 × 8] 가중치를 $\overrightarrow{weight}$라고 하고 입력 노드 8개를 하나의 8비트 값으로 놓은 값과 -1을 0으로 바꾼 후 [8 × 1] 가중치를 8비트 값으로 놓은 값을 각각 in_8, $weight_8$ 라고하자. 그렇다면 두 벡터 값의 Dot product 값은 [수식 1]로 표현해 줄 수 있다.

$$\overrightarrow{in} \bullet \overrightarrow{weight} = 2 \times Popcount(in_8\ XNOR\ weight_8) - N(in_8)$$

[수식 1]

[수식 1]이 성립하는 예를 들어보자.

BNN에서 입력값 $\overrightarrow{A}$ = [1 -1 -1 1 -1], 가중치값 $\overrightarrow{B}$ = [-1 1 1 1 1] 이라고 하자.

입력값에 가중치를 곱하여 모두 누적한 값은 다음 연산과정과 같다.

$\overrightarrow{A} \bullet \overrightarrow{B}$ = (1 × -1) + (-1 × 1) + (-1 × 1) + (1 × 1) + (-1 × 1) = -3

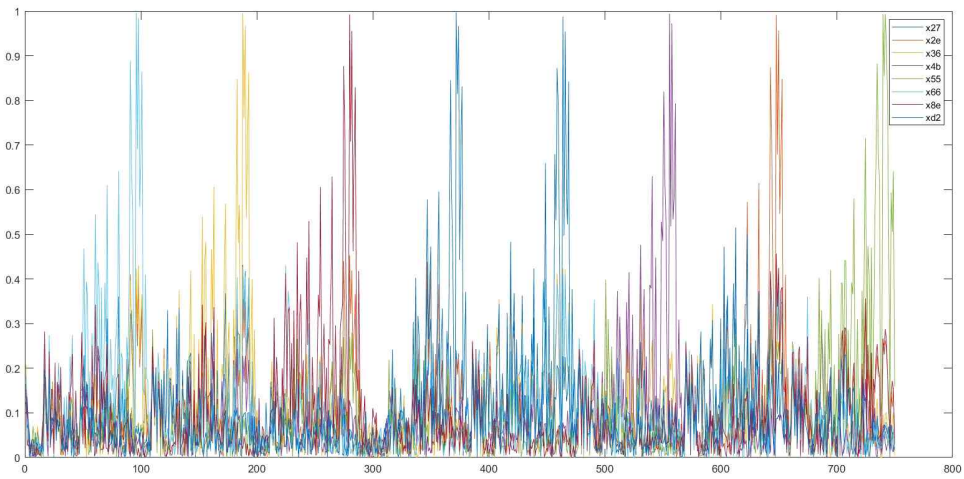
-1을 0으로 두$XNOR$과 $Popcount$에 의한 연산 결과는 다음과 같다.

$Popcount(A_5\ XNOR\ B_5)$ = 1 이고 $N(A_5) = 5$ 이므로 $2 \times Popcount(A_5\ XNOR\ B_5) - N(A_5)$ = -3

주어진 입력값 정보들과 첫 번째 가중치를 0~255(8비트) 값 중 하나로 두고 $XNOR$, $Popcount(X)$, $N(X)$ 3가지 연산을 활용하여 중간값을 구한다. 구한 중간값을 바탕으로 주어진 파형을 활용하여 Correlation Power Analysis를 수행한 결과는 [표 2]와 같다. 또한 [그림 1]을 통해 [표 2]에서 구한 첫 번째 가중치 값들의 연산 순서를 알 수 있다.

첫 번째 가중치	상관계수
0x66	0.995761
0x36	0.995134
0x8e	0.992615
0xd2	0.997031
0x27	0.986751
0x4b	0.994735
0x2e	0.990768
0x55	0.992425

[표 2] Correlation Power Analysis 결과

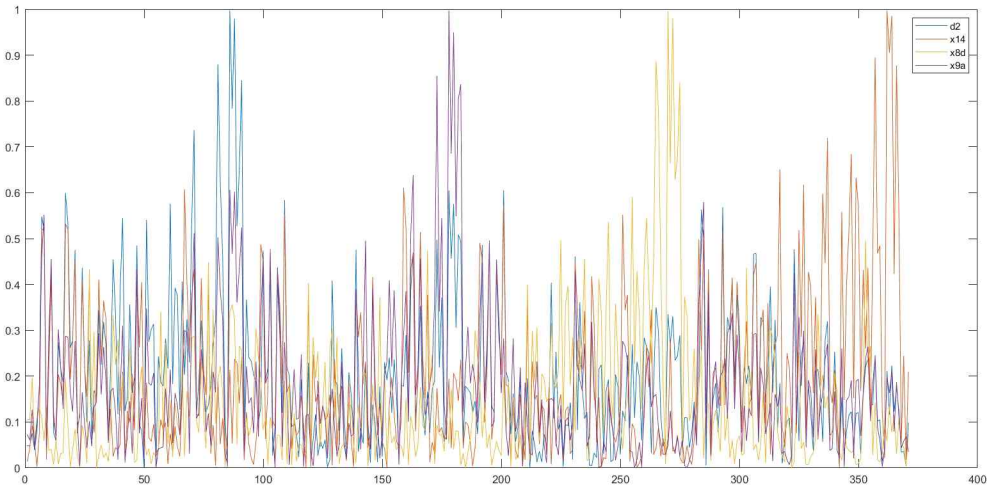


[그림 1]

두 번째 가중치는 위에서 구한 첫 번째 가중치를 활용하여 위와 똑같은 방법으로 4개의 값을 구할 수 있다. 그 결과는 [표 3]과 같다. 또한 [그림 2]을 통해 [표 3]에서 구한 두 번째 가중치 값들의 연산 순서를 알 수 있다.

두 번째 가중치	상관계수
0xd2	0.996417
0x9a	0.997555
0x8d	0.995449
0x14	0.996548

[표 3] Correlation Power Analysis 결과-2



[그림 2]

3. 위의 찾은 가중치를 바탕으로 복구한 Flag의 ASCII 코드는 다음과 같다.

SCA_is-POWERFUL!