Probing the Machine Learning Network Defense Models

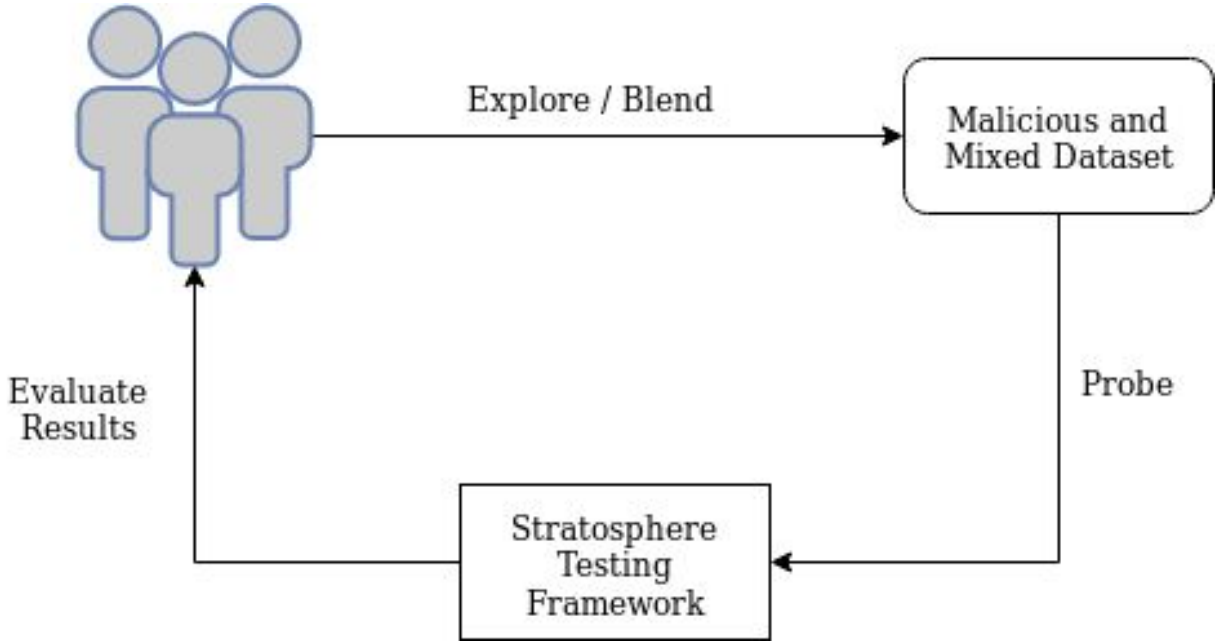
The StratoKite Team
(Tam, Sri, Omkar)

Stratosphere IPS

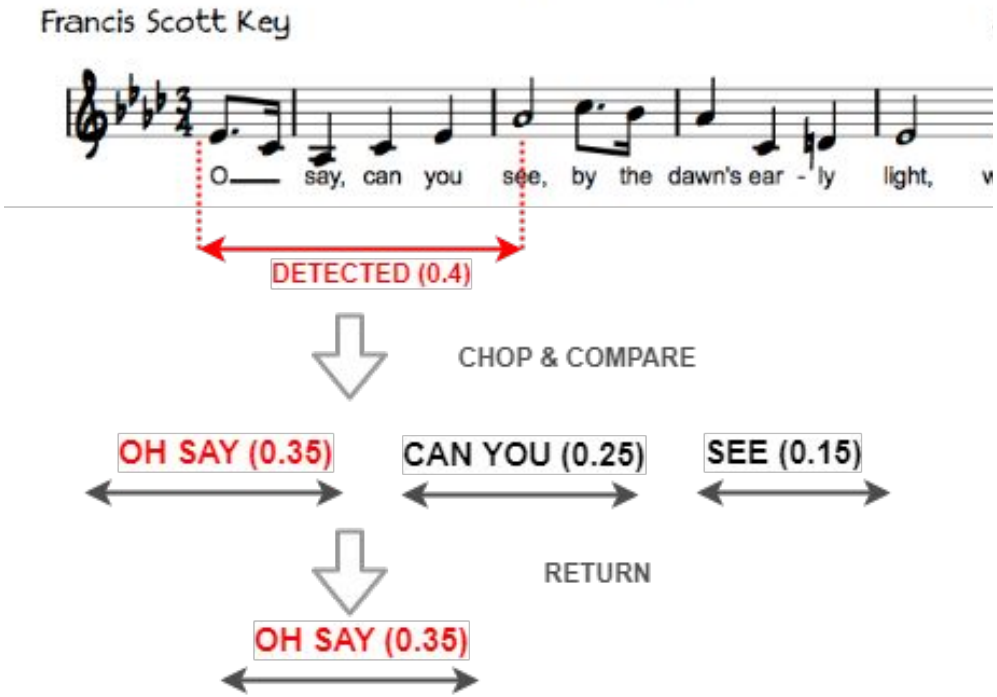
- The 4 Tuple: <Src IP, Dest IP, Dest Port, Protocol>

- It Model the states based on four features:
  - Size of the flow
  - Duration of the flow
  - Periodicity of the flow
  - Time between consecutive flows

Methodology



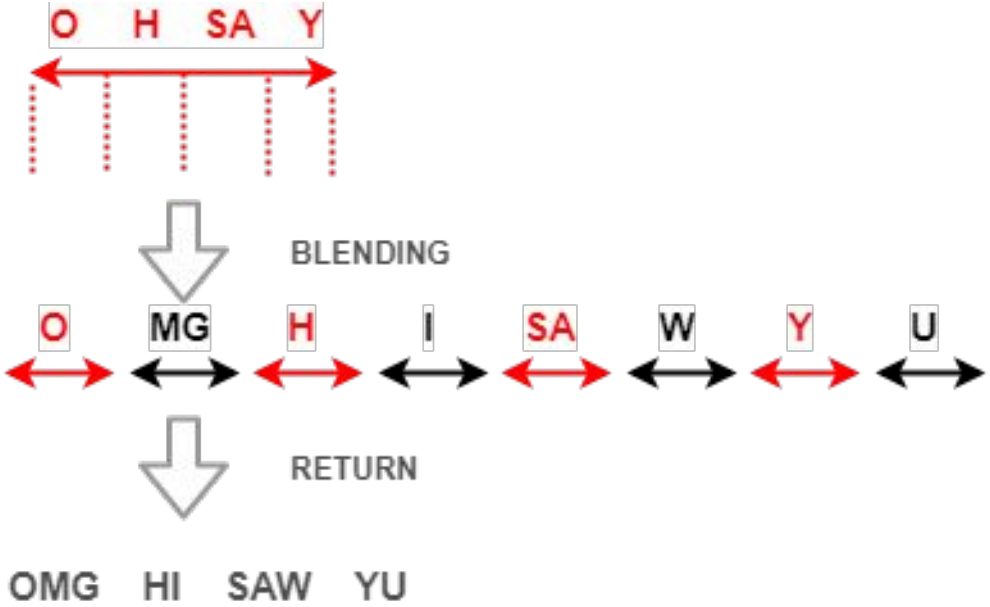
Methodology - Explore Function



Algorithm 1 Explore algorithm

```
1:  m ←malicious-payloads          ▷ locate pure malicious contents
2:  score ←detect(m)               ▷ get detection score of m
3:  M[n] ←chop(m)                  ▷ chop m into n sections
4:  procedure EXPLORE(M)
5:      hotspot ←0
6:      i ←0
7:      for i < n do
8:          s1 ←detect(M[i])
9:          s2 ←detect(M - M[i])   ▷ M without M[i]
10:         if argmax(s1, s2) > score then
11:             score ←argmax(s1, s2)
12:             hotspot ←i
13:     return timeframe(hotspot)  ▷ Return start/end time
```

Methodology - Blend Function



Algorithm 2 Blending algorithm

```
m ←malicious-payloads                ▷ pure malicious contents
n ←normal-payloads                   ▷ non-malicious contents
procedure BLEND(n,m)
    frame[start, end] ←Explore(m)
    M[3] ←chop(m, frame[start], frame[end])
    N ←extract(n)                    ▷ take a portion of n
    M[2] ←interlace(M[2],N)
    export ←(M[1] + M[2] + M[3])
    export ←timeSync(export)
    return export
```

Results

Experiment 1:

S.no	Type of packets	Slot 1	Slot 2	Slot 3	Factor of Stratosphere	No.of Malicious Detections
1	ALL	00-05	05-10	10-15	Baseline	2
2	ALL	-	05-10	10-15	Duration	1
3	ALL	00-05	-	10-15	Duration	0
4	ALL	00-05	05-10	-	Duration	0
5	ALL	05-10	10-15	00-05	Periodicity	3
6	ALL	05-10	00-05	10-15	Periodicity	3
7	ALL	10-15	00-05	05-10	Periodicity	3
8	ALL	10-15	05-10	00-05	Periodicity	3
9	DNS	00-05	05-10	10-15	Size(Reduction)	3
10	DNS	-	05-10	10-15	Size(Reduction) and Duration	1
11	DNS	00-05	-	10-15	Size(Reduction and Duration	0
12	DNS	00-05	05-10	-	Size(Reduction) and Duration	1
13	DNS	05-10	10-15	00-05	Size(Reduction) and Periodicity	3
14	DNS	05-10	00-05	10-15	Size(Reduction) and Periodicity	3
15	DNS	10-15	00-05	05-10	Size(Reduction) and Periodicity	3
16	DNS	10-15	05-10	00-05	Size(Reduction) and Periodicity	3

Results

Experiment 2:

S.no	Type of packets	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	No. of Malicious Detections
1	ALL	D5-1	M5-1	D5-2	M5-2	D5-3	M5-3	D5-4	-	0
2	ALL	D5-1	D5-2	M5-1	D5-3	M5-2	D5-4	M5-3	-	0
3	ALL	D5-1	D5-2	D3-1	M5-1	D5-3	M5-2	D5-4	M5-3	0
4	ALL	D3-1	M5-1	D3-2	M5-2	D3-3	M5-3	D3-4	-	0

Stratosphere-Results

Conclusion and Future Work

- The Stratosphere IPS is not stable because the results are surprisingly good i.e. 100% success rate and also there a lot of other issues as well.

- We can improve this by probing for longer time periods and also by automating the attacks.