Offline and Live Testing of Evasion Resilience in Network Intrusion Detection Systems

Leo Juan Christian Kreibich
Chih-Hung Lin Vern Paxson

iCAST

The Problem of *Evasion*

- Presence of adversary raises **fundamental** problems for Network Intrusion Detection Systems (NIDS)
  - Network traffic passively analyzed from within a network is inherently **ambiguous**
- Examples:
  - *How will end-system reassemble inconsistent fragments?*
  - *What about inconsistent TCP segments?*
  - *What sequence #s in RSTs will tear down a connection?*
  - *Inconsistent UDP length fields?*
  - > 70 others! [HKP01]

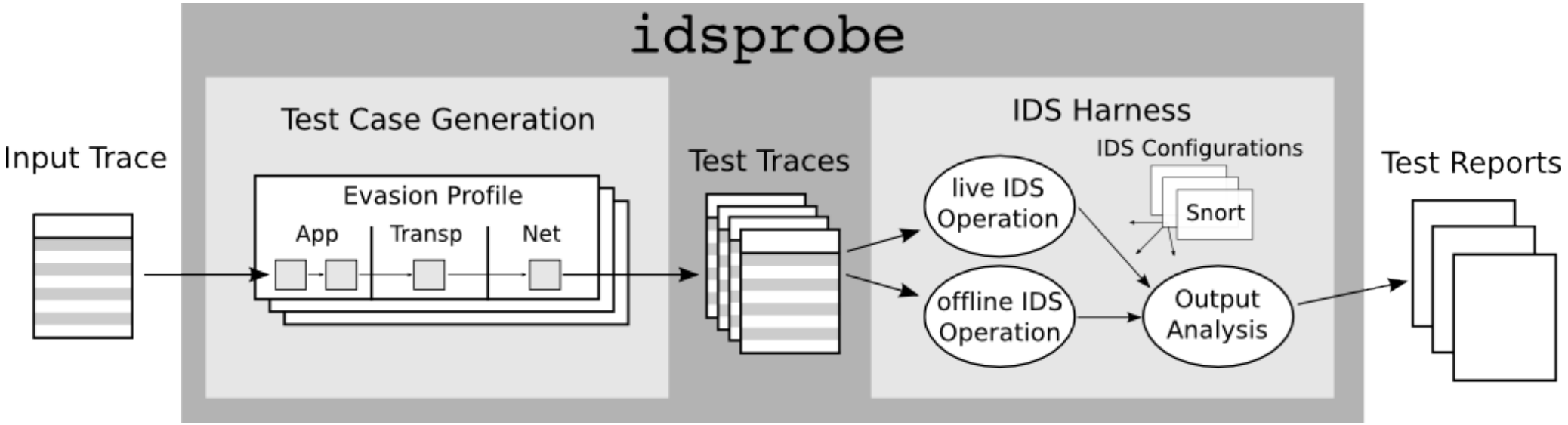
The Problem of *Evasion, con't*

- Evasions can occur at **different semantic levels** (network/transport/app.)
- Can't alert on mere presence of ambiguity due to the problem of "crud"
  - I.e., real-world traffic full of weird-but-benign ambiguities
- Analyzing network traffic at a high semantic level requires extensive **state** … which an adversary can **target**.

How Well Do Today's NIDS Resist Evasion?

- Answer: we **don't know**
- Vendors rarely discuss the issue
  - "*Trust us, our system is hardened*"
  - Does not provide a market advantage
- Goal of our **`idsprobe`** framework:
  - To provide sound, repeatable means to assess how well network intrusion detection systems perform in the face of evasions.

idsprobe Architecture



Trace-based `idsprobe` results

- We compared Bro 1.2.1 to Snort 2.6.1.4
- 196 test traces generated from 5 input traces containing basic HTTP GETs
- Correct signature matching in both NIDS
- But: **substantial** differences in evasion-related alerts

Trace-based `idsprobe` results, cont'd

- Snort over-reports non-issues and misses real evasions:
  - Benign right-aligned partial retransmission flagged as TCP checksum change
  - Nonsensical “evasive FIN” detections

```
[**] [111:24:1] (spp_stream4) possible EVASIVE FIN detection [**]
03/19-00:00:09.176188 10.48.0.1:2010 -> 10.48.0.81:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:77
***AP*** Seq: 0x92A Ack: 0x33928A9F Win: 0x8000 TcpLen: 20
```

  - *Sole* correct alert: overlapping IP fragments
  - Snort 2.8.0.1 fixed some issues, but introduced new ones: inconsistent forward retransmission overlap no longer detected

Trace-based `idsprobe` results, cont'd

- Observations from long-term operation
  - 24h trace of ICSI uplink
  - **Striking** absence of consensus
- Result:

  Detection of evasive maneuvers remains far less developed than basic signature matching.

Trace-based `idsprobe` results, cont'd

BRO 1.2

14,591	ContentGap
7,546	AckAboveHole
2,249	window_recision
735	bad_TCP_checksum
460	SYN_with_data
311	possible_split_routing
290	data_before_established
98	bad_ICMP_checksum
85	above_hole_data_without_any_acks
35	connection_originator_SYN_ack
30	bad_TCP_header_len
18	inappropriate_FIN
15	SYN_seq_jump
15	premature_connection_reuse
9	active_connection_reuse
8	data_after_reset
3	SYN_inside_connection
3	SYN_after_reset
3	bad_SYN_ack
2	TCP_christmas
1	RetransmissionInconsistency
1	FIN_advanced_last_seq
1	bad_UDP_checksum
26,509	

SNORT 2.6

161,862	(spp_stream4) possible EVASIVE FIN detection
36,873	(spp_stream4) possible EVASIVE RST detection
27,384	(spp_stream4) TCP CHECKSUM CHANGED ON RETRANSMISSION
1,933	(spp_stream4) Possible RETRANSMISSION detection
458	(spp_stream4) DATA ON SYN detection
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
228,640	

SNORT 2.8

4,844	TCP Timestamp is outside of PAWS window
2,058	Data sent on stream not accepting data
807	Bad segment, adjusted size $<= 0$
461	Data on SYN packet
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
5	Data sent on stream after TCP Reset
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
8,305	

Trace-based `idsprobe` results, cont'd

BRO 1.2

14,591	ContentGap
7,546	AckAboveHole
2,249	window_recision
735	bad_TCP_checksum
460	SYN_with_data
311	possible_split_routing
290	data_before_established
98	bad_ICMP_checksum
85	above_hole_data_without_any_acks
35	connection_originator_SYN_ack
30	bad_TCP_header_len
18	inappropriate_FIN
15	SYN_seq_jump
15	premature_connection_reuse
9	active_connection_reuse
8	data_after_reset
3	SYN_inside_connection
3	SYN_after_reset
3	bad_SYN_ack
2	TCP_christmas
1	RetransmissionInconsistency
1	FIN_advanced_last_seq
1	bad_UDP_checksum
26,509	

SNORT 2.6

161,862	(spp_stream4) possible EVASIVE FIN detection
36,873	(spp_stream4) possible EVASIVE RST detection
27,384	(spp_stream4) TCP CHECKSUM CHANGED ON RETRANSMISSION
1,933	(spp_stream4) Possible RETRANSMISSION detection
458	(spp_stream4) DATA ON SYN detection
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
228,640	

SNORT 2.8

4,844	TCP Timestamp is outside of PAWS window
2,058	Data sent on stream not accepting data
807	Bad segment, adjusted size <= 0
461	Data on SYN packet
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
5	Data sent on stream after TCP Reset
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
8,305	

Trace-based `idsprobe` results, cont'd

BRO 1.2

14,591	ContentGap
7,546	AckAboveHole
2,249	window_recision
735	bad_TCP_checksum
460	SYN_with_data
311	possible_split_routing
290	data_before_established
98	bad_ICMP_checksum
85	above_hole_data_without_any_acks
35	connection_originator_SYN_ack
30	bad_TCP_header_len
18	inappropriate_FIN
15	SYN_seq_jump
15	premature_connection_reuse
9	active_connection_reuse
8	data_after_reset
3	SYN_inside_connection
3	SYN_after_reset
3	bad_SYN_ack
2	TCP_christmas
1	RetransmissionInconsistency
1	FIN_advanced_last_seq
1	bad_UDP_checksum
26,509	

SNORT 2.6

161,862	(spp_stream4) possible EVASIVE FIN detection
36,873	(spp_stream4) possible EVASIVE RST detection
27,384	(spp_stream4) TCP CHECKSUM CHANGED ON RETRANSMISSION
1,933	(spp_stream4) Possible RETRANSMISSION detection
458	(spp_stream4) DATA ON SYN detection
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
228,640	

SNORT 2.8

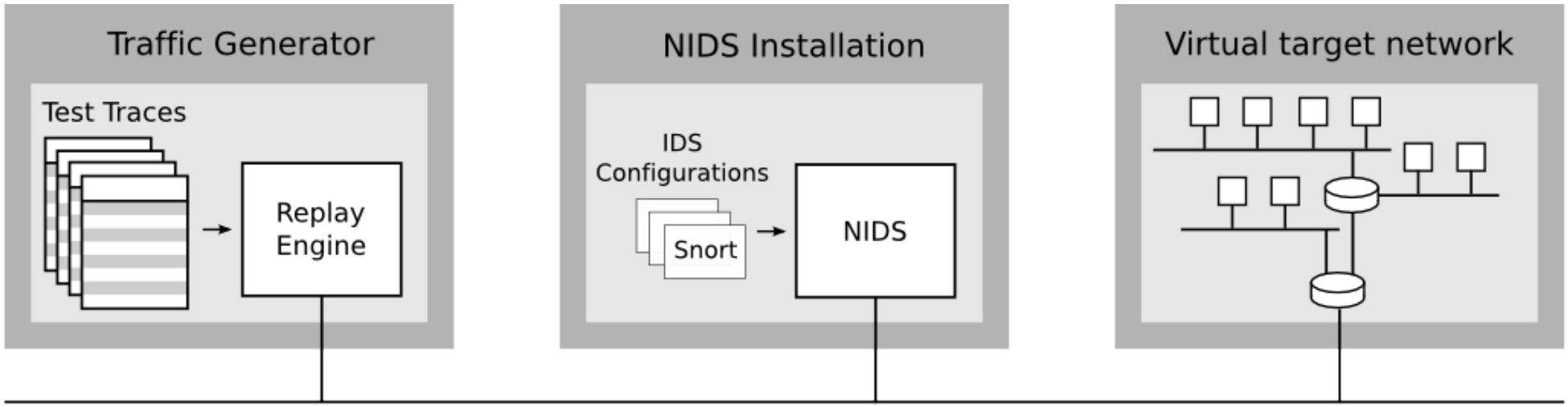
4,844	TCP Timestamp is outside of PAWS window
2,058	Data sent on stream not accepting data
807	Bad segment, adjusted size <= 0
461	Data on SYN packet
67	(snort_decoder) WARNING: ICMP Original IP Header Truncated!
30	(snort_decoder) WARNING: TCP Data Offset is less than 5!
18	(snort_decoder): Truncated Tcp Options
12	(snort_decoder): Experimental Tcp Options found
5	Data sent on stream after TCP Reset
2	(snort_decoder): Tcp Options found with bad lengths
1	(snort_decoder) WARNING: ICMP Original IP Fragmented and Offset Not 0!
8,305	

Live Testing

- Capturing full range of evasion threats and defenses requires on-line testing as well as off-line
- Additional threats:
  - Resource exhaustion (CPU, memory) …
    - … leading to packet drops
- Defenses:
  - Normalization [Handley, Paxson, Kreibich, USENIX SEC 2001]
  - Active mapping [Shankar & Paxson, IEEE S&P 2003]
  - Host-based disambiguation [Dreger et al., DIMVA 2005]

Live Testing Architecture

- Leverage off-line testing components
- Synthesize end systems when not required (e.g., for normalization)



Summary

- We built a framework for introducing evasive maneuvers into traffic traces
- Striking absence of consensus in output of commonly used open-source NIDSs
- Questions?