

Intrusion Detection in High-Speed Networks: From Packets to Flows and Back

Falko Dressler

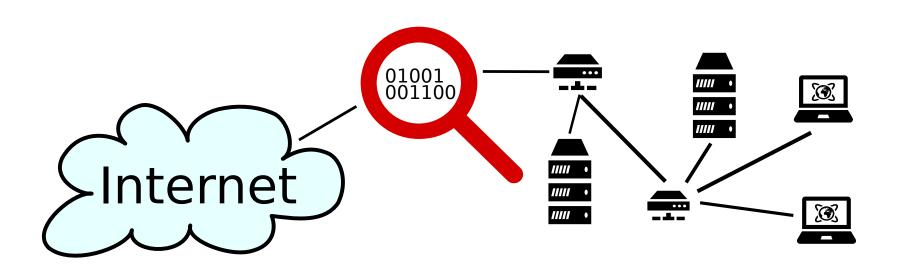


Network Monitoring



Network Monitoring

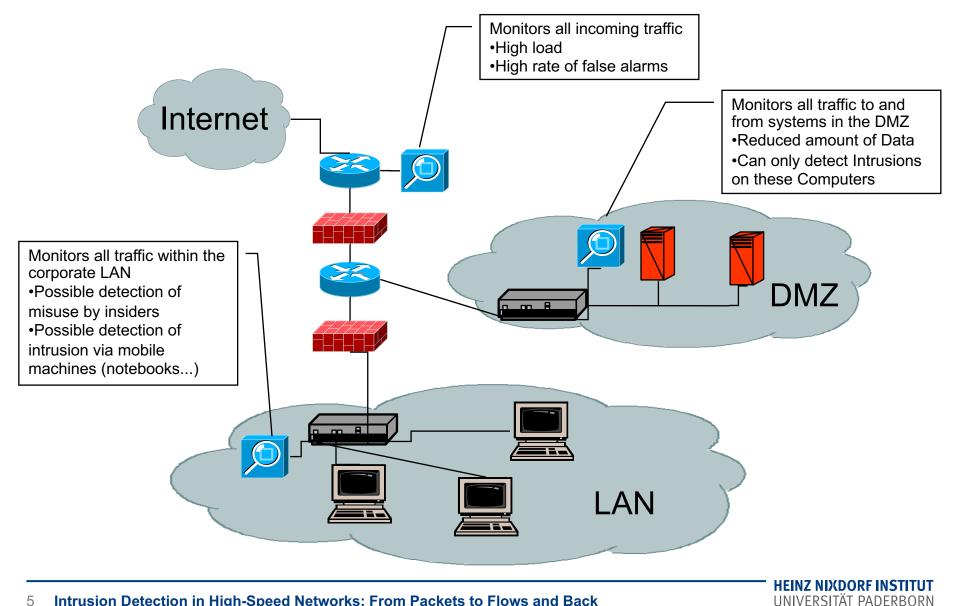
- Observing network traffic for:
 - Analysis (performance, statistics, troubleshooting, accounting)
 - Intrusion detection
 - Attack prevention



Intrusion Detection



Placement of a Network Intrusion Detection System



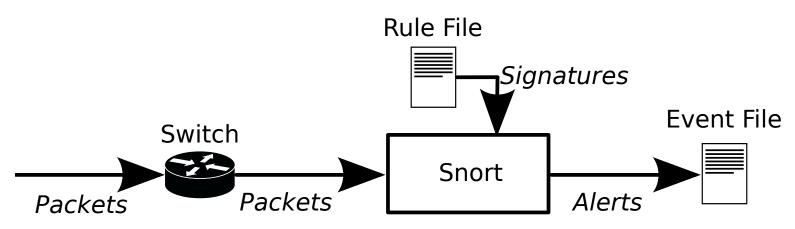
Network Intrusion Detection Systems (IDS)

- Analyze network traffic for malicious activity
- Anomaly-based IDS
 - Have a model of 'normal' traffic
 - Detect and alert deviations from 'normal' traffic
 - + all sorts of attacks
 - higher false positive rate
- Signature-based IDS
 - Have rule-set of known attacks and incidents
 - If packet/stream satisfies rules alarm is triggered

UNIVERSITAT PADERBORN

- + low false positive rate
- no novel attacks
- \rightarrow Example: Snort

Signature-based IDS: Snort



- Signature analysis is very performance hungry:
 - Decoding of packets
 Preprocessing data
 Detection phase
 Snort
 1. Decoding
 2. Preprocessors
 3. Detection phase
 Snort
 Snort
 Snort
 Snort
 Snort
 Snort
 Decoding of packets
 Snort
 Snor
 Snort

UNIVERSITAT PADERBORN

Snort with 5000 rules can handle 130k pkts/s

Signature-based IDS: Snort

Mainly signature based, each intrusion needs a predefined rule

```
alert tcp $HOME_NET any -> any 9996 \
```

```
(msg:"Sasser ftp script to transfer up.exe"; \
content:"|5F75702E657865|"; depth:250; flags:A+; \
classtype: misc-activity; sid:1000000; rev:3)
```

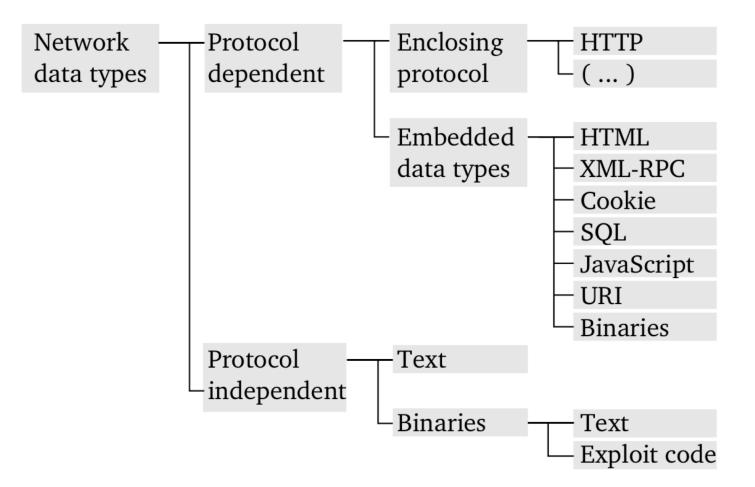
- Three step processing of captured information (capturing is done by libpcap):
 - Preprocessing (normalized and reassembled packets)
 - Detection Engine works on the data and decides what action should be taken

UNIVERSITAT PADERBORN

Action is taken (log, alert, pass)

Signature-based IDS: Snort

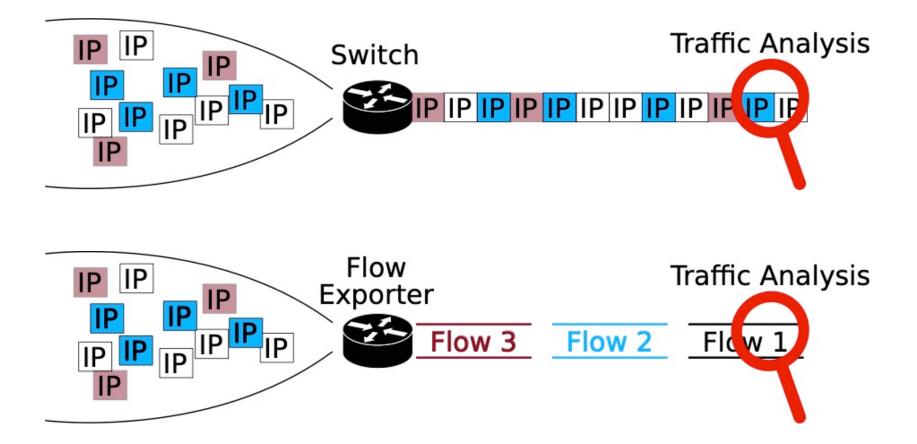
Rule processing



From Packets to Flows



From Packets to Flows

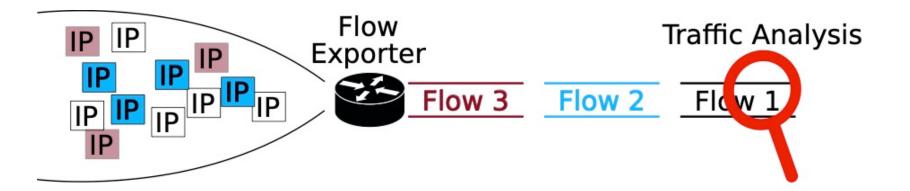


HEINZ NIXDORF INSTITUT

UNIVERSITÄT PADERBORN

Flow-based Traffic Analysis

- Flows are "condensed" network traffic data
- Packets with same properties go into same Flow
- IPFIX supported by most industry grade switches
- Flow fields are configurable



UNIVERSITAT PADERBORN

IPFIX: IP Flow Information Export

- Example IPFIX Flow Record:
- +--- Ipfix Data Record (id=999)
- '- sourceIPv4Address :10.0.2.15
- '- destinationIPv4Address :93.184.216.34

:50488

:80

:13

:2304

- '- sourceTransportPort
- '- destinationTransportPort
- '- packetTotalCount
- '- octetDeltaCount

Flow-based IDS



Signature-based Intrusion Detection on IPFIX Flows

Snort rule:

```
alert tcp any any -> any any
(msg:"Example Alert";
content:"GET"; http_method;
content:"/evil.jpg"; http_uri;
sid:1234567; rev:0;)
```

- IPFIX flow:
- +--- Ipfix Data Record (id=999)
- '- sourceIPv4Address
- '- destinationIPv4Address
- '- sourceTransportPort
- '- destinationTransportPort

UNIVERSITAT PADERBORN

- '- packetTotalCount
- '- octetDeltaCount

```
+---
```

No app. layer information in IPFIX flows

IPFIX and **HTTP**

- IPFIX Flow Record w/ HTTP Data:
- +--- Ipfix Data Record (id=999)
- sourceIPv4Address :10.0.2.15
 destinationIPv4Address :93 IANA B4
 sourceTransportPort :93 IANA B4
 destination HTTP fields now standardized with IANA B4
 destination HTTP fields now standardized with IANA B4
 httpRequestMethod :'GET'
- '- httpRequestTarget
- '- httpMessageVersion
- '- httpRequestHost

- :'/images/logo.png'
- :'HTTP/1.0'
- :'example.com'

Signature-based Intrusion Detection on IPFIX Flows

Snort rule:

```
alert tcp any any -> any any
(msg:"Example Alert";
content:"GET"; http_method;
content:"/evil.jpg"; http_uri;
sid:1234567; rev:0;)
```

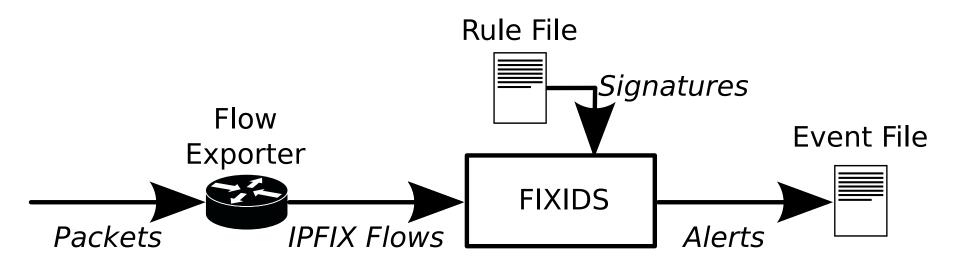
IPFIX flow:

+--- Ipfix Data Record (id=999)
+- ...
'- sourceIPv4Address
'- httpRequestMethod :'GET'
'- httpRequestTarget :'/evil.jpg'
'- httpMessageVersion :'HTTP/1.1'
'- httpRequestHost :bad.com'

+---

FIXIDS

- IPFIX-based signature-based intrusion detection system
 - Signature-based Intrusion Detection (using Snort signatures)
 - on IPFIX flows (using standardized HTTP IPFIX fields)

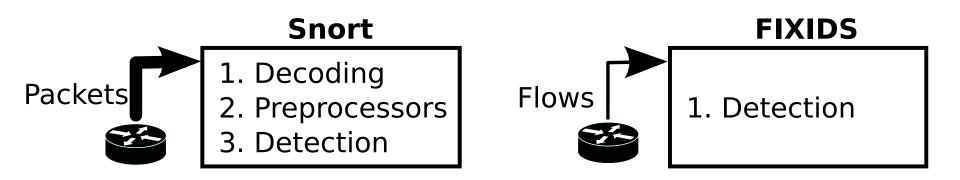


UNIVERSITAT PADERBORN

Traditional Signature IDS (Snort) vs. FIXIDS

 Snort receives packets from a switch FIXIDS receives IPFIX flows from a flow exporting device (e.g., switch)

UNIVERSITAT PADERBORN



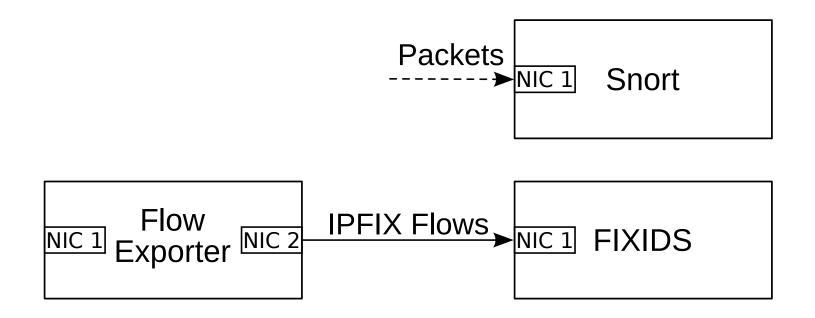
FIXIDS has to handle less than 0.5% of the data volume of Snort

Performance



Evaluation: Experiment Setup

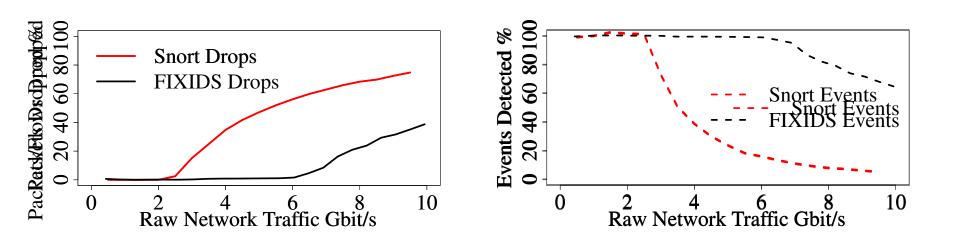
- Compare results of Snort and FIXIDS analyzing the same traffic, using the same signatures
- Replayed with increasing speed



UNIVERSITAT PADERBORN

Evaluation: Results

- Snort vs. FIXIDS: Same traffic, same signatures
- Replayed with increasing speed



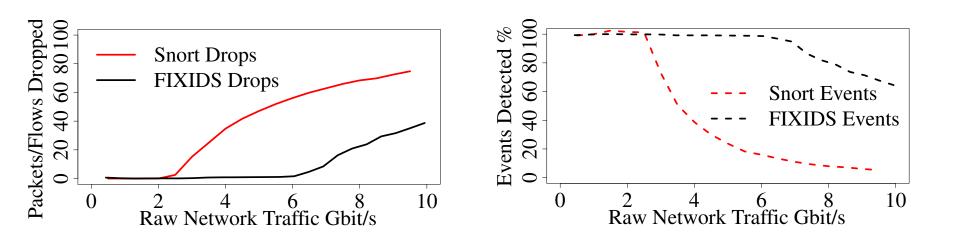
UNIVERSITÄT PADERBORN

Evaluation: Results

- Snort:
 - 2 Gbit/s (136k Pkts/s):
 0% Drops
 - 9.5 Gbit/s: >70% Drops

- FIXIDS:
 - 6 Gbit/s (14000 flows/s):
 0% Drops
 - 9.5 Gbit/s (22000 flows/s): 40% Drops

UNIVERSITÄT PADERBORN



Testing IDS



How to test a NIDS?

- Real traffic?
 - hard to get
 - public traces: old, no payload
 - contains only very few attacks
- Manually creating attack traffic?
 - time intensive
 - cumbersome
- In general, traces do not contain enough **unique** attacks

UNIVERSITAT PADERBORN

GENESIDS

- Generating Events for Signature-based Intrusion Detection Systems
- INPUT: Set of attack descriptions
 - Snort syntax
 - HTTP attacks
- OUTPUT: Stateful network traffic containing attack patterns
 - One flow per attack
 - Annotated with an attack ID

Rule example

alert tcp any any -> any any (msg:"This is an example rule"; content:"POST"; http method; uricontent:"|2F|evil.jpg"; Time Source pcre:"/AttackB 1 0.000000 10.0.0.111 2 0.051498 131.234.188.5 3 0.051561 10.0.0.111 4 0.051747 10.0.0.111 sid:1234567; r 5 0.101175 131.234.188.5 6 0.105167 131.234.188.5

131.234.188.5 TCP 74 56300 → 80 [SYN] Seg=0 Win=292 10.0.0.111 TCP 74 80 - 56300 [SYN, ACK] Seg=0 Ac 131.234.188.5 TCP 66 56300 → 80 [ACK] Seg=1 Ack=1 131.234.188.5 170 POST /evil.ipg HTTP/1.1 HTTP 10.0.0.111 TCP 66 80 → 56300 [ACK] Seg=1 Ack=105 597 HTTP/1.1 301 Moved Permanently 10.0.0.111 HTTP 7 0.105218 10.0.0.111 131.234.188.5 TCP 66 56300 → 80 [ACK] Seg=105 Ack=5 10.0.0.111 TCP 66 56300 → 80 [FIN, ACK] Seg=105 . 8 0.105541 131.234.188.5 9 0.152631 131.234.188.5 10.0.0.111 TCP 66 80 → 56300 [FIN, ACK] Seq=532 10.0.0.111 10 0.152684 131.234.188.5 TCP 66 56300 → 80 [ACK] Seq=106 Ack=5 genesids -f ext - Hypertext Transfer Protocor POST /evil.jpg HTTP/1.1\r\n Host: ccs-labs.org\r\n Rulesid: 1234567\r\n e0 91 f5 79 5d 42 b6 ce 8b 47 9f 3b 08 00 45 00 ...y]B.. .G.:..E. 0010 00 9c 84 19 40 00 40 06 6b e4 0a 00 00 6f 83 ea@.@. k....o.. 7b cf 36 76 cf bb 80 18P.. {.6v.... bc 05 db ec 00 50 f2 c4 08 0a 00 29 ff e6 fc 3b 00 e5 4d ce 00 00 01 01 . . M) . . . ; dc e5 50 4f 53 54 20 2f 65 76 69 6c 2e 6a 70 67 ..POST / evil.jpg 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host: 20 48 54 50 2f 31 2e 0060 20 63 63 73 2d 6c 61 62 73 2e 6f 72 67 0d 0a 52 ccs-lab s.org..R 75 6c 65 73 69 64 3a 20 31 32 33 34 35 36 37 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 8o 3a .Content -Length: 0090 20 31 39 0d 0a 0d 0a 31 32 33 34 35 41 4 74 61 19....1 2345Atta 63 6b 42 6f 64 79 2d 56 36 75 ckBody-V 6u 00a0 HEIN7 NIXDORF INSTITUT

Destination

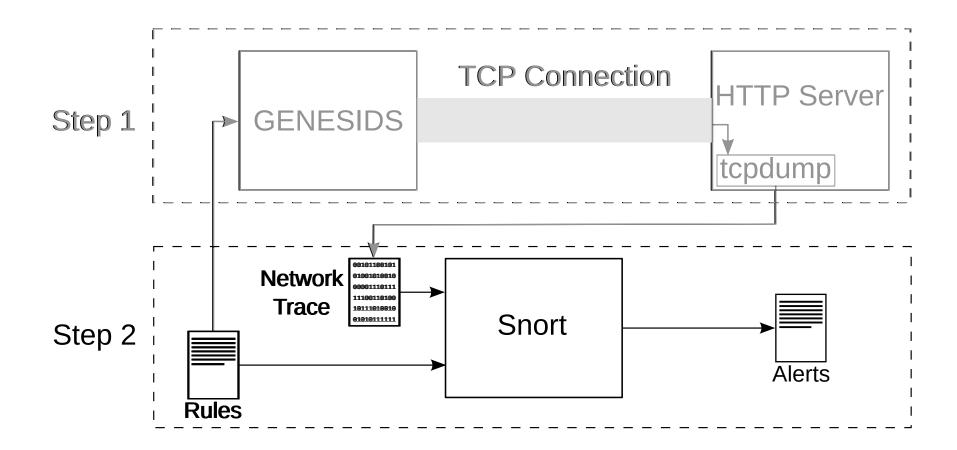
Protocol Lengtl Info

UNIVERSITÄT PADERBORN

GENESIDS Evaluation: Goals & Rules

- Ability to generate a variety of different attacks
- Generated attacks trigger expected event
- All supported Snort rules from:
 - Snort.org subscriber rule-set
 - Snort.org community rule-set
 - Emerging Threats rule-set
- TOTAL 8101 different rules

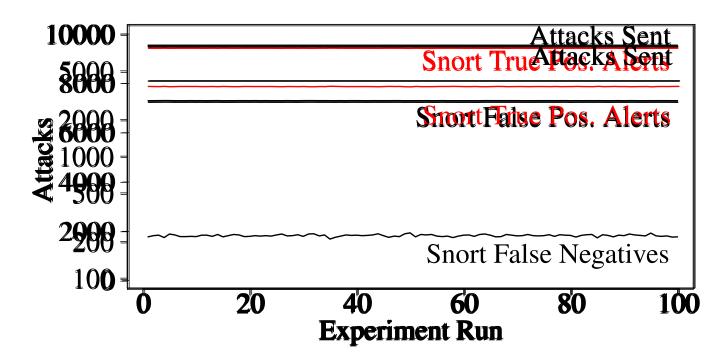
GENESIDS Evaluation Steps



HEINZ NIXDORF INSTITUT

UNIVERSITÄT PADERBORN

Evaluation Results: Generated Attacks

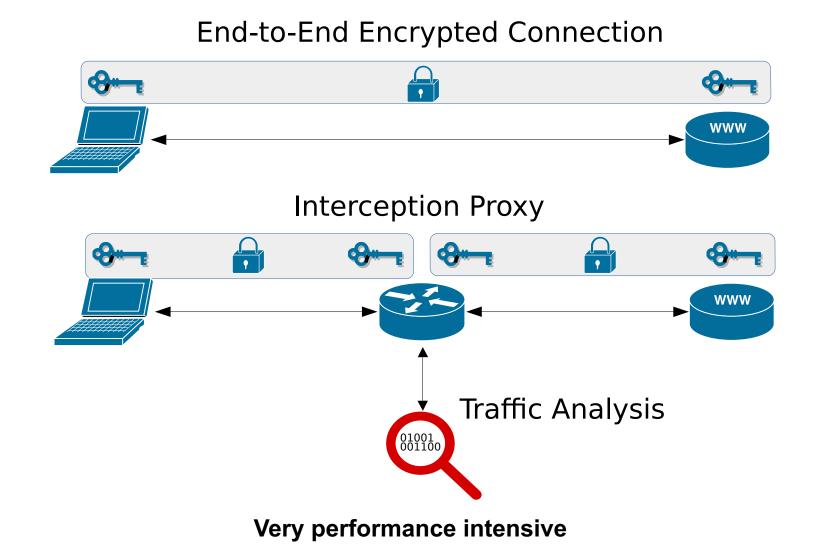


- GENESIDS: 8101 attacks generated (out of 8101 rules)
- Snort: 7877 (avg) true positive alerts triggered (out of 8101)
- Snort: 2847 (avg) false positive alerts triggered (62% triggered by 3 rules)
- Snort: 223 (avg) false negatives (generated attacks that did not trigger the corresponding alert)

Open Challenges



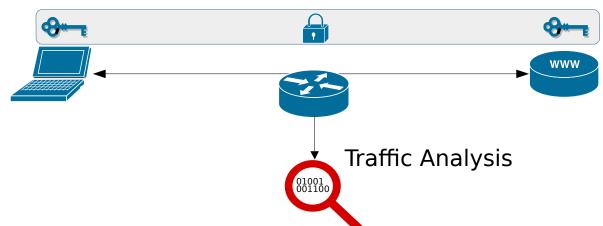
Network Monitoring on Encrypted Traffic



HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN

Passive Monitoring on Encrypted Traffic

- Using statistical properties and machine learning
- Only categorization possible (e.g., application)

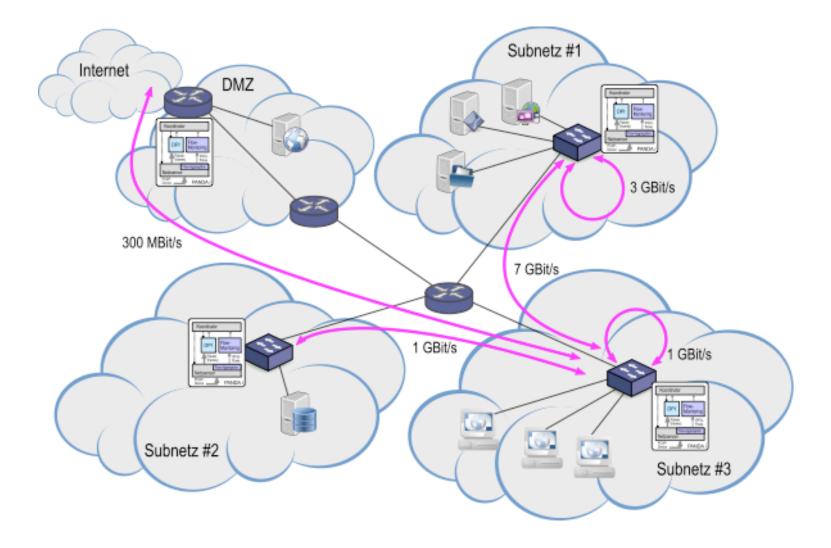


End-to-End Encrypted Connection

- How to passively detect malware (communication) in encrypted traffic?
- More general: How to foster strong encryption without sacrificing intrusion detection accuracy?

UNIVERSITAT PADERBORN

Where to Look for Attacks

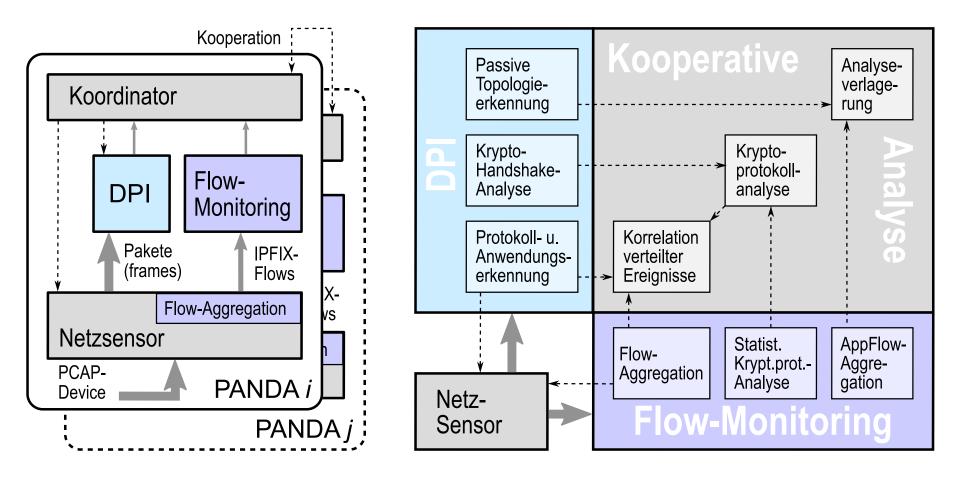


HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN

DFG Project PANDA



PANDA – Precise Attack Detection for Network Domains by Application Classification

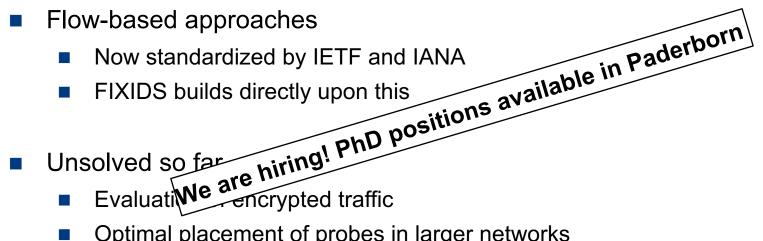


Conclusion



Conclusion

- Network Monitoring and IDS
 - Fundamental parts of every modern security solution
 - Flexible packet-based analysis is just too slow



- Optimal placement of probes in larger networks
- ... as can be seen, there are many open challenges and questions for another decade of interesting research ©

UNIVERSITAT PADERBORN