Intrusion Detection Evaluation

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 8-2

ravi.utsa@gmail.com
www.profsandhu.com

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1),

IDS Categorization

Property	IDS Type
Monitored platform	Host based
	Network based
	Hybrid
Attack detection method	Misuse based
	Anomaly based
	Hybrid
Deployment architecture	Nondistributed
	Distributed

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)
Table 1, p12-3

IDS Categorization

Property	IDS Type
Monitored platform	Host based
	Network based
	Hybrid
Attack detection method	Misuse based
	Anomaly based
	Hybrid
Deployment architecture	Nondistributed
	Distributed

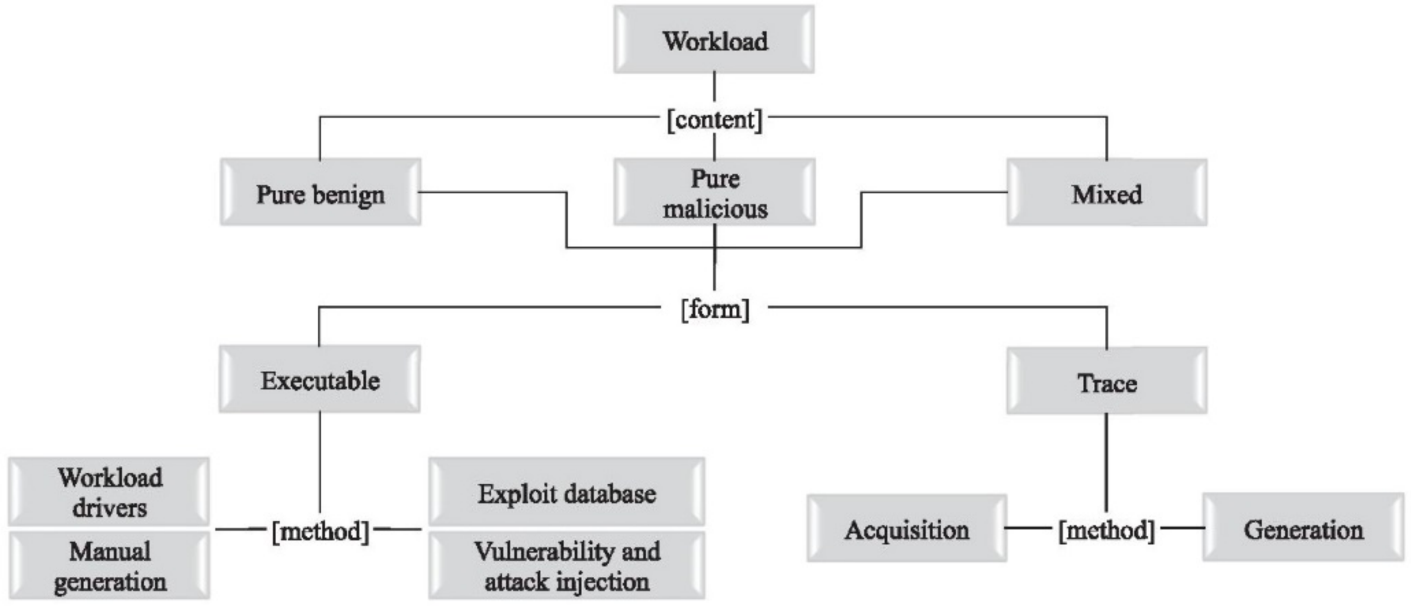
Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)
Table 1, p12-3

Design Space

- Workloads
- Metrics
- Measurement methodology

Workloads

Workloads



Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems:
A survey of common practices. ACM Computing Surveys (CSUR), 48(1),
Figure 1, p 12-4

Workloads

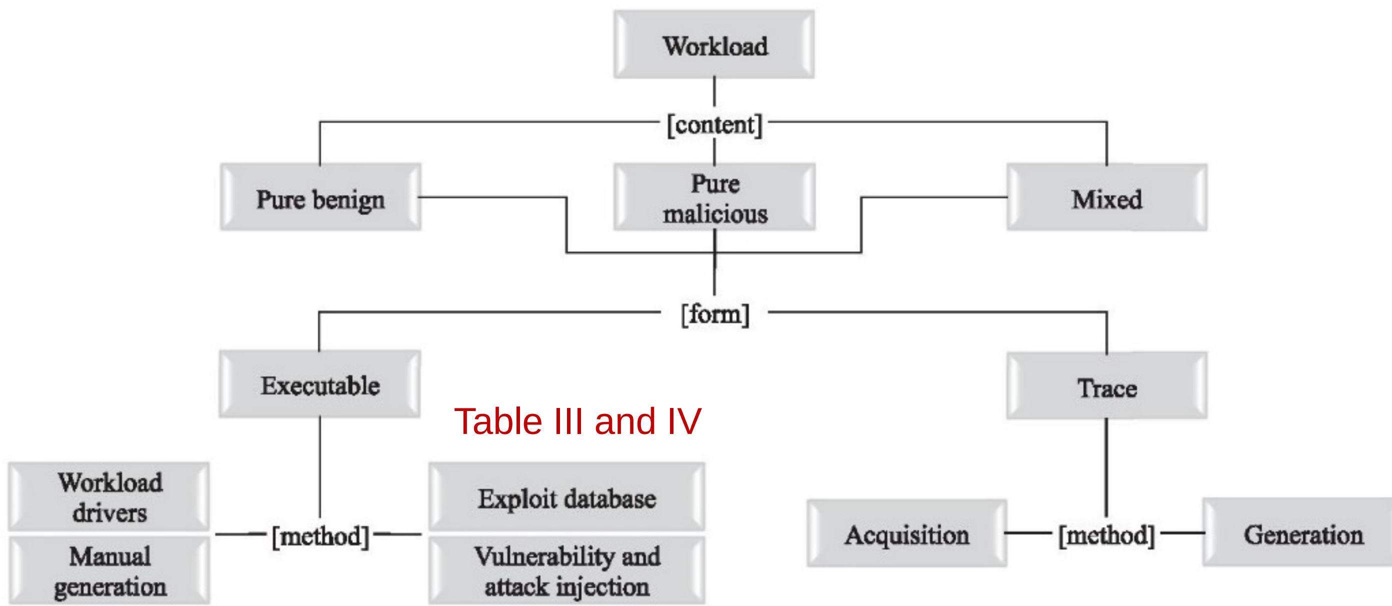


Table II

Table III and IV

Figure 2

Publicly available traces
DARPA 98, 99, 00
KDD 99 (derivative)

Symantec onsite testing

Table V

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1),
Figure 1, p 12-4

Honeypots

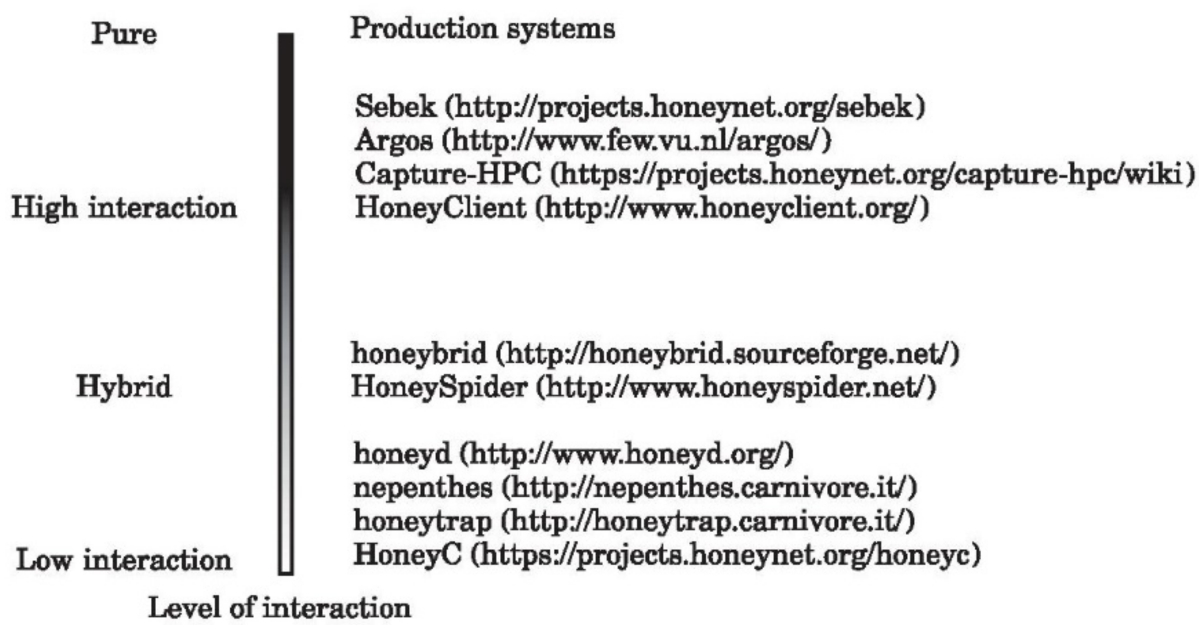
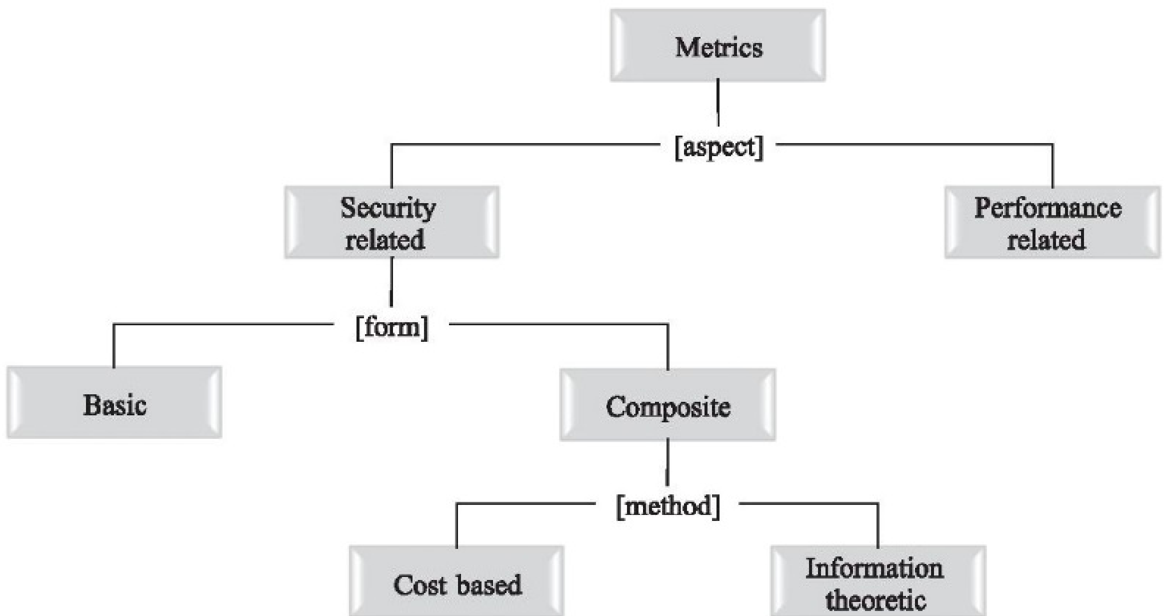


Fig. 3. Honeypots of different levels of interaction.

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1), Figure 3, p 12-14

Metrics

Metrics



Not discussed in lecture

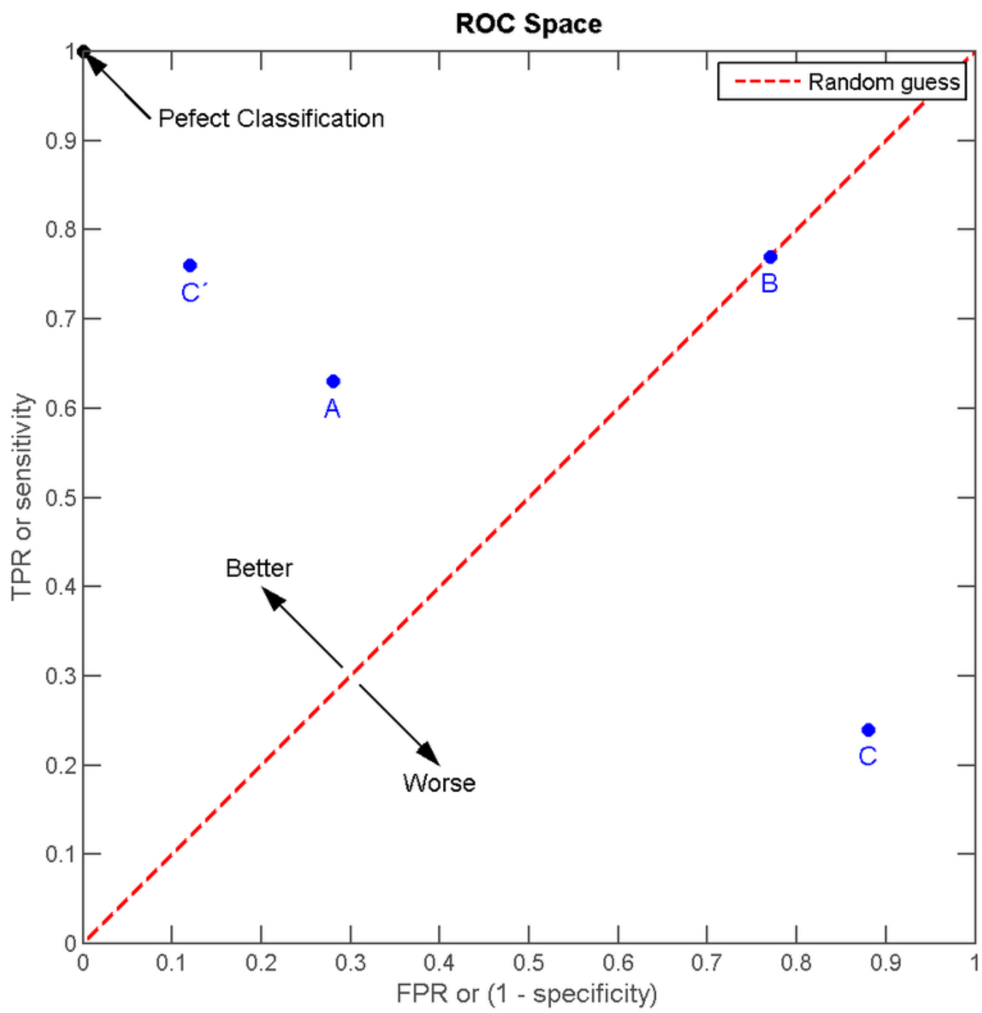
Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1), Figure 4, p12-15

Metrics: Basic

Basic	False-negative rate	$\beta = P(\neg A \mid I)$
	True-positive rate	$1 - \beta = 1 - P(\neg A \mid I) = P(A \mid I)$
	False-positive rate	$\alpha = P(A \mid \neg I)$
	True-negative rate	$1 - \alpha = 1 - P(A \mid \neg I) = P(\neg A \mid \neg I)$
Dependent on base rate	Positive predictive value	$P(I \mid A) = \frac{P(I)P(A \mid I)}{P(I)P(A \mid I) + P(\neg I)P(A \mid \neg I)}$
	Negative predictive value	$P(\neg I \mid \neg A) = \frac{P(\neg I)P(\neg A \mid \neg I)}{P(\neg I)P(\neg A \mid \neg I) + P(I)P(\neg A \mid I)}$

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1),.
Table VI, p 12-16

Receiver Operating Curve (ROC)



https://en.wikipedia.org/wiki/Receiver_operating_characteristic

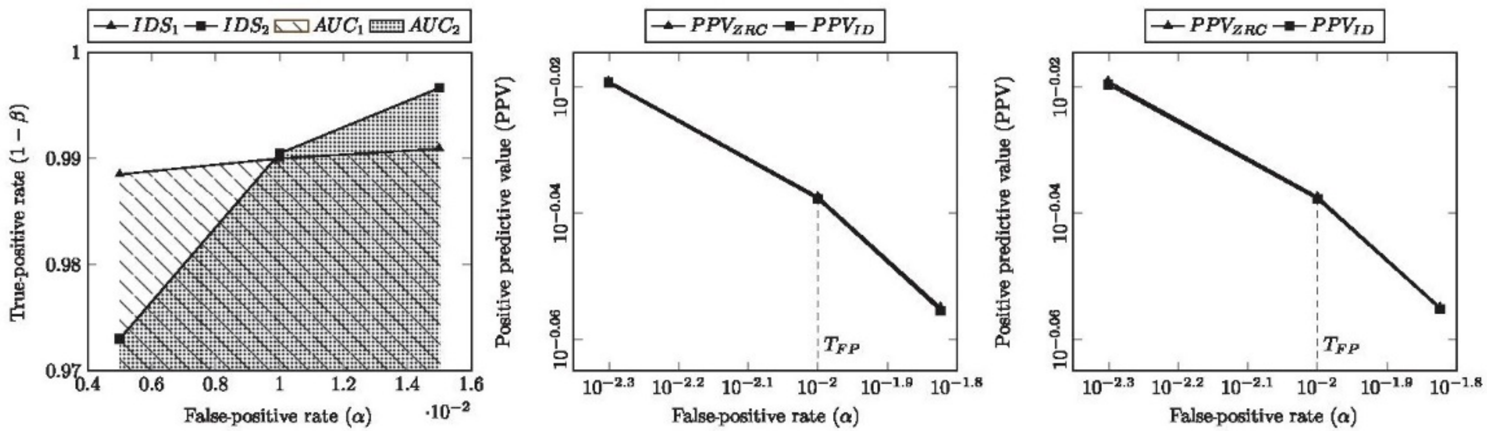
ROC Limitations

- Intrusion detection is not a binary yes/no problem
- Unit of measurement is ambiguous
  - Flow versus packet
- Does not account for base rate P(I)

Intrusion Detection Effectiveness

Table VII. Values of $1-\beta$, PPV_{ID}, C_{exp}, C_{rec}, and C_{ID} for IDS_1 and IDS_2

		IDS_1				IDS_2			
α	PPV_{ZRC}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}
0.005	0,9569	0.9885	0,9565	**0.016**	**0.9159**	0.973	0,9558	0.032	**0.8867**
0.010	0,9174	0.99	0,9167	0.019	0.8807	0.99047	0,9167	0.019	0.8817
0.015	0,8811	0.9909	0,8801	0.022	0.8509	0.99664	0,8807	**0.017**	0.8635



(a) (b) IDS_1 (c) IDS_2

Fig. 5. IDS comparison with ROC curves (a) and the intrusion detection effectiveness metric (b, c).

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)

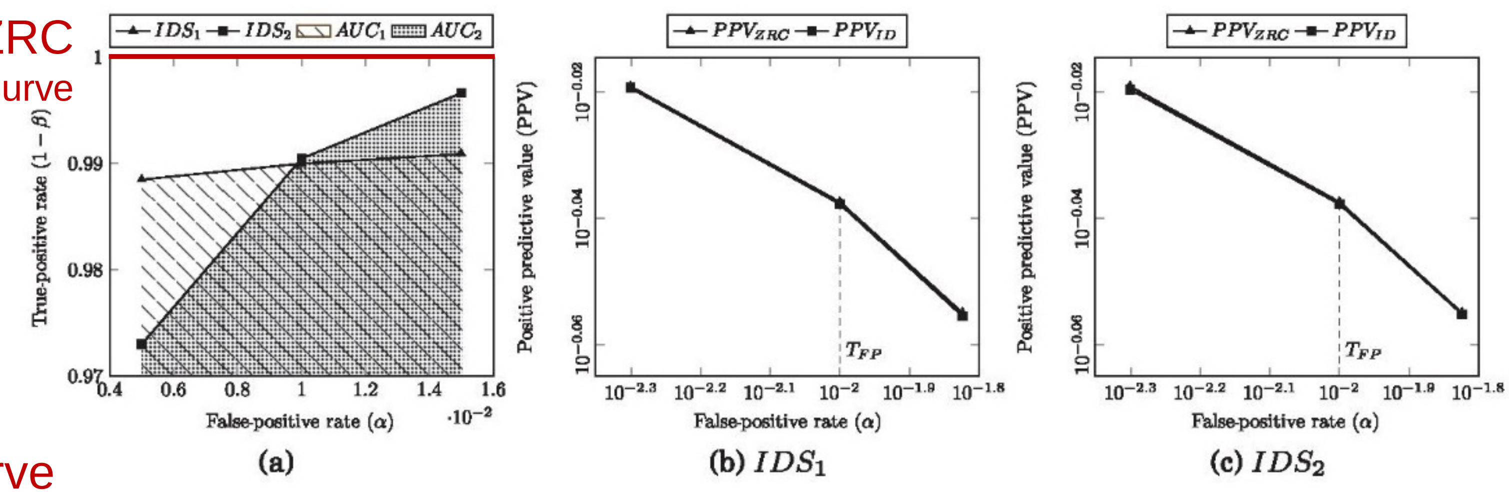
Intrusion Detection Effectiveness

Table VII. Values of $1-\beta$, PPV_{ID}, C_{exp}, C_{rec}, and C_{ID} for IDS_1 and IDS_2

		IDS_1				IDS_2			
α	PPV_{ZRC}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}
0.005	0,9569	0.9885	0,9565	**0.016**	**0.9159**	0.973	0,9558	0.032	**0.8867**
0.010	0,9174	0.99	0,9167	0.019	0.8807	0.99047	0,9167	0.019	0.8817
0.015	0,8811	0.9909	0,8801	0.022	0.8509	0.99664	0,8807	**0.017**	0.8635

ZRC

Zero Reference Curve



Compare area under ROC curve

Fig. 5. IDS comparison with ROC curves (a) and the intrusion detection effectiveness metric (b, c).

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)

Intrusion Detection Effectiveness

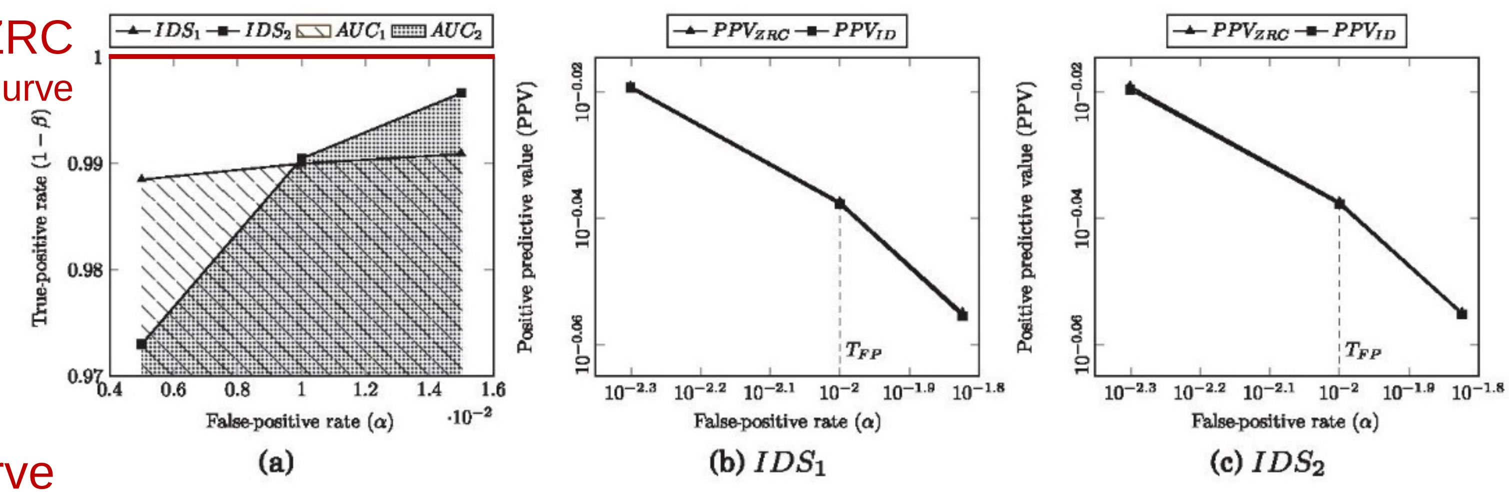
Assumes Base rate, P(I) = 0.1

Table VII. Values of $1-\beta$, PPV_{ID}, C_{exp}, C_{rec}, and C_{ID} for IDS_1 and IDS_2

		IDS_1				IDS_2			
α	PPV_{ZRC}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}
0.005	0,9569	0.9885	0,9565	**0.016**	**0.9159**	0.973	0,9558	0.032	**0.8867**
0.010	0,9174	0.99	0,9167	0.019	0.8807	0.99047	0,9167	0.019	0.8817
0.015	0,8811	0.9909	0,8801	0.022	0.8509	0.99664	0,8807	**0.017**	0.8635

ZRC

Zero Reference Curve



Compare area under ROC curve

Fig. 5. IDS comparison with ROC curves (a) and the intrusion detection effectiveness metric (b, c).

T_{FP}: max acceptable false positive rate
Compare area difference between
PPV_{ZRC} and PPV_{IDS} up to T_{FP}

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)
.

Metrics: Cost-Based

These p_1 p_2 p_3 are different, apply to false alert filter

C_α: cost of false positive
C_β: cost of false negative
$C = C_\beta/C_\alpha$

$p_1 = P(A)$
$p_2 = P(I|A)$
$p_3 = P(I|\neg A)$

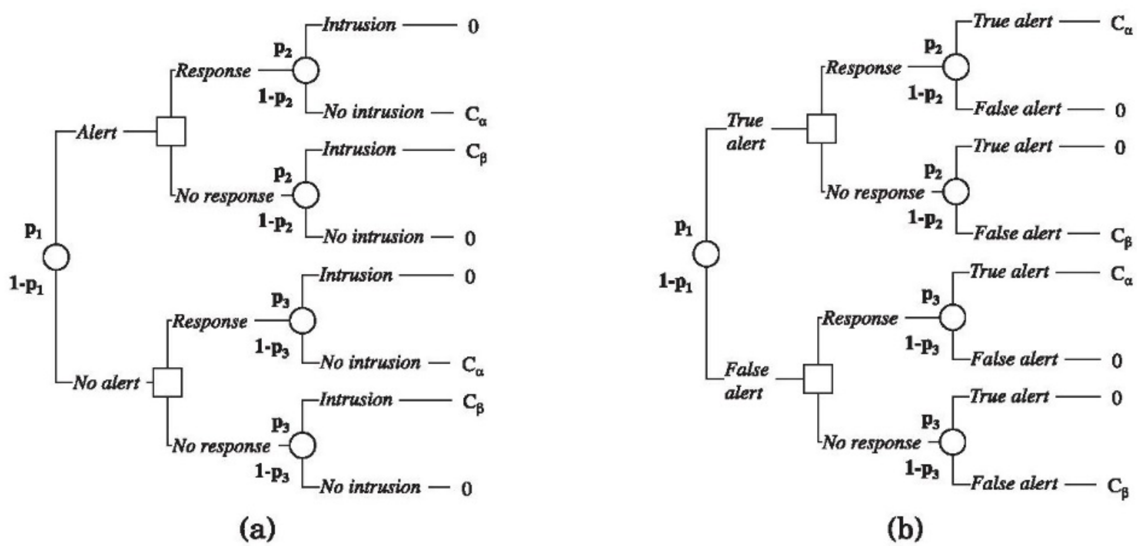


Fig. 6. Decision tree for calculating expected cost (a) and relative expected cost (b).

$$C_{exp} = Min(C\beta B,(1-\alpha)(1-B)) + Min(C(1-\beta)B,\alpha(1-B))$$

$$C_{rec} = C\beta B + \alpha(1-B)$$

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)
Figure 6

Metrics: Cost-Based

Table VII. Values of $1-\beta$, PPV_{ID}, C_{exp}, C_{rec}, and C_{ID} for IDS_1 and IDS_2

		IDS_1				IDS_2			
α	PPV_{ZRC}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}	$1-\beta$	PPV_{ID}	$C_{exp/rec}$	C_{ID}
0.005	0,9569	0.9885	0,9565	**0.016**	**0.9159**	0.973	0,9558	0.032	**0.8867**
0.010	0,9174	0.99	0,9167	0.019	0.8807	0.99047	0,9167	0.019	0.8817
0.015	0,8811	0.9909	0,8801	0.022	0.8509	0.99664	0,8807	**0.017**	0.8635

Assumptions:
B = 0.1
C = 10
α, β same for base IDS and its false alarm filter

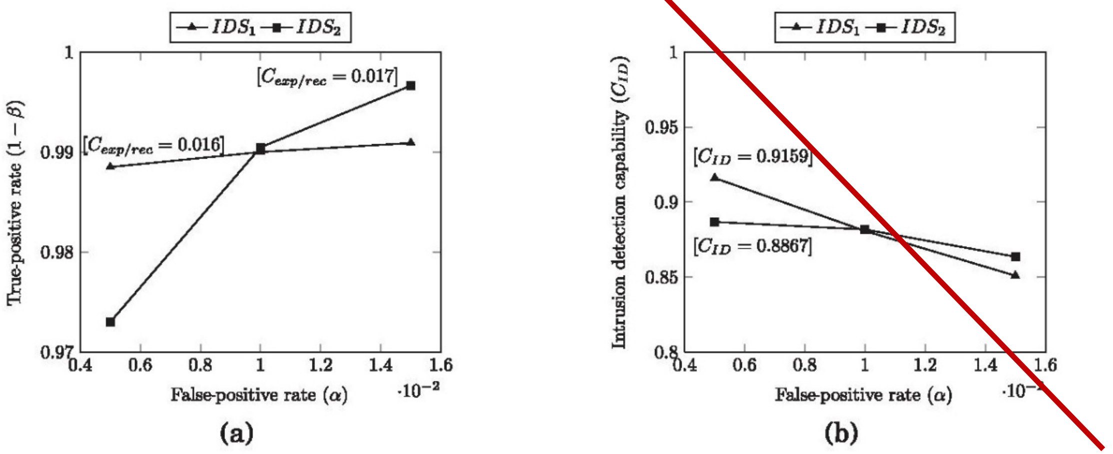


Fig. 7. IDS comparison with the expected cost and relative expected cost metric (a) and the intrusion detection capability metric (b).

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)

Measurement Methodology

Measurement Methodology

Table VIII. IDS Evaluation Design Space: Measurement Methodology

IDS Property	Workloads [Content]	Metrics [Aspect]	[Form]
Attack Detection Related			
Attack detection accuracy	Mixed	Security related	Basic, composite
Attack coverage	Pure malicious	Security related	Basic
Resistance to evasion techniques	Pure malicious, mixed	Security related	Basic
Attack detection and reporting speed	Mixed	Performance related	n/a
Resource Consumption Related			
CPU consumption Memory consumption Network consumption	Pure benign	Performance related	n/a
Performance overhead	Pure benign	Performance related	n/a
Workload processing capacity	Pure benign	Performance related	n/a

Definitions of IDS Properties

IDS Property	Definition
Attack detection accuracy	The attack detection accuracy of an IDS in the presence of mixed workloads.
Attack coverage	The attack detection accuracy of an IDS in the presence of attacks without any background benign activity.
Performance overhead	The overhead incurred by an IDS on the system and/or network environment where it is deployed. Under overhead, we understand performance degradation of users' tasks/operations caused by (a) consumption of system resources (e.g., CPU, memory) by the IDS and/or (b) interception and analysis of the workloads of users' tasks/operations (e.g., network packets) by the IDS.
Workload processing capacity	The rate of arrival of workloads to an IDS for processing in relation to the amount of workloads that the IDS discards (i.e., does not manage to process). For instance, in the context of network-based IDSes, capacity is normally measured as the rate of arrival of network packets to an IDS over time in relation to the amount of discarded packets over time. The capacity of an IDS may also be defined as the maximum workload processing rate of the IDS such that there are no discarded workloads.

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)

Case Study: Snort

Table X. Attack Coverage of Snort

Targeted Vulnerability (CVE ID)	Platform	Detected
CVE-2011-3192	Apache	x
CVE-2010-1870	Apache Struts	✓
CVE-2012-0391	Apache Struts	x
CVE-2013-2251	Apache Struts	x
CVE-2013-2115/CVE-2013-1966	Apache Struts	✓
CVE-2009-0580	Apache Tomcat	x
CVE-2009-3843	Apache Tomcat	x
CVE-2010-2227	Apache Tomcat	x

✓, detected; x, not detected.

True positive rate = 2/8 = 0.25

Table XI. Resistance to Evasion Techniques of Snort

Evasion Technique	Targeted Vulnerability (CVE ID)	
	CVE-2010-1870	CVE-2013-2115/CVE-2013-1966
HTTP::uri_use_backslashes	✓	✓
HTTP::uri_fake_end	✓	✓
HTTP::pad_get_params	✓	x
HTTP::uri_fake_params_start	✓	✓
HTTP::uri_encode_mode (u-random; hex-random)	✓	x
HTTP::pad_method_uri_count	✓	✓
HTTP::method_random_valid	✓	x
HTTP::header_folding	✓	✓
HTTP::uri_full_url	✓	✓
HTTP::pad_post_params	✓	x
HTTP::uri_dir_fake_relative	✓	✓
HTTP::pad_uri_version_type (apache; tab)	✓	✓
HTTP::uri_dir_self_reference	✓	✓
HTTP::method_random_case	✓	✓

✓, detected; x, not detected.

True positive rate = 24/28 = 0.85

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)

Case Study: Snort

Table XII. Attack Detection Accuracy of Snort:
Basic Metrics (seconds=120)

Configuration	Metrics			
	α	$1-\beta$	PPV	NPV
count=6	0.0008	0.333	0.9788	0.9310
count=5	0.0011	0.416	0.9768	0.9390
count=4	0.0013	0.5	0.9771	0.9473
count=3	0.0017	0.624	0.9761	0.9598
count=2	0.0024	0.833	0.9747	0.9817
Default configuration	0.0026	0.958	0.9762	0.9953

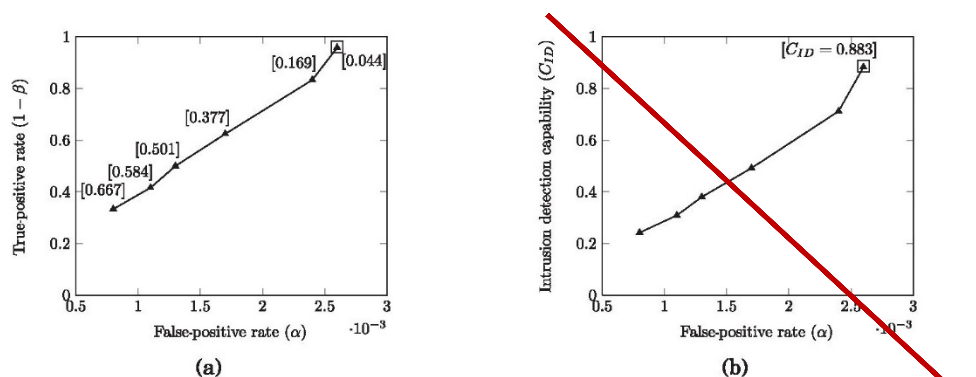


Fig. 8. Attack detection accuracy of Snort: composite metrics. ROC curve and estimated costs (a) and C_{ID} curve (b) (□ marks an optimal operating point).

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1),

Case Study: Snort

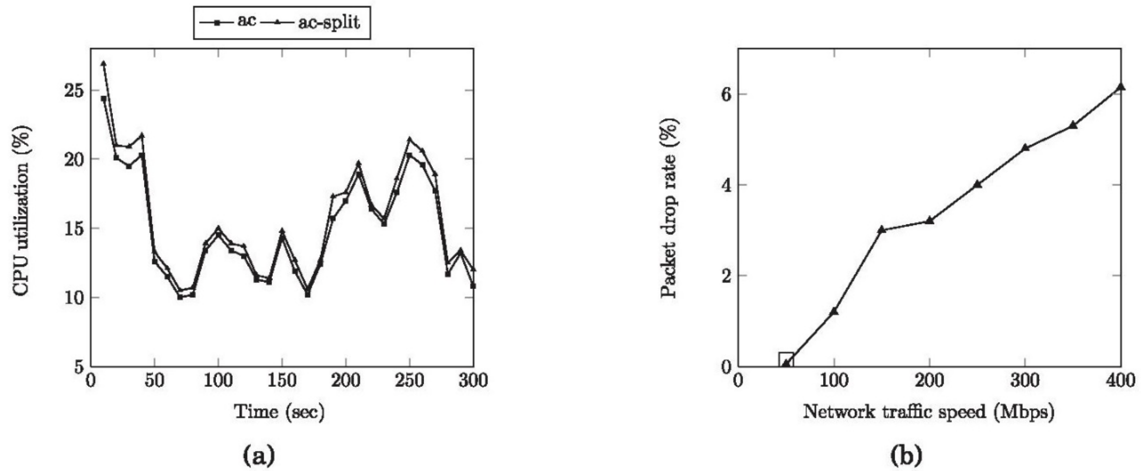


Fig. 9. CPU consumption of Snort (a) and packet drop rate of Snort (b) (□ marks the data point whose x value is the network traffic speed that corresponds to the maximum workload processing rate of Snort such that there are no discarded workloads).

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D., 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1)