Intrusion Detection

Dr Christopher D. McDermott

Outline

1. Introduction
2. IDS Categorisation
3. Intrusion Data Sources
4. Techniques for implementation
5. Threat Intelligence
6. Trends, Insider Threats & Operational Technology
7. IDS Signatures
8. Performance Metrics
9. Datasets
10. IDS Evasion Techniques

Introduction

Intrusion:

- Any kind of unauthorised activity that causes damage to an information system
- Any attack that could pose a possible threat to the information confidentiality, integrity or availability

Goal:

- To identify malicious network traffic and computer usage that cannot be identified by a firewall

IDS Categorisation

Signature-based IDS (SIDS)

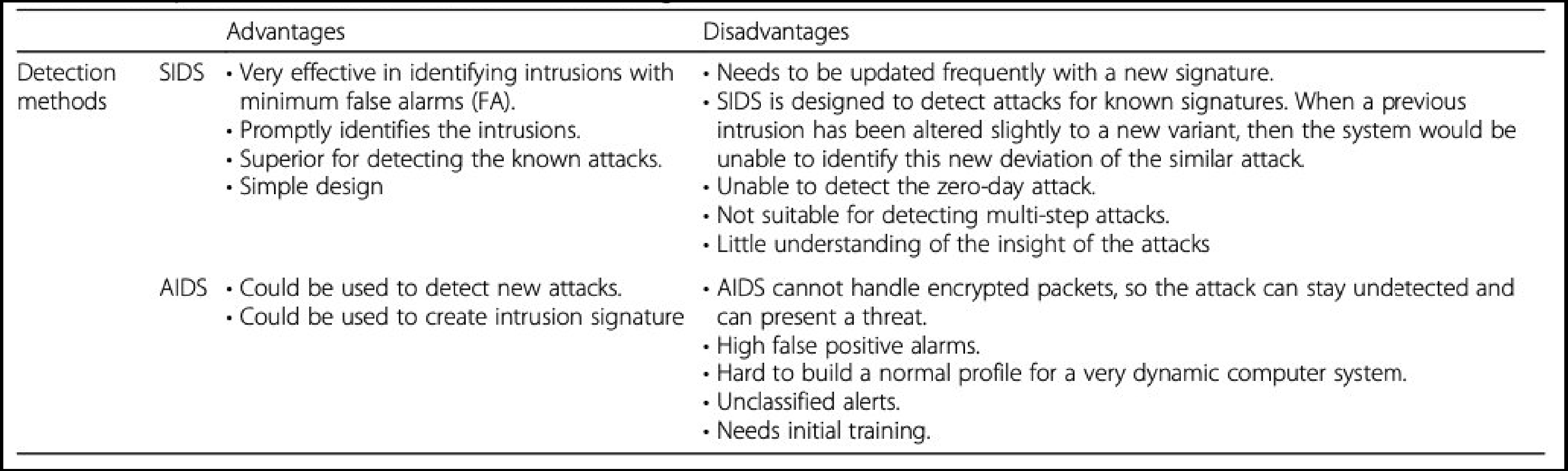
- Pattern matching techniques also known as ‘Knowledge-based’ or ‘Misuse Detection’
- Signature matches a suspected intrusion with previously known intrusion
- Compare current set of activities against existing signature and raise an alarm if match found
- High accuracy for known attacks; Lower accuracy for zero day attacks
- Sophisticated SIDS can extract signature information from multiple packets; requires SIDS to recall content of earlier packets

IDS Categorisation

Anomaly-based IDS (AIDS)

- Normal model of behaviour is created using machine-learning, statistical-based or knowledge-based methods
- Any significant deviation between observed behaviour and the model is regarded as an anomaly (interpreted as an intrusion)
- Assumption is malicious behaviour differs from typical user behaviour

IDS Categorisation Comparison

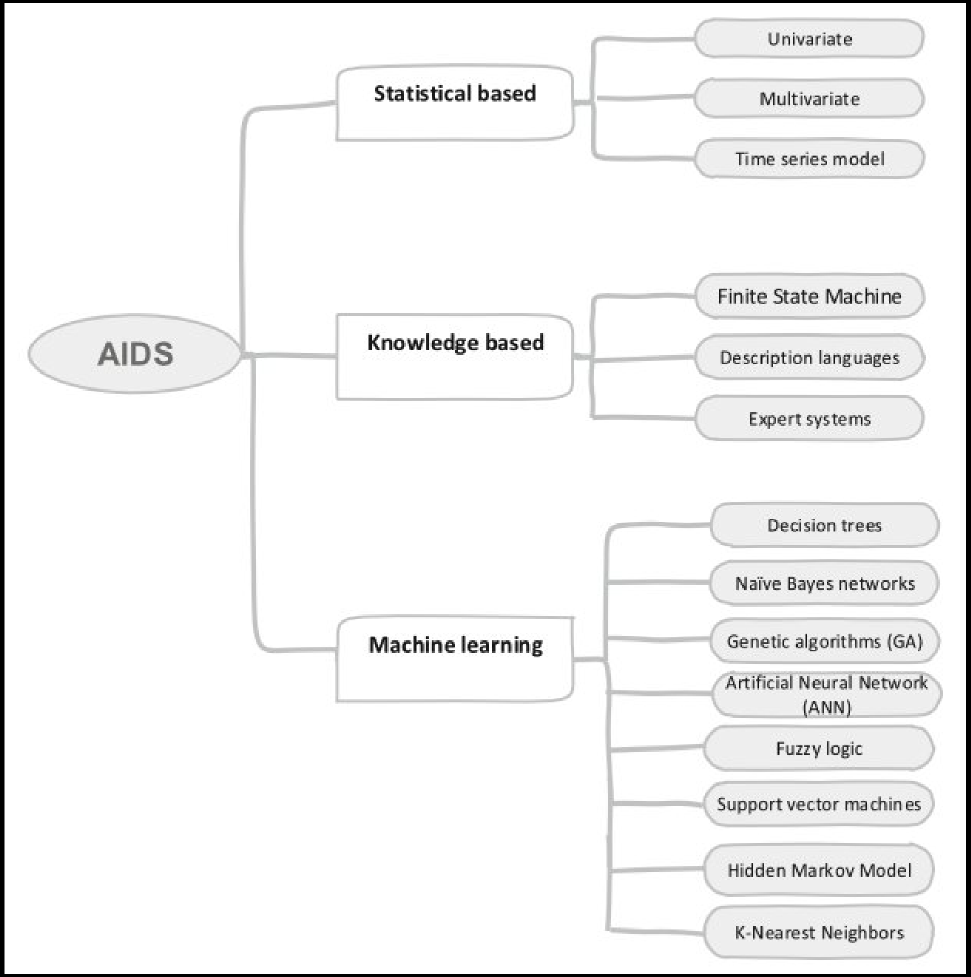


		Advantages	Disadvantages
Detection methods	SIDS	• Very effective in identifying intrusions with minimum false alarms (FA). • Promptly identifies the intrusions. • Superior for detecting the known attacks. • Simple design	• Needs to be updated frequently with a new signature. • SIDS is designed to detect attacks for known signatures. When a previous intrusion has been altered slightly to a new variant, then the system would be unable to identify this new deviation of the similar attack. • Unable to detect the zero-day attack. • Not suitable for detecting multi-step attacks. • Little understanding of the insight of the attacks
	AIDS	• Could be used to detect new attacks. • Could be used to create intrusion signature	• AIDS cannot handle encrypted packets, so the attack can stay undetected and can present a threat. • High false positive alarms. • Hard to build a normal profile for a very dynamic computer system. • Unclassified alerts. • Needs initial training.

IDS Categorisation (AIDS)

Method	Characteristics	Example
Statistics based	•Needs a large amount of knowledge of statistics •Simple but less accurate •Real-time •Easy to implement •Hash function could be used for identification.	Bhuyan, et al.
Pattern-based	•Easy to implement •Hash function could be used for identification.	Liao, et al. Riesen and Bunke
Rule-based	•The computational cost of rule-based systems could be very high because rules need pattern matching. •It is very hard to estimate what actions are going to occur and when •Requires a large number of rules for determining all possible attacks. •Low false positive rate •High detection rate	Hall, et al.
State-based	•Probabilistic, self-training •Low false positive rate.	Kenkre, et al.
Heuristic-based	•It needs knowledge and experience •Experimental and evolutionary learning	Abbasi, et al. Butun, et al.

Techniques for Implementing AIDS



- Statistical: collect and examine data records in a set of items to build model of normal behaviour
- Knowledge-based: identify requested actions from existing data such a protocols
- Machine-learning: acquire complex pattern-matching from training data

Intrusion Data Sources

Host-based IDS (HIDS)

- Inspect data that originates from the host system
- Audit sources such as: operating system, window server logs, firewalls logs, application system audits, or database logs
- Can deter insider attacks that do not involve network traffic

Network-based IDS (NIDS)

- Monitors network traffic extracted through packet capture, NetFlow
- Limited ability to inspect ALL data (sampling)
- Deployed at a number of positions

Threat Intelligence

Strategic Intelligence

- High-level information used by executives and decision-makers.

Tactical Intelligence

- Focuses on specific Indicators of Compromise (IoCs) like IP addresses, malware hashes, and phishing URLs.

Operational Intelligence

- Provides deeper insights into threat actor behaviour and attack techniques.

Technical Intelligence

- Detailed information about malware, vulnerabilities, exploits, and attack techniques.

Threat Intelligence Feeds

Open-Source

- AlienVault OTX, AbuseIPDB, MalwareBazaar

Commercial

- FireEye, Recorded Future, IBM X-Force

Government & Industry

- CISA, FS-ISAC, MITRE CTI

Integrating Threat Intelligence

Automated Integration

- STIX/TAXII protocols to share threat intelligence with IDS.
- IDS can ingest real-time IoCs from threat intelligence platforms.

Manual Rule Updates

- Security teams manually update IDS rules based on TI reports.

SIEM Integration

- TI-enhanced IDS alerts can be sent to SIEM & SOAR platforms for automated response.

Insider Threats

Insider Threats

- Malicious Insiders
- Accidental Insiders

Detection Techniques

- User behaviour Analytics (UBA)
- Deception-based Detection

Operational Technology

IDS in SCADA and ICS Environments

- Critical infrastructure (power grids, oil pipelines)

IT vs OT Security needs

Aspect	IT Security	OT Security
Primary Focus	Confidentiality & Integrity	Availability & safety
System Updates	Frequent patches & upgrades	Legacy systems, rarely updated
Attack Consequences	Data breaches, downtime	Physical damage, safety risks

Challenges in OT IDS

- Real-time detection, legacy systems, availability

Trends in IDS

AI & Deep Learning-Basded IDS

- Uses advanced AI models (CNNs, LSTMs, transformers) to detect complex intrusions.

Federated Learning

- Enables multiple entities to train models without sharing raw data, improving privacy.

Explainable AI (XAI

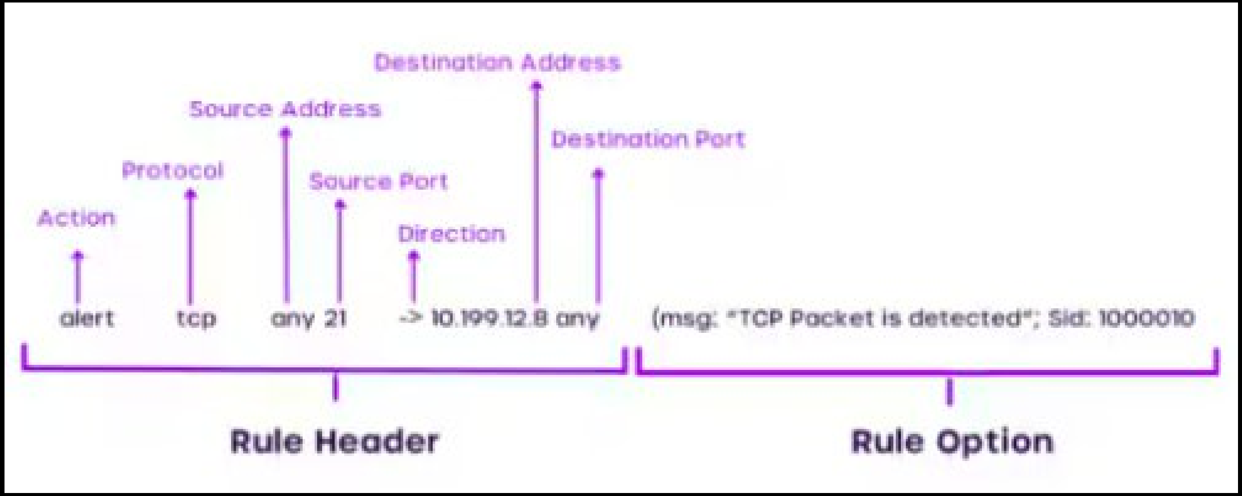
- Ensures AI-driven IDS models provide clear explanations for alerts.

Zero Trust

- Integrating IDS into Zero Trust architecture to continuously validate threats.

IDS Signatures

Snort IDS rules



```
alert tcp any 21 -> 10.199.12.8 any (msg: "TCP Packet is detected"; Sid: 1000010
```

action protocol sourceip sourceport -> destinationip destinationport (options)

Types

- Alert, block, drop, file identification, file rule, logging, pass, service

IDS Signatures

Snort IDS rules

alert icmp any any > $HOME_NET any (msg:”ICMP External Ping”; sid:1; rev:1;)

alert icmp any any > $HOME_NET any (msg:”ICMP External Ping”; sid:1; rev:1;)

alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP Traffic Detected"; flow:to_server,established; sid:100001;)

alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP Traffic Detected"; flow:to_server,established; sid:100001;)

Chat GPT is your friend!

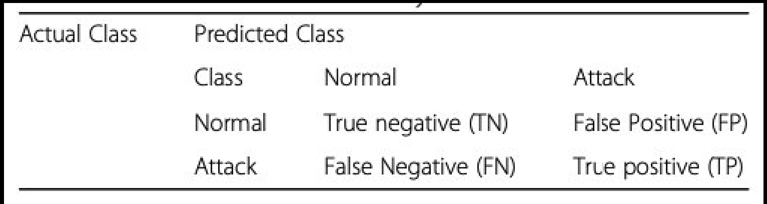
IDS Signatures

Best Practice .... according to Splunk

- Overly broad rules and inefficient writing
- Syntax and documentation errors
- Improper flow direction and content matching issues
- Neglecting rule order and protocol specifics
- Inadequate testing and over reliance on default rules
- Incomplete validation and analysis

Performance Metrics

Confusion Matrix



Actual Class	Predicted Class		
	Class	Normal	Attack
	Normal	True negative (TN)	False Positive (FP)
	Attack	False Negative (FN)	True positive (TP)

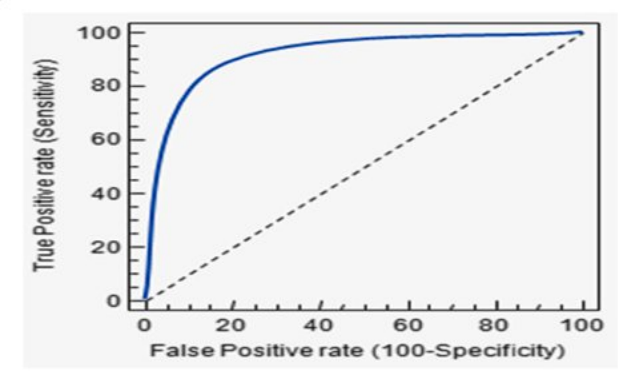
$$\text{TPR} = \frac{TP}{TP+FN}$$

$$\text{FNR} = \frac{FN}{FN+TP}$$

$$\text{FPR} = \frac{FP}{FP+TN}$$

$$\text{ACCURACY} = \frac{TP+TN}{TP+TN+FP+FN}$$

Receiver Operating Characteristics (ROC)



Performance Metrics

$\text{TPR} = \frac{TP}{TP+FN}$ anomalies that are successfully detected

$\text{FNR} = \frac{FN}{FN+TP}$ normal activities that are incorrectly classified as intrusive

$\text{FPR} = \frac{FP}{FP+TN}$ anomalies that are missed and classified as normal

$$\text{ACCURACY} = \frac{TP+TN}{TP+TN+FP+FN}$$

$\text{Precision (P)} = \frac{TP}{TP+FP} \in [0,1]$

$\text{Recall (R)} = \frac{TP}{TP+FN} \in [0,1]$

$$\text{F Measure } (\text{F}_1) = 2 * \frac{P * R}{P+R} \in [0,1]$$

Datasets

- DARPA / KDD Cup99
- CAIDA
- NSL-KDD
- ISCX 2012
- ADFA-LD & ADFA-WD
- CICIDS 2017
- Mirai-RGU (My dataset)

IDS Evasion Techniques

Fragmentation

Flooding

Obfuscation

Encryption

Sources

Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials 16(1):303–336

K. Riesen and H. Bunke, "IAM graph database repository for graph based pattern recognition and machine learning," in Structural, syntactic, and statistical pattern recognition: joint IAPR international workshop, SSPR & SPR 2008, Orlando, USA, December 4–6, 2008. Proceedings, N. da Vitoria Lobo et al., Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 287–297

Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH (2009) The WEKA data mining software: an update. ACM SIGKDD explorations newsletter 11(1):10–18

Kenkre PS, Pai A, Colaco L (2015b) Real Time Intrusion Detection and Prevention System. Springer International Publishing, Cham, pp 405–411

Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials 16(1):303–336

A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, and S. Etalle, "On emulation-based network intrusion detection systems," in Research in attacks, intrusions and defenses: 17th international symposium, RAID 2014, Gothenburg, Sweden, September 17–19, 2014. Proceedings, A. Stavrou, H. Bos, and G. Portokalidis, Eds. Cham: Springer International Publishing, 2014, pp. 384–404

Snort rules 101: Examples & use cases for Snort Network Defense (no date) Splunk. Available at: https://www.splunk.com/en_us/blog/learn/snort-rules.html (Accessed: 07 February 2025).