
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

# Intrusion Detection and Prevention Systems – Part 1

**Dr. Sandra Scott-Hayward**

CSC3064 Lecture 13

School of Electronics, Electrical Engineering and Computer Science

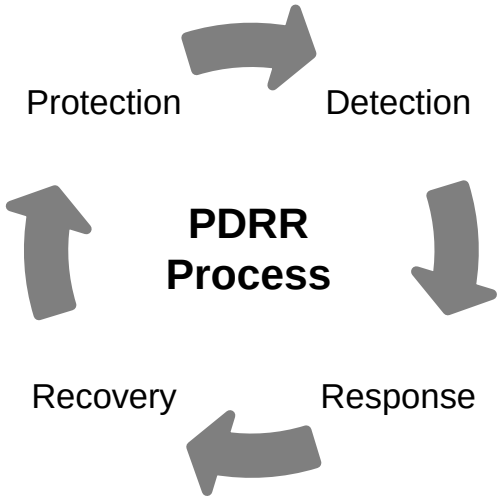
# Session Overview

- Intrusion Detection Systems
  - Host-based (HIDS), Network-based (NIDS)
  - Signature-based detection
  - Anomaly-based detection

**References:**
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007

# What is an intrusion?

- Definition:
  - An *intrusion* is an action or set of actions aimed at compromising the confidentiality, integrity or availability of a service or system.
- Principal defense categories:
  - Prevention
  - Detection
  - Response




QUEEN'S UNIVERSITY BELFAST

# Examples of intrusion

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

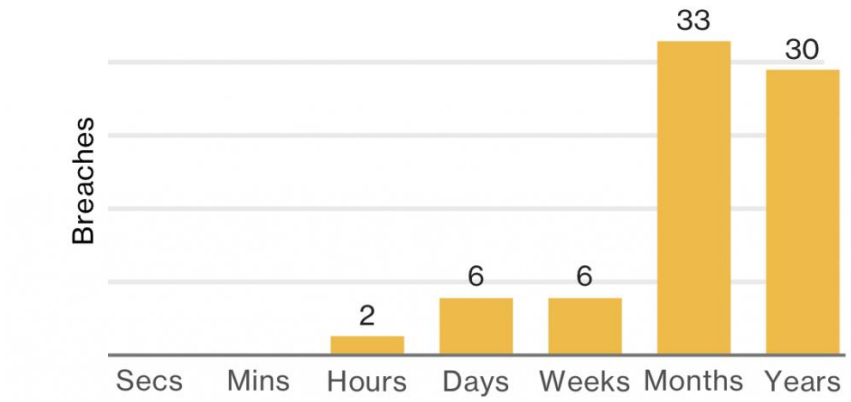
QUEEN'S UNIVERSITY BELFAST

# How long to discover an intrusion?

Table 1: Breach Detection Gap Examples

| Victim | Reported | Time to Discovery |
|---|---|---|
| Michaels Stores | Jan 2014 | 8 Months |
| Home Depot | Sept 2014 | 5 months |
| PF Chang's | July 2014 | 11 months[4] |
| Sony | Nov 2014 | ~1 Year |
| Office of Personnel Management (OPM) | June 2015 | ~1 Year |
| Trump Hotels | Sept 2015 | ~1 Year |
| Undisclosed Mandiant client | 2015 | 8.5 years |

https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you




2017 Verizon Data Breach Investigations Report

Figure 45: Breach discovery timeline within Insider and Privilege Misuse (n=77)

## Breaches Happen in Hours…

But Go Undetected for Months or Even Years


Source: 2013 Data Breach Investigations Report

Timespan of events by percent of breaches

QUEEN'S UNIVERSITY BELFAST

# Goal of Intrusion Detection Systems

- Overall goal: Supervision of computer systems and communication infrastructures in order to detect intrusions and misuse

- Why detection of attackers?
  - Full protection is usually not possible!
  - Security measures too expensive or low flexibility, e.g. H/W protection fixed (ASICs)
  - Because legitimate users get annoyed by too many preventive measures and may even start to circumvent them (introducing new vulnerabilities)
  - Because preventive measures may fail:
    - Incomplete or erroneous specification / implementation / configuration
    - Inadequate deployment by users (just think of passwords...)

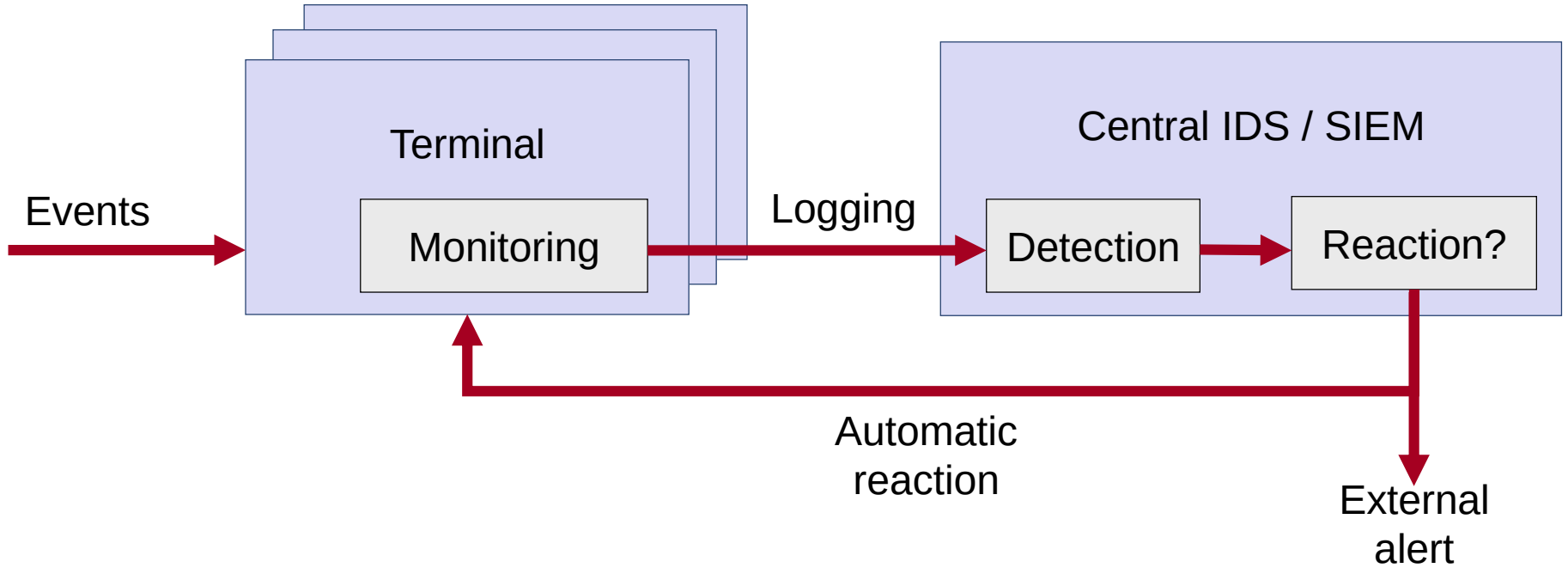
- What can be attained with intrusion detection?
  - Detection of attacks and attackers
  - Detection of system misuse (includes misuse by legitimate users)

QUEEN'S UNIVERSITY BELFAST

# Intrusion Detection

- A system's second line of defense
- Is based on the assumption that the behaviour of the intruder differs from that of a legitimate user in ways that can be quantified
- Considerations:
  - If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data compromised
  - An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions
  - Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility

# Operation of Intrusion Detection Systems




QUEEN'S UNIVERSITY BELFAST

# Security Incident and Event Management

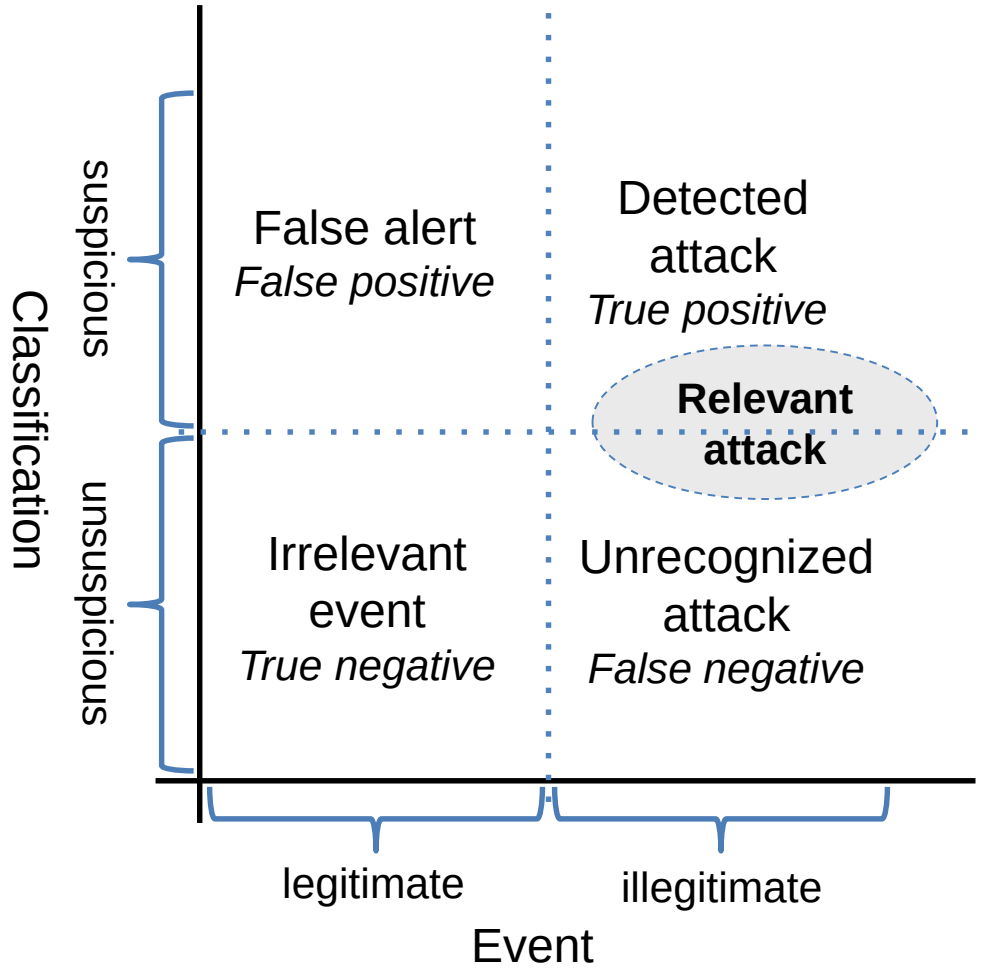

https://espincorp.wordpress.com/2013/04/17/security-information-and-event-management-siem-trend-challenges-and-solutions/

QUEEN'S UNIVERSITY BELFAST

# Tasks of an Intrusion Detection System

- *Audit:*
  - Recording of all security relevant events of a supervised system
  - Preprocessing and management of recorded audit data
- *Detection:*
  - Automatic analysis of audit data
  - Approaches:
    - Signature analysis
    - Abnormal behavior detection (based on knowledge)
    - Anomaly detection (based on learned “normal level”)
  - Types of errors:
    - *False positive:* a non-malicious action is reported as an intrusion
    - *False negative:* an intrusion is not detected
- *Response:*
  - Reporting of detected attacks (alerts)
  - Potentially also initiating countermeasures (reaction)

# Detection Quality




Accuracy = $\frac{TP+FP}{TP+FP+TN+FN}$

Sensitivity (TPR) = $\frac{TP}{TP+FN}$

Precision (PPV) = $\frac{TP}{TP+FP}$

QUEEN'S UNIVERSITY BELFAST

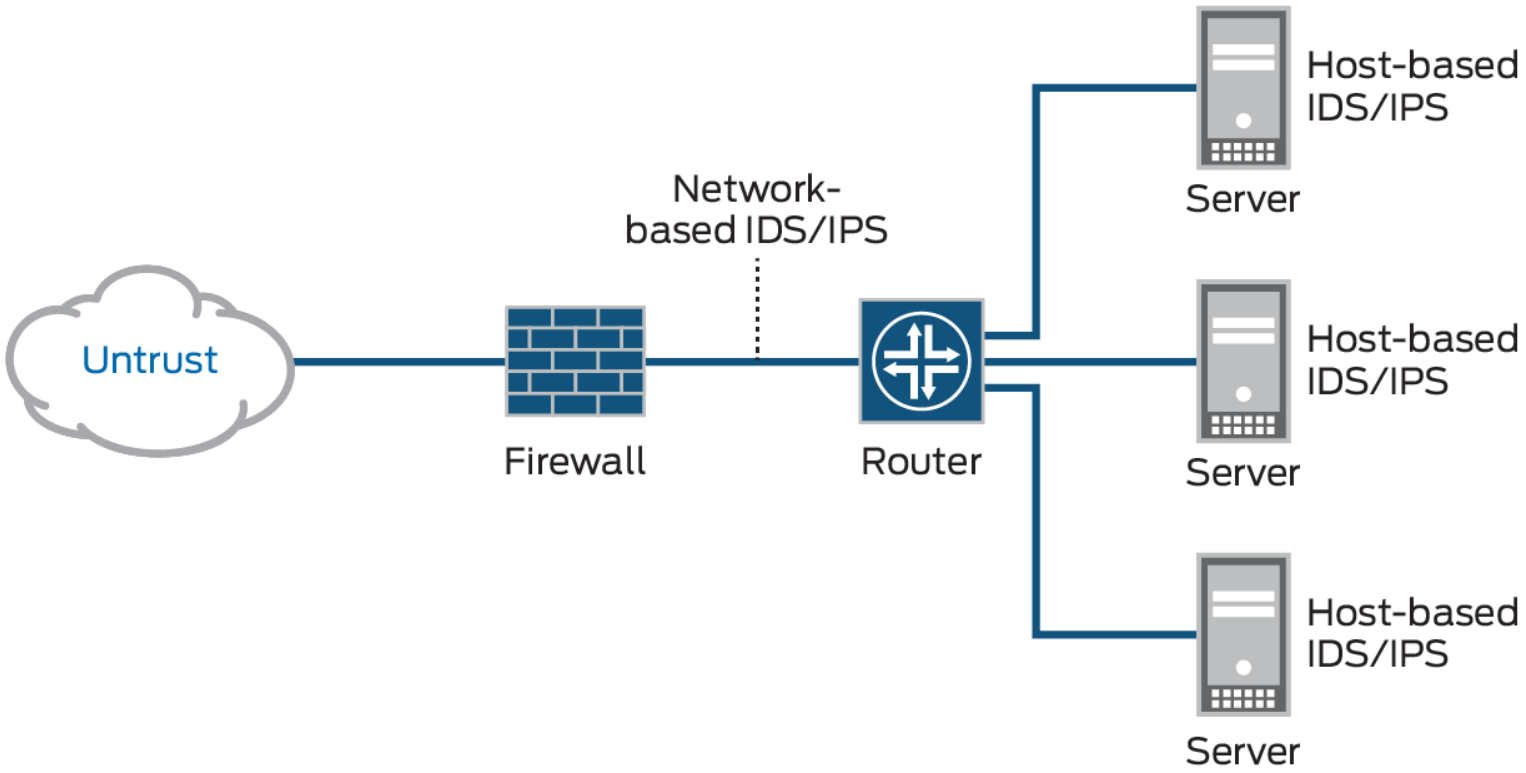
# Detection Quality

- To be of practical use, an intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable level
  - If only a small percentage of actual intrusions are detected, the system provides a false sense of security
  - If the system frequently triggers an alert when there is no intrusion, then either system managers will begin to ignore the alarms or much time will be wasted analyzing the false alarms

# Requirements of IDS

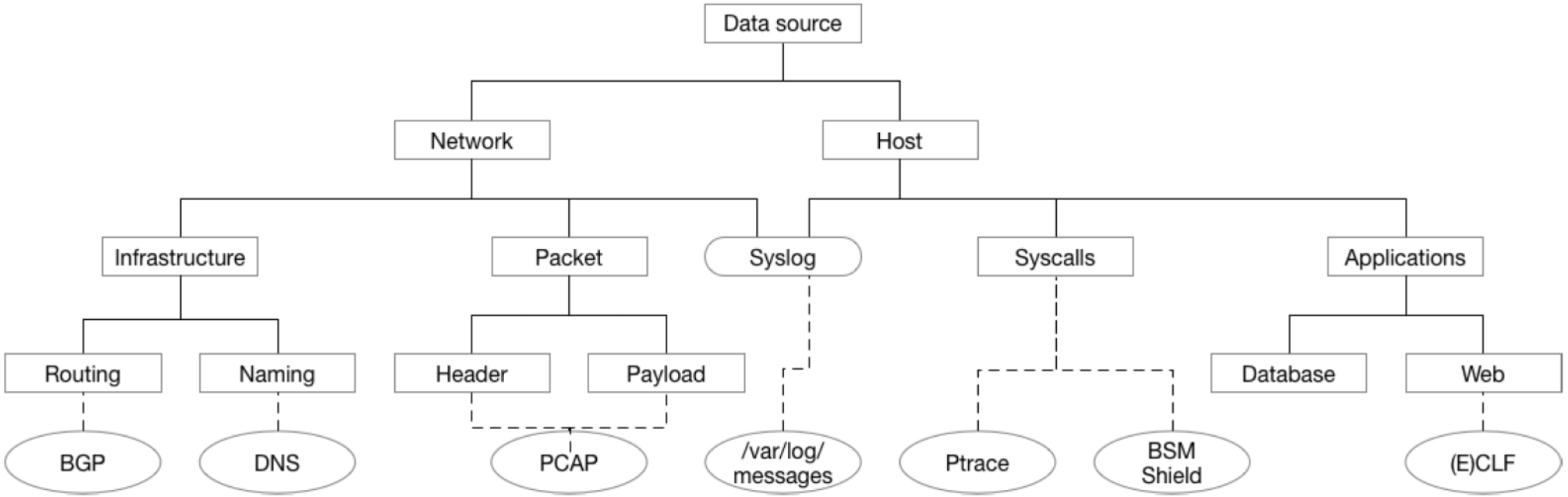
- High accuracy (= low rate of false positives and false negatives)
- Easy to integrate into a system / network
- Easy to configure & maintain
- Autonomous and fault tolerant operation
- Low resource requirements
- Self protection, so that an IDS itself can not easily be deactivated by a deliberate attack (in order to conceal subsequent attacks)

# Host-based IDS vs. Network-based IDS




QUEEN'S UNIVERSITY BELFAST

# Data sources




QUEEN'S UNIVERSITY BELFAST

# Host Intrusion Detection System (HIDS)

- Works on information available on a system i.e. host-based actions:
  - OS and application logs
  - System file modification
  - Illegal file access
  - Login behavior (invalid tries, times)
  - Analysis of system resource consumption
  - Searches for viruses, rootkits etc.
- Can detect attacks by insiders, e.g. when files are copied to USB sticks illegally, but:
  - Has to be installed on every system
    - Hard to manage on a large number of systems
    - Not available for every platform (e.g. routers, printers, medical devices etc.)
    - May be disabled by the attacker!
  - Produces lots of (potentially non-useful) information
  - Often no real-time analysis but pre-defined time intervals

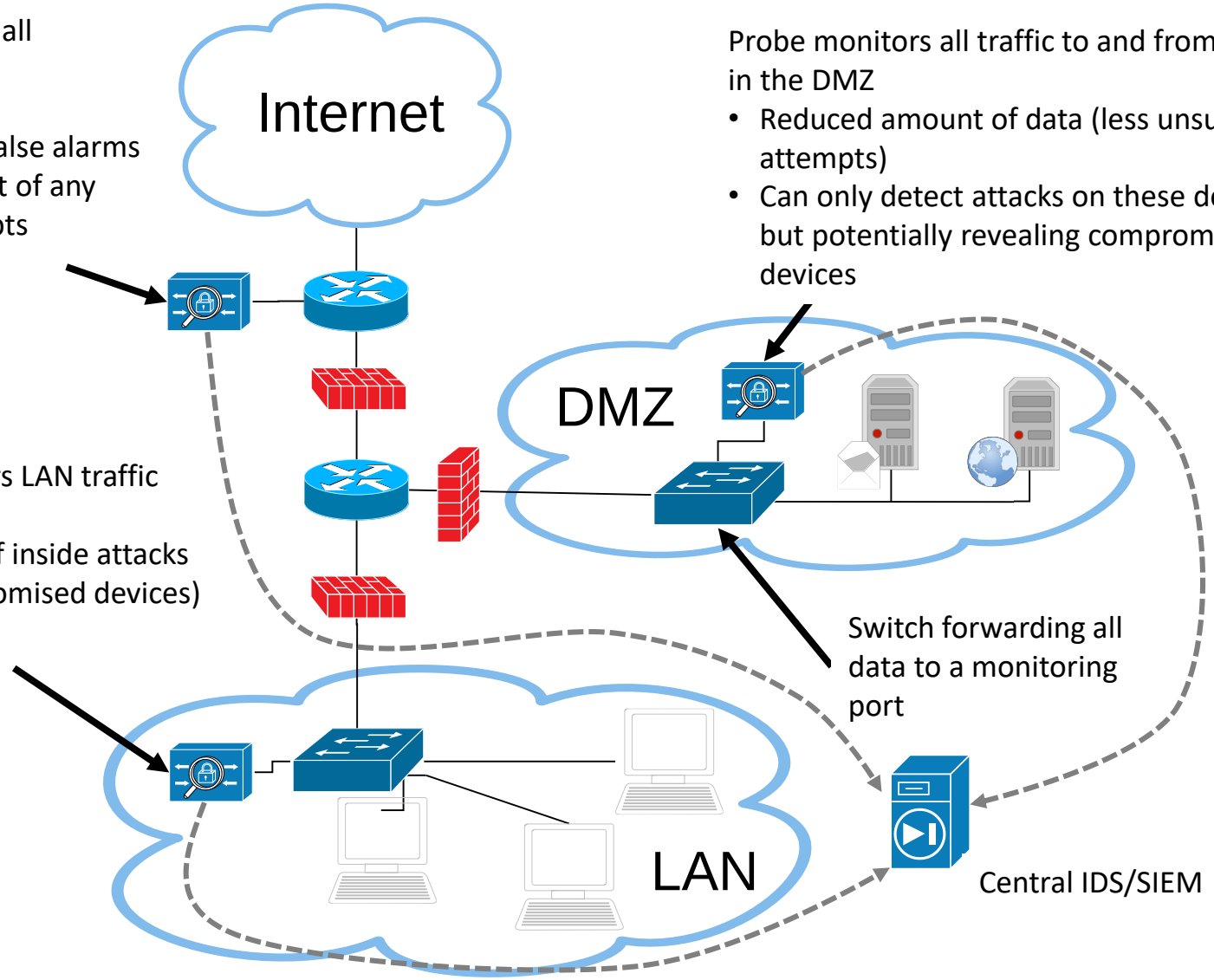
# Network Intrusion Detection System (NIDS)

- Analysis of flow of information on the network i.e. network monitoring
- Can detect, for example, invalid packets, attacks on application layer, DDoS, spoofing attacks, port scans
- Can not detect offline attacks, e.g. files copied to a USB stick
- Often used on network hubs, to monitor a segment of the network
- In reality, also produces lots of (potentially non-useful) information

# Placement of a Network Intrusion Detection System

Probe monitors all incoming traffic
- High load
- High rate of false alarms
- Measurement of any attack attempts

Probe monitors all traffic to and from systems in the DMZ
- Reduced amount of data (less unsuccessful attempts)
- Can only detect attacks on these devices, but potentially revealing compromised LAN devices




Probe monitors LAN traffic
- Low load
- Detection of inside attacks (e.g. compromised devices)

Switch forwarding all data to a monitoring port

Monitoring Network

Central IDS/SIEM

QUEEN'S UNIVERSITY BELFAST

# Intrusion Detection Message Exchange Format

- Intrusion Detection Message Exchange Format (IDMEF)
  - IETF Intrusion Detection WG
    - The Intrusion Detection Message Exchange Format (RFC 4765)
    - Intrusion Detection Message Exchange Requirements (RFC 4766)
    - The Intrusion Detection Exchange Protocol (RFC 4767)
  - Defines messages between probes and central components
  - Allows (in principle) to combine devices from different vendors

# Intrusion Detection Message Exchange Format

- Message types
  - Heartbeat message
  - Alert message (ToolAlert, OverflowAlert, CorrelationAlert)
  - ...

- Event report
  - Analyzer: entity which emitted the alert
  - Classification: what attack has been detected
  - Source: any combination of multiple objects describing a network node, a user, a process, or a service
  - Target: any combination of multiple objects describing a network node, a user, a process, a service, or a file
  - Assessment: severity of the attack and confidence of the analyzer about the validity of the alert
  - Additional information in (name, value) pairs

# Signature-based Detection

- Basic idea:
  - Some attack patterns can be described with sufficient detail → specification of “attack signatures”
  - Event generated if packet(s) contains known attack signatures
- Identifying attack signatures:
  - Analyzing vulnerabilities
  - Analyzing past attacks that have been recorded in the audit
- Specifying attack signatures:
  - Based on identified knowledge, “rules” describing attacks are specified
  - Most IDS offer specification techniques for describing rules

# Signature-based detection – Example: Snort

Each detected attack type needs a predefined rule:

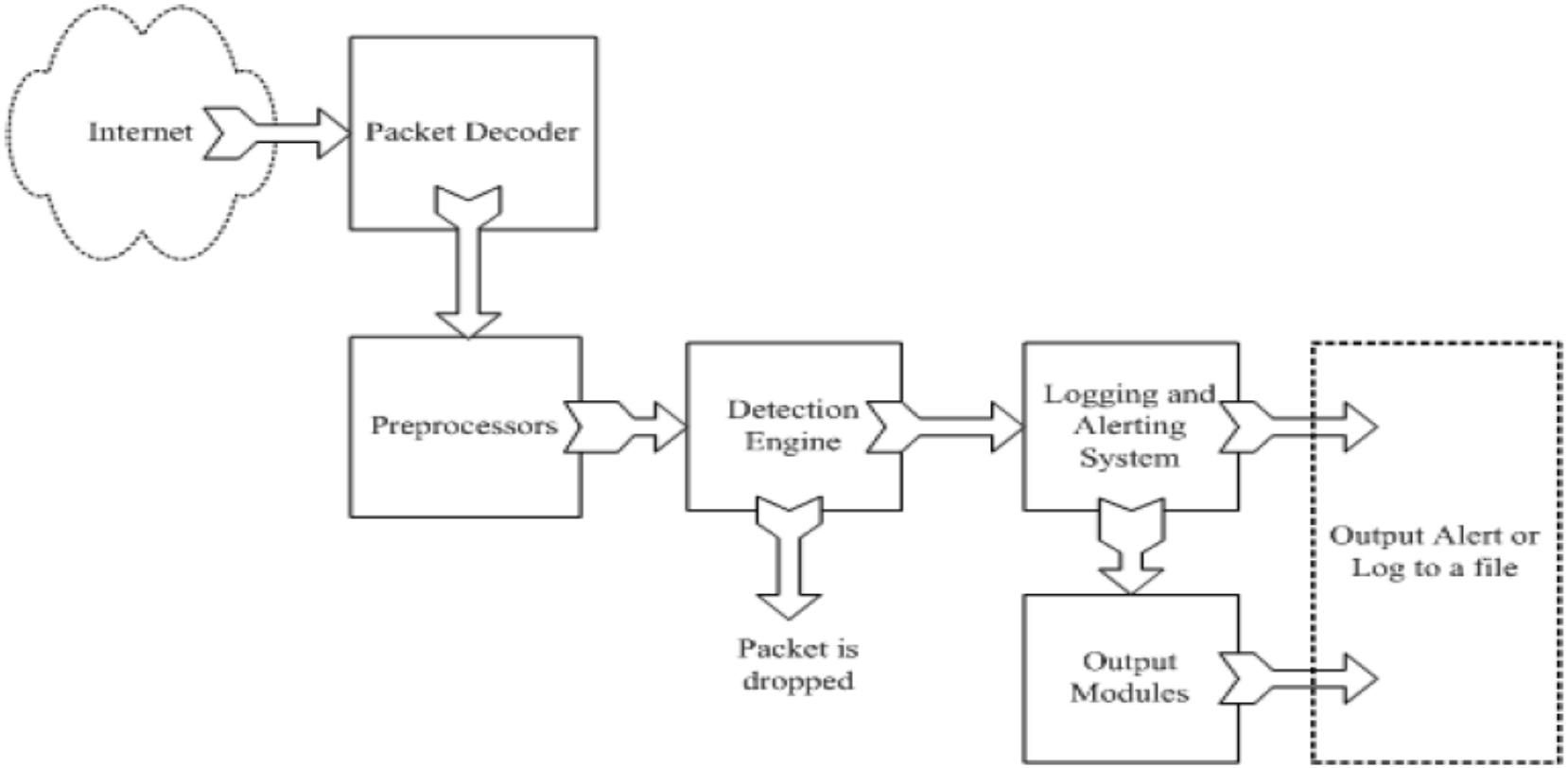
```
alert icmp $EXTERNAL_NET any -> $HOME_NET any
   (msg: "Ping-of-Death detected";
    dsize: > 10000;
    sid: 3737844653)
```

- Shall detect Ping-of-Death packets, i.e., packets that are unusually large and crash the operating system
- What do these packets look like at layer 3 (and below)
  - MTU is usually 1,500 bytes
  - → at least 7 packets!

- Requires preprocessing of packets!

QUEEN'S UNIVERSITY BELFAST

# Snort




http://www.snort.org/

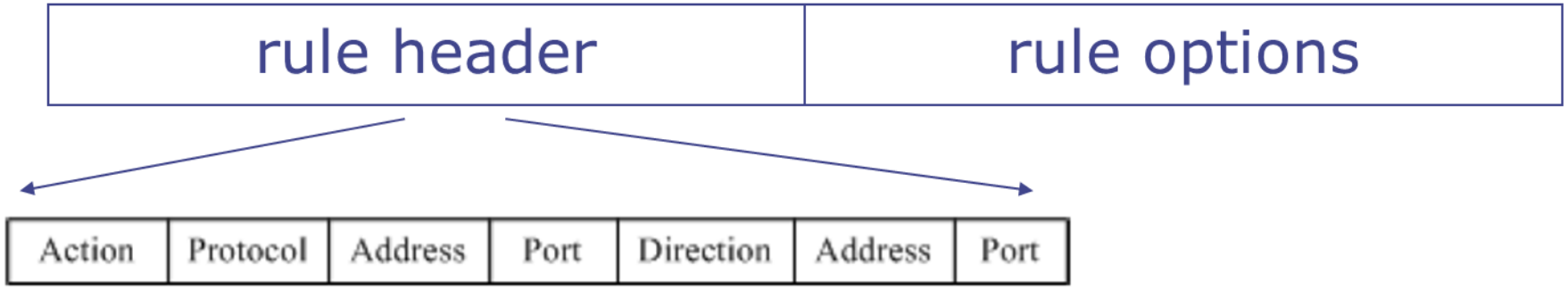
**Source:** Rafeeq Ur Rehman, *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID.*

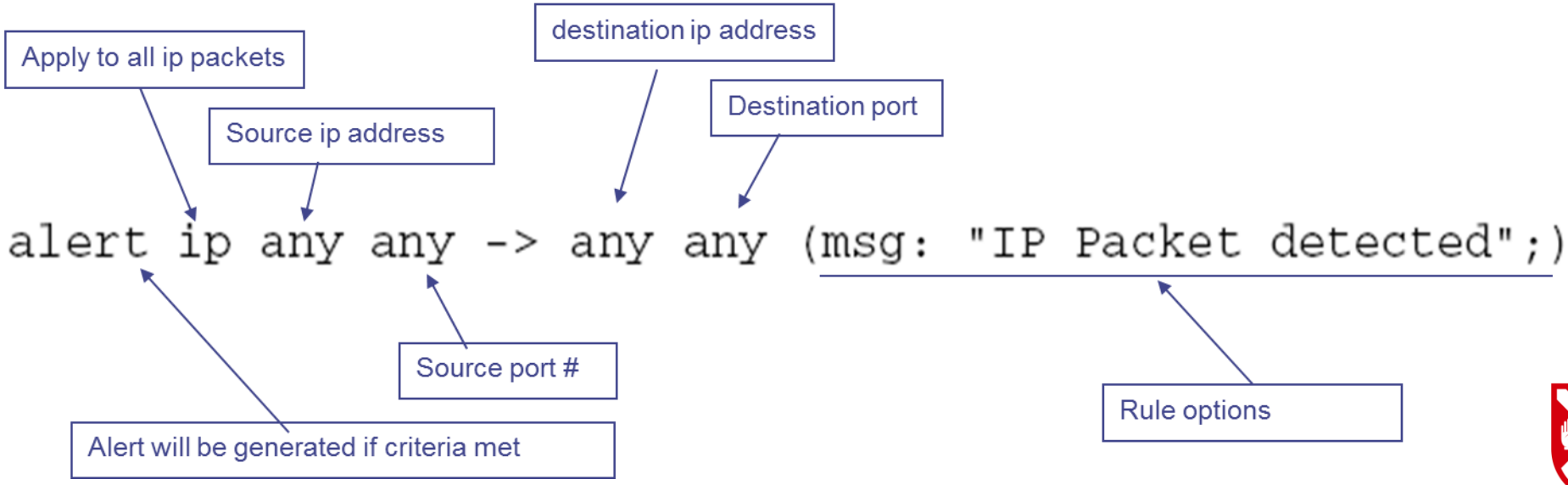
QUEEN'S UNIVERSITY BELFAST

# Snort components

- Packet Decoder
  - input from Ethernet, PPP etc.
- Preprocessor:
  - detect anomalies in packet headers
  - packet defragmentation
  - decode HTTP URI
  - reassemble TCP streams
- Detection Engine: applies rules to packets
- Logging and Alerting System
- Output Modules: alerts, log, other output

# Snort detection rules




QUEEN'S UNIVERSITY BELFAST

# Signature-based detection – Example: Snort

More sophisticated example, checking for mail server buffer overflows:

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25
   (msg:"SERVER-MAIL RCPT TO overflow";
    flow:to_server,established;
    content:"rcpt to|3A|";
    nocase;
    isdataat:256,relative;
    pcre:"/^RCPT TO\x3a\s*\x3c?[^\n\x3e]{256}/im";
    classtype:attempted-admin;
    sid:654;
    rev:23;)
```

Quick check

Better check – looking for specific content in packet payload (requires TCP reassembly)

Very slow regular expression check

QUEEN'S UNIVERSITY BELFAST

# Signature-based detection - Properties

- Advantages:
  - Easy to setup
  - In some environments acceptable false positive rate
- Drawbacks:
  - Requires prior knowledge of all potential attacks
  - Signature database requires continuous updating
    - Large databases, difficult to maintain
  - High rate of false negatives if signature database is not adapted or up-to-date
  - IP & TCP preprocessing requires significant resources
  - Possibility of bypassing:
    - Attackers being aware of a certain IDS may try to craft attacks that are not covered by any signature
    - May be tested offline!

# Behaviour/Anomaly-based Detection

- Basic idea – detect behavior that differs significantly from normal use
- Users and systems have “normal” use pattern:
  - Activity pattern
  - Used protocols & protocol states
  - Accessed servers
  - Traffic volumes
  - …
- Assumption: “behavior” can be described by an administrator
  - Needs a specification, e.g., in a rule language
  - For generic protocols such a description may be predefined
- Analysis:
  - Events matched against rules
  - Abnormal behaviour will be reported

QUEEN'S UNIVERSITY BELFAST

# Detection of Abnormal Behaviour – Example Systems

- NetSTAT
  - Early academic example
  - Compares network traffic in probes with fact base
- StealthWatch
  - Commercial system
  - Analyses flow information in switches, i.e., using Cisco NetFlow or sFlow
  - Can detect network scans, worm spreading, DoS attacks …
- Bro Security Monitor
  - Long-living open source project
  - Performs stateful protocol analysis
  - Reports protocol deviations, e.g., undocumented commands
  - Converts packets captured into series of events


QUEEN'S UNIVERSITY BELFAST

# Detection of Abnormal Behaviour – Properties

- Advantages:
  - Approach can detect unknown attacks
  - Attacks cannot easily be prepared to avoid detection
  - If well set up: acceptable false positive rate
  - Events quite easy to interpret

- Drawbacks:
  - High administrative effort

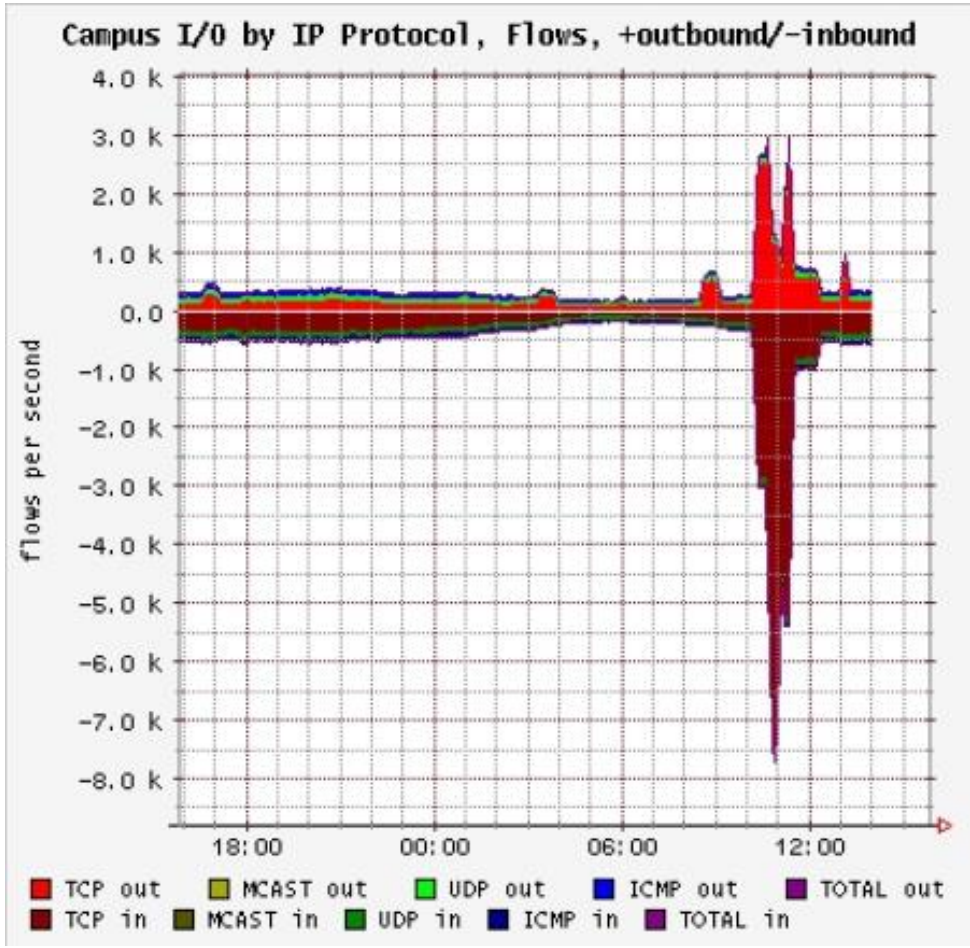
# Automatic Anomaly Detection - Overview

- Basic idea – detect behavior that differs significantly from normal use, which is automatically learned
- Assumption: “normal user behavior” can be described statistically
  - Requires a learning phase / specification of normal behavior
  - Can learn significantly more features than an administrator is able to specify manually!
- Analysis:
  - Compares recorded events with reference profile of normal behavior
  - Use statistics and anomaly detection techniques to find outliers
  - Report if there is a timely correlation of a significant number of outliers

QUEEN'S UNIVERSITY BELFAST

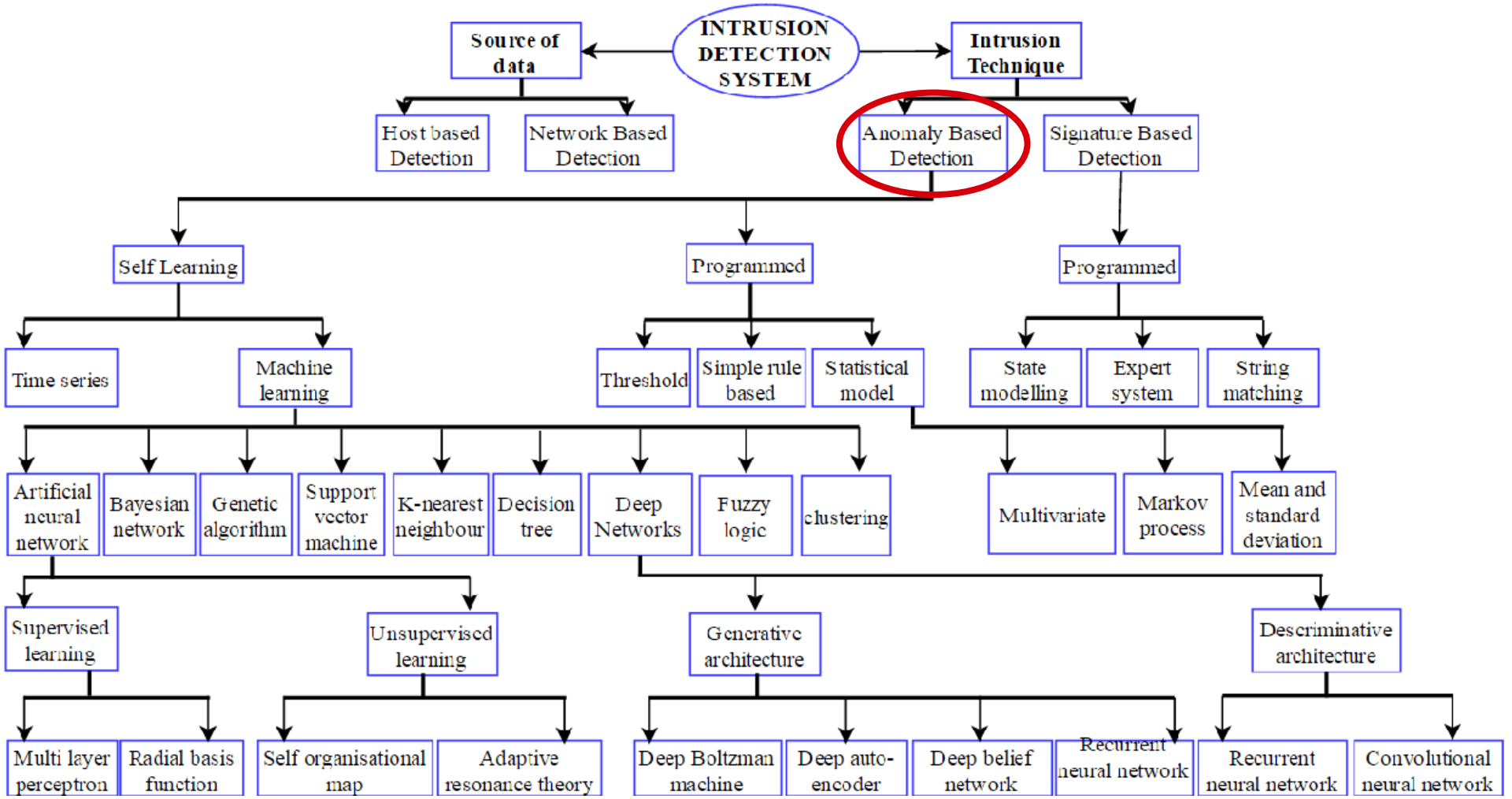
# Automatic Anomaly Detection - Example

- Network abuse anomalies
  - DoS flood attacks
  - Port scans



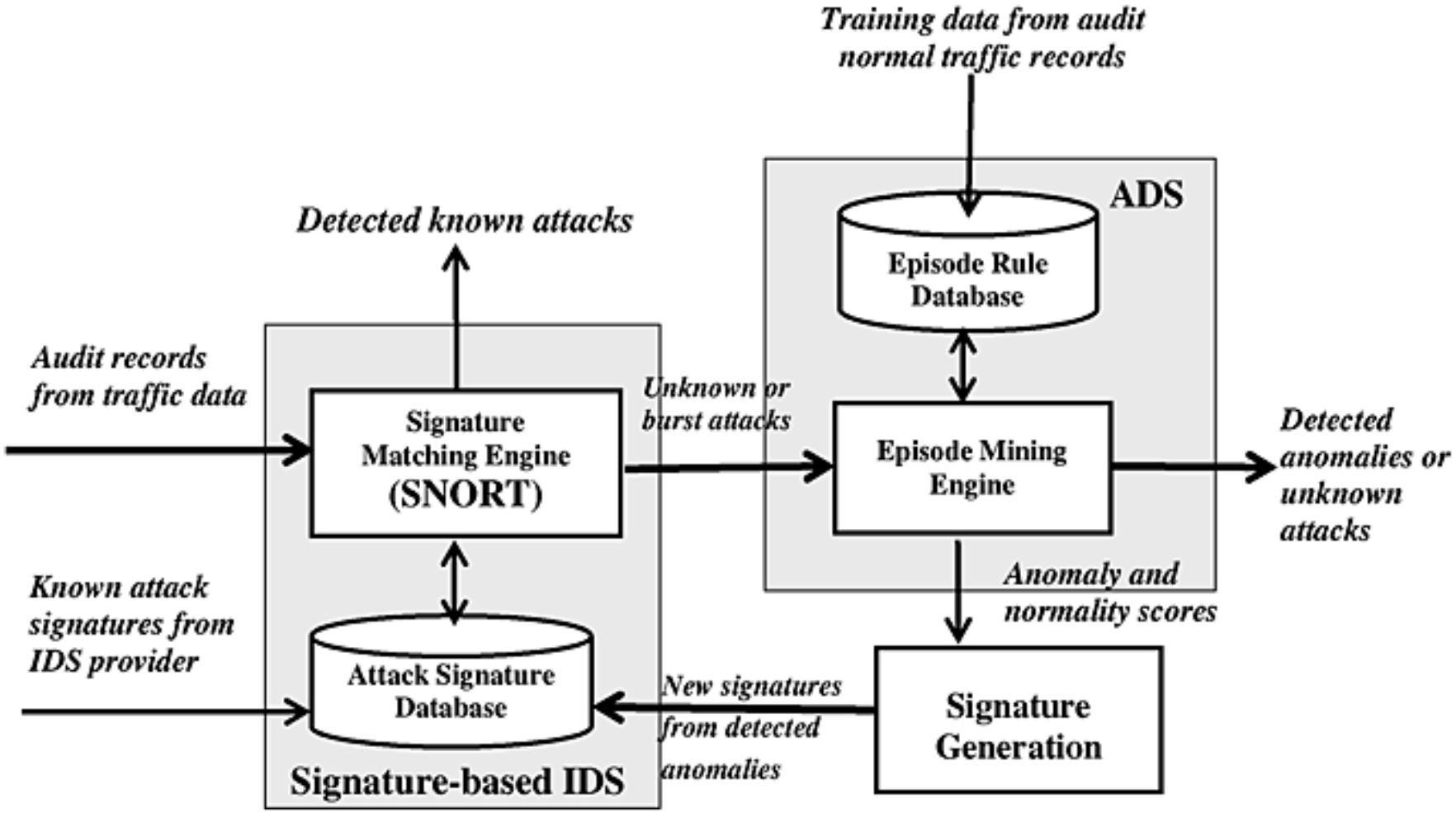

QUEEN'S UNIVERSITY BELFAST

# Anomaly Based Detection Techniques




QUEEN'S UNIVERSITY BELFAST

# Hybrid IDS Model



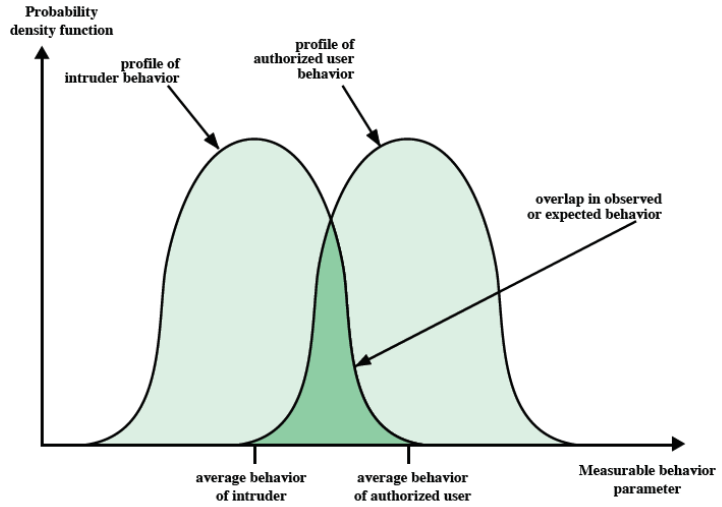

*Source:* IEEE Computer Society

QUEEN'S UNIVERSITY BELFAST

# Automatic Anomaly Detection - Properties

- Advantages:
  - Can detect unknown attacks
  - Comparably easy to setup
- Drawbacks:
  - Privacy:
    - Collecting user specific usage patterns
    - Work-related or personal habits
  - Requires continuous refreshing of normal behavior patterns
  - High amount of false positives
  - Even true positives often difficult to interpret (not linked to a specific attack signature)

  - If a normal behavior pattern matches an attack pattern, this kind of attack will not be detected ($\rightarrow$ false negative)




QUEEN'S UNIVERSITY BELFAST

# Summary: Properties of IDS approaches

- Signature-based Detection:
  - Requires high effort in specification of rules (can be leveraged by multiple usage; comparable to sharing of virus description)
  - Effective detection of attacks that have been described in rule database
  - Unknown attacks cannot be detected
- Detection of Abnormal Behavior
  - Extremely high effort to set up
  - Possibility to detect some unknown attacks
- Anomaly Detection:
  - Can detect unknown (zero-day attacks)
  - Theoretically challenging
  - Realization expensive in terms of required data and analysis capabilities

# Questions?

Next Session: IDPS – Part 2

Friday, 01 March 2019

QUEEN'S UNIVERSITY BELFAST