Intrusion Detection Systems

Ramin Sadre

Intrusion Detection Systems (IDS)

- The job of an IDS is to detect intrusions
- *Intrusions* = unwanted/malicious activities in a system
  - Information retrieval attacks (scans,…)
  - Stealing information
  - Denial of service attacks
  - …

Types of IDS

- There are many different IDS
- IDS can be classified by:
  - How they react to attacks
  - What detection method they use
  - What kind of data they rely on
  - Where they are deployed
  - ...
- Example: Spam filter
  - Reaction: Block mail, adapt filter rules,...
  - Detection method: Blacklists, Baysian filter,...
  - Input data: Mails
  - Where: On mailserver or in mail client

Reaction

- When an intrusion (or intrusion attempt) has been detected, actions can be taken:
  - *Passive*: Raising an alarm
  - *Active*: Block the intruder or even do a counter-attack (is that legal?)
- In larger systems (e.g. a company network), IDS are often (at least partly) active
  - Otherwise, the system would not be maintainable
- However, an active IDS can become dangerous if it takes incorrect decisions (*False Positives*)
  - Attackers could attack the IDS to provoke incorrect decisions! (e.g. using spoofed IP addresses)

Detection Method

- Two basic detection principles:

1. **Signature/knowledge/misuse based**:
   - Look for patterns/signatures of known attacks
   - Example: "Block all mails containing the word ‘Cheap’"
   - Pro: Very precise when attack is known
   - Con: Difficult to detect new/modified attacks (0-day)
2. **Anomaly/behavior based**
   - Look for deviations from normal behavior
   - Example: "Block all IPs that send more than 100 mails per day"
   - Pro: Can detect new attacks
   - Con: Somebody has to define what normality means in the monitored system. Normality can change over time!

Audit source location

- What kind of data source is the IDS monitoring for suspicious activities?
- Many possible sources, depending where the IDS is located
- Two basic types of IDS:
  1. Host-based IDS
  2. Network-based IDS

Host-based IDS

- IDS is located on the host that it should monitor
- Examples:
  - Your mail client
  - Many webservers verify incoming HTTP requests before execution
  - The anti-virus on your computer
- Possible data sources:
  - Incoming e-mails
  - Incoming/outgoing network traffic
  - File access
  - Call of operating system functions
  - Log files (OS, apache,…)
  - …

Network-based IDS

- The IDS monitors the network traffic
- Observation point: “network tap”
  - IDS obtains a copy of traffic through the mirror port of a router or switch
- Traffic can be monitored at different levels of detail
  - *Deep Packet Inspection* (DPI) = Look into every packet and analyze its content. Nowadays, rather limited, since most services are using encryption (TLS)
  - Packet headers = Only look at packet headers (IP addresses, port numbers,…)
  - Flows = Only look at connection summaries, not at every packet

    "At 22:30, host 1.1.1.1 exchanged 20 packets on port 23 with 2.2.2.2"

A DPI-based IDS: Snort

https://www.snort.org/

- Most widely deployed IDS in the Internet
- Compares the monitored traffic against a set of rules
- If a rule matches, an alarm is raised
- Database contains thousands of rules
- Can be deployed as
  - Host-based: monitors traffic of host
  - Network-based: monitors traffic in a network

Snort rules: Examples

```
alert icmp any any -> any any
(msg: "ICMP packet detected!"; sid: 1;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg: "MALWARE-CNC Win.Trojan.NanoBot/Perseus server
heartbeat request attempt";
flow: to_client,established;
dsize: 36;
content: "|20 00 00 00 2B FF 4B F4|";
depth: 8;
metadata:impact_flag red, policy balanced-ips drop,
policy security-ips drop;
sid:39582; rev:1;)
```

Pros and Cons of Host-based IDS

- Pros:
  - Very detailed data sources available for every aspect of the monitored system
  - Encrypted data (e.g. HTTPS) not a problem if the IDS runs inside the application (e.g. inside a webserver)

- Cons:
  - Can consume a lot of CPU and memory on the host
  - Only sees the activity of one single host. The big picture is missing.
  - Cannot stop attacks against the network link of the host, for example a bandwidth-consuming DoS attack

Pros and Cons of Network-based IDS

- Pros:
  - Can be deployed on a dedicated machine
  - Can monitor the activity of the entire network
  - Flow monitoring scalable to high-speed networks >50 Gbps. Many routers can export flow records in real time.
- Cons:
  - Only sees the network traffic, not what is happening on the hosts
  - DPI is expensive and requires special designs for >10 Gbps networks (hardware, distributed IDS,...)
  - DPI cannot analyze encrypted traffic (HTTPS!)
  - Flows are good for detection of brute-force DoS attacks but not very useful for attacks where the packet payload is important

DPI speed

- Free DPI-based IDS: *snort*, *bro, suricata*
- DPI is very resource consuming if done in fast networks
  - You need special network interfaces that can receive ≥10 Gbps traffic without drops
  - But also CPU power!
  - Will also depend on the number and complexity of your rules/scripts, therefore very hard to give general recommendations
- In 2014, the bro authors recommended 1 CPU *core* per 80 Mbps of traffic
- Snort can handle 800 Mbps per *processor* (whatever that means)

DPI speed (2)

- DPI-based IDS like snort or bro are complex:
  - They have parsers and analyzers for many protocols at different protocol layers (UDP, TCP, DNS, HTTP,…)
  - The traffic stream has to be re-assembled. Otherwise, the attacker would simply split the attack on several fragments or segments
  - Often, there are *stateful*: They do not analyze single packets but also the state of the TCP connection. Example: When a SYN-ACK packet arrives, they remember whether the previous packet was a SYN packet

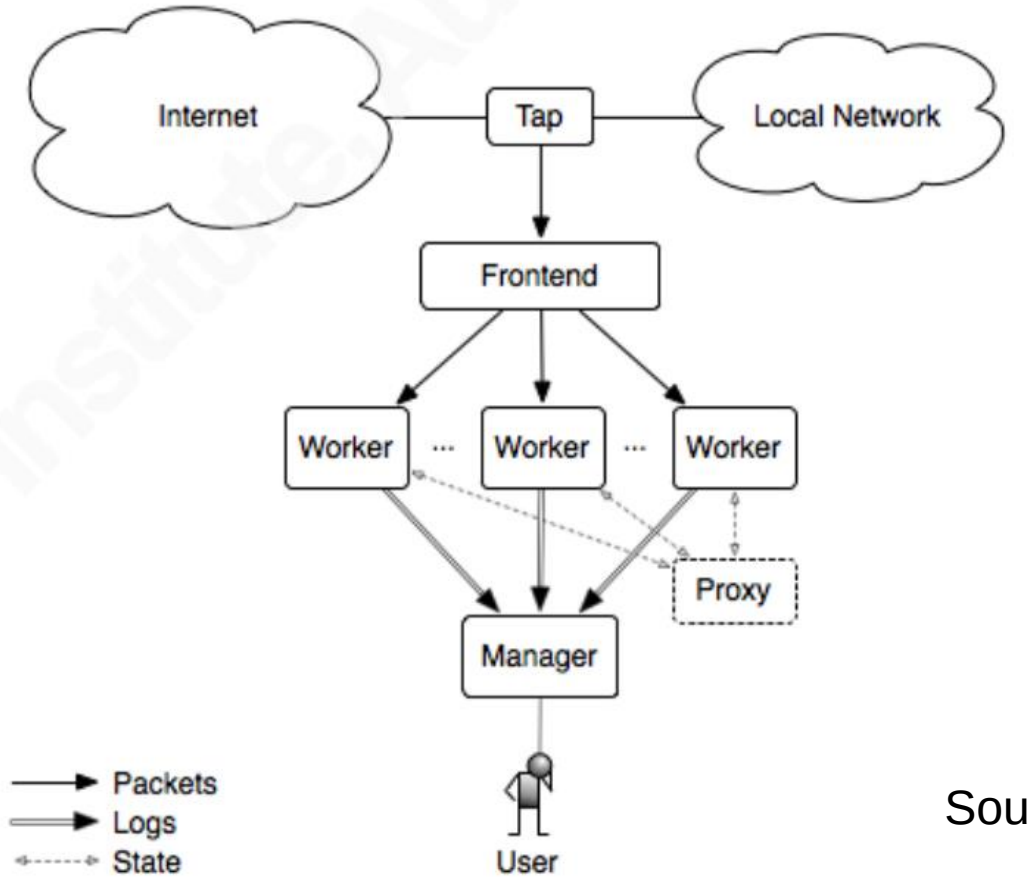
Improving speed and detection performance

- Speed and detection performance of IDS can be improved by more advanced designs

- **Collaborative IDS**: IDS instances can exchange information in order to improve detection quality
- **Hierarchical IDS**: Small and fast IDS can forward analysis results to “bigger” IDS for further analysis
- Example: Modern anti-virus (especially for Windows)
  - Report incidents to central server
  - Regularly receive updates
  - Can rely on cloud-based detection engines for further analysis

Load-balancing for Bro

If the traffic is too much for a single machine, the load has to be distributed



Source: bro.org

Intrusion Detection vs Anomaly Detection

- **Anomaly detection** = broader than intrusion detection
  - Also includes detection of errors of failures
- Example: Network operators have software & hardware to monitor link status, packet losses, etc. of their networks
  - Detection principles are similar to IDS
  - Often these systems also help with *root cause analysis: What is the source of the anomaly?*

- There is also the term **Intrusion Prevention System** (IPS)
  - Some people use IPS = IDS
  - Some people use IPS = IDS + countermeasures