Chapter 1

Intrusion Detection Systems

Introduction

With the birth of the smart grid as the next step of evolution for grid infrastructure, with the improvements that the smart grid came with, like improved reliability, automation, and faster detection and response to failures, it also came with its own set of risks and disadvantages. mainly due to the fact that it is composed of multiple components and systems that are connected to the internet, like wireless networks and sensors, smart meters, and IoT devices, making it an easy target for hackers. independent groups or state actors whose goal is to cause as much damage as possible or to collect valuable data. On top of those components, there are legacy systems that the smart grid relies on that are known for their many and major security vulnerabilities, which are all easy targets, for example, Supervisory Control and Data Acquisition (SCADA). As an example of those risks and weaknesses, we can look at the situation Ukraine found itself in after Russia targeted their smart grid systems in 2015, leaving 80,000 Ukrainian households without power for 3 to 6 hours. **?**.

That's why it is important to protect the smart grid system from cyberattacks by employing IDS, IPS, and IDPS. as the second line of defense in case encryption and authorization were unsuccessful in stopping the cyberattack from targeting the smart grid system.

1.1 Intrusion detection systems (IDS)

An intrusion detection system is a piece of hardware or software that is responsible for detecting suspicious and malicious activity, and in a network or an information system, the anomaly can either be reported to a systems administrator or saved to a security information and even management system (SIEM), the SIEM combines the output from multiple sources, then uses some filtering techniques to decide if the reported activity is malicious. **?** An IDS on its own cannot stop intrusions; it can only detect and report them. However, with its evolution, the intrusion prevention system (IPS) or intrusion detection and prevention system (IDPS) can counter an attack. **?**

1.2 Intrusion detection systems architecture

Intrusion detection systems, like any complex system, are made of multiple interoperating components with a specific task assigned to each component. Although the functioning of an IDS changes vastly between different types of IDSs (different in deployment or detection methods), they all share a common general architecture, which is composed of the following components as shown in Figure 1.1 **?**:

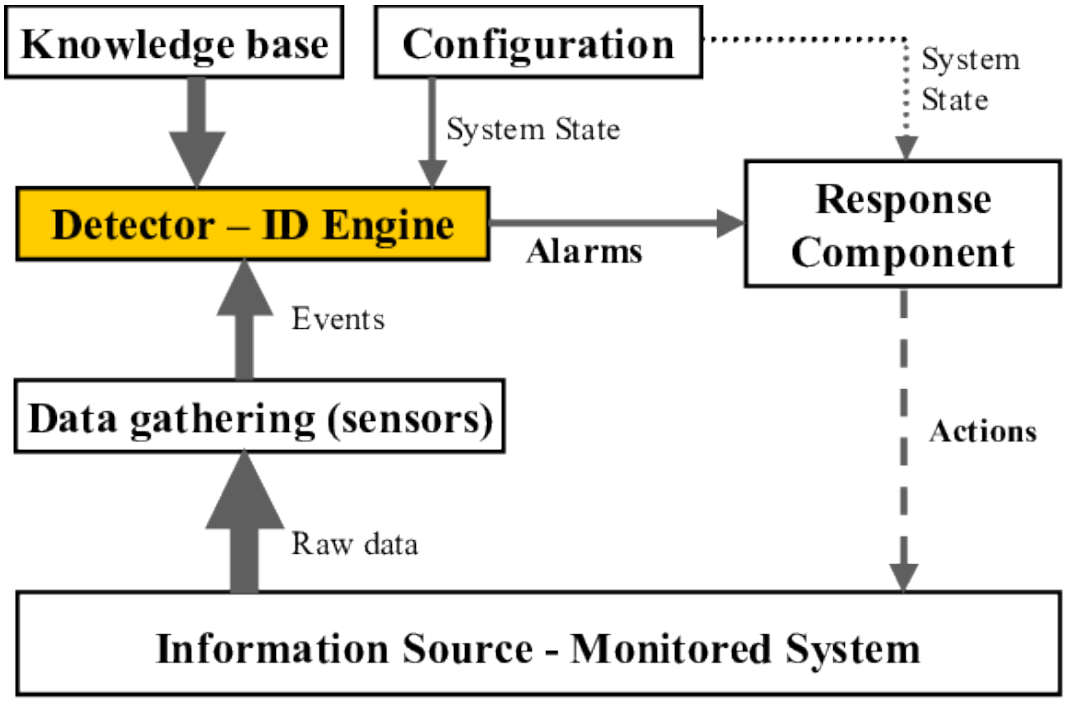

Figure 1.1: IDS architecture **?**

- Data gathering components (sensor): tasked with collecting information from the monitored environment.

- Detector (IDS engine): analyzes the data collected by the sensor to determine the presence of suspicious activity.
- Knowledge base(database): the database that stores information collected previously by sensors about known attacks that allows the engine to determine the suspesious activity.
- Configuration component: defines settings and the behaviour of the system.
- Response component: this component is responsible for responding to the detected intrusion and either attempts to prevent the intrusion (IPS) or reports it to a human administrator (IDS).

1.3 Intrusion detection systems classification

Intrusion detection systems are classified according to two criteria of classification, which as shown in Figure 1.2 are:

- deployment method **?**
- detection method **?**

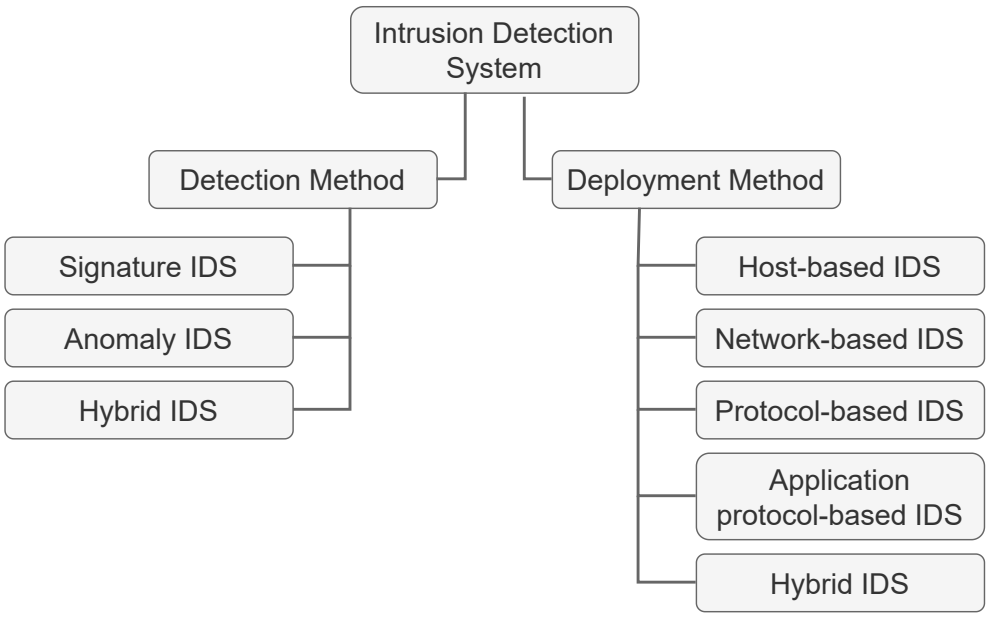

Figure 1.2: IDS classification taxonomy

1.3.1 Deployment methods

The deployment of IDS involves several methods that ensure effective monitoring and detection of potential threats. Here are some common deployment methods for IDS.

1.3.1.1 NIDS

Network intrusion detection systems are the most commonly used commercial IDS. They are usually placed at the start edge of the sub-network, right after the firewall (if one exists), so they can have access to all inbound traffic to all devices on the network **?**. NIDS protects the networks from cyber attacks and threats by scanning and monitoring TCP/IP packets for known attack signatures and reporting them to the administrator **?**

Some benefits of using a NIDS are that a few well-placed NIDS can be enough to cover an entire large network. In addition, their deployment requires minimal refactoring of the network, meaning easy installation **?**. But the downsides are that they cannot detect threats with inaccurately constructed attack signatures and cannot analyze encrypted traffic, and it is hard to work with networks operating at 10 Gbps **?**.

With a NIDS, one would ideally scan all inbound and outbound traffic; however, doing so might create a bottleneck that would impair the overall speed of the network.

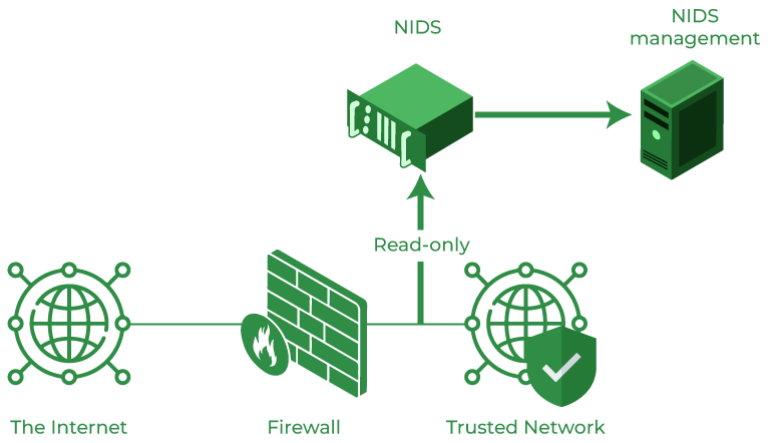

Figure 1.3: NIDS **?**

1.3.1.2 HIDS

Unlike NIDS, HIDS run on individual devices in a network, making it's threat detection scope more focused. They monitor all incoming and outgoing traffic and alert the administrator if suspicious or malicious activity is detected.

It is considered to be more reliable than NIDS because it has access to files in the operating system, and it can detect if a file has been tampered with by keeping snapshots of previous versions of those system files and comparing them to the current version to decide if it has been tampered with. **?**

This type of IDS uses 2 sources of information inside the device's operating system:

- system audit trails: operating system audit trails are created by the kernel making them very detailed because the kernel has access to everything in an OS. **?**
- system logs: less complex the system audit trails making them easier to understand. **?**

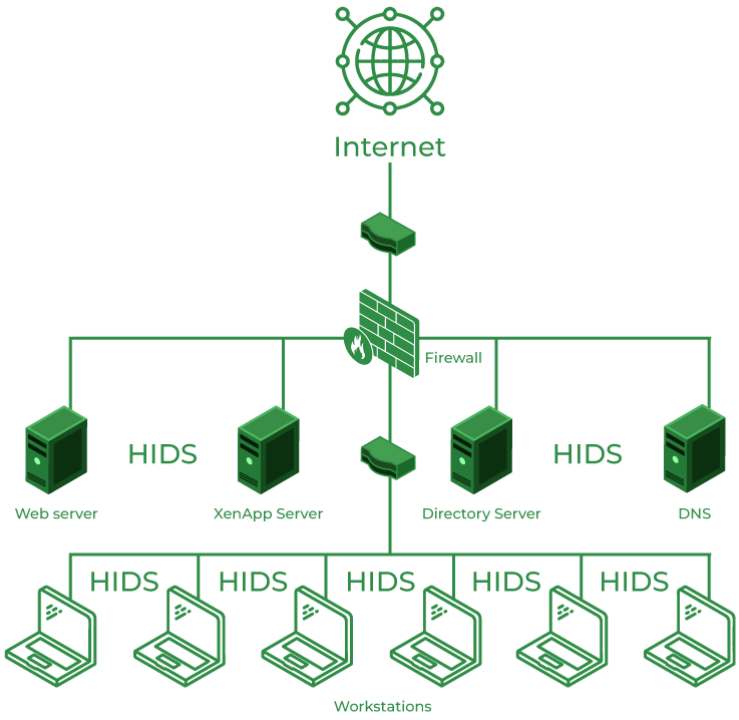

Figure 1.4: HIDS **?**

1.3.1.3 Other types of IDS

uncommon types with specific functions usually, used together with NIDS or HIDS to augment their detection capabilities.

- Protocol intrusion detection system (PIDS): this type of IDS monitors the protocol in use (like HTTP or HTTPS) between the server and the client. PIDS is usually placed at the front end of the server. **?**
- Application protocol detection system (APIDS): specialized in application security, it analyzes the packets of application-specific protocols (like MySQL) to determine the presence of suspicious activity. APIDS are usually placed on groups of servers. **?**
- hybrid detection system: it is a combination of two or more of any of the previously defined IDSs. It is more reliable than any individual IDS because it has access to the data accessible to all of the used IDSs, providing it with a network-wide view. **?**

1.3.2 Detection methods

There are two primary methodes of detection for IDS which are anomaly-based and signature-based (which is also known as misuse intrusion detection or knowledge-based intrusion detection). **?**

1.3.2.1 Signature-based detection

SIDs define patterns in known cyberattacks and store them in a database as signatures. The SID then analyzes system activity and search for a pattern of suspicious activity that matches previously documented attacks's signatures. This method provides high detection capabilities against known attacks. even though it cannot detect new attacks. On top of that, the database of previous attacks is very large, and having to compare internet packets to this database is resource- and time-consuming. **?**

1.3.2.2 Anomaly-based detection

AIDs can identify abnormal behaviour in the environment it is used in, this type of IDS first observes and models the normal behaviours then compares the trffic to this model to determine the presnece of suspesious activity. the constructed model is created based on the data collected by observing the behaviour of the system over a specific period of time of normal operation. **?**

AIDs often lead to a lot of false negatives because the normal activity varies alot over time, althout it is better than SIDs in detecting new and unknown attacks. it can also be used to provide new data for the signature-based detection systems. **?**

1.3.2.3 Hybrid detection

Hybrid IDS uses both Signature based and anomaly based detection althout it's not widely used because it is still in development. **?**

1.3.2.4 Signature-based VS Anomaly-based detection

table of pros and cons sigVSano.tex

Table 1.1: An example of tables

	Signature-based	Anomaly-based
Pros	▶ simple and effective against know attacks ▶ fewer false positives	▶ Ineffecitve againts new and unknown attacks ▶ slow if the database is large ▶ database needs to be cosntantly constanlty maintained and updated
Cons	▶ can detect new and unknown attacks ▶ can provide data to Signature-based detection	▶ more false negatives ▶ needs training to build normal behaviour models

The biggest disadvantage of an IDS is its inability to react to attacks and actively block malicious activity. That's why it was necessary to create a new system to overcome those drawbacks, which is IDPS, also known as IDPS, IDPS just like IDS monitors the activity of a network or a host scanning for attacks or malicious acitvity, the difference between them is that IDPS can actively block and prevent intrusions which it detects, IDPS can drop malicious internet packets, block traffic from a certain IP address or to a certain host, server, application or any targeted resource, it can also detect reconnaissance activity like port and host scans which indecates a potential future attack.

1.4 Evolutions of IDS: IPS/IDPS

The main drawback of an IDS is its inability to perform a response for the attack and actively prevent malicious activity. Because of that, a new system was developed to remove those vulnerabilities, and called IDPS, even though IDPS is similar to IDS when monitoring the network or host for the presence of attacks or malicious activity, it is different from IDS as it can be used to prevent such intrusion automatically, for example it can drop malicious packets from the internet, block or ban the IP address or the suspected traffic to the host, server or application, etc, Additionally, it is also able to recognise reconnaissance, such as port and host scans, which would suggest a future possible attack. **?**

1.5 IPS/IDPS classification

Just like IDS, IDPS is classified based on two criteria, including their deployment and detection methods as shown in Figure 1.5 are:

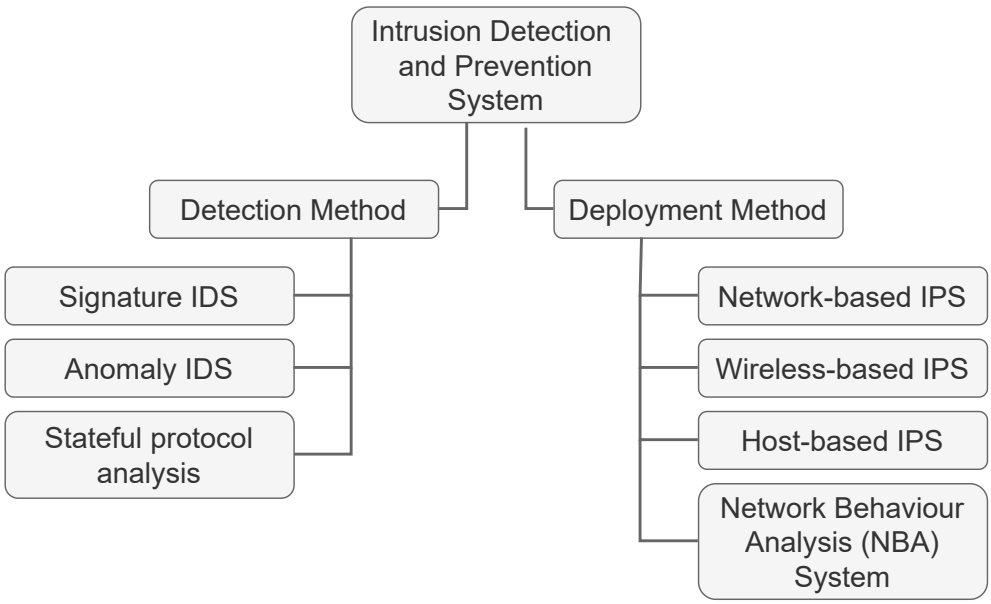

Figure 1.5: IDPS classification taxonomy

1.5.1 Deployment methods

1.5.1.1 Network-based Prevention System (NIPS)

A network-based prevention system (NIPS) is a network-based intrusion prevention system. It checks all internet packets inbound and outbound in a network, making it possible to detect suspicious activity. these monitoring devices are placed at a strategic point right at the start of a sub-network, usually being right behind the firewall. NIPS might also be placed within the network to watch over movement of data from important assets such as critical data centers or any other device. **?**

1.5.1.2 Wireless-based Prevention System (WIPS)

A wireless intrusion prevention system (WIPS) is designed to monitor wireless network protocols for any signs of suspicious activity, like unauthorized users or devices connected to the the wifi in question. Once a WIPS notices that an unknown entity has connected to a wireless network, it can automatically cut the connection. A WIPS can also be utilized to recognize misconfigured and unsecure devices operating on a wifi network, and set up even to intercept man-in-the-middle attacks.**?**

1.5.1.3 Host-based Prevention System (HIPS)

A host-based intrusion prevention system (HIPS) is installed in a particular device such as a laptop or server and monitors only the traffic that comes and goes through it. HIPS are commonly paired up with NIPS to provide additional protection for critical assets. In addition, HIPS can stop malware from moving between devices on the same network, as may happen when ransomware is unleashed.**?**

1.5.1.4 Network Behaviour Analysis (NBA) System

A network behavior analysis (NBA) is a type of IPS that monitors the packets of a network, but unlike other types of IPS, this one focuses on high-level details like source/distonation IP addresses, ports, and the number of packets transmitted by those IP addresses. It uses an anomaly-based detection method that is effective in detecting and blocking abnormal behavior like DDoS attacks and communications with malware-infected devices.**?**

1.5.2 detection methods

detection methods are the same in IPS as in IDS with stateful protocol analysis beign exclusive to IDPS, IDPS usually uses multiple detection methodes at the same time to broaden it's detection rates. **?**

IDPS has 3 primary detection methodes:

- Signature-based: Signature based detection is fairly similar to that of IDS with the difference beign that IDPS is capable of blocking or countring the detected intrusion
- Anomaly-based: the same thing applies to Anomaly-based detection as the detection phase is the same between IDS and IDPS
- Stateful protocol analysis applies the technique of comparing observed user behavior with predefined profiles that define what is regarded as normal activity. What sets it apart from anomaly-based detection is that stateful protocol analysis employs vendor-specific profiles which define normal behavior of a protocol. In this type of IPS, network, transport, and application layer protocol states will be tracked in order for the Intrusion Detection Prevention System (IDPS) to understand the state transitions. Consequently, when a user logs into an FTP session in an unauthenticated state, he can only execute basic commands such as viewing help information or providing login credentials. As a result, this allows the Intrusion Detection and Prevention System to differentiate between suspicious and benign actions by checking whether they conform to what is expected at that particular point or not after pair requests with responses and successfully authenticating. **?**

1.6 Machine learning based intrusion detection system

1.6.1 A general AI-based NIDS methodology

1.7 conclusion