LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 30B

**APPLICATION PROTOCOL-BASED INTRUSION DETECTION SYSTEM**

**TASK 30B:**

* Could you provide a detailed explanation of Application based intrusion detection system, along its functionalities and deployment contexts.

[](https://internationalsecurityjournal.com/types-of-intrusion-detection-system/)

As the number of cyberattacks and intrusions continue to rise, monitoring and securing your company’s network has never been more pressing.

In 2021 alone, the FBI’s Internet Crime Complaint Center (IC3) received [more than 800,000 complaints](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf) about data breaches, malware and more. These complaints totaled [nearly $7 billion](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf) in losses—and they only represent the *reported* cases.

An Application Protocol-based Intrusion Detection System (APIDS) is designed to monitor and analyze application-specific protocols to detect malicious activities. It operates at the application layer, typically deployed between a web server and an SQL database to detect SQL injections and other application-level threats. It can detect anomalies in the application traffic that may indicate an attack, such as SQL injection attempts, cross-site scripting (XSS) attacks, or other vulnerabilities specific to the application layer.

APIDS complements other security measures like firewalls and intrusion prevention systems (IPS) by focusing on the application layer, where many security threats often originate. By monitoring application protocols, APIDS can help identify and mitigate threats that might bypass other security measures.

At a basic level an APIDS would look for, and enforce, the correct (legal) use of the protocol.

However at a more advanced level the APIDS can learn, be taught or even reduce what is often an infinite protocol set, to an acceptable understanding of the [subset](https://en.wikipedia.org/wiki/Subset) of that application protocol that is used by the application being monitored/protected.

Thus, an APIDS, correctly configured, will allow an application to be "[fingerprinted](https://en.wikipedia.org/wiki/Fingerprint)", thus should that application be subverted or changed, so will the fingerprint change.

**Why are Intrusion Detection Systems Needed?**



Intrusion Detection Systems stand as indispensable components in the cybersecurity landscape, fulfilling critical roles that fortify the digital defense infrastructure.

Their necessity arises from their ability to detect potential threats in real-time and monitor network and system activities.

This real-time detection capability allows organizations to swiftly identify and respond to unauthorized activities, mitigating risks before they escalate.

Moreover, IDS contribute significantly to risk mitigation by providing prompt responses to potential intrusions.

Their ability to raise immediate alerts enables cybersecurity teams to take proactive measures, preventing or minimizing the impact of security breaches.

Additionally, IDS offer comprehensive insights into the nature and source of attacks, facilitating a deeper understanding of cybersecurity threats.

Although both Intrusion Detection Systems and Firewalls play integral roles in bolstering network security, their functionalities diverge.

A Firewall operates as a proactive barrier, managing incoming and outgoing network traffic according to predefined security rules.

This preventive measure aims to establish a secure perimeter by allowing or blocking data packets based on established criteria.

On the other hand, an Intrusion Detection System takes on a more vigilant role within the network security landscape.

Instead of solely focusing on traffic regulation, IDS actively monitors and detects potential threats within the network.

It serves as a reactive mechanism, providing real-time alerts and comprehensive insights into suspicious activities that may indicate unauthorized access or potential security breaches.

While Firewalls emphasize access control and traffic management, IDS prioritizes the identification and response to anomalies or malicious activities occurring within the network.

The world of cybersecurity relies heavily on Intrusion Detection Systems to safeguard digital assets and maintain the integrity of networks and systems.

Understanding the different types of Intrusion Detection Systems, and the critical role of IDS provides a foundation for creating robust defense mechanisms against the ever-evolving landscape of cyber threats.

With the continuous evolution of digital threats, the role of IDS remains pivotal in ensuring a secure and resilient cyberspace.