CS4404 Discussion Assignment 1

Network protocols could be classified into three broad groups: communication protocols, management protocols, and security protocols. In your opinion, which of these groups of protocols should be given the highest priority/consideration while designing a network? Justify your answer with detailed reasoning.

Your Discussion should be a minimum of 300 words in length.

Network protocols serve as the bedrock, establishing unified standards that enable diverse users to communicate effectively by adhering to a shared protocol. Striking a balance among communication, management, and security stands as a cornerstone in network design.

However, given the escalating cyber threats, prioritizing security protocols over other considerations appears justified. Security protocols encompass critical functionalities outlined in (Network Protocol Definition | Computer Protocol | Computer Networks | CompTIA, n.d.):

**Encryption:**

The encryption protocol necessitates users to input their credentials before accessing resources, acting as a fundamental defense against unauthorized access.

**Entity Authentication:**

This protocol empowers systems to mandate identity verification from devices and users before accessing secure areas, ensuring legitimate access.

**Transportation Security:**

Safeguarding data during transit from one point to another is a pivotal aspect of these protocols, shielding it from interception or tampering.

One prevalent example illustrating secured communication is SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), as detailed in (What Is SSL/TLS Encryption? | F5, n.d.). These encryption protocols fortify the exchange of sensitive data such as passwords, payments, and private personal information.

Here's a breakdown of its functioning over port 443, the HTTPS communication:

* The client initiates a request to the server through HTTPS.
* The server furnishes the client with its certificate and public key.
* Verification of these elements occurs by the client with a trusted root certificate authority (such as IdenTrust and DigiCert, as indicated in Usage Statistics and Market Share of SSL Certificate Authorities for Websites, November 2023, n.d.) to validate the certificate's legitimacy.
* A negotiation between the client and server ensues to establish the most robust encryption mutually supported.
* The client encrypts a session secret key using the server's public key and transmits it back to the server.
* Utilizing its private key, the server decrypts the client communication, establishing a secure session.

It's paramount to highlight that a well-designed network, lacking adequate security measures, remains vulnerable to data breaches and service disruptions. Such vulnerabilities pose significant risks and potential losses to organizations relying on such a network."

**Reference**

*Network Protocol Definition | Computer Protocol | Computer Networks | CompTIA*. (n.d.). Retrieved November 19, 2023, from https://www.comptia.org/content/guides/what-is-a-network-protocol

*Usage Statistics and Market Share of SSL Certificate Authorities for Websites, November 2023*. (n.d.). Retrieved November 19, 2023, from https://w3techs.com/technologies/overview/ssl\_certificate

*What is SSL/TLS Encryption? | F5*. (n.d.). Retrieved November 19, 2023, from https://www.f5.com/glossary/ssl-tls-encryption