# Connection Security in Modern Computing

An Overview of Techniques, Protocols, and Best Practices

Presented By: Devin Young

# Overview of Connection Security

- Connection security is the implementation of specific practices and protocols that are designed to protect communication across networks from threat actors looking to gain unauthorized access, tamper with, or intercept data

Connection security is significant because:

- Businesses heavily rely on digital communication, which means that security measures must be in place to protect the confidentiality, integrity, and availability of data involved with that communication
- Key in preventing cybersecurity attacks and ensuring regulatory compliance

# Threats and Vulnerabilities Associated with Insecure Connections

Threats:

- Man-in-the-Middle Attacks
- Eavesdropping
- Denial of Service Attacks
- Session Hijacking
- Cross-site scripting

Vulnerabilities:

- Weak Authentication/Authorization Checks
- Lack of Encryption
- Lack of Certificate Validation


(GeeksforGeeks, 2025a)

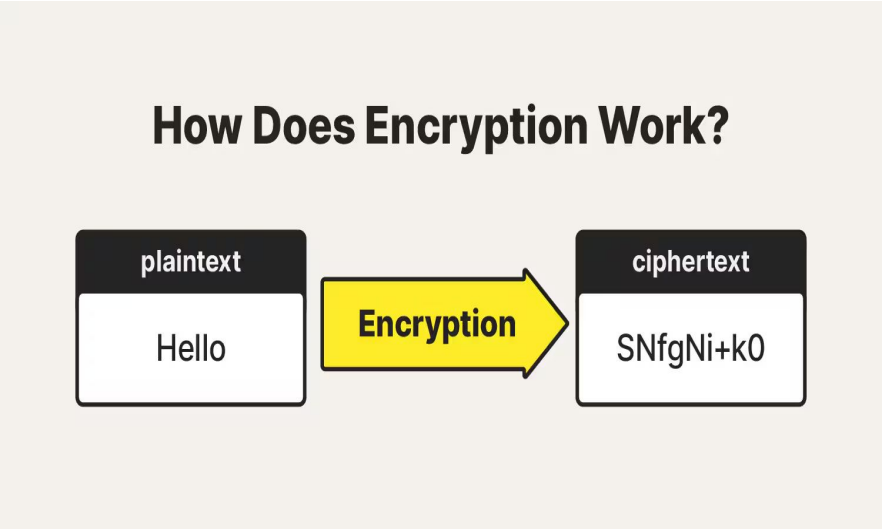
# Examples of Security Breaches Due to Compromised Connections

- National Public Data Breach (2024) - An unencrypted database with data involving 2.9 billion U.S. citizens was compromised by a cyber criminal group called USDoD (National Public Data Breach Publishes Private Data of 2.9B U.S. Citizens, 2024)

- Capital One Data Breach (2019) - The threat actor behind the data breach “exploited a configuration vulnerability in Amazon Web Services (AWS) storage buckets to gain unauthorized access to personal information of credit card customers and applicants” (What Happened in the Capital One Data Breach? | Twingate, n.d.)

- Microsoft Data Leak (2024) - The “Misconfiguration of an endpoint caused a leakage of 2.4 TB of data of Microsoft’s customers” (Firch, 2022)

# Encryption




(Stouffer, 2024)

- Transforms readable data into an unreadable format called ciphertext, to ensure that only those who are authorized to access it can decipher it
- Plays a significant role in connection security by masking various aspects of the communication between networks with locks that can only be opened with specific keys
- In addition, key management is extremely important in ensuring secure communication because if keys aren't stored, distributed, and rotated securely, unauthorized decryption can occur

# Asymmetric vs Symmetric Encryption Algorithms

**Symmetric Encryption**

- Only requires a single key for both encryption and decryption (GeeksforGeeks, 2025)
- Encryption process is fast (GeeksforGeeks, 2025)
- Keys are typically 128 or 256 bits long (GeeksforGeeks, 2025)
- Used for handling a large amount of data (GeeksforGeeks, 2025)

**Asymmetric Encryption**

- Requires a public key and private key, with one being used for encryption and one being used for decryption (GeeksforGeeks, 2025)
- Encryption process is slow (GeeksforGeeks, 2025)
- Keys are 2058 bits long or higher (GeeksforGeeks, 2025)
- Used for handling small amounts of data (GeeksforGeeks, 2025)

# Secure Network Protocols

- **IPsec Protocol (Layer 3) -** Protocol and algorithm suite that encrypts and authenticates packets of data that move across public networks (Cato Networks, 2024)

- **SSL/TLS Protocol (Layer 5)** - Encrypts data with algorithms similar to clients and servers in a client-server architecture, authenticates data origins, and ensures message integrity (Cato Networks, 2024)

- **SNMP (Layer 7) -** Network device management and monitoring protocol that uses a shared language for devices to communicate with one another via a network management system, featuring packet encryption, integrity checks, and authentication checks (Cato Networks, 2024)

- **HTTPS (Layer 7)** - Secures communication sessions between browsers and websites (Cato Networks, 2024)

- **SSH** - Transfers encrypted data over an unsecured network, acting as a cryptographic network protocol (GeeksforGeeks, 2024b)

# Secure Network Protocols: Strengths and Weaknesses

## Strengths

- IPsec - Highly flexible, supports VPNs
- SSL/TLS - Strong encryption, well-established standard
- SSH - Strong encryption, public key cryptography
- HTTPS - Relies on authentication, ensures data integrity
- SNMP - Centralized management, scalable, efficient for basic monitoring

## Weaknesses

- IPsec - Complex configuration
- SSL/TLS - Outdated versions are vulnerable, as well as weak cipher suites
- SSH - Vulnerable if passwords are weak or poorly configured keys are used
- HTTPS - Managing digital certificates can become complex, and encryption/decryption process can add latency
- SNMP - Earlier versions lack encryption, not able to transfer large amounts of data, basic error handling capabilities

# Scenarios where Specific Protocols are Preferred

- **IPsec Protocol (Layer 3)** - Preferred when there is an extreme need for encryption, integrity checks, and authentication of packets (used for securing entire network communications; such as site-to-site VPNs and mobile device security)

- **SSL/TLS Protocol (Layer 5)** - Preferred for securing client and server applications (ideal when encrypted data transmission and authentication are required between two applications or devices, such as a web server needing to ensure a secure communication with a web browser

- **SNMP (Layer 7)** - Preferred when the management of network devices requires authentication, encryption of data, and protection against unauthorized access (network administrators can use this to monitor the health of network devices)

- **HTTPS (Layer 7)** - Preferred and essential in scenarios where secure web browsing or data transmission through web interfaces is required (essential for E-Commerce transactions and online communications)

- **SSH** - Preferred and is always the go-to when the need for encrypted remote command-line access and secure data transfer over insecure networks is necessary (such as when a network administrator needs to access a remote server to configure settings)

# Best Practices for Implementing Connection Security

**Securing Web Applications:**

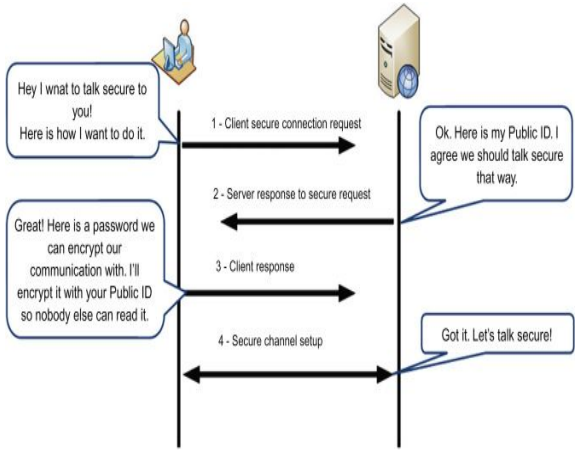
- Use HTTPS (ensures all web traffic is encrypted with SSL/TLS and protects against man-in-the-middle attacks
- Implement secure cookies
- Restrict the sources of executable scripts (content security policy)
- Regularly scan for vulnerabilities using automated tools
- Enforce two-factor authentication

**Securing Enterprise Networks:**

- Use IPsec or SSL VPNs for remote access to an internal network
- Create subnets to segment a network to prevent initial access and minimize lateral movement if a threat actor infiltrates it
- Deploy firewalls and access control lists to control incoming and outgoing traffic and ensure that all traffic within the network is authorized
- Implement IDS and IPS to detect and block suspicious activity such as port scanning and exploit attempts
- Encrypt data in transit and at rest (such as AES and IPsec)
- Regularly patch all network devices to ensure they receive the latest security patches

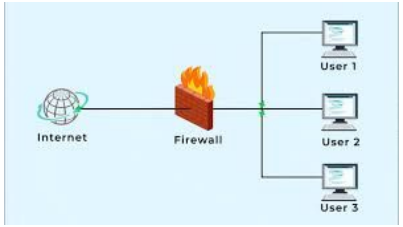
**Securing IOT Devices:**

- Use SSL/TLS for secure communication between IOT devices and cloud services, encrypt data in transit and at rest, and segment the network
- Require two-factor authentication
- Regularly update device firmware, use secure boot and integrity checks
- Disable unnecessary features




(Secure Connection, 2025)

# Roles of Firewalls, IDS/IPS, and etc. in Connection Security




(Hardware Firewall - An Overview, 2023)

**Firewalls:**

- Allow or block traffic based on predefined security rules or policies (Daniel & Daniel, 2023)

**Network-level firewalls filter traffic at the network layer, and include:**

- Packet filtering firewalls, stateful inspection firewalls, and next generation firewalls (Daniel & Daniel, 2023)

**Web application firewalls:**

- Protect web applications from attacks such as SQL injection, cross-site scripting, DDOS, as well as filter and monitor HTTP traffic (Daniel & Daniel, 2023)

**IDS/IPS:**

- Intrusion detection systems automatically alert cybersecurity professionals about potential intrusions, while intrusion prevention systems automatically block malicious traffic and quarantine compromised devices (Daniel & Daniel, 2023)
- At the network level, IDS/IPS monitors inbound and outbound traffic to detect known attack patterns, even if the signature is unknown (Daniel & Daniel, 2023)

**Other Security Tools:**

- Antivirus and antimalware software (endpoint security) ensure that malicious software doesn't compromise secure connections (Daniel & Daniel, 2023)
- Public key infrastructure allows the use of digital certificates and asymmetric encryption (Daniel & Daniel, 2023)

# Guidelines for Configuring Secure Connections Using Selected Protocols

1. Configure **firewalls** to strengthen internal and external network defense by controlling incoming and outgoing traffic
2. Implement appropriate **authentication and access control mechanisms** such as two factor authentication, role-based access control, and enforcing the creation of strong complex passwords
3. Set up SSL or IPsec **VPNs** to allow employees to access the internal network remotely in a secure way, while establishing encrypted tunnels to prevent unauthorized access into the internal network
4. Configure selected **IDS and IPS** to monitor and block various cybersecurity attacks, which includes the monitoring of network protocols and network security protocols being used
5. Create **subnets** to isolate systems and make it more difficult for threat actors to laterally move across the network
6. Implement up-to-date **encryption protocols** such as SSL/TLS for web traffic
7. Update **antivirus** and **antimalware software**
8. Regularly **patch** network devices
9. Configure **logging** and monitoring mechanisms with SIEMS, etc. to monitor network activity
10. **Train** employees and spread security awareness throughout the company

# Emerging Trends and Technologies

Quantum Cryptography:

- With quantum computers being able to break traditional algorithms by solving mathematical problems that are used to currently used to secure network enterprise infrastructures, another form of cryptography specifically created to defend against the use of quantum computers for malicious intent is on the rise

Blockchain Technology:

- Can enhance security by enabling tamper-resistant interactions between parties without relying on centralized authorities regarding communication protocols, identity management, and transaction validation, which is emerging because it reduces the need for third party intervention

Network Security Protocols

- New network security protocols will be an emerging trend because network security protocols strengthen the security for digital communication, and it is important to constantly improve network security protocols to provide the best security for devices that communicate across networks

# Bibliography


Cato Networks. (2024, February 18). 6 Network security Protocols you should know | Cato Networks.

https://www.catonetworks.com/network-security/network-security-protocols/

Daniel, & Daniel. (2023, October 18). Understanding network Security Protocols: your essential guide. CERTAURI.

https://www.certauri.com/understanding-network-security-protocols-your-essential-guide/

Firch, J. (2022, October 26). 2.4 TB data leak caused by Microsoft's misconfiguration. PurpleSec.

https://purplesec.us/breach-report/microsoft-data-leak/

GeeksforGeeks. (2025, February 5). Difference between symmetric and asymmetric key encryption.

GeeksforGeeks.

https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

GeeksforGeeks. (2025a, January 10). Top 10 cybersecurity threats in 2025. GeeksforGeeks.

https://www.geeksforgeeks.org/cybersecurity-threats/

# Bibliography


GeeksforGeeks. (2024b, October 18). What are SSH Keys? GeeksforGeeks.

https://www.geeksforgeeks.org/introduction-to-ssh-secure-shell-keys/

Hardware Firewall - An Overview. MilesWeb. (2023, September 22).

https://www.milesweb.com/blog/website-security/hardware-firewall-an-overview/

How to configure network security protocols? (2025, January 27). Ubuntu Ask.

https://ubuntuask.com/blog/how-to-configure-network-security-protocols

National Public Data breach publishes private data of 2.9B U.S. citizens. (2024,

August 19). Security Intelligence.

https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/

Secure Connection. ScienceDirect. (n.d.-b). https://www.sciencedirect.com/topics/computer-science/secure-connection

Stouffer, C. (2024, June 30). What is encryption? How it works + types of encryption.

https://us.norton.com/blog/privacy/what-is-encryption

What happened in the Capital One data breach? | Twingate. (n.d.).

https://www.twingate.com/blog/tips/capital-one-data-breach