Information Security Research #2

Delgerekh Ariunbileg

November 19, 2025

1 Topics

1.1 Humans are said to be the weakest link in any security system. Give an example for each, along with a brief justification for your response.

A situation in which human failure could lead to a compromise of encrypted data. Social engineering is a common attack method used by threat actors to exploit human weakness and insufficient cybersecurity training. In a hypothetical scenario, threat actors may develop a sophisticated spear phishing email targeted at an employee within a given organization. Prior to launching the attack, they would likely conduct reconnaissance to gather publicly available information about the target, including the people they work with, tools/applications used in the workplace, or frequently visited cafes and public work places.

Once they have gathered enough information, these threat actors can launch their sophisticated attack. They may spoof an email address to impersonate a trusted colleague, manager, or contractor, often using language urging to take immediate action. Spearphishing attacks are notoriously effective attack methods, accounting for 66% of successful breaches [5].

With inadequate email filtering and comprehensive spear fishing detection training, employees may unintentionally share encrypted files with threat actors. While encryption ensures data protection during transit and at rest, human weakness can lead to failure to follow security protocols, which can undermine confidentiality of organizational information.

A situation in which human failure could lead to a compromise of identification and authentication. In this day and age, passwords need to be complex and unique to resist brute force attacks. However, a source of human error originates from the reuse of passwords across personal and workplace accounts. Humans tend to prefer convenience over security, therefore they will often choose easily memorizable passwords rather than devoting themselves to strong password policies. If an organization lacks the strict implementation of complex passwords, employees are likely to engage in such risky behavior [13].

Some common human error prone password creation behaviors include the avoidance of special characters and/or the incorporation of personal information, such as the names of family members, significant dates or years, or favorite sports teams [10][12]. Once personal credentials are compromised, threat actors could utilize them to gain unauthorized access to organizational networks through company email domains.

A situation in which human failure could lead to a compromise of access control. Physical access control exploits due to human failure are often overlooked. Piggybacking or tailgating is a common technique that attackers could use to gain access to an organization's physical premise and assets [2]. Human failure is illustrated when an employee allows an individual to follow them inside a facility without authorization of a proxy card. This vulnerability stems from human inability to hold others accountable or reluctance to challenge another person.

Once the threat actors have gained unauthorized access, they can easily gather devices or other assets from what appears to be a secure environment [2].

1.2 List one security issue dealt with at each level of the OSI protocol stack.

Physical Layer The physical layer oversees the transmission and receival of raw data over physical media such as cables and wires. Security threats at this level can involve direct interference with the network's hardware [3]. For example, threat actors may cut or split cables to cause a DoS attack, which disrupts connectivity and prevents access for legitimate users. In addition, packet sniffing can occur commonly at this layer, with the attacker intercepting data across the network to capture sensitive information [11].

Data Link Layer This data link layer is responsible for ensuring that data transfer occurs between two connected nodes over the network. The layer manages error detection and ensures to check for proper data formatting and control of the flow [3]. A security consideration at this layer includes spoofing, which can be manifested as a Man in the Middle Attack, where an attacker pretends to be on both sides of a communication avenue, intercepting and manipulating traffic [9]. These attackers could also hijack the session, allowing them to impersonate a legitimate user and steal information or perform unauthorized actions.

Network Layer The network layer is primarily responsible for planning how data packets are routed across the network, in the most efficient method possible [3]. A possible security threat could involve a DDoS attack, where a router is overwhelmed with a surmount of false requests, making it obsolete to accept real requests and disrupting network availability [9].

Transport Layer The transport layer ensures that packets are reliably transmitted in the correct order. The layer is also responsible for segmenting the data to be reassembled later [3]. At this layer, SYN flood attacks, which is a type of DDoS attack, exploit the lack of acknowledgement within a TCP handshake [11]. A flood of these half-opened sessions can utilize resources, possibly causing a network crash or preventing legitimate users from accessing the network.

Session Layer The session layer ensures that a connection between a local and remote device is faultlessly established, maintained, and terminated. Additionally, this layer is responsible for creating checkpoints during the transmission of data, which creates synchronization and recovery in the case of interruptions [3]. A common security threat can involve a Man in the Middle Attack, where an attacker intercepts the session to eavesdrop and steal information [9]. The threat actor could even manipulate data being exchanged between the devices.

Presentation Layer The presentation layer converts data into a universal format that applications can interpret, making sure to handle tasks such as character translation and data compression. The layer also manages encryption and decryption to ensure the confidentiality and integrity of data [9]. This layer faces considerable risk from Secure Sockets Layer (SSL) hijacking, in which an attacker creates an illegitimate certificate for a legitimate site frequently visited by the user [6]. The user assumes they have a trusted and secure connection, when in reality they are connected to a proxy site. This ultimately compromises data security by allowing access to sensitive information.

Application Layer The application layer is perhaps the most vulnerable, as it directly provides services and interactions for the end user. These actions can range anywhere from mail services to file transfers, ensuring that applications can communicate with other applications [3]. There are many security considerations here, including various viruses, phishing attacks, and injection attacks, just to list a few [9]. Since this layer involves direct human-computer interaction, it faces significant risk from human errors and ill-intended exploitation, making security measures and ZTA essential.

1.3 Discuss the role of symmetric and asymmetric cryptography in securing modern communication systems. In your answer, explain how they differ in terms of key management, performance, and typical use cases. Provide one real-world example for each type.

Symmetric and asymmetric cryptography methods are both fundamental in protecting and securing digital information in this day and age. Both methods encrypt information, which is a process that scrambles data to protect access from those unauthorized to access the information. Encryption enables security by keeping information a secret, either the key itself or the methodology used to generate the key, ultimately ensuring confidentiality and integrity of data.

Symmetric cryptography relies on the use of a single key for both encryption and decryption, which requires the sharing of the key prior to the exchange. Key management for symmetric cryptography requires a secure channel for the exchange of keys, and a scaling error occurs for a large number of users. On the plus side, symmetric encryption algorithms require much less computation power which makes them faster to run and optimal for organizations hoping to utilize this method to scramble large amounts of data. Some common symmetric algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES) [4].

In real life applications, symmetric cryptography is ideal when speed is an organization's priority over utmost security [8]. For example, symmetric cryptography usage is ideal for firms within the financial sector, since they must protect sensitive client data during transactions. Their priority is to protect large amounts of data from cyberattacks, particularly exfiltration [7]. All in all, symmetric cryptography offers efficiency and speed.

Contrastingly, asymmetric encryption relies on a set of private and public keys. A public key is openly shared, allowing the messenger to encrypt using that key [1]. The recipient can then only decrypt that message by using a private key. Asymmetric cryptography does not require a secure channel for the exchange of keys but does require the existence of a public key infrastructure (PKI) in order to authenticate public keys. However, the upkeep of PKIs increases complexity and requires more computational resources, making asymmetric encryption slower and less ideal for encrypting large amounts of data. Some common asymmetric algorithms include RSA and Elliptic Curve Cryptography (ECC).

Asymmetric cryptography is the preferred method when security is scrutinized and speed is not a top priority [8]. Asymmetric cryptography is used within blockchain technology, where it is crucial to confirm the identity of cryptocurrency owners in order to securely handle transactions. Security is of the utmost importance, which ensures data authenticity and prevents interference [7].

[1] Badman, Annie, and Matthew Kosinski. "What is Asymmetric Encryption?" *www.IBM.com*, www.ibm.com/think/topics/asymmetric-encryption.

[2] Benecki, Nancy. "'Piggybacking' can open doors to security problems." *www.dla.mil*, www.dla.mil/About-DLA/News/News-Article-View/Article/3559637/piggybacking-can-open-doors-to-security-problems/.

[3] FORTRA. "An overview of the OSI model and its security threats." *www.tripwire.com*, www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats.

[4] IBM. "What Is Symmetric Encryption?" *www.IBM.com*, www.ibm.com/think/topics/symmetric-encryption.

[5] ---. "What is Spear Phishing?" *www.IBM.com*, www.ibm.com/think/topics/spear-phishing.

[6] Invicti. "SSL Hijacking." *www.invicti.com*, 31 Oct. 2025, www.invicti.com/learn/mitm-ssl-hijacking.

[7] KeyFactor. "When to Use Symmetric Encryption vs. Asymmetric Encryption." *www.keyfactor.com*, www.keyfactor.com/blog/symmetric-vs-asymmetric-encryption/.

[8] The Law.Institute. "Comparing Symmetric-Key and Asymmetric-Key Encryption Schemes." *thelaw.institute*, 20 Apr. 2025, https://thelaw.institute/cyberspace-technology-and-social-issues/symmetric-vs-asymmetric-key-encryption-comparison/

[9] McIlvenny, Joseph. "Radio-Frequency Attacks: Securing the OSI Stack." *www.sei.cmu.edu*, 20 Oct. 2025, www.sei.cmu.edu/blog/radio-frequency-attacks-securing-the-osi-stack/.

[10] NordPass. "Top 200 Most Common Passwords." *www.nordpass.com*, nordpass.com/most-common-passwords-list/.

[11] Stackscale. "OSI Model: 7 Layers & Common Security Attacks." *www.Stackscale.com*, www.stackscale.com/blog/osi-model/.

[12] Trevino, Aranza. "Eight Common Password Mistakes." *Keeper Security Blog - Cybersecurity News & Product Updates*, 7 July 2025, www.keepersecurity.com/blog/2022/10/25/8-most-common-password-mistakes/.

[13] White, Marcus. "Password Reuse: A Hidden Danger You Can't Ignore." *Specops Software*, 18 Mar. 2025, specopssoft.com/blog/password-reuse-hidden-danger/.