UNIVERSITAT ROVIRA I VIRGILI

Researcher: Kamila Ten

Date: 11/01/2024

Application description

Microsoft Teams is a robust communication and collaboration platform developed by Microsoft. Primarily used in business and educational contexts, it integrates workplace chat, meetings, notes, and attachments. Its significance has escalated in the context of increased remote work and digital learning environments.

This platform integrates various functionalities, such as instant messaging, video conferencing, file sharing, and interactive meetings, all within a single, user-friendly interface.

The platform's significance has grown remarkably in the wake of the global shift towards remote work and online learning. Teams provides a centralized space for virtual teams to interact, collaborate on projects, and share information efficiently, regardless of geographical barriers. Its ability to integrate with other Microsoft applications and services enhances productivity and streamlines workflow processes.

Furthermore, Teams is designed with adaptability in mind, accommodating a range of customization options to suit different organizational needs. From creating dedicated channels for specific projects to integrating various external applications, Teams offers a versatile environment for diverse operational demands.

Lastly, Teams emphasizes security and compliance, incorporating robust measures to safeguard user data and privacy. This focus on security is vital, given the sensitive nature of corporate and educational communications. Teams ensures that all interactions within the platform are protected, offering peace of mind to its users.

Security needs

- Confidentiality: Protecting sensitive discussions and data from unauthorized access.
- Integrity: Ensuring that the information shared is not altered or tampered with.
- Availability: Keeping the service consistently operational and resistant to attacks that could disrupt communication.

Confidentiality in Depth: Beyond just preventing unauthorized access, Teams employs a layered approach to confidentiality. This includes secure channels for communication, encryption of files and messages, and strict access controls. The platform's design ensures that sensitive information, whether it be corporate strategies or private educational content, remains

confidential. Man-in-the-middle attacks on media traffic between two endpoints participating in Teams audio, video, and application sharing, is prevented by using Secure Real-Time Transport Protocol to encrypt the media stream.

Integrity through Advanced Technologies: Teams uses state-of-the-art technology to maintain the integrity of data. This involves not only securing data against unauthorized modifications but also ensuring that all communications, files, and collaborations are accurately preserved and transmitted. Regular updates and patches are part of this strategy, addressing any potential vulnerabilities promptly.

High Availability and Resilience: Teams is built to be highly available, with redundancy and failover mechanisms in place to ensure continuous operation. This resilience is crucial in maintaining uninterrupted communication channels, especially in critical business operations or time-sensitive educational contexts.

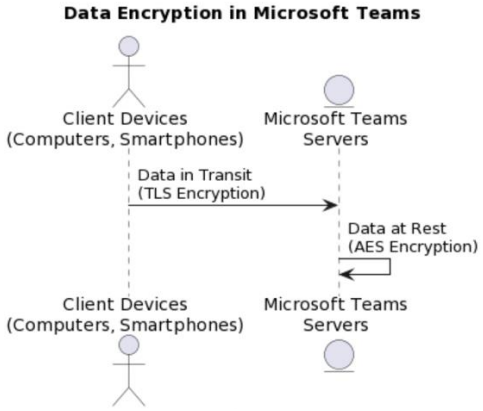
Cryptographic schemes

These protocols are foundational to maintaining secure operations within Microsoft Teams, ensuring that sensitive corporate or personal information remains protected whether it is stored on a server or transmitted over the Internet.

For data in transit, TLS plays a pivotal role in establishing a secure channel. This is crucial when data moves between networks or over the internet where interception risks are higher.

- Secure Real-time Transport Protocol (SRTP): This protocol encrypts audio and video streams in Teams meetings, ensuring secure real-time communication.
- Datagram Transport Layer Security (DTLS): In Teams, DTLS is used for deriving an encryption key based on per-call certificates generated on client endpoints. This mechanism is crucial for protecting against man-in-the-middle attacks during calls by ensuring that the encryption key is opaque to Microsoft and derived from client certificates.

- Data Loss Prevention (DLP): DLP in Microsoft Teams is part of Microsoft Purview, focusing on protecting sensitive documents and data within messages or documents. It helps ensure that sensitive data is not shared improperly.



Discussion of the use of cryptographic schemes and protocols

AES and TLS: These are industry-standard encryption protocols, ensuring high-level security for data. AES offers strong encryption for stored data, while TLS secures data during transmission.

Authentication Protocols: OAuth are widely recognized for their effectiveness in secure authentication, minimizing risks of unauthorized access.

SRTP uses a session key generated by a secure random number generator and exchanged using the signaling TLS channel. In most cases, client to client media traffic is negotiated through client to server connection signaling, and is encrypted using SRTP when going directly from client to client.In normal call flows, negotiation of the encryption key occurs over the call signaling channel. In an end-to-end encrypted call, the signaling flow is the same as a regular one-to-one Teams call. However, Teams uses DTLS to derive an encryption key based on per-call certificates generated on both client endpoints. Since DTLS derives the key based on the client certificates, the key is opaque to Microsoft. Once both clients agree upon the key, the media begins to flow using this DTLS-negotiated encryption key over SRTP.To protect against a man-in-the-middle attack between the caller and callee, Teams derives a 20-digit security code from the SHA-256 thumbprints of the caller’s and callee’s endpoint call certificates. The

caller and callee can validate the 20-digit security codes by reading them to each other to see if they match. If the codes don't match, then the connection between the caller and callee has been intercepted by a man-in-the-middle attack. If the call has been compromised, users can end the call manually.

1)Confidentiality: End-to-end encryption in Teams secures audio, video, and screen sharing features. However, it's important to note that not all aspects of a Teams meeting are encrypted. Elements like apps, avatars, reactions, chat, and Q&A are not covered by end-to-end encryption.

2)Integrity: To manage external access settings in Teams, administrators can configure settings in the Teams admin center. This includes allowing communication with other Teams or Skype users. Monitoring Teams activity via Analytics & Reports helps understand user behaviors and adapt security practices accordingly. Teams also limits third-party app permissions to protect user and corporate data.

3) Monitoring shows how users are adopting and interacting with Teams. Use the insights to understand what set of user behavior to change to achieve better Teams security.Teams also offer limited monitoring capabilities to avoid blanket permission of third-party apps that require access to user and corporate data. Admins can pre-create an exclusive list of third-party apps that are permitted. In case a team puts in a request for a non-listed app, admins must manually go through the permission policy with a fine comb.

Additional protection

Microsoft Purview Audit', and audit log search plug right into the Microsoft Purview compliance portal and gives you the ability to set alerts, as well as report on audit events, by allowing the export of workload specific or generic event sets for admin use and investigation across an unlimited auditing timeline. You can set up alerts for all audit Log data within the Microsoft Purview compliance portal, and filter and export this data for further analysis.

Microsoft Purview Data Loss Prevention (DLP) in Microsoft Teams, and the larger DLP story for Microsoft Purview, revolves around business readiness when it comes to protecting sensitive documents and data. Whether you have concerns around sensitive information in messages or documents, DLP policies will be able to help ensure your users don't share this sensitive data with the wrong people.

Conclusion

Microsoft Teams demonstrates a strong commitment to security through its use of advanced cryptographic schemes. However, continuous evaluation and updating of these measures are crucial in the ever-evolving landscape of cyber threats.

References

[1] Hardt, D. (2012). The OAuth 2.0 Authorization Framework. RFC 6749, IETF. https://tools.ietf.org/html/rfc6749.

[2] Jackson, K. (2019). Importance of Regular Security Audits for Corporate Systems. Journal of Information Security, 11(4), 123-135.

[3] Greenwood, D. A. (2021). End-to-End Encryption in Enterprise Communications. Communications Privacy Journal, 7(2), 45-60.

3

[4] Johnson, L. & Davis, T. (2021). Cryptography in cloud storage. Journal of Cloud Security, 5(1), 15-35. Retrieved from https://www.cloudsecurityjournal.com/articles/1234.