KOMPUTIKA

NEWSLETTER

October 2024
Issue #2

Striking the Balance: Secure Networks and Privacy.

INSIDE

—

TAG
[Opinion]
[NGFW] [Research]
[Network Security]
[Cyber Security]

—

AFFLIATION

Senior Lecturer
Professor

—

Department of
Computer Systems and
Technology

Is Privacy the Price We Pay for Stronger Security?

– By Faiz Zaki, Nor Badrul Anuar

As modern organizations increasingly rely on networked applications, the demand for security visibility has never been greater. Detecting and responding to sophisticated cyber threats requires deep insight into network traffic, making techniques like network traffic classification essential. However, this heightened visibility often comes at the expense of user privacy, risking exposure of private communications and sensitive information. Hence, the challenge lies in balancing the need for robust network security with the preservation of individual privacy, while navigating the technical complexities and legal constraints associated with these practices.

Among common practices include Secure Socket Layer (SSL) decryption that has become a standard tool for gaining insight into encrypted traffic, which now constitutes most internet communication. Additionally, encryption is often exploited by attackers to obscure their payload in sophisticated attacks. As such, by decrypting SSL traffic, security systems can inspect data for potential threats and malware.

This process has become integral to Next-Generation Firewalls (NGFW), which are designed to go beyond traditional packet filtering to provide advanced security features like intrusion prevention, application awareness, and deeper content inspection. NGFWs leverage SSL decryption to analyze encrypted traffic and enforce security policies more effectively.

Now it begs the question.

If NGFW can decrypt our traffic for content inspection using SSL decryption, where is our privacy?Or does SSL decryption in NGFW presents another attack surface for attackers to target since data are now in plain sight?For that reason, more than 40% organizations forgo SSL decryption for concerns over privacy despite the justifiable benefits mentioned earlier. In essence, there are two key challenges with SSL decryption:

- *Data and user privacy*. How can we find the much-needed balance in ensuring privacy?
- *Performance and resource consumption*. Decryption consumes a lot of computational resources and causes performance degradation.

Therefore, researchers at the Center of Research for Cyber Security and Network (CSNET) are actively working on novel techniques to achieve visibility without compromising privacy. Among alternative include focusing on metadata and side-channel analysis rather than content decryption. Metadata, such as packet sizes, flow durations and traffic patterns can provide valuable insights into potential threats without requiring full access to the contents of network communications. The focus on side-channel information and metadata also addresses the resource-heavy nature of SSL decryption. By analyzing encrypted traffic without the need for decryption, organizations can reduce the computational burden on their systems, making it a more scalable and efficient solution. This approach complements NGFWs, allowing them to operate more efficiently by reducing the need for full traffic decryption while still offering effective threat detection capabilities.

In summary, the tension between network security and privacy is a growing concern in today's increasingly digital world. SSL decryption, while useful for gaining visibility into encrypted traffic, carries significant risks in terms of privacy violations and resource consumption. As privacy laws continue to evolve and user expectations for data protection rise, organizations must rethink their approaches to network security. Alternative strategies as mentioned earlier can strike a better balance between security and privacy, ensuring compliance with data protection regulations while maintaining robust network defenses. This shift toward privacy-preserving security practices promises to reshape how organizations approach the protection of their networks in the face of evolving cyber threats.