SMART GRID SECURITY

Security plus of TLS 1.3

TLS 1.3 vs 1.2 in the context of the increasing security requirements of smart grid energy systems

TLS introduction and applications

SECURE COMMUNICATION IS BECOMING INCREASINGLY IMPORTANT IN INDUSTRIAL NETWORKS DUE TO THE STEADY GROWTH OF VARIOUS ETHERNET PROTOCOLS AND IIOT APPLICATIONS. IN THE AREA OF CRITICAL INFRASTRUCTURES, SUCH AS ENERGY NETWORKS AND SMART GRID APPLICATIONS, SECURING COMMUNICATION IS ALSO A KEY ISSUE.

In order to guarantee confidentiality, authenticity and integrity during data transmission, more and more applications are using the TLS (Transport Layer Security) protocol, which originally became known in connection with the HTTP protocol. Since the introduction of the latest TLS version 1.3 in 2018, which has significant advantages in terms of security and performance compared to the previous version TLS 1.2, TLS 1.3 is increasingly supported in the industrial environment.
This white paper shows which changes and innovations have been made in TLS 1.3 compared to its predecessor TLS 1.2 in order to increase the security of the protocol and thereby illustrates why the migration to the latest version is necessary from a security point of view.

Why use TLS 1.3 instead of TLS 1.2?

- Elimination of insecure crypto algorithms and methods
- TLS 1.3 guarantees “Forward Secrecy”
- Addition of algorithms based on Elliptic Curve Cryptography (ECC)
- Cryptographically secured TLS Handshake
- Faster connection setup – less Roundtrips between Client and Server

New Features and changes of TLS 1.3

ELIMINATION OF OUTDATED ALGORITHMS AND CIPHERS

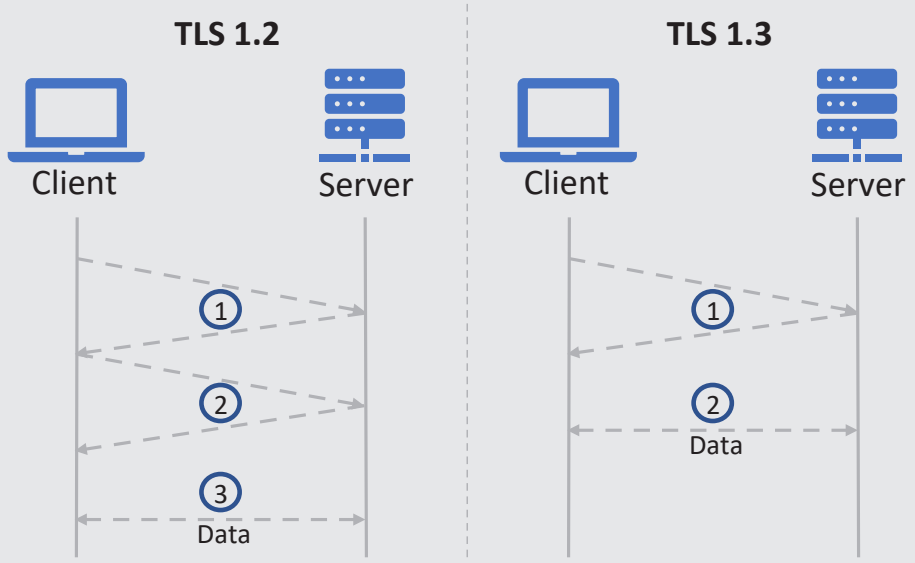
During the development of TLS version 1.3, all known security vulnerabilities of the previous version 1.2 were analyzed and all obsolete and insecure procedures were eliminated. Therefore, the key exchange mechanism based on RSA was removed and the Ephemeral Diffie-Hellmann key exchange was defined as mandatory. As a result, TLS 1.3 guarantees “forward secrecy” when exchanging the symmetric session key, because the shared session key is not transmitted over the network and is only valid for one session. Disclosure or recording of a long-term private key can therefore not lead to the calculation of past session keys and it’s not possible to decrypt a communication retrospectively.

With TLS, the actual data is encrypted using symmetric encryption methods. Therefore, either stream ciphers, which use a fixed-size key to generate a key stream that is then used for encryption, or block ciphers are used. A block cipher is designed for encrypting fixed-size messages and for the encryption of shorter messages, extra data needs to be added at the end of the message. TLS 1.3 forbids the use of the block cipher mode CBC, because this so-called padding was very often implemented incorrectly and thus man-in-the-middle attacks could be practiced. This made it possible for attackers to guess transmitted data, such as cookies or authentication data. However, not only block ciphers were eliminated but also the stream cipher RC4, as it is no longer considered secure after successful attacks in the past. Since it is not sufficient to protect only the confidentiality of the transmitted messages, but also the integrity must be guaranteed, the MAC-then Encrypt procedure was used for all older TLS versions including 1.2. This involves first applying a message authentication code (MAC) to the plaintext of the message and then encrypting everything.

This procedure has subsequently been shown to be a design flaw, as several attack methods have been discovered in the meantime. TLS 1.3 eliminates this problem since from this version on only AEAD ciphers (Authenticated Encryption with Associated Data) may be used. AEAD ciphers are more secure because the historically decoupled steps of authentication and encryption are combined in one single operation. In addition to the unsecure ciphers and cipher modes, the already broken hashing algorithms SHA1 and MD5 are also not part of the newest TLS version any longer.

Version	Published	Security
SSL 2.0	1995	Insecure, deprecated
SSL 2.0	1996	Insecure, deprecated
TLS 1.0	1999	Insecure, deprecated
TLS 1.1	2006	Insecure, deprecated
TLS 1.2	2008	Depends on cipher and client mitigations
TLS 1.3	2018	Secure

TLS protocol versions and security level



TLS 1.3 allows data transmission already at the second round-trip between client and server. This fast handshake during connection set-up leads to an increased performance compared to TLS 1.2.

ADDITION OF MORE SECURE METHODS

Compared to TLS 1.2, TLS 1.3 not only removes insecure and obsolete methods but also adds new features to increase security. For example, the TLS 1.3 specification includes algorithms based on elliptic curves. Since calculations based on elliptic curves are very difficult to calculate back, elliptic curve cryptography (ECC) is much more efficient than other methods based on the use of very large prime numbers. Procedures such as the Diffie-Hellmann key exchange, which is mandatory for TLS 1.3, can be applied to elliptic curves. This means that less computing power is required for the same level of security.

In addition, with TLS 1.3, the majority of the connection setup is encrypted and digitally signed. Therefore, it is no longer possible to find out the name of the server by listening to the handshake messages. Older TLS versions transmit the certificate in plaintext and because of that attackers are able to identify which server a client is connecting to. Besides, this innovation means that it is no longer possible for an attacker to use a man-in-the-middle to shorten the list of supported cryptographic methods exchanged between the client and server when establishing a connection to achieve a downgrade to an insecure method.

PERFORMANCE BOOST AND LESS LATENCY

One of the biggest advantages of TLS 1.3 compared to the previous versions is the increase in performance. This is achieved, among other things, by the fact that there are significantly fewer combinations of security parameters from which the cipher suite is formed. The cipher suite refers to the composition of the algorithms and mechanisms used to establish a secure TLS channel between client and server. Reducing the number of supported cipher suites and the resulting reduced complexity during

connection set-up enables a faster handshake. With TLS 1.3, for example, data is transmitted already at the second round-trip between server and client, whereas with TLS 1.2 data packets are not sent until the third round-trip. This significant improvement is also made possible by the fact that the client already makes assumptions about the procedures supported by the server when establishing the connection. Therefore, he already sends key material on suspicion in order to bypass a second roundtrip for the exchange of administrative information.

Another new feature concerns the performance increase during session resumption. By storing key material for later connections, it is possible to transmit data already in the first packet and thus enable zero-roundtrips (0-RTT) for the exchange of administrative information. The latency minimization this achieves can be particularly beneficial in IIoT and edge infrastructures. However, there are some limitations to 0-RTT mode, such as not changing the state on the server to minimize the risk of replay attacks.

Conclusion: TLS 1.3 – faster and more secure

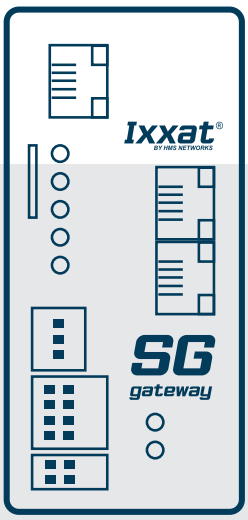
As we have seen, encrypted connections via TLS 1.3 are not only more secure but also faster than encrypting with TLS 1.2. Due to the many security advantages, the implementation of the latest protocol version is thus necessary from a security point of view.

CHOOSE A SOLUTION THAT SUPPORTS TLS 1.3

The setup of modern and networked smart grid applications requires multiple wireless and wired connections over a wide variety of Ethernet protocols. In order to make communication in energy networks secure, solutions and devices for this area should support TLS 1.3.

The Ixxat SG-gateways from HMS Industrial Networks therefore support TLS 1.3 for communication with the integrated web server, MQTT traffic and for applications in combination with OpenVPN.

Ixxat SG-gateway – Secure Smart Grid communication using TLS 1.3



Consistent data communication across all system levels with all devices is the backbone of the smart grid. The transparent connection of the control room, cloud, local controls, IEDs and sensors is a big task.
The Ixxat SG-gateways are valuable helpers to approach cross-system communication easily and securely.

Ixxat SG-gateways combine an impressive range of features in one small but easy to use, secure and robust device – being the perfect solution for digitalizing substations in power generation, distribution and usage.

- Unique combination of the relevant protocols in energy automation (IEC 61850, IEC 60870…), industrial systems (Modbus, EtherNet/IP…), sensors (Modbus, analog, WLAN) and IoT (MQTT, OPC-UA…).
- A small, safe, easily configurable and robust device: ideal for retrofitting!
- The on-board WEBPLC enables “edge computing”
- High data security: data transmission via TLS 1.3 and VPN, user management, protected configurations, encrypted and signed firmware.

www.ixxat.com/energy