NXP EdgeLock™ SE050

Use Case:
Wi-Fi Credential Protection

Adding a secure element to a device, gateway, or router that uses Wi-Fi for wireless connectivity simplifies network onboarding and protects the network from attack by using certificate-based authentication and government-grade encryption.

APPLICATIONS

Routers

Gateways

CHALLENGE

Throughout the Internet of Things (IoT), Wi-Fi technology based on the IEEE 802.11 standard is used to connect individual edge devices, such as eLocks or speakers, to gateways and routers, and to connect gateways and routers to broader networks and the cloud.

Wi-Fi connections already represent a significant portion of IoT connections, in residential and industrial applications that connect all kinds of devices to the network. What's more, the arrival of Wi-Fi 6, which offers significant improvements in performance and battery life, is expected to make Wi-Fi an even more prominent part of the IoT.

Broader adoption of IoT devices with Wi-Fi connections places pressure on device manufacturers to make deployment quick and simple, so end users experience a hassle-free installation. In particular, the process by which a new device gains access to the network, referred to as onboarding, needs to be as simple as possible.

Also, as the number of Wi-Fi connections grows, however, so do the security risks. That's because Wi-Fi connected devices are often targeted by hackers, looking for entry points to the network so they can do some kind of harm, whether it's mounting a DDoS attack, taking malicious control of other devices, or exposing private data.

There are several Wi-Fi protocols that can be used to protect IoT devices and the gateways and routers they connect to. One of the best approaches is defined by the Wi-Fi Alliance, the independent organization that runs a certification program based on industry-recognized best practices. Their approach uses the latest versions of Wi-Fi protected Access (WPA) and government-grade AES encryption, with support for certificate-based authentication using the Extensible Authentication Protocol (EAP).

PLUG&TRUST

NXP

The EAP-TLS framework is widely regarded as the most secure approach to authentication, since both sides of the transaction, the client and the server, use certificates, and the user- and session-based security keys can be dynamically generated to secure subsequent communications between the Wi-Fi client and the access point. For users who connect to and use a network service, Remote Authentication Dial-In User Service (RADIUS) is a common client-server networking protocol for Authentication, Authorization, and Accounting (AAA or Triple A) management.

Whichever combination of protocols the design uses, however, it's best to store the security keys in hardware. That's because silicon-based security provides a high level of protection and, as a result, minimizes risk when Wi-Fi devices connect to the network.

SOLUTION

The EdgeLock SE050 is a tamper-resistant platform designed for multiple IoT Security use cases based on strong protection of security keys and certificates. It also supports the latest WPA-EAP-TLS security protocols as well as cryptographic functions, such as HKDF, PBKDF2, and secure SCP channel protection.

The EdgeLock SE050 saves on development time because it comes with preinstalled security code and preconfigured with credentials, added during production or before shipment from a distributor. The preconfigured credentials provide the IoT device with an identity, which simplifies network onboarding and makes it more secure.

The credentials are used by the authentication process when the device connects to a Wi-Fi router and, as a result, help protect the network from unauthorized access.

Because the credentials never leave the IC, the chain of trust is preserved during the entire product lifecycle. The result is true end-to-end security based on a root of trust for devices that use Wi-Fi.

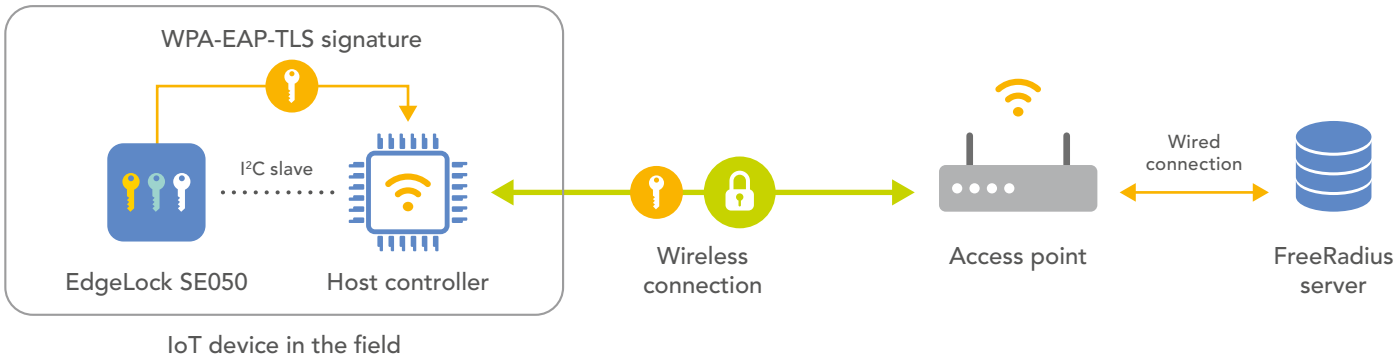
As shown in the block diagram, the EdgeLock SE050 provides the IoT device with a secure identity, which is then used for authentication whenever connecting to a Wi-Fi router. The EdgeLock SE050 connects to the host controller using an I²C slave interface. Connection to the Wi-Fi network is established by middleware, which uses the preconfigured credentials in the EdgeLock SE050 as part of authentication process.

LEARN MORE

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock SE050. The EdgeLock SE050 Product Page links to detailed specs, designs tools & software, training & support, and more.

- **NXP Design Community**
  https://community.nxp.com/community/identification-security/secure-authentication/overview
- **EdgeLock SE050 Product Page**
  www.nxp.com/SE050

BLOCK DIAGRAM



Find more information on **www.nxp.com/SE050**

Date of release: June 2020

PLUG &TRUST