Z-Wave SDK 6.71

INTRODUCING S2 SECURITY

Overview

- What is S2?
- New in protocol 6.71
- How to implement
  - New end devices
  - New gateways
  - Existing end devices
  - Existing gateways
- Migrating existing networks

What is security S2?

Why update security?

- Some shortcomings identified in S0
  - S0 was focused on access control devices
    - A secure network model for all device types is needed
  - S0 vulnerability during inclusion process
    - Narrow window of in-band unsecure transmission of encryption keys during inclusion
- Security more important in IoT than ever
  - More and more devices being connected
  - Flexible and secure IoT networks is a requirement for broader application of smart devices
- Implementing security must be easy
  - Z-Wave S2 protocol builds in the secure inclusion process and encrypted communication
  - Device manufacturers can focus on design and functional differentiation without having to worry about security

What is s2?

- Unique device specific key [DSK] for every secure device
  - Enables validation of device identity and prevents man-in-the-middle compromises to security
- Widely accepted secure cryptographic key exchange methods during inclusion
  - Proven and tested methods
- Out of band key exchange for product authentication
  - Combined with device specific key to prevent eavesdropping and man-in-the-middle attack vectors
- Multiple groups of secure devices
  - Allows segmentation of a network into different permissions and capabilities
  - Ensures flexibility in device design without compromising overall network security
  - Enables secure communication for all device types

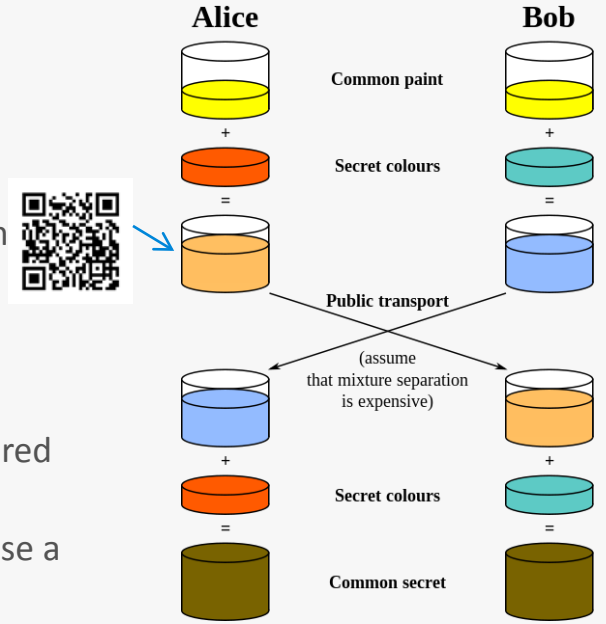
Device specific key

zws2dsk: 34028-23669-20938-46346-33746-07431-56821-14553

- Unique 40 digits key for each device
- Printed on the device
  - 40 digits representing 16 bytes
  - Optional QR code for easy reference
  - First two bytes (5 digits) of code underlined
    - Used for manual key entry if QR scanning is not used

cryptographic key exchange methods

- Elliptic Curve Diffie-Hellman (ECDH)
  - Elliptic curve cryptography (ECC)
    - Achieves high levels of cryptographic security with less computation power than for example RSA
  - Diffie-Hellman key exchange
    - Achieves shared secret between two parties without easy means of eavesdropping
    - Used to ensure both parties can trust origin of messages to come from other party
  - Z-Wave implementation
    - Uses the public ECDH keys only during inclusion for establishing of shared secret between controller and authenticated device
    - Public keys cannot be used to decrypt normal network traffic as that use a different set of keys



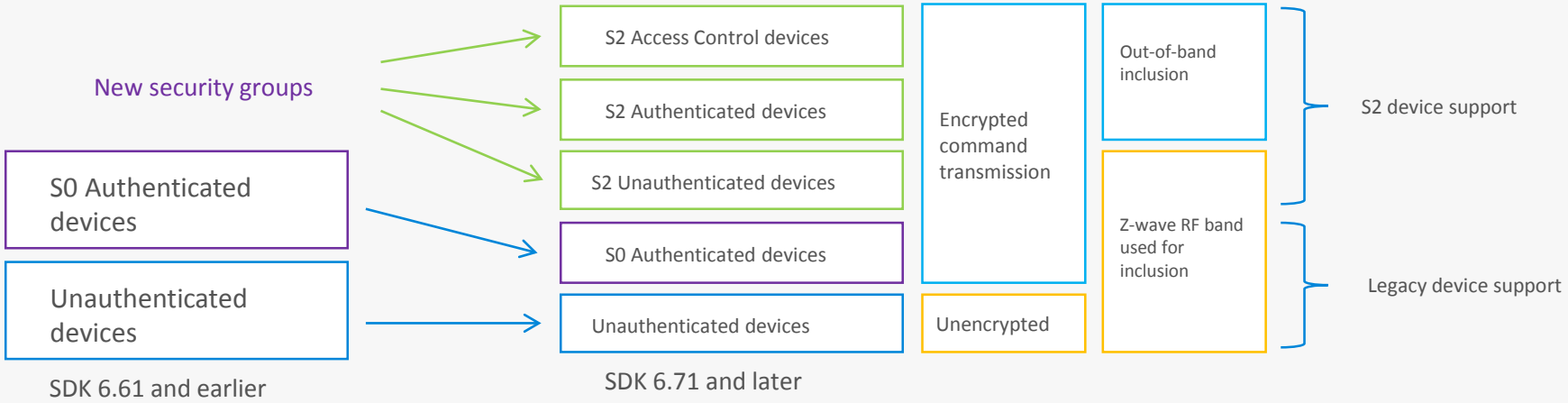
Out of band key exchange

- Removes possibility for man-in-the-middle impersonation of devices during inclusion
  - Used in S2-Authenticated and S2-AccessControl

- Visual Scan or manual entering of code in controller allows controller to validate that it is not communicating with an impersonating device
  - First 5 digits of the zws2dsk are obfuscated in the RF transmission (replaced with 0's)
  - User needs to enter the missing digits by reading them off the label (or scanning QR) to continue the inclusion process
  - The remaining digits is shown to the user in the gateway user interface. So that the user can confirm the identity of the device requesting the missing digits by comparing the full key.

Multiple Security groups

- Increased security through better compartmentalization of secure devices
  - Each device only knows the keys of the groups it is authorized as part of
  - Devices cannot control other devices' functions if they are not part of the same groups
  - Physical extraction of secure keys from a non-secure device is not possible – they are never in the memory of a device not authenticated for the secure groups
  - All encrypted command transmission use the same 128bit level of security but with a different shared key for each group
  - A device can be a member of multiple groups



What device types are in each group?

S2 Unauthenticated	S2 Authenticated	S2 Access Control
•Devices that have not implemented out of band inclusion methods •End devices that are physically exposed and/or not relevant to include in the authenticad group •End devices that need to be controlled by other S2 unauthenticated devices via associations	•All types of secure end devices including, but not limited to: •Door/Window sensors •Switches •Other sensors •Valves •Window blind motors •Etc. •Secondary controllers that does not need to control access control devices	•Door locks •Garage door openers •Controllers that need to control access control devices

- Device manufacturers not making access control devices should aim at including their devices in the **S2 Authenticated** group to maximize network security
  - The S2 Access Control group is not using more secure communication than S2 Authenticated. The improved security comes from segmenting the network so that access control devices are only accessible by controllers that need to control them
  - Devices in S2 Auhtenticated group cannot be controlled by devices in a lower security group. In some system setups it may be required to include end devices at lower authentication levels due to backwards compatibility reasons
- The S2 Unauthenticated group should be used as a fall-back if implementation of unique and visible ZWS2DSKs are not possible on the product, or if the device is of a type physically exposed to be compromised

Release overview

What’s new in 6.71

New Features - Protocol

The Z-Wave 500 Series SDK version 6.7x contains the following major enhancements compared to SDK version 6.6x:

- New improved second-generation security solution (S2 based on Security 2 Command Class) for a routing slave and an enhanced 232 slave with respect to authentication levels, initial key exchange, communication overhead, multicast support etc. However, the routing slave has dedicated implementation with optimized memory use because it is without an external NVM.

- Introduction of a new client side authentication enabling OTA firmware update from a S0 device to a S2 device. This method makes it possible to enter the QR code of a controller onto joining device (client side authentication). Specifically targeted door locks having a keypad.

- Introduction of a new Inclusion Controller Command Class allowing inclusion controller to inform the SIS that a new node has been added, and that the SIS will have to perform any additional required setup operation. Examples of such setup operations could be Z-Wave Plus Lifeline configuration or Security 2 bootstrapping.

- The Sensor PIR application is now based on a routing slave instead of an enhanced 232 slave.

- The enhanced 232 slave still supports applications having 128KB external NVM. This enables migration to SDK 6.7x based applications on existing products.

New features - Tools

- An improved Z-Wave Plus framework resulting in a simpler application development due to flexible NIF configuration, extended task and event handler, simpler command class handling, integrated multicast handling, integrated multichannel handling etc.
- The production test improved for a final product.
- Network key saved into zlf log file generated by Zniffer enabling support of customers developing security 2 applications.
- New Micro RF Link features such as the RxSweep writing output to a UART terminal for documentation of measurements.
- New Z-Wave PC Controller features such as inclusion controller support using SIS as thrust center for security 2 key exchange, client side authentication support, configuration of Application Priority Route (APR) and Z/IP Gateway client application.

New End devices

Implementation

New End devices

- With S2 Authenticated or Access Control inclusion
  - Create new firmware based on 6.71
  - Create production process with unique zwS2dsk and printed labels for each device
  - Select the appropriate security group for the device type
    - S2 – Access Control for door locks and other perimiter access device types
    - S2 – Authenticated for all other secure device types

- For use with S2-Unauthenticated inclusion
  - Create new firmware based on 6.71

New Controllers/gateway devices

Implementation

New controllers or gateways devices

- With support for all security groups
  - Create new firmware based on 6.71
  - Create production process with unique zwS2dsk and printed labels for each device
  - Ensure method for displaying zw2dsk in user interface
    - A new key will be generated each time the controller is included into a network for improved security
  - Implement method for the user to enter zws2dsks when including authenticated and access control end devices
  - Implement method for the user to use client-side authentication
    - To allow users to elevate OTA upgraded S0 devices to S2 should they support that functionality
  - Implement inclusion controller command class to improve user experience and security in networks with multiple controllers
  - Recommended: Ensure that the device can be firmware upgraded
    - To allow for future updates to be applied

- For use with S2-Unauthenticated inclusion
  - Not recommended
  - Create new firmware based on 6.71
  - Only usable for simple remotes
    - It will not be able to control any authenticated devices

Existing End devices

Implementation

Update existing end devices

- In-field OTA
  - Create new firmware based on 6.71
  - Update devices in field
  - Devices need to be re-included to join S2-Unauthenticated group
    - Default OTA behavior is to keep device in the group it was part of previously (S0 devices stay as S0, unauthenticated stay as unauthenticated)
  - Devices cannot join S2-Authenticated or S2-AccessControl groups unless they have keypads and can use client-side inclusion

- Production line update
  - Follow guidelines for new end devices

Existing Controllers/gateway devices

Implementation

Existing controllers or gateways devices

- With support for all security groups
  - Create new firmware based on 6.71
    - Frameworks will help get security set up correctly
  - Create production process with unique zwS2dsk and printed labels for each device
    - For new devices produced
  - Ensure method for displaying zw2dsk in user interface
    - A new key will be generated each time the controller is included into a network for improved security
    - This is particularly important if the device is not primary controller and used in a network where the primary controller is also updated
  - Implement method for the user to enter zws2dsks when including authenticated and access control end devices
  - Implement method for the user to use client-side authentication
    - To allow users to elevate OTA upgraded S0 devices to S2 should they support that functionality
  - Implement inclusion controller command class to improve user experience and security in networks with multiple controllers
  - Recommended: Ensure that the device can be firmware upgraded
    - To allow for future updates to be applied
  - Recommended: Implement method for user to be guided through re-inclusion of end devices that are also upgraded to support S2

- For use with S2-Unauthenticated inclusion
  - Not recommended
  - Create new firmware based on 6.71
    - Frameworks will help get security set up correctly
  - Only usable for simple remotes
    - It will not be able to control any authenticated devices

Migrating existing networks

Reasons to migrate end customers

- Make full use of new devices with S2 included
- Upgrade security of existing networks for security conscious customers
- Supervision Command Class
  - Continuous status on all SET commands, such as Door lock operation

Reasons not to migrate end customers

- Not all devices in the network can be upgraded

- No easy physical access to the network

Different upgrade paths

- Full upgrade
  - All devices are upgraded to firmware supporting S2
  - Requires re-inclusion of all devices
  - Upgrade to S2 access control and S2 authenticated groups require devices that support client-side-inclusion
  - New devices are provided with S2-capable firmware
  - System is entirely consisting of devices in the three S2 secure groups

- Partial upgrade
  - Controller/gateway is upgraded to support S2
  - Critical devices, such as door locks, are upgraded to support S2
  - Door locks are re-included using client-side-inclusion to be part of S2-AccessControl security group (requires physical access to device)
  - All other existing devices are left in the unauthenticated or S0 groups
  - New devices are provided with S2-capable firmware and included in appropriate security groups

- Gateway-only upgrade
  - Only the gateway/controller is upgraded to support S2
  - Existing devices are left in current security groups (S0 or unauthenticated)
  - New devices are provided with S2-capable firmware and included in appropriate groups
  - Can be done entirely remote, and select devices can be upgraded when a service technician is on site at a later time

- Only end device upgrade
  - If only an end device is upgraded to support S2 and the gateway/controller remains with an older protocol version it is not possible to utilize S2 security improvements
  - S2 devices will need to fall-back to S0 or unauthenticated for the device to be included