Software Design Specification

Security considerations in Home Control installations

Document No.:	SDS13349
Version:	3
Description:	Problem analysis and manufacturer guidelines
Written By:	ABR;BBR
Date:	2018-03-05
Reviewed By:	ABR;JFR;MKIDMOSE;NTJ
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2018-03-05	11:52:42	NTJ	Niels Thybo Johansen	

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20150930	NTJ/ ABR	ALL	First revision
2	20160128	ABR	most	Minor editorial corrections.
3	20180302	BBR	All	Added Silicon Labs template

Table of Contents

1 ABBREVIATIONS

Abbreviation	Explanation

2 INTRODUCTION

The Internet has become a dangerous place.

Z-Wave as a technology started in local wireless networks in a friendly world. The technology allowed many logical networks to co-exist in the same air but nothing prevented eavesdropping of sensor data or direct injection of packets to control actuators in the home.

With the advent of connected door locks, security was added in the form of S0 which maintains the convenience of classic Z-Wave inclusion. In security, there is always a price to pay, either as reduced convenience or reduced security protection. With S0, the price is that the network key is disclosed during the key exchange. This trust model was considered sufficient for years, but the growing popularity of Z-Wave makes it more attractive to conceive attacks on Z-Wave networks.

The addition of gateways allows Z-Wave resources to be accessed from the outside. This adds new levels of user convenience to the Z-Wave ecosystem. Unfortunately, it also increases the risk of unauthorized use of resources in the Z-Wave network via gateways

This document discusses the potential threats to gateways and Z-Wave resources and outlines ways to eliminate or mitigate those threats.

2.1 Audience and prerequisites

The audience of this document is Z-Wave partners and Silicon Labs.

3 USE CASES AND RECOMMENDED REMEDY

This chapter describes situations, where the network environment or network components are compromised in some way. Some situations may be more critical than others.

Section 3.1 through 3.5 describes a number of attacks outside of the Z-Wave mesh network

> Gateways may experience intensive attacks via compromised LAN clients or directly from the Internet.
>
> **Criticality:** ‘High’

Section 3.6 describes a number of attacks on the Z-Wave mesh network.

> Z-Wave security is a tradeoff between not being too power-hungry in terms of battery or CPU cycles while providing a sufficient protection.
>
> **Criticality:** ‘Medium’

3.1 Local access to IP backbone

This section evaluates situations where an intruder has access to the local LAN. The access may be locally or via a compromised device which connects to the Internet.

Criticality: ‘High’, as the attack easily scales from one homeowner to a larger community.

3.1.1 Eavesdropping or injecting IP encapsulated Z-Wave commands

A Z/IP gateway may mark the UDP Z/IP Packet content as trusted by setting the “Secure Origin” bit in the Z/IP Packet header. In intruder may intercept UDP packets from the LAN and inject malicious packets which a receiving Z/IP gateway forwards securely over Z-Wave to a trusting device, e.g. a door lock.

Remedy: Z/IP communication over the LAN should use DTLS protection.

3.1.2 Compromised PC or smart phone

No PC or smart phone can be trusted today. They may have been compromised by malicious web pages or mail attachments.

Remedy: Z-Wave client applications should use a strong pre-shared key to communicate to the gateway.

3.1.3 WiFi WPS vulnerability used to gain access

By exploiting the vulnerability of WiFi WPS pin-based network setup, a hacker may mount a brute-force attack to get access to the WiFi network. It only requires a few thousand attempts.

Remedy: Completely disable WPS pin setup. If WPS pin setup is desired, make sure that the pseudo-random number generator is correctly implemented. Further, add an exponentially growing delay to responses for each new connection request to make brute force attacks impractical.

3.2 Administration interface attacks

This section evaluates situations where an intruder gains access to the gateway via untrusted interfaces. The cases are not specific for Z-Wave gateways but a Z-Wave gateway may be just as vulnerable to these attacks as any other IP based gateway or router.

Criticality: ‘High’, as the attack easily scales from one homeowner to a larger community.

3.2.1 Remote gateway administration interface via Internet

Most users will never want to manage the gateway remotely and they do not understand the security implications of enabling an administration interface towards the Internet.

Remedy: Disable remote administration by default or even disable the feature permanently; only allowing management via the LAN or via a protected VPN.

3.2.2 Remote gateway administration interface via WiFi

WiFi WPA2 security is acknowledged to be quite good. Still, there is a theoretical risk that an attacker in a parked car can gain access to the WiFi network, for instance by exploiting the vulnerability of WiFi WPS. Once onto the WiFi network, the attacker may aim his weapon on the gateway administration interface.

Remedy: Disable the administration interface on the WiFi interface; only allowing management via the cabled LAN.

3.2.3 Z-Wave network management via gateway administration interface

A hacker may initiate an “Add Node” operation via the gateway administration interface to include a rogue node and learn the shared network key. This attack will work for S0 as well as for S2 security.

Remedy: The gateway should not accept Z-Wave network management instructions via the administration interface from any network interface unless a trusted secure connection is used.

As an extra protection, the gateway may only allow the addition of new devices if a physical button is activated on the gateway. This will prevent attacks that enable the “Add Node” state in the gateway and subsequently add a rogue node to the network while logging the S0 key.

3.3 Z/IP Service attacks

This section evaluates situations where an intruder manipulates Z-Wave resources via the Z/IP Service hosted by the gateway. The cases are specific for Z/IP based Z-Wave gateways.

Criticality: ‘High’, as the attack easily scales from one homeowner to a larger community.

3.3.1 Z-Wave network management via Z/IP service

A hacker may initiate an “Add Node” operation via the Z/IP Service interface to include a rogue node and learn the shared network key. This attack will work for S0 as well as for S2 security.

Remedy: The gateway should not accept Z-Wave network management instructions via the Z/IP Service interface from any network interface unless DTLS or a trusted VPN connection is used.

As an extra protection, the gateway may only allow the addition of new devices if a physical button is activated on the gateway. This will prevent attacks that enable the “Add Node” state in the gateway and subsequently add a rogue node to the network while logging the S0 key.

3.4 Compromised gateway

This section evaluates situations where an intruder can access the gateway via the LAN. The access may be directly from the Internet but will often be via a compromised device in the LAN.

Criticality: ‘High’, as the attack easily scales from one homeowner to a larger community.

3.4.1 Default username and password attacks

Historically, routers and other network devices have shipped with a predefined username and a default password. A classic example is the username “admin” and the password “password”. Many other variants exist. Long lists may be found on the Internet.
Such product documentation recommended that users changed the password. Unfortunately, most users never followed that advice. And if the password was changed, the well-known username “admin” remained active. Thus, the login security was in reality reduced to one-factor protection.

Recently, security experts recommended that the factory default username and password is unique for each shipped device. This caused some manufacturers to auto-generate usernames and passwords containing the LAN MAC address or parts of it. One such example is the username “IDA051C0”.

Unfortunately, an attacker with access to the LAN can also determine the MAC address of the gateway. Thus, the username can also be guessed.

Remedy: Generate genuinely unique usernames and passwords based on different parts of the serial number. Provide the username and the password in an out-of-band form, e.g. as a removable printed label on the back of the gateway.
Require that the user logs in and creates a new username and password in order for the gateway to start working. Then disable the original username and password (after warning the user). Only a reset to factory default settings will restore the original username and password printed on the label. Z-Wave network keys are renewed during a factory default reset,

3.4.2 Too easy passwords

Many attacks use a list of well-known passwords. When asked to not use normal names and words, users have a tendency to use short and simple passwords as they are simpler to remember. It is not trivial for a constrained network device to look for all existing names and words. One approach is to require that users construct passwords which contains uppercase and lowercase letters, numbers and special characters, but this actually limits the scope of passwords that an attacker has to try.

Remedy: Require that passwords are at least 8 characters but allow for more. Require that passwords contain a certain number of character groups but do not require that all groups are necessarily included.

3.4.3 Brute force username and password hacking

It is frequently seen that a login system provides user friendly messages like “Unknown user” and “Invalid password”. An attacker may launch a script based attack to determine the password and the username. Many login requests may be issued every second. The user friendly messages may be used to identify usernames since the message “Invalid password” indicates that an existing username has been found.

Remedy: Always report the same error, e.g. “Invalid username or password”; even if the username is correct but the password is wrong.
For each attempt, double the time before another login attempt can be made. Store the current waiting time in non-volatile memory, so that repeated system restarts do not reset the timer.

3.4.4 Default local IP subnet prefix

A first level of attack on a local gateway is to determine the IP address of the gateway. Attacks such as cross-site scripting may trick the user’s browser to attempt logging into the gateway. Such attacks are a lot easier if the device has a default IP subnet prefix.

Remedy: Choose a random prefix in the valid range of private IP subnet prefixes (10.*.*.*, 172.x.*.*, 192.168.*.*, fd00::/8) and host address.

This will not stop patient hackers but it may make automated attack tools give up before they find anything of interest.

3.4.5 OS, firewall vulnerabilities

New vulnerabilities are found each day in operating systems and firewall packages.

Some manufacturers offer the user to send firmware update notification emails during product registration but many users never register their products and if the user gets another email address later, the user may never receive the update notification mails.

Remedy: Enable automated firmware updates from the manufacturer portal by default.

3.4.6 IP Services enabled by default

Many operating systems and IP stacks come with a number of IP services (UDP and TCP ports) enabled even though there is no actual need for these services in the actual gateway. The more ways a hacker can find into a system, the larger is the risk that an attack recipe can be found on the Internet.

Remedy: Only enable the IP services that are actually needed. Configure the firewall to allow only relevant service requests.

3.5 Compromised client

This section evaluates situations where a client device has been compromised by an attacker.

Criticality: 'High', as the attack easily scales from one homeowner to a larger community.

3.5.1 Unprotected Pre-Shared Key

No PC or smart phone can be trusted today. They may have been compromised by malicious web pages or mail attachments.
Thus, local application data cannot be trusted. This is a problem if that local application data is a Pre-Shared Key that is supposed to provide application end-to-end protection for client-to-gateway communication.

Remedy: Z-Wave client applications must store their pre-shared key in a secure way. Implementation will vary across smart phones, tablets and PC OSes.

3.6 Local access to Z-Wave wireless network

This section evaluates situations where an intruder has access to the local RF medium.

Criticality: 'Medium', as the attack does not easily scale from one homeowner to a larger community.

There is a host of good reasons to protect communication against eavesdropping and replay attacks. However, even the best wireless security protocols cannot protect a house against a brick being thrown through the window.

Z-Wave security is a tradeoff between not being too power-hungry in terms of battery or CPU cycles while providing a sufficient protection, knowing that ultimately, an intruder may enter through the window.

3.6.1 Disgruntled ex-boyfriend / Local neighborhood blackmailing

Considered simple sabotage, an adversary may inject Z-Wave commands from a specially crafted transmitter. For instance, it may be used to frequently turn light on and off and to change temperature to great dismay of the inhabitant.

A more professional variant is a local criminal who demands that the user pays an amount of money to stop the attacks.

Remedy: Use S0 or S2 security encryption between all nodes may prevent the injection of commands. Replay attacks are also eliminated this way.

3.6.2 Theft from newly built house using logged S0 network key

Professional criminals may hide a logging device which logs all Z-Wave activity around a newly built house. When the technician includes a secure device, the S0 key exchange is also logged. At a later time, after the home owners have moved in, the criminals may use the network key to send an "Unlock" command to the networked door lock, leaving no physical traces of intrusion in the house.

Remedy:

Use the S2 security option. By requiring security S2 encryption for all commands to the door lock, it is not possible for an intruder to capture the network key via logging. S2 key exchange uses out-of-band authentication and Diffie-Hellman key exchange.

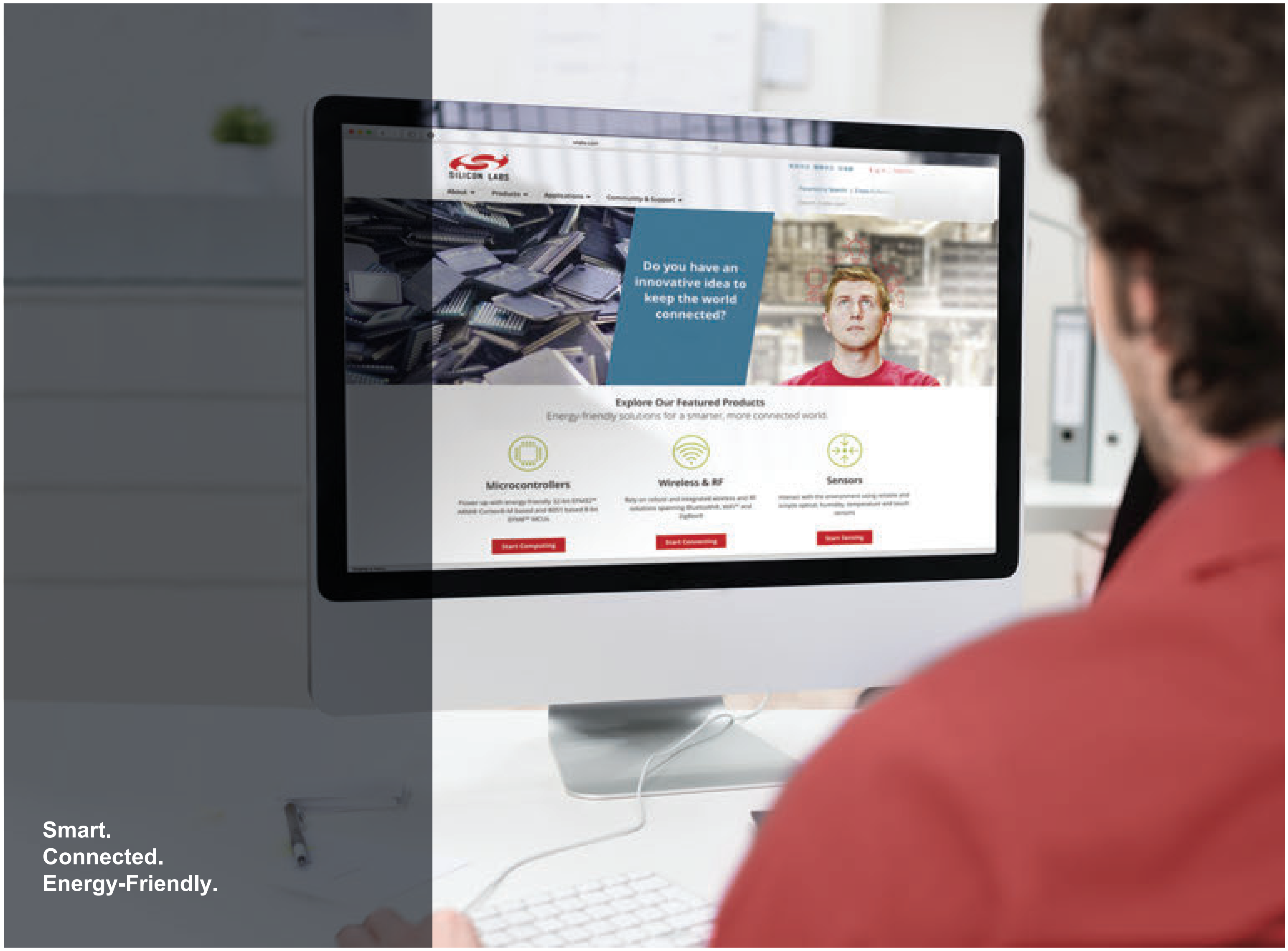
3.6.3 Theft from existing house using logged S0 network key

Professional criminals may set up a jamming device which deliberately injects noise to prevent the acknowledgement of certain transmissions (e.g. the door lock) until the homeowners are so annoyed that they call a technician. When the technician excludes the apparently failing device and includes a new one, the jamming device records the key exchange. The recorded key may now be used to send an "Unlock" command to the lock, leaving no physical traces of intrusion in the house.

The attack will most likely go un-noticed. A gateway could theoretically monitor the RSSI levels of the idle network. If noise is shaped a short bursts and synchronized to specific commands, such monitoring might be able to detect higher levels but this cannot be guaranteed.

Remedy:

Use the S2 security option. By requiring security S2 encryption for all commands to the door lock, it is not possible for an intruder to capture the network key via logging. S2 key exchange uses out-of-band authentication and Diffie-Hellman key exchange


SILICON LABS
About
Products
Applications
Community & Support
Do you have an innovative idea to keep the world connected?
Explore Our Featured Products
Energy-friendly solutions for a smarter, more connected world.
Microcontrollers
Wireless & RF
Sensors
Start Computing
Start Connecting
Start Sensing

Smart.
Connected.
Energy-Friendly.

Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

Disclaimer
Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information
Silicon Laboratories Inc.® , Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOmodem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, Z-Wave and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com