Operate General Purpose I/O with Strong Security

Introduction

Embedded electronic authentication ensures that sub-systems, accessories and peripherals used with or within a piece of equipment are not counterfeit. Additionally, by employing electronic authentication, manufacturers can more fully control the usage and performance of their products. Depending on the application, electronic authentication helps to maintain product reliability, accuracy, safety, and security to protect an OEM's R&D investment.

Threat

Consider the "Internet-of-Things" remote lock open/close application in Figure 1. The server wishes to issue an "open" instruction to a network connected, remote, 'smart' locking mechanism (containing a network capable controller). To prevent an intruder from opening the lock, it is imperative that the instructions coming from the remote server are verified as authentic. It is also desirable to verify the authenticity of the lock to ensure that it has not been replaced by a counterfeit. Mutual authentication of the server and lock can be achieved by locating an electronic authentication device within the lock itself. The lock and server send challenges to one another. If the responses to the respective challenges are satisfactory, mutual authentication is assured. Having successfully completed the authentication process, a "pass" signal is sent to the controller which enables it to perform the desired action, namely, opening the lock.

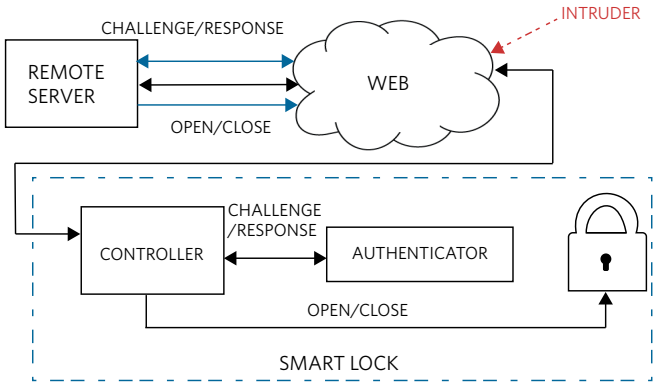

Figure 1. Typical remote lock opening/closing application

However, there is a potential point of vulnerability in this arrangement. The controller is ultimately responsible for the action of opening and closing the lock. The unsecured controller is vulnerable to attack from an intruder who could take control of it and configure it to ignore the pass/fail result from the authentication device. The intruder would then be able to open or close the lock at will.

Solution

Clearly, it would be desirable to overcome this vulnerability by taking the responsibility for opening and closing the lock away from the unsecured controller. One way of achieving this would be to use an electronic authentication device which has the capability of not only authenticating the server but which also has responsibility for opening and closing the locking mechanism.

Maxim's DS28C36 is the first electronic authentication device with secure general purpose I/O (GPIO). While continuing to perform the desired mutual authentication function as before, the presence of two dedicated GPIO pins with secure state control and state sensing ensures all instructions from the remote server to the lock are processed using a strong cryptographic protocol. A suggested usage of the DS28C36 in the previous remote lock opening scenario is show in Figure 2:

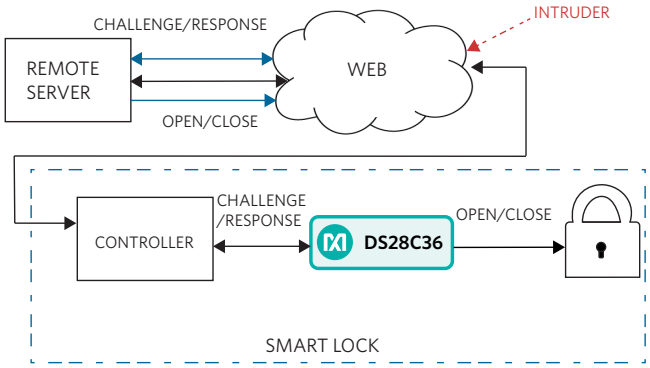

Figure 2. Secure remote lock opening/closing using the DS28C36

In this scenario, the authentication takes place between the remote server and the DS28C36. In the event of an intruder attack, the DS28C36 has the capability to disable the GPIO, preventing the loss of control of the locking mechanism. Figure 3 outlines the crypto sequence between the remote server and DS28C36 to accomplish the secure lock control using ECDSA authentication. In addition to being the only electronic authentication device available with secure GPIO functionality, the DS28C36 can also detect and prevent replay attacks.

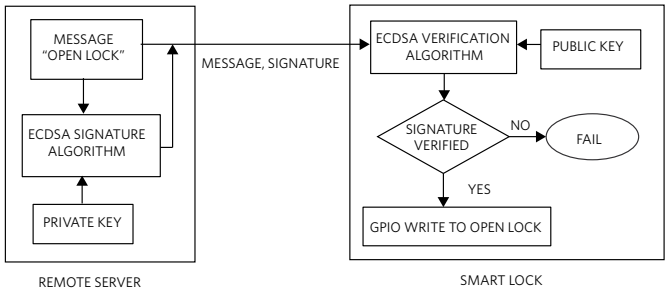

Figure 3. Crypto sequence for ECDSA authenticated GPIO control

Features

The DS28C36 includes a wide set of features, such as bi-directional secure authentication with both asymmetric ECDSA and symmetric SHA-256 based HMAC; optional secure protection of user-programmable memory with either ECDSA or SHA-256 authentication; secure storage of sensitive data with encrypted host-to-device and device-to-host transmission combined with ECDH based key establishment; GPIO with state control and state sensing with optional secure authentication; and system secure boot/download verification with optional GPIO pass/fail indication.

Conclusion

While most electronic authentication devices can guarantee the authenticity of a peripheral device connected to a host controller, they do not guarantee secure communication between them. The innovative inclusion of two securely controlled GPIO pins on the Maxim DS28C36 makes it the only secure authentication device available to address this issue. Additional applications that would benefit from this functionality include industrial automation where actuators, valves, and relays must be securely controlled.

Learn more:
Authentication Applications
DS28C36 data sheet

Design Solutions No. 11

Need Design Support?
Call 888 MAXIM-IC (888 629-4642)

Maxim Integrated
160 Rio Robles
San Jose, CA 95134 USA
408-601-1000
maximintegrated.com