Technical Article

IoT Security Made Simple with SimpleLink™ Wi-Fi® CC3100 and CC3200 Devices

Gil Reiter

The Internet of Things (IoT) connects billions of devices and brings a huge opportunity for businesses to grow. However, billions of new connected devices also brings billions of new opportunities for hackers to steal intellectual property (IP), compromise users' property and invade their privacy.

While consumer awareness for Internet security grows as more security breaches at large companies are revealed to the public, secure Internet communication technology has advanced to a level that provides online banking, e-commerce and government services. State-of-the-art Internet security relies on advanced cryptographic algorithms, powerful computers and collaboration between major Internet companies and users. The common security capabilities available to Internet applications today include the following:

- **Private communication** – Information exchanged between parties is encrypted, such that an eavesdropper cannot understand it.
- **End-point authentication –** Communicating parties confirm each other's identity prior to any information exchange to prevent attackers from using a false identity to access information and gain unauthorized control of a remote device.
- **Information authentication** – Critical information including transaction data and software updates are digitally signed to authenticate its origin and prevent malware installation.

These security capabilities largely rely on a few fundamental building blocks, including:

- Stable **cryptographic ciphers** such as the Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA2) and the public key ciphers RSA and ECC. When used properly with an adequate key size, these ciphers have no known practical attack.
- The **Transport Layer Security (TLS)** protocol, superseding its predecessor Secure Sockets Layer (SSL) protocol, provides the framework for establishing a secure communication channel between two parties. It handles both information encryption and end-point authentication, and relies on the cryptographic ciphers mentioned above.
- **Public key infrastructure (PKI)** provides the building blocks for authentication and trust through a digital certificate standard and **certificate authorities (CA)** such as Symantec and others.

The benefit of using these well-known ciphers and protocols in IoT applications is two-fold. First, it relies on proven technology that is widely deployed and tested by the industry at a mega-scale. Second, it allows harnessing the power of already deployed Internet services (e.g. email, social media) as well as the public key infrastructure provided by CAs.

Although Internet security technology is widely available, recent research from Symantec Security suggests that many deployed IoT devices have not implemented adequate security measures. There are likely multiple reasons for these security gaps, but vendor awareness, software complexity and implementation costs are probably at the top of the list.

Many IoT devices are based on low-end microcontrollers (MCUs) that have limited processing power and memory. Some devices don't have a user interface and many are designed by OEMs with little to no experience in Internet security. This brings about one of the biggest challenges in the IoT today - enabling robust security for low-end devices and making implementation easy for OEMs.

To overcome these challenges, the Texas Instruments SimpleLink™ Wi-Fi® CC3100 and CC3200 devices offer a TLS stack integrated on-chip with highly abstracted and easy-to-use APIs. These devices also include on-chip hardware cryptographic accelerators that perform the complex computational tasks swiftly and efficiently.

Moreover, other MCU solutions offer a TLS stack that runs on the application's MCU and needs to be integrated by the application developer. Not only that these solutions put more burden on the application developer and require a deeper understanding of the TLS protocol, they are also more vulnerable to security breaches due to software bugs, memory leaks and malicious software attacks. The CC3100 wireless network processor and CC3200 wireless MCU, on the other hand, run the TLS stack on a fire-walled network processor, keeping it isolated from the application code and would therefore be more secure than a solution running the application code and the TLS stack on the same processor.

By using the SimpleLink Wi-Fi CC3100 wireless network processor, customers can secure Internet connectivity to any MCU by offloading the TLS implementation from the MCU. The CC3200 wireless MCU has the same TLS capabilities like the CC3100, while completely offloading its integrated applications MCU from all Internet security tasks.

To summarize, securing Internet communication to IoT devices is vital. While TLS is the most deployed security protocol in the Internet, its implementation usually requires significant processing power and memory. Many IoT devices are low-end and low-power and cannot afford traditional TLS implementations. On-chip cryptographic hardware accelerators and the TLS engine offered by the SimpleLink Wi-Fi CC3100 and CC3200 devices can offload the MCU in low-end IoT devices and help customers meet their security objectives by bringing the benefits of TLS to any IoT device.

For more information, visit: www.ti.com/simplelinkwifi.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265