Cryptography effectively protects IoT devices from remote upgrade attacks

January 7 , 2026

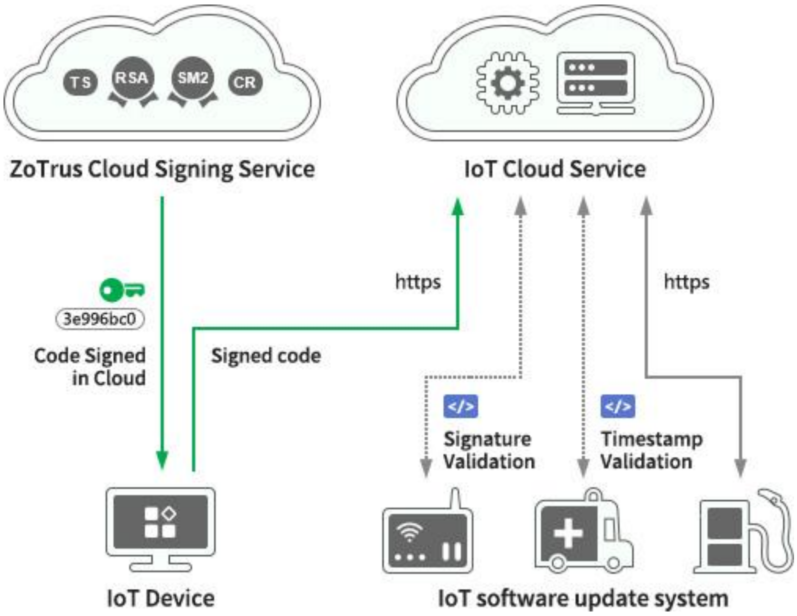
Currently, malicious attacks targeting various IoT devices are constantly emerging, such as gas station equipment, water supply equipment, and power supply equipment, with potentially devastating consequences. While major security vendors have launched their own IoT security protection systems and solutions, their effectiveness remains unclear. However, it assumes that these critical systems have purchased and deployed security protection measures, yet they still experience a constant stream of attacks and ransomware attacks. This raises serious questions about the effectiveness of traditional security methods. This article presents a new solution: a zero trust security solution based on cryptographic technology. This solution can simply and efficiently protect IoT devices from remote attacks, including various ransomware attacks. This approach is also applicable to the security of the increasingly popular intelligent connected vehicles.

The author analyzed several attack cases, most of which involved malicious attacks resulting from Over-The-Air (OTA) remote software upgrades. With the widespread adoption of 5G and the increasing prevalence of IoT devices, connectivity has become a mandatory default configuration. This is not only for data exchange and remote control between devices and cloud systems, but also for convenient remote maintenance and software upgrades to meet users' evolving needs. However, remote upgrades generally suffer from two major security vulnerabilities that make them easy targets for attackers. First, the use of the HTTP plaintext protocol for communication with the cloud system, this makes it easy for various communication data to be illegally intercepted, providing attackers with easy opportunities. Second, OTA remote software upgrades often fail to verify the legitimate origin of the software.

To effectively prevent remote upgrade attacks, based on the third principle of Zero Trust: zero trust software code without a digital signature, only trust software code with a trusted digital signature. All OTA upgrade software must have a trusted digital signature, and the device system must verify that the upgraded software has a trusted digital signature before installation. "Never trust" upgrade packages without digital signature and "always verify" whether received upgraded packages have a digital signature and whether it has a trusted digital signature! It's that simple. Without complex and expensive security systems, it can effectively prevent remote upgrade attacks by malicious software, thereby ensuring the security of IoT device systems!

Implementing verification of digital signatures for codes is only one effective measure. It's also necessary to adhere to the Zero Trust Principle: trust only HTTPS encrypted connections and not HTTP plain text connections. If a device system connects to the cloud system via HTTP, attackers can steal various communication data. Once they know the communication traffic is for distributing upgrade software to the device, they can tamper with data packets in the traffic to replace the upgraded software with malicious software used for attacks. If the device system doesn't verify whether the software has a trusted digital signature, it will automatically install this malicious software according to the principle of implicit trust, leading to device system paralysis or ransomware attacks.

In other words, to prevent remote upgrade attacks on IoT devices, it is essential to implement HTTPS encrypted connections to the server, rather than HTTP plain text connections. This prevents data leakage and tampering attacks during communication between the device and the cloud system, cutting off the channel for malicious code distribution. Simultaneously, the device must continuously verify the digital signature of each delivered upgrade package, ensuring it contains a trusted digital signature and a timestamp signature. The timestamp signature is also used to verify the trustworthiness of the upgrade software and assist in determining whether the upgrade behavior is suspicious.



Remote IoT device systems must verify crucial information such as the trustworthiness of the SSL certificate in the HTTPS encrypted connection, its match with the connected domain name, and whether the SSL certificate has been revoked, ensuring that HTTPS can correctly connect to the correct cloud server. Furthermore, verifying the digital signature of the upgrade package requires confirming that the certificate issuer is a trusted root CA certificate, that the code signing certificate used for the digital signature has not been revoked, that the digital signer is the software vendor designated by the device system, that the timestamp signature is trustworthy, and that the signature time aligns with the scheduled upgrade time. Only by completing these necessary verifications can the validity of the code signature of the upgrade package received through the HTTPS encrypted channel be guaranteed, allowing a decision to install the upgrade package based on the verification results.

For critical IoT systems, in addition to verifying the identity of the server and upgrade code, the server should also verify the trusted identity of the device. Otherwise, it may encounter impersonated devices connecting to the server, thereby enabling attacks on the server and revealing the communication mechanisms of IoT devices. Based on Zero Trust Principle Six: do not trust devices without trusted digital identities, only trust devices with trusted digital identities. Each device must have a trusted identity certificate to prove its trusted identity when connecting to the server. Only then will the server establish a secure connection and encrypted communication. Device control data can be encrypted using the device's identity certificate public key. After receiving control commands, the device decrypts them using its private key and verifies the digital signature of the command before executing the control command. Only in this way can the communication and operational security of remote devices be guaranteed. This cryptographic security mechanism also applies to the communication security of vehicle-to-everything (V2X) networks.

In summary, to ensure that IoT devices are not subject to malicious attacks, it is essential to adhere to the zero trust principles and strengthen cryptographic applications. This includes not only encrypting the connection between the device and the server, but also verifying whether the distributed software code has a trusted digital signature. Simultaneously, the server must also verify the trusted identity of the device. Only by achieving trusted devices, trusted code, and trusted encrypted communication links can we truly protect IoT devices from malicious attacks and effectively ensure the safe and reliable operation of IoT devices.

Richard Wang

August 7, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 111 articles in English (more than 151K words) and 252 articles in Chinese (more than 741K characters in total).