TAPROOT® security

NIST, MITRE, Penn State November 5, 2018

Dear colleagues,

Taproot Security is a private firm advising companies, government agencies, and policymakers on vital cybersecurity matters.

Thank you for the opportunity to comment on your draft white paper “IoT Trust Concerns”. Our feedback primarily concerns topic #11 Security:

By way of background, our threat modeling indicates the most common or vulnerable IoT attack vectors are supply chain, command & control subversion, denial of service, and data leakage / eavesdropping. Some of these are clearly addressed in the white paper, others less so.

12.2 recommends IETF’s *Manufacturer Usage Description* (MUD) to mitigate risks posed by default device passwords. In theory MUD might reduce default password risk by restricting network locations allowed to connect and authenticate. But to effectively mitigate default passwords we must eliminate them.

MUD is a promising protocol, but its primary virtue isn’t making default passwords less dangerous. Rather than promote MUD as a work-around for that purpose, the white paper should encourage IoT manufacturers to preset random unique-per-device factory passwords. The paper mentions this as an “advanced idea” but in fact such a scheme can be implemented more easily and cheaply than MUD.

A device password can be easily created, paired with a serial number, hashed, and stored in a central database. The need for a database can be avoided by deriving a password from the serial number (e.g., via salted hash with a secret salt), encoding it as a string, and storing it in the device. The need for password injection at the factory can be avoided by allowing a device to “phone home” on first use, mutually authenticate using its temporary default password, and receive a new password in response.

Better yet, IoT devices could move away from passwords altogether, and adopt more secure cryptographic methods to authenticate instead (e.g., mutual https with protected private key).

12.2 focuses on device passwords but does not seem to address server passwords. Mutual authentication between device and server is required to thwart command & control subversion that tricks a device into accepting malicious commands in various ways (e.g., DNS poisoning) in order to alter its normal behavior (e.g., launch DDoS attacks). The paper should recommend devices authenticate servers through methods such as mutual TLS (with appropriate key management). Fixed server passwords should be discouraged, although they’re better than having no server authentication at all.

The paper could also recommend devices use server IP addresses rather than host names in order to avoid DNS attacks. (MUD relies on URLs that generally include host names.) Note the above remarks regarding servers apply also to peers. In a P2P distributed discovery environment, such as mentioned in section 18, devices must mutually authenticate one another.

12.3 recommends IETF's *IoT Firmware Update Architecture* to mitigate risk of malicious firmware updates/patches. This would also improve manufacturers' ability to simply fix bugs. We concur in principle, but as the paper notes, the IETF architecture is an "emerging standard". (The most recent version of the RFC expired last September.) While it looks promising, it may be premature for NIST to endorse it before it undergoes more comment and vetting.

Section 12 is silent regarding encryption. While arguably less critical to IoT than mutual authentication, network communications should be encrypted to mitigate a variety of threats, including eavesdropping. Many IoT devices communicate sensitive personal data (e.g., home camera video). Recommending mutual TLS (with appropriate key management) would address this.

Please note some of these comments may apply also to NIST special publication SP 800-163 and/or NISTIR 8228.

Thank you for this opportunity to share our perspective on IoT security.

Sincerely,

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com