Public Comments from

François-Frédéric Ozog
Shokubai.tech
GSA TIES lead for automotive multi-tenancy group

I – Indirect attacks mitigation

Time synchronization, DNS server and smtp servers can be consequential for the proper behavior of home devices.

Time tampering: if your home security policies depend on the time of the day, tampering with time may allow attackers to benefit from lower level protection. Usually, IoT devices get their reference time from a pre-configured network time server. If those are foreign controlled, consumers of a country may find themselves more exposed.

There should be a requirement to get those network time servers from the telecom operator. This configuration can be automated at onboarding time as part of matter process.

DNS servers are used to translate from internet names to IP addresses. This may be used by IoTs such as a door lock to check a number of things. Default DNS servers may be introduced in some devices and point to foreign, may be compromised servers. Malicious attackers may leverage DNS requests to identify with good probability when people are in-house or out for vacation.

There should be a requirement to get those network time servers from the telecom operator. This configuration can be automated at onboarding time as part of matter process.

SMTP servers are used to send mails or alerts. Should those servers be compromised, alerts may not arrive at their intended destination.

There should be a requirement to get those network time servers from the telecom operator. This configuration can be automated at onboarding time as part of matter process.

II – attack detection

It is very important to complement security with breach detection. That is many times forgotten unfortunately despite it is instrumental in reducing the impact of a successful attack.

Out of detection mechanisms, IETF Manufacturer Usage Description Specification (https://datatracker.ietf.org/doc/rfc8520/) is very simple yet powerful.

It raise the alarm when a device is conducting traffic that does not correspond to its spec. We don’t know how the security was breached, but we can act on a breach as soon as it happen.