Cybersecurity – Secure authentication and encryption in the IoT systems

Marek Ostafil, Smart Secure Networks, Polish IoT & AI Cluster - SINOTAIC

Smart Secure Networks

sinotaic

"The nightmare headline for me is
100,000 refrigerators attack Bank of America"

Dr Vint Cerf

What does reality look like?

Over 80% of all cyber threats result from the use of weak user protection systems (passwords or biometric technologies used as a single solution.

The use of passwords in authentication between devices and the very easy theft of access data allows for the takeover of control over devices and entire systems and/or their paralysis.

Over 80% of communication between intelligent devices is not secured or encrypted in any way. This allows for the takeover of all data during its transmission.

We must remember that we are taking part in a cyber war that is taking place every minute and in the form of a thousand incidents a day around the world.

This Internet-of-Things (IoT) brings with it major advantages and enormous potential.

Its exceptionally fast growth, however, has unintentionally prioritised speed and connectivity over security and unfortunately, IoT networks are prone to infiltration and cyber attacks in the form of identity theft, phishing, DDoS attacks, data theft and more.

Many connected devices are only required to complete simple, singular tasks and so they are often designed with low battery power, computational ability and processor speeds.

Key areas of cybersecurity in IoT

For us, cybersecurity areas in IoT networks will mean:

- user,

- device (Thing),

- data (including their transmission).

One of the most important elements of the IoT network is collecting and processing data in order to provide a sufficient amount of structured information to enable making good decisions.

So, in IoT cybersecurity, securing the method of collection (device), distribution and access (user) to data and information (data) will be the key.

Most of today's encryption methodologies are not capable of protecting these simple devices. As a result, both the devices and data in the IoT network are vulnerable to cyber attacks.

Inadvertently, across all IoT networks from Smart Cities and Smart Buildings to Smart Factories and Smart Cars, an army of connected devices that cannot adequately protect themselves has been built. These gaping security holes are already delivering consequences to many aspects of business and society.

So, while we know them the world over as ‘smart devices’, they have also been described as ‘dumb robots’ in many ways - as they lack the memory, electrical, and computational power to handle demanding algorithms like AES 128 or AES 256.

Keep in mind that these are the encryption specifications for electronic data that have been adopted worldwide for nearly 20 years.

Passwords are the weakest element of IT security. Authentication largely depends on password usage for both: user and device credentials that have countless weaknesses and vulnerabilities. Unfortunately, while we, as human users, use passwords to authenticate and access information every day, machines and devices in the IoT world do the same thing again using passwords.

It is this lack of secure device-to-device authentication that is leaving networks vulnerable and open to attack.

The infamous Mirai attack brought this precise issue into the global security spotlight. Every system is only as strong as its weakest link and this gaping weakness that exists right across our IoT ecosystem has consequences for companies and organizations of all sizes.

Most encryption modules as we know them are based on PKI (Public Key Infrastructure) which uses a pair of encryption keys: one public, one private. The public key is related to the private key mathematically, so it is possible, in theory, to get the private key from the public key.

The only way forward was to develop a methodology that matches the limited computational power while delivering the highest levels of protection possible. ELIoT Pro Lightweight Encryption (LE) is purpose-built, while incorporating uniquely strong authentication technology, to tackle one of the key cyber security concerns of the next decade.

cordis.europa.eu/project/id/822641

ELIoT Pro end-to-end cybersecurity solution was financed by the European Commission's SME Instrument / Horizon 2020 program

While all IoT devices are not equal, they do need to be afforded an equal level of protection in the context of growing connectivity meaning no one device can become the single point of entry that hackers need - as “a system is only as strong as its weakest link.”

Without the capacity to handle complex or demanding encryption methodologies and the fact that device battery life is affected by computing activities and memory usage, these devices are wide-open to attack.

Traffic and data being sent between devices require encryption and LE incorporates the concept of ‘entanglement’, its unique characteristic that sets it apart from other developments in the cyber security world.

This is where authentication that deploys encryption creates a degree of entanglement and as a result, substantially stronger security delivering mutual authentication. In simple terms, the better devices ‘know’ or recognise each other, the stronger the authentication is.

The concept is completed with the two-layered approach to cyber security for IoT devices. By combining secure, passwordfree Human to Machine **(H2M)** authentication and Machine to Machine **(M2M)** authentication with LE.

H2M: **Replace passwords with superior authentication protocols**

ELIoT Pro is based on the theory that as a first step, passwords must be eliminated for machine to machine authentication, wiping out the possibility of unauthorised access. Our authentication protocol uses one-time audio token technology or one-time passwords transmitted by an ultra-sonic signal.

M2M**: 'Lighten' encryption to ensure readability on devices of all specifications**

ELIoT Pro provides equally ultra-high levels of security to all types of IoT devices regardless of their memory/ computational power limits. ELIoT Pro introduces an entirely new "language" of communication through LE for all IoT devices which is understandable even for the simplest units on the market.

Questions?

Thank you for your attention!

marek.ostafil@ssnetworks.eu

Smart Secure Networks

sinotaic