FRANÇAIS ENGLISH

leti
cea tech

TILT

IOT SECURITY:
WHY AND HOW?

WHAT IS TILT?

TILT explains why and how IoT data flows can be secured using lightweight, efficient encryption mechanisms. By their nature, embedded systems have limited resources (size, computing power, battery life). Lightweight encrypted tunnels can satisfy these constraints. Their features include authenticating peers before communication begins and, once the tunnel is open, encrypting and signing the information exchanged between them.

APPLICATIONS

Security for all types of connected devices:

- consumer,
- industrial,
- medical devices,
- etc.

Development carried out through the IRT Nanoelec PULSE program.

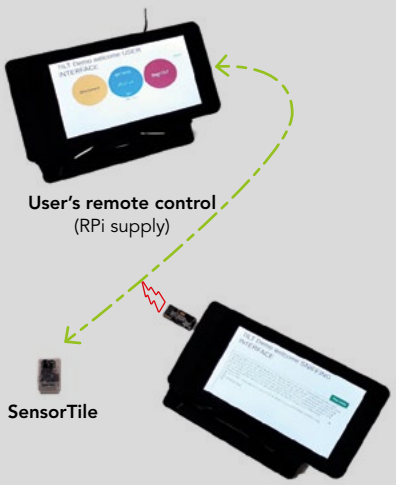
NANOELEC.

WHAT'S NEW?

TILT is the first lightweight encrypted tunnel that adapts to the situations, requirements and constraints of different hardware architectures.
TILT is customizable, allowing the use of different encryption mechanisms (crypto-agile architecture).
The demonstrator establishes communication between a connected device (an IoT sensor) and a data concentrator unit using the BLE (bluetooth low energy) protocol. The chosen sensor is based on the STM SensorTile development board, which is characteristic of an IoT node: small size (13.5 × 13.5 mm), restricted battery life and computing power (microcontroller).

Hardware:
- IoT sensor: STM SensorTile;
- Supervisory gateway: Raspberry Pi 3 model B+;
- Spy terminal: Raspberry Pi 3 model B+ equipped with a USB BLE sniffer;
- Low-cost hardware, easily accessible, to demonstrate how easy the system is to set up.

Scenario:
Once the connection is established, the IoT node can be interrogated via a graphical interface on the supervisory gateway touchscreen to retrieve a temperature value. Another battery-powered mobile terminal with a BLE sniffer plays the role of the spy. Every time the IoT node is interrogated, the temperature values are displayed unencrypted on the spy's screen. Encrypted communication using the lightweight encrypted tunnel is then activated on the supervisory gateway connected to the IoT node.
The packets received are still displayed on the spy's screen, but they cannot be decrypted and the temperature information cannot be displayed.



Without tilt 26C

With tilt 160 4 219 16 67 24 16 223 137 48 15 197 167 242 61 227 250 126 77 147 UNKNOWN CHARACTER

WHAT'S NEXT?

- Implementation of additional cryptographic mechanisms and new post-quantum protocols;
- Studies to improve performance and implementation costs (computation and power consumption).

INTERESTED IN THIS TECHNOLOGY?

Contact:
Marion Andrillat
marion.andrillat@cea.fr
+33 438 784 651

CEA-Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 avenue des Martyrs | 38054 Grenoble Cedex 9 | France
www.leti-cea.com
@CEA_Leti CEALeti CEA-Leti