FRANCE 2030 PROGRAMME DE RECHERCHE RÉSEAUX DU FUTUR

cea | cnrs | Institut Mines-Télécom

Elsa Lopez Perez | AIO Inria Paris

Inria

PC 8 - HISEC

Backwards-compatible Next-Generation Security for the Internet-of-Things infrastructure

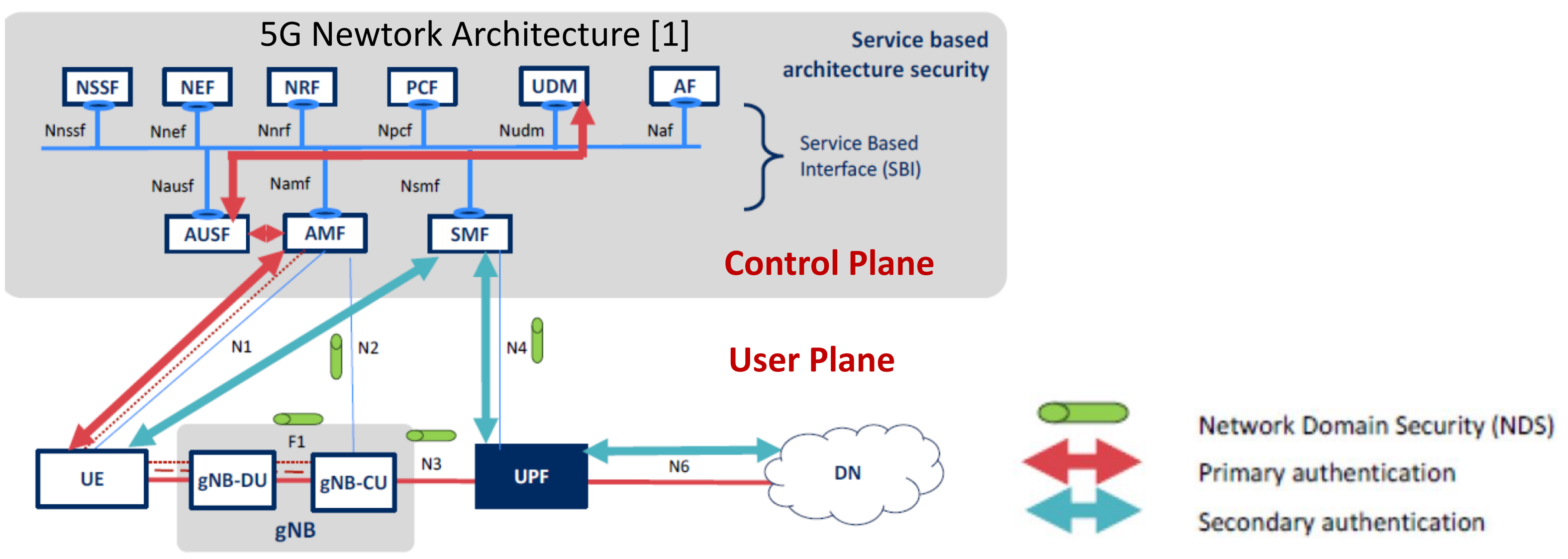
Context

*Next-generation cellular networks are expected to connect tens of billions of IoT devices by 2030. These devices often operate under **constraints** that traditional security protocols weren't designed to accommodate.*

Network Access Authentication:

- Process by which a network verifies the identity of a device.
- 5G uses the **Extensible Authentication Protocol (EAP)**, an authentication framework used for **authenticating devices** (the EAP peers) **before they are authorized to access the internet and other network services**
- EAP is standardized by the Internet Engineering Task Force (IETF)

1. **Primary Authentication (5G-AKA/EAP-AKA): First** authentication that a User Equipment performs when it tries to **access** a **5G Network**. The 5G-AKA is a specific EAP method used here.
2. **Secondary Authentication (EAP-AKA, EAP-TLS, EAP-TTLS): optional** additional layer of authentication that can occur **after** a successful **primary authentication**. It is used for user connections to set up user plane connections to data networks outside of the mobile operator domain.



[1] https://devopedia.org/5g-authentication

The Challenge:

How to enhance the security of existing IoT deployments while maintaining compatibility with deployed infrastructure and integrating them with Next-G Networks.

Attack Scenario: Compromise of long term credentials

Scenario: A hospital uses portable medical monitors connected to the 5G network. These devices use **SIM-based primary authentication** via standard **EAP-AKA** to connect to the network, and then use **EAP-AKA as secondary authentication** to access patient medical records.

The Attack

Compromise of a sensor's long-term SIM key → Passive collection of encrypted data → Retroactive decryption of past communication

EAP-AKA does not provide Perfect Forward Secrecy (PFS)

The Solution: EDHOC via EAP as secondary authentication

EDHOC (Ephemeral Diffie-Hellman Over COSE) is an authentication and key exchange (AKE) protocol used by peers running on constrained devices. It uses asymmetric cryptography, providing **Perfect Forward Secrecy (PFS)**.

Compromise of a sensor's long-term SIM key → EAP-EDHOC establishes **ephemeral session keys** with **PFS** → Past communication remains **encrypted** and **secure**

Currently EDHOC supports authentication with Static Diffie-Hellman keys and Signatures

To increase compatibility and facilitate migration of legacy devices authenticating with PSKs, we need to define a new PSK-based authentication method

Research and Methodology

- EDHOC was developed by **the Internet Engineering Task Force (IETF) Lightweight Authenticated Key Exchange (LAKE)** Working Group as a response to the requirements of constrained environments.
- The **integration** of **PSK-based** authentication method is an area of **focus** within the LAKE Working Group

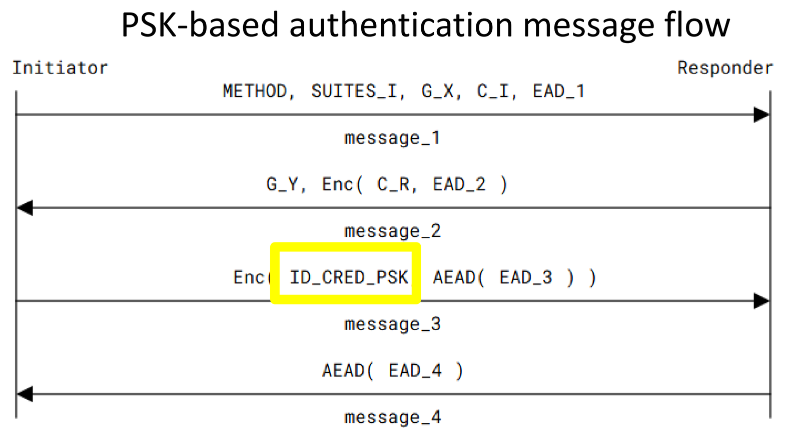
Methodology:

Identify the problem → Model it → Simulation → Experiment → Standardization / Parallel process / Formal Analysis

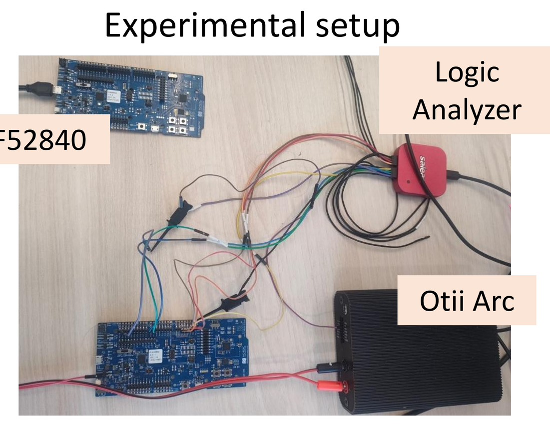
Experimental Setup

- Performance metrics (time, memory, energy) are measured using the **nRF52840** development board, the **Saleae Logic Analyzer** and **Otii Arc** (power profiler device)

PSK-based authentication message flow



Experimental setup



- Coordinate **formal analysis** (symbolic and formal)

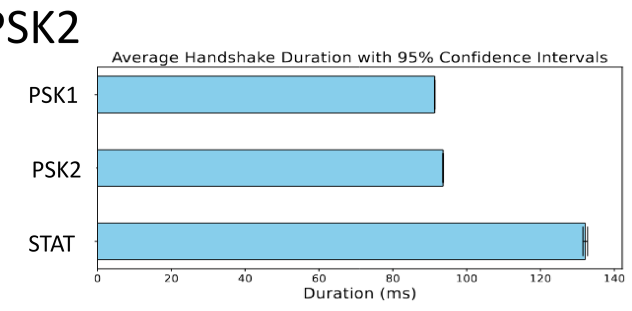
Results and scientific collaboration

Benchmark of the PSK-based EDHOC

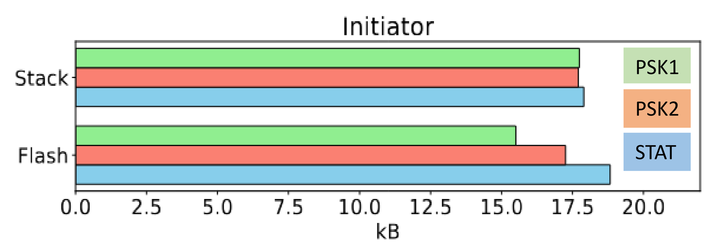
- Two variants (PSK1/PSK2) were presented to the Working Group
- As a result of the analysis, the **IETF has adopted PSK2**, described in an **Internet Draft** [3]. Performance analysis includes:

1. **Time duration and energy consumption:**
   - Both PSK1/PKS2 are **faster** than Stat-Stat method
   - PSK1 consumes slightly less than PSK2

Role	Met	Max Current (mA)	Min Current (mA)	Avg Current (mA)	Time (ms)
Init.	PSK1	15.16	10.96	13.83	91.34
	PSK2	16.53	12.26	15.20	93.60
	STAT	14.96	10.73	13.61	131.15



2. **Memory consumption:**
   - Stack and flash memory
   - More code instructions = higher flash memory for PSK2



3. **Security and Privacy**
   - **PSK1** does **not** offer **identity protection**

Collaborations

- University of Murcia
- Ericsson
- University of Limoges XLIM

xlim | UNIVERSIDAD DE MURCIA | ERICSSON

[3] E. Lopez-Perez, G. S. Selander, J. Preuß Mattsson, and R. Marin-Lopez, EDHOC PSK authentication, Internet-Draft draft-lopez-lake-edhoc-psk-01, July 2024, work-in-Progress. [Online]. Available:https://datatracker.ietf.org/doc/draft-lopez-lake-edhoc-psk/03/