... in the Internet of Things

Bachelor Project (PO)
Scenario Description
Hamburg 20.03.2023

José Álamos jose.alamos@haw-hamburg.de
Leandro Lanzieri leandro.lanzieri@haw-hamburg.de

Prof. Dr. Thomas C. Schmidt — INET AG, Dept. Informatik HAW Hamburg — t.schmidt@haw-hamburg.de

A bit about us: José I. Álamos

- Received his B.Sc in Civil Engineering and Dipl.Ing in Electrical Engineering at the Pontifical Catholic University of Chile.
- Since 2018 works as a Research Assistant at the Hamburg University of Applied Sciences where he focuses on LPWAN link-layer protocol design and got involved as a RIOT maintainer.
- He is currently pursuing his PhD in collaboration with the Free University of Berlin within a research project that aims for enabling efficient, reliable and secure LPWAN communication over the LoRa modulation by using appropriate link and physical layer techniques.

A bit about us: Leandro Lanzieri

- Studied Electrical Engineering, then he obtained his Master's degree in Embedded Systems at the University of Buenos Aires, with a thesis in collaboration with the Hamburg University of Applied Sciences.
- He has worked at the INET group of HAW Hamburg since 2018 as a research assistant where he focused on secure IoT protocols and got involved in RIOT OS as a maintainer.
- He is currently pursuing his PhD in collaboration with DESY on a research project, which aims to analyse data from operational records, environmental measurements and experiments, in order to find early indicators of hardware deterioration of the embedded sensor systems at the European XFEL.

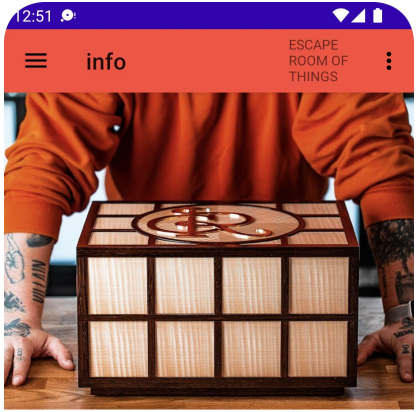
Last year’s project:

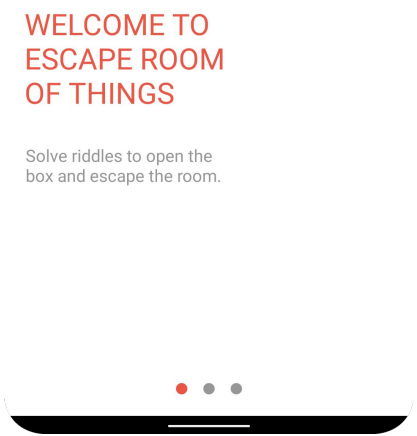
Escape Room of Things

A secure plug-n-play Escape Room

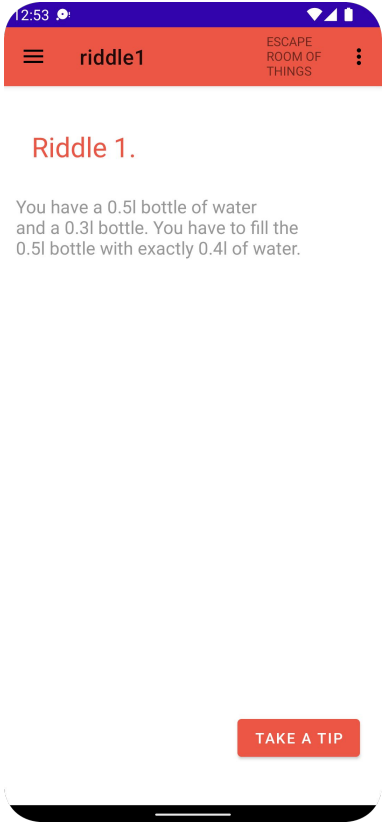
Escape Room of Things

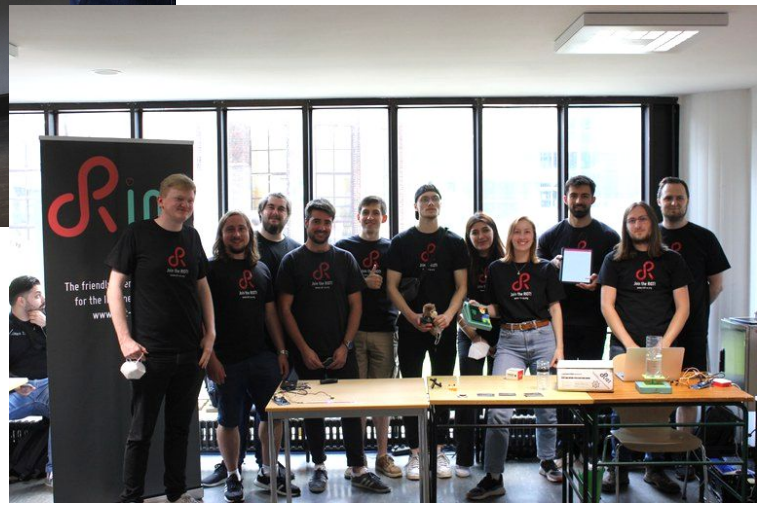
- Multiple wireless puzzle nodes.
- Encrypted and authenticated node communication:
  - Credentials installed on flash.
  - QR code for on-boarding.
  - CoAPs (DTLS).
- Central control tracking status of all puzzles.
- Mobile app:
  - Users get instructions and tips.
  - Admins can add new nodes and configure the rooms.





Escape Room of Things





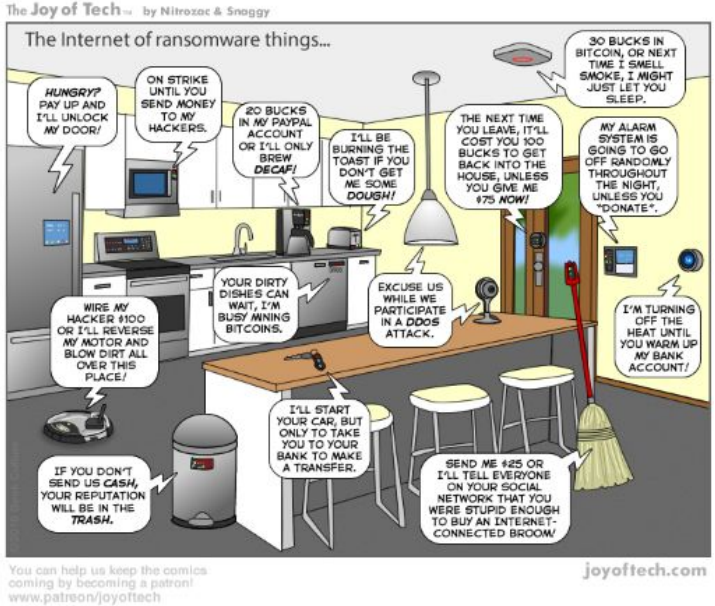
Secure Smart Supply Chain

A Challenge of **Security on the IoT**

Motivation

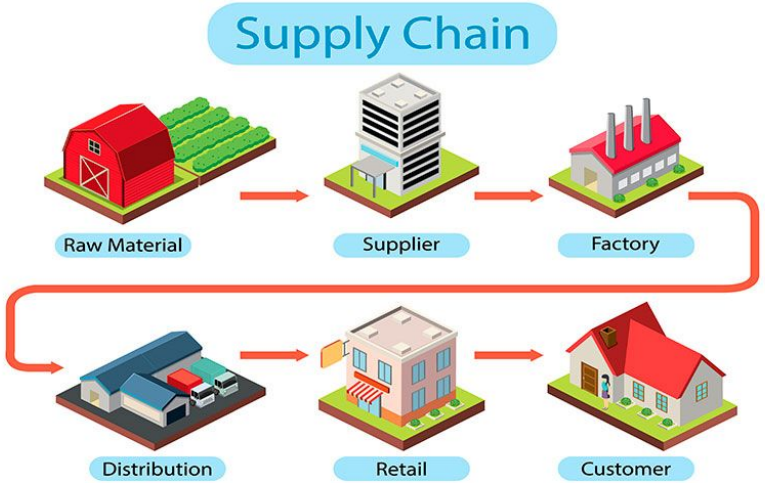
+30 billion devices by 2027

- **Security**
  - Rise of cybercrime.
  - We need: **C**onfidentiality, **I**ntegrity, **A**uthentication.
- **Interoperability**
  - Increasing number of vendors with custom solutions, results in incompatibility silos.
  - Open standards help foster better communication between devices from different vendors.
- **Open implementations**
  - Reduce development costs.
  - Accelerate innovation.
  - Open review process enhances security.



Secure Smart Supply Chain

- The global supply chain is vulnerable to theft, tampering and fraud.
- We want to build **smart containers** that:
  - Increase **transparency and security**.
  - Provide real-time information about the cargo.
  - Use standardized IoT technologies to ensure **reliability and interoperability** among containers.



Project High-Level Requirements

- The smart container collects **verified** readings from multiple sensors (e.g., temperature, humidity, pressure, door status, location, etc.), formatted in SenML.
- A summary of the values is sent via **LoRaWAN**.
- The full series of readings is **locally stored**, and available to be read by an operator.
- A **web app** displays the updated data from all containers.

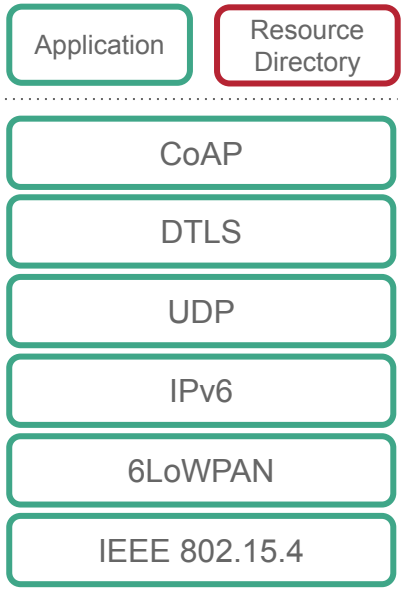
Project Technical Requirements

- Locally all sensors communicate with the concentrator node via CoAP over IEEE 802.15.4.
- **Security:** Communication should be encrypted and data should be signed. The local storage should also be encrypted.
- A bootstrap mechanism is required to establish initial trust between server and concentrator, and between concentrator and sensors.

Technologies

We will utilize open standards to ensure security and interoperability

- Resource discovery: **CoAP - Resource directory**
- Application: **CoAP, Link Format**
- Transport: **UDP + DTLS**
- Network: **IPv6 + 6LoWPAN**
- Radio + MAC Layer (local): **IEEE 802.15.4**
- Radio + MAC Layer (remote): LoRaWAN



Typical IoT networking stack

Proposed Teams

The following team organisation **is a suggestion:**

- **Concentrator node**
  - LoRaWAN communication.
  - Data reception and storage.
- **Sensor nodes**
  - Device reading.
  - Wireless communication.
- **Web application**
  - Backend and communication with LoRaWAN application Server.
  - Frontend.
- **Security**
  - Local communication encryption, data signing and verification, credential distribution.

Formalities & Tools

- **MS Teams (code xr414us)**
  - https://support.microsoft.com/en-us/office/use-a-link-or-code-to-join-a-team-c957af50-df15-46e3-b5c4-067547b64548
  - **GitHub**
    - Everyone should send to MS Teams
      - Name
      - GitHub username
      - HAW email address
    - Project code will be in https://github.com/smartuni
- **Milestone presentations**
  - Mandatory and on site: 3 + 1 presentations, slides, documented source code checked-in
- **Final documentation**: Hackster.io
  - Project documentation and description linked to GitHub repository
  - https://www.hackster.io/riot-os

Material

- Calendar and slides
  - https://inet.haw-hamburg.de/teaching/ss-2023/riot-im-internet-of-things

- RIOT Tutorial
  - https://github.com/smartuni/exercises

Questions?