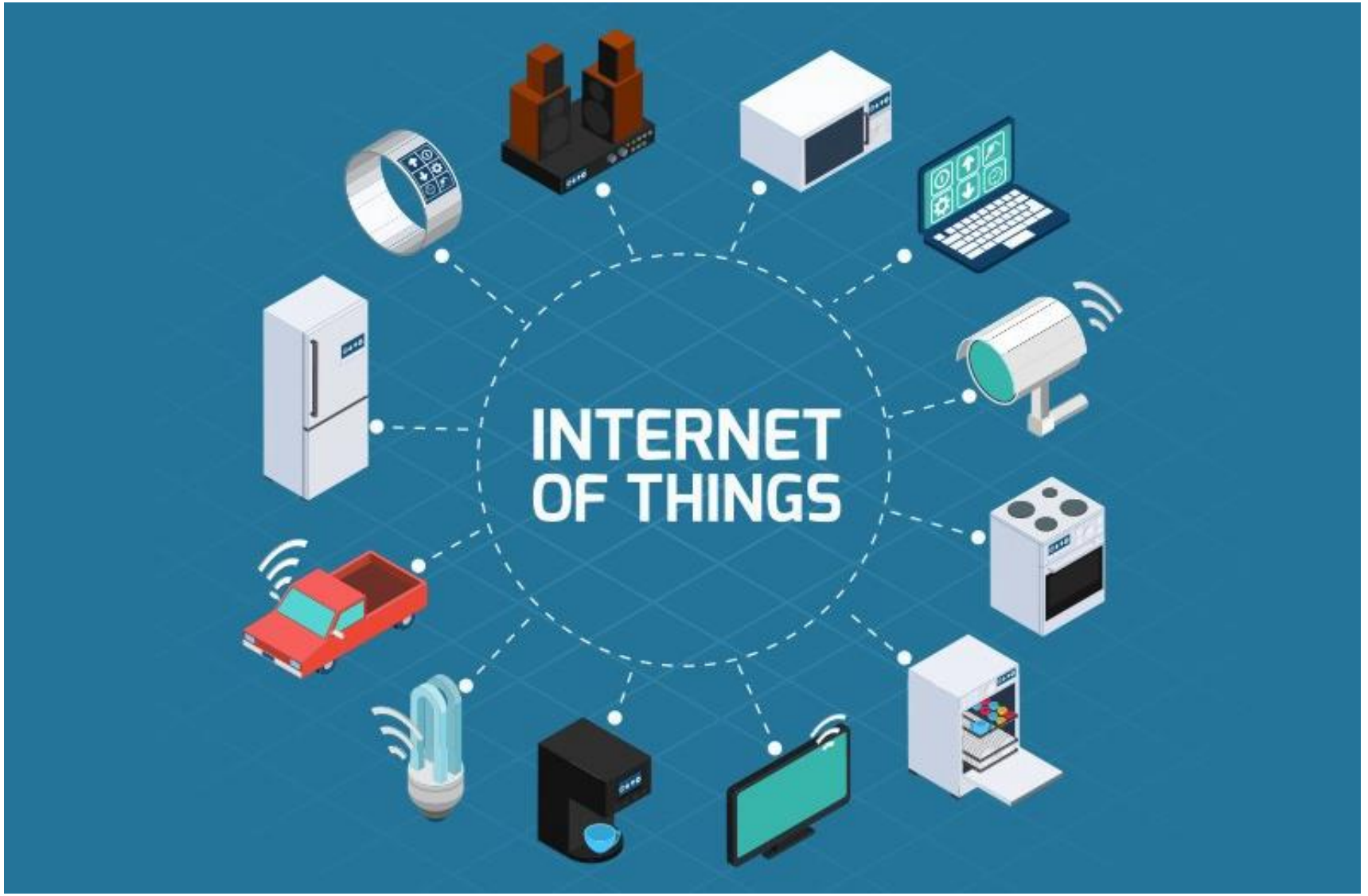
SSF Octopi Project

Alejandro Russo (PI)
russo@chalmers.se

IoT is here!



Root problems

I. Lack of security expertise
II. Low-level programming languages
III. No system-wide control

Goal:
Security-by-Design

To develop technology for securely programming IoT systems

A technology that can be used by developers on their daily activities: *programming languages*

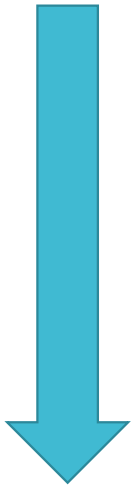
Approach

Using high-level languages

- Root problems of insecurities:
  I. ~~Lack of security expertise~~
  II. ~~Low-level programming languages~~
  III. ~~No system-wide control~~

Research Challenge

Pushing high-level languages guarantees and abstractions



Constrained embedded devices

Domain Specific Languages (DSL)

Data Privacy

Information-flow Control

Resources

Testing

Code generation

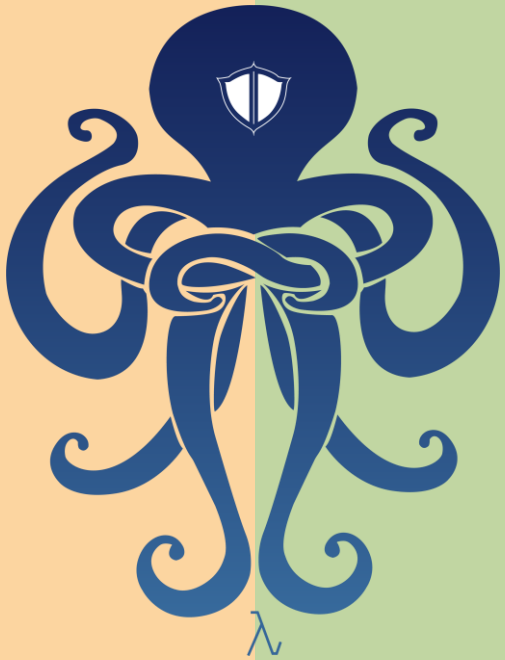
Clean slate

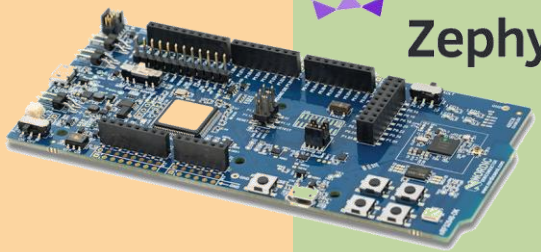
DSL

C code

DSL

Virtual Machine





Secure Hardware

DPella

- **A Programming Framework for Differential Privacy with Accuracy Concentration Bounds. IEEE S&P 2020, TOPLAS 2021**
- **Spin-off company** dpella — unleash the power of analytics
- **Proof-of-concept with Ericsson**

Exploring privacy-preserving data analysis

Many of our clients in the automotive sector face a multitude of obstacles when sharing data. These clients need an effective solution to protect their customers' privacy while leveraging metadata to optimize products and improve user experience. The same is true for many actors outside of the automotive sector as well.

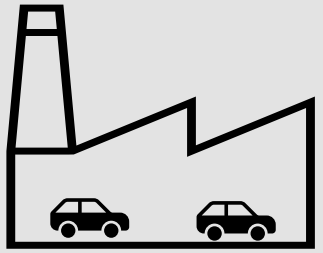
SEP 21, 2022 | 4 min.

Ignacio Herrera
Senior Solutions Architect, IoT & Connected Vehicles

Alejandro Russo
Co-founder & CEO/CTO, DPella

Marco Gaboardi
Co-founder & Chief Scientist, DPella

ERICSSON

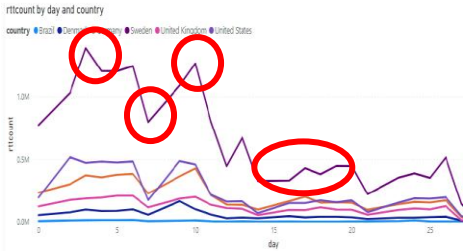


Connected vehicles data packages

Learn

Analytics Trends

Peaks, Valleys, Flat areas are identifiable



Protect

Telco Operator detailed performance

dpella

At single sample level (events)

Domain Specific Languages (DSL)

Data Privacy

Information-flow Control

Resources

Testing

Code generation

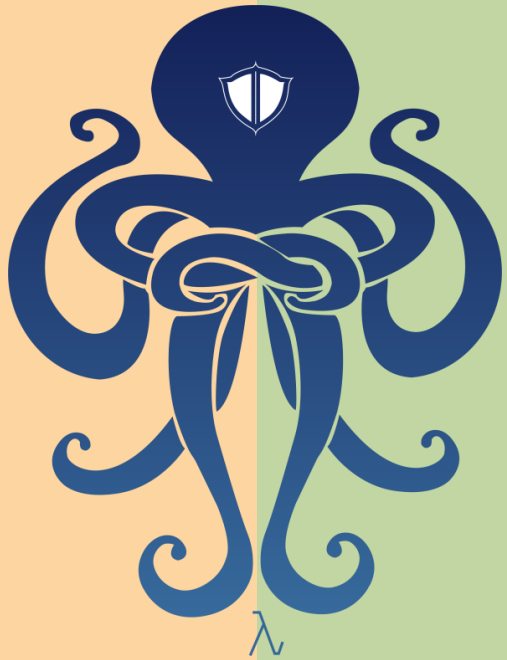
Clean slate

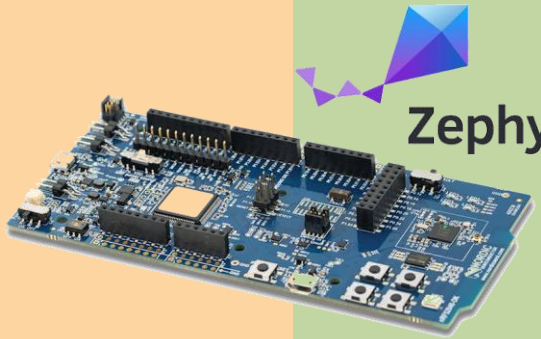
DSL

C code

DSL

Virtual Machine





Secure Hardware

Confidential Computing

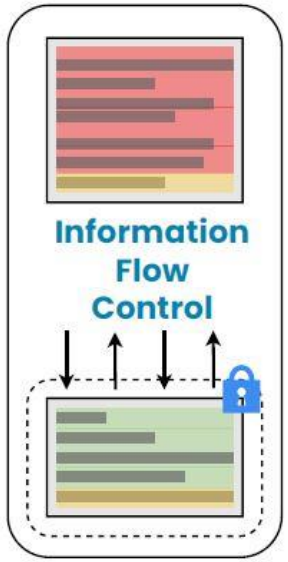

```
sendData :: TEE SalaryRef -> TEE () -> Salary
         -> TEE ()
sendData ref unlock salary = do
  entries <- addSalary ref salary
  when (length entries + 1 > 2) unlock

getAvg :: TEE SalaryRef -> TEE Float
getAvg ref = do
  st <- readTEERef ref
  return $ (sum st) / length st

clientApp :: API -> Client ()
clientApp api = do
  salary <- readLn
  onTEE (send api <> salary)
  average <- tryTEE (avg api)
  print $ show average

app :: App Done
app = do
  ref <- liftTEERef []
  (avg, unlock, lock) <- flowlock $ getAvg ref
  send <- secure $ sendData ref unlock
  runClient $ clientApp $ API send avg
```

Automatic Partitioning



Code generation

Clean slate

re Hardware

Selected publications

- Normalization for Fitch-style Modal Calculi, ICFP 2022 (distinguished work)
- From fine- to coarse-grained dynamic information flow control and back. POPL 2019 (distinguished work)
- Faceted Secure Multi Execution. CCS 2018.
- A Programming Framework for Differential Privacy with Accuracy Concentration Bounds. IEEE S&P 2020.
- Practical normalization by evaluation for EDSLs. Haskell 2021.
  Code - github.com/nachivpn/nbe-edsl
- Hailstorm: A Statically-Typed, Purely Functional Language for IoT Applications. PPDP 2019.
  Code - github.com/Abhiroop/hailstorm
- Towards secure IoT programming in Haskell. Haskell 2020.
  Code - github.com/OctopiChalmers/haski
- Higher-order concurrency for microcontrollers. MPLR 2020.
  Code - github.com/svenssonjoel/Sense-VM
- Cephalopode: A custom processor aimed at functional language execution for IoT devices. MEMOCODE 2020.
  Code - github.com/cjhseger/FP_HW
- Stately: An FSM Design Tool. MEMOCODE 2020.
  Code - github.com/popje-chalmers/stately
- Optimising Faceted Secure Multi-Execution. CSF 2019

Domain Specific Languages (DSL)

Data Privacy

Resources

Code

ate

DSL

V

Alejandro Russo

Mary Sheeran

Koen Claessen

Carl Seger

John Hughes

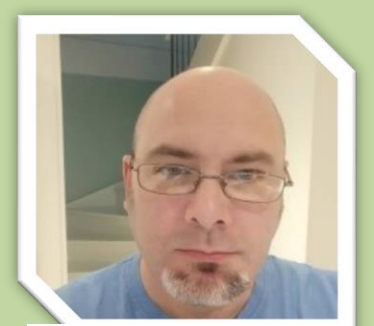
Nachiappan Valliappan

Jeremy Pope

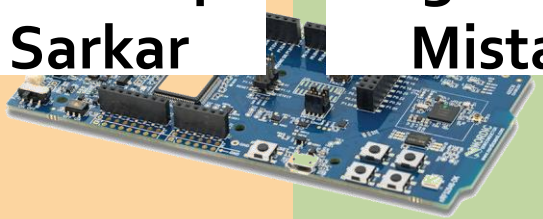
Abhiroop Sarkar

Agustín Mista

Robert Krook



Joel Svensson



Secure Hardware