cyberwatching.eu

The European watch on cybersecurity & privacy

Cybersecurity challenges in the IoT era

Webinar | December 11, 2019

Funded by the European Commission
Horizon 2020 – Grant # 740129

cyberwatching.eu

The European watch on cybersecurity & privacy

Using IoT platform security with mF2C to develop scalable secure edge-to-cloud applications

Funded by the European Commission
Horizon 2020 – Grant # 740129

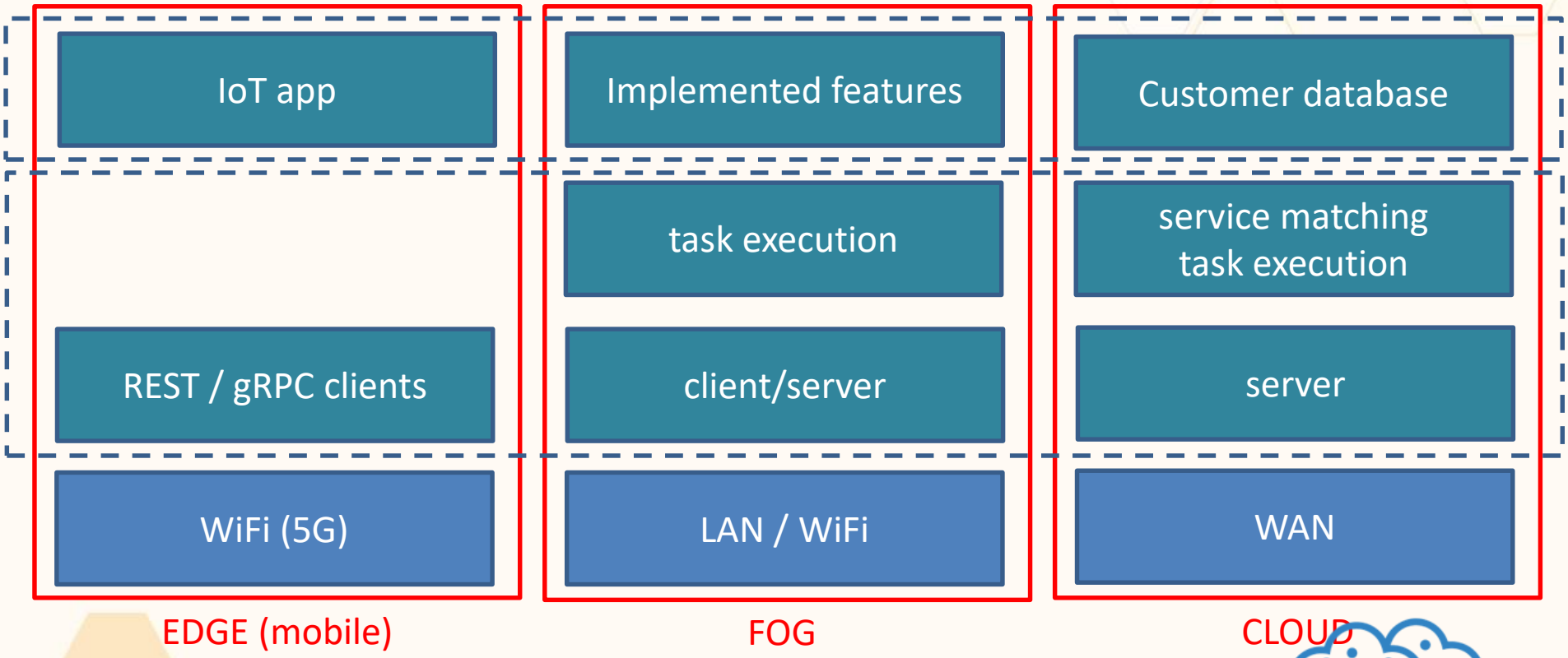
IoT Challenges

- Trust/Reputation of IoT
  - "Why should I trust this?"
- Legacy of IoT
  - Loads of insecure stuff already out there
- Barriers to building new applications
  - Have you ever programmed a microcontroller?
  - Limited devices (comp/mem/storage.)
- Keeping it secure
  - Potentially huge "attack surface"
  - Human factors, human bias

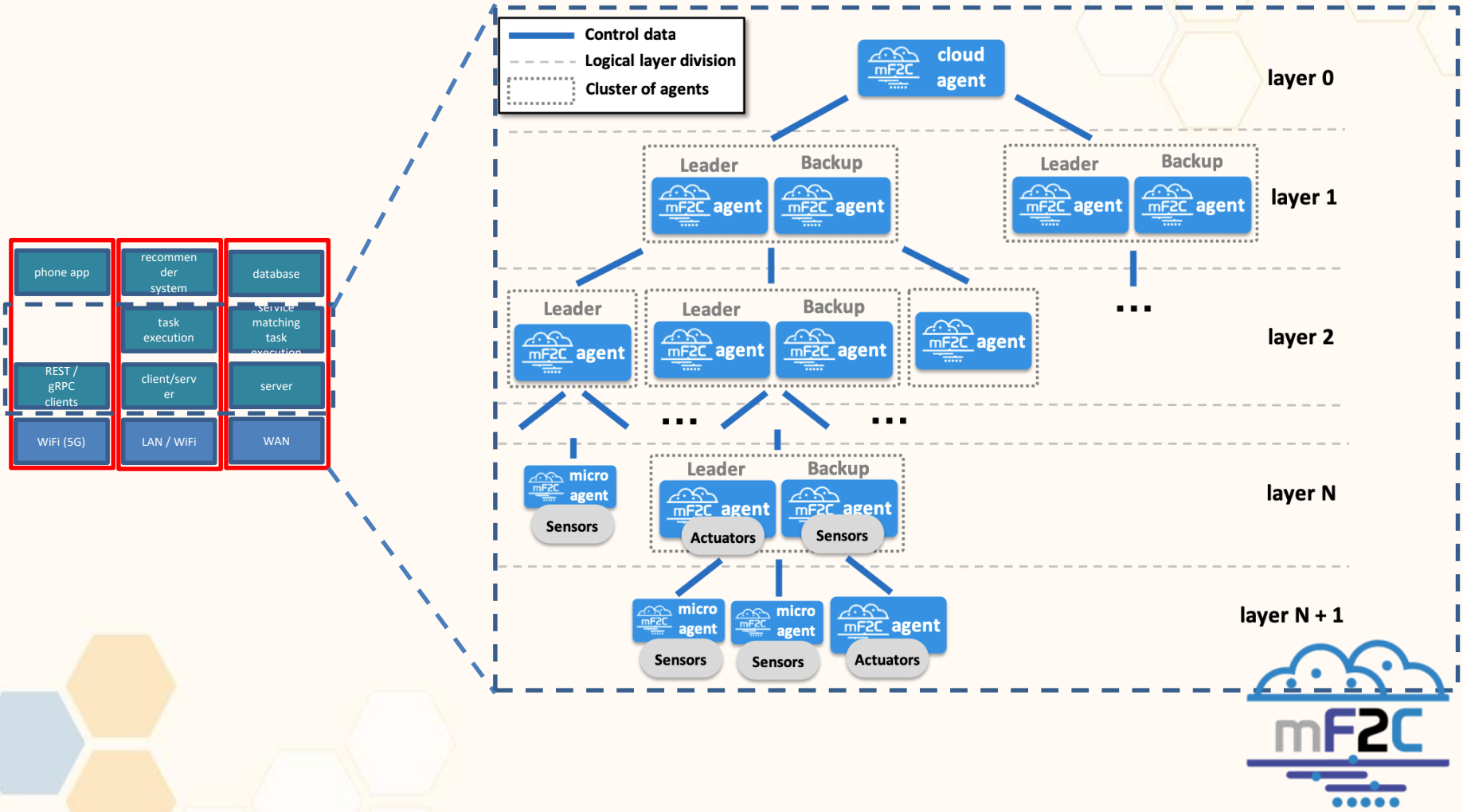
Platform Premises

- mF2C focuses on edge->fog->cloud applications
  - Tasks/data pushed to higher level if needed
- Build a *platform* for building applications
- Three use case applications:
  - Building sensors for emergencies (e.g. earthquakes)
  - Smart boats for boat sensor/location/harbour
  - Airport hub for traveller assistance

Generic Application
OSI (near enough) stack view



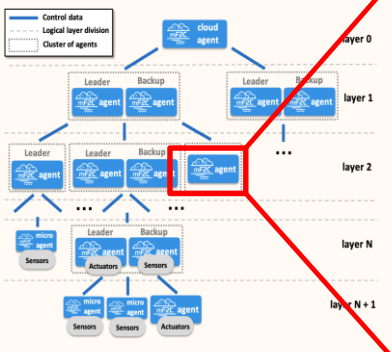
Platform Architecture



Security Features

- Usually, device == 1 agent
  - Or microagent for smaller devices
- Device id tracks device lifetime
- Certification Authority in the cloud
  - Certificates to capable (fog) devices
  - Private key generated by (capable) device
  - Gateway gives access to cloud service
  - No Internet access for unauthenticated devices
- Edgier devices have private (typ. a serial bus) link to foggier devices

Zooming in further



mF2C Agent

Platform Manager

Service Orchestration

- Lifecycle management
- SLA management

Service Management

- Categorization
- QoS Providing
- QoS Enforcement

Distributed Exec. Runtime

- Task Management
- Task Scheduling
- COMPSs
- Policies

Telemetry Monitoring

- Landscaper
- Recomender
- Analytics Engine

Agent Controller

Resource Management

- Discovery
- Policies
- Identification
- Categorization - Monitoring

User Management

- Profiling
- Sharing model
- Assessment

- Event Manager
- GUI

APIs: Docker | Kubernetes | Swarm | CIMI

Data Management: Dataclay

Security: Reverse Proxy | CAU Client | AC library

Addressing the challenges - Trust

- PKI for all participants
  - Distinct PKI roots for infrastructure and agents
  - Optionally distinct PKI for application
- CI/CD through Docker containers
- Trust model for security
- Application data
  - PUBLIC for unprotected
  - PROTECTED for integrity protected
  - PRIVATE for integrity and confidentiality

Addressing Challenges – Legacy

- mF2C builds entirely new applications, so no legacy?
- Some users bring own devices
- => botnet detection

- Early work on botnet detection
  - Distinguish attack from (say) emergency
  - Remote control of router/firewalls

Addressing Challenges - Barriers

- Build application on platform
  - … however, mF2C is a research project

:-)

- Open source
- High TRL on some components
- Lots of clever people adding lots of clever features
- Some code written by professional programmers and RSEs

:-(

- Platform has more features than a given app might need?
- Low TRL on some components
- Some code written by students rather than RSEs?

Addressing Challenges – Future

- mF2C updates through its CD framework
- Phone app (airport use case) through app store
- Edge hardware/firmware not addressed in project
  - (e.g. Azure Sphere..)
- Those pesky humans...
  - Make it easier to do the Right Thing
  - Need transparency for GDPR, too

Thanks!

- https://mf2c-project.eu/
- https://github.com/mF2C/

=> jens.jensen@stfc.ac.uk

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730929. Any dissemination of results here presented reflects only the consortium view. The Research Executive Agency is not responsible for any use that may be made of the information it contains.