Review Open Call F4Fp-SME-1

Cyberattack Readiness Assessment of IoT Platforms (CReAT)

Digiotouch

Soumya Kanti Datta

Digiotouch OU, Estonia

soumya@digiotouch.com

FEC5

Copenhagen, 24-25 April 2019

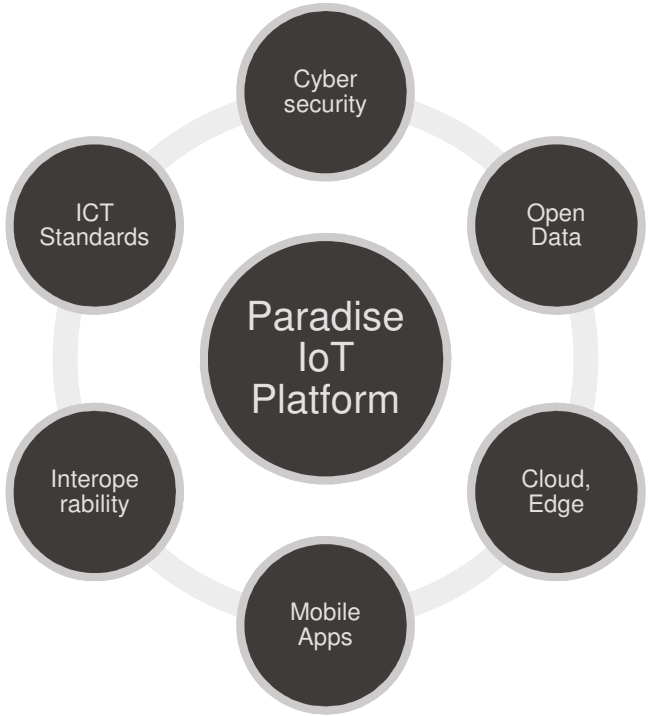
Outline

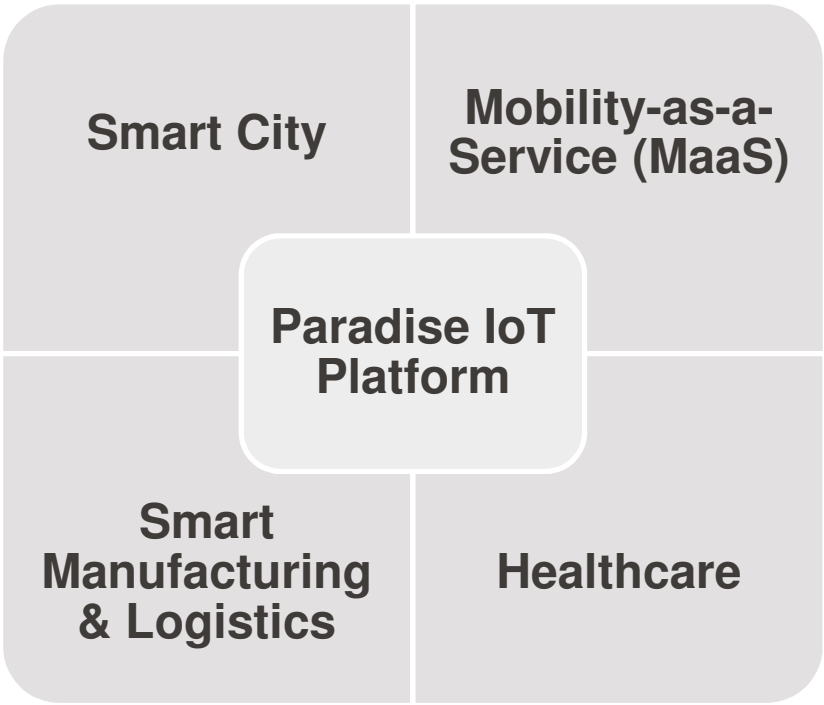
- Digiotouch description
- CReAT experiment description
- CReAT project results
- Business impacts
- Feedback
- Conclusion

Digiotouch Background

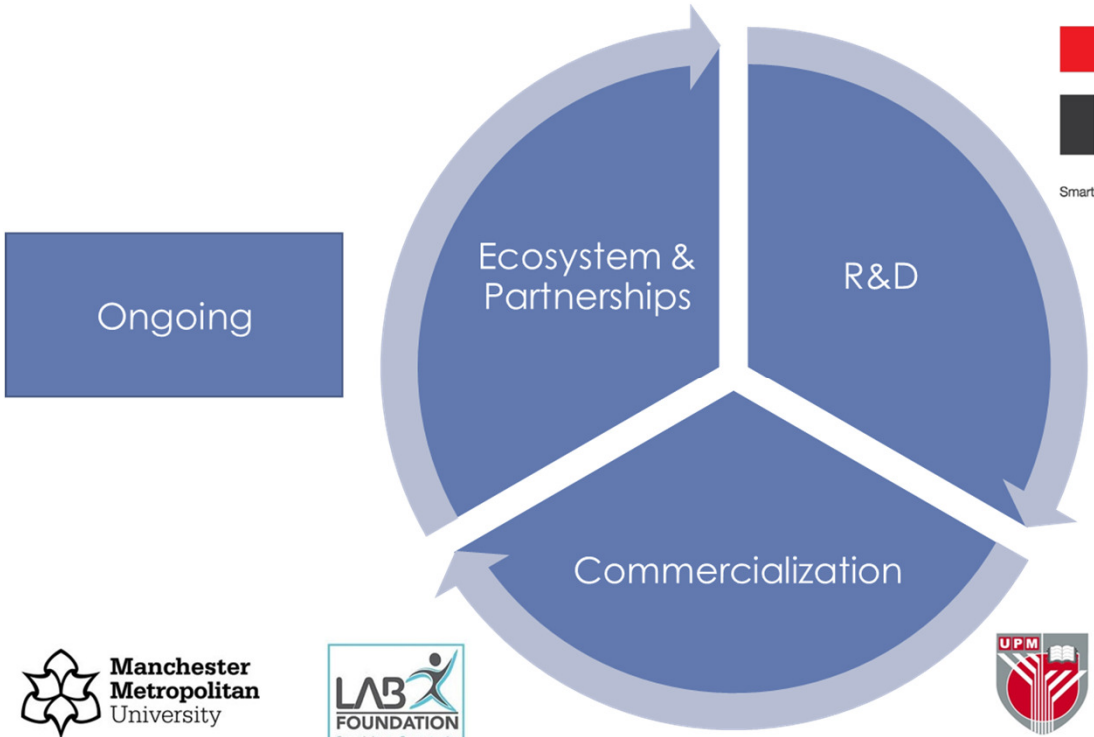
Digiotouch Core Business

- Sustainable and Secure Digital Transformation
  - Cloud based, secure, End-to-End Paradise IoT Platform





Digiotouch Operations



CReAT Experiment Description

Experiment Description (1/2)

Concept and objectives

1. The CReAT experiment is designed to develop a novel industrial solution in terms of a Cybersecurity framework to perform
    1. Cyberattack risk assessment of the IoT Platforms.
    2. Cyberattack resilience readiness.
2. Test Cyberattack resilience readiness of Digiotouch's Paradise IoT Platform by launching three simulated and known cyberattacks -
    1. DDoS
    2. Insufficient authentication/authorization
    3. Insecure Cloud web services

Experiment Description (2/2)

Background

- IoT devices and Platforms are increasingly targeted with Cyberattacks.
    - Q3 2017 saw enterprises experiencing an average of 237 monthly DDoS attacks.
    - How to increase Cyber resilience of IoT infrastructure.
    - DT's Paradise IoT Platform experienced service outage through DDoS.

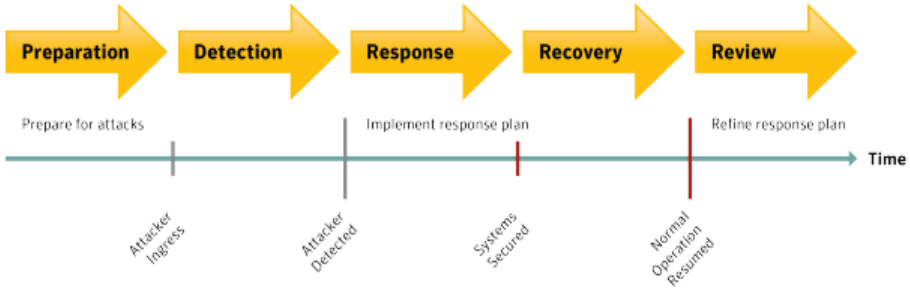
Motivation

- Provide state-of-the-art Cybersecurity in the Cloud based Paradise IoT Platform.
- Protect DT and its customers IoT assets from Cyberattacks.
- Strengthen brand value of DT in IoT market.

CReAT Cybersecurity Framework

Cybersecurity Risk Assessment

Cyberattack resilience

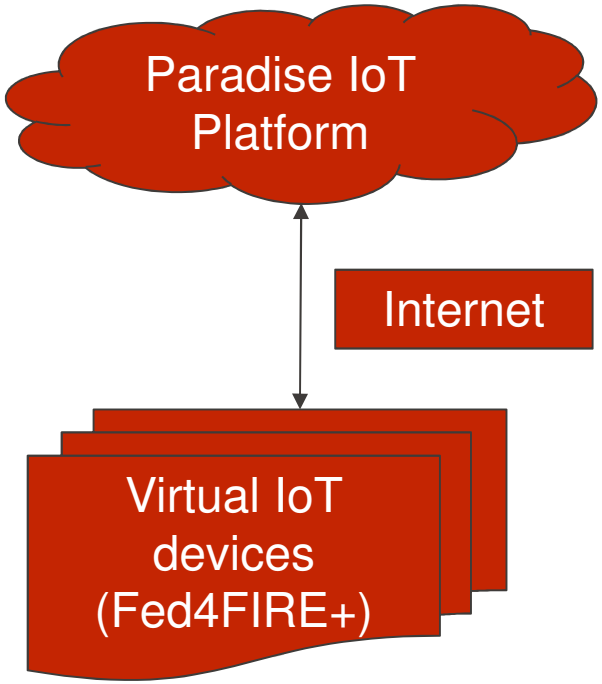


Cyberattack resilience readiness

- Readiness is measured in % of completion of above five steps.

Experiment Setup

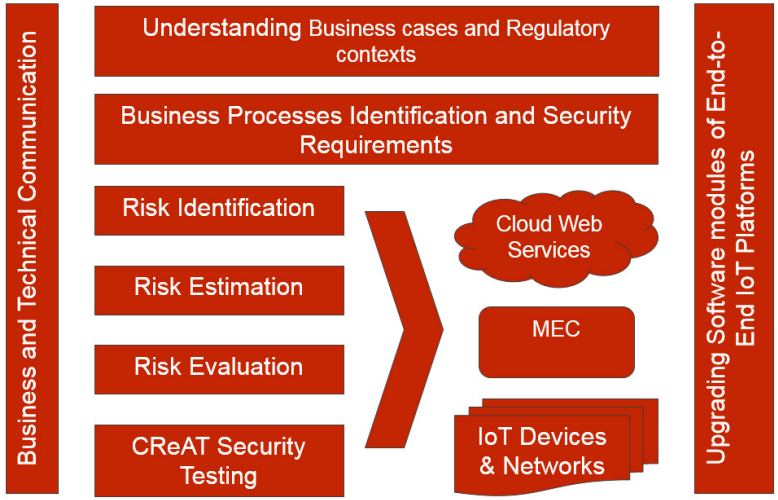
Experiment Architecture



Project Results

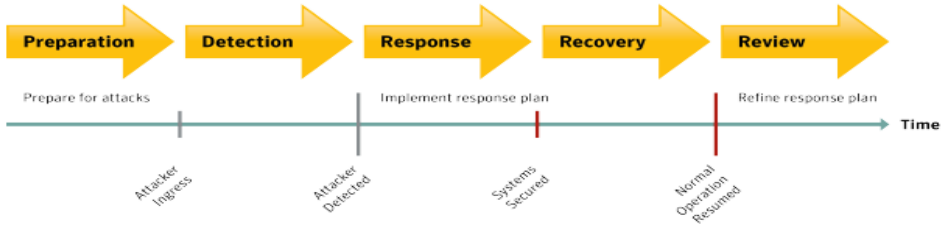
CReAT Experiment Results (1/2)

CREAT FRAMEWORK



TWO MAIN ASPECTS

- Risk Assessment
  - Performed on Paradise IoT Platform
- Cyber resilience
  - Five steps



CReAT Experiement Results (2/2)

LESSONS LEARNT

- DT's Cloud based Paradise IoT Platform is secure by design to withstand
  - Insecure authentication and authorization attack.
    - This is accomplished using a combination of JSON Web Token (JWT) and middleware validatiing the token before allowing access to Paradise web services.
  - Insecure web services
    - Currently all nine web services are secure by design.
  - DDoS
    - With ~100 IoT devices sending 1mbps traffic is sufficient to bring down the Cloud based web services.
    - DT is working on a DDoS attack mitigation plan with the Cloud Infrastructure provider.

Business Impacts

Business Impact (1/5)

UPGRADED PRODUCT AND SERVICES

- DT's Cloud based Paradise IoT Platform has been upgraded with the developed Cybersecurity framework.
    - Cloud infrastructure to be upgraded soon to combat DDoS attacks.
    - Web services are secure by design.

Business Impact (2/5)

BUSINESS DEVELOPMENT

- Two potential customers
    - Brettex (UK) – connecting water resources
    - Universiti Putra Malaysia – smart campus use case
- DT to launch a paid MOOC on Cybersecurity
    - Target Q3 2019
    - Additional revenue stream

Business Impact (3/5)

SUSTAINABILITY

- Upgraded Paradise IoT Platform
    - Commercialization through IoT market and Cybersecurity training.
- Ongoing EU H2020 Projects
    - ACTIVAGE project open call – AMICA (Feb 2019 – Jan 2020)
- Upcoming H2020 and Horizon Euorpe Calls
    - Two open call proposals submitted
    - One H2020 proposal submitted (MG-4-5-2019)

Business Impact (4/5)

VALUE PERCEIVED

- Upgrading DT's main product – Paradise IoT Platform
- Business development
- Availability of Testbed infrastructures

WHY FED4FIRE+

- Support in terms of
  - Federation of Testbeds available through single account
  - Grant for successful experiments
  - Technical aspects

Business Impact (5/5)

HOW FED4FIRE+ HELPED DT?

- Financial grant to support the experiment.
- Experimentally validating that Paradise web services are secure by design.
- Technical support during experimentation phase.
- Support for Stage 2 preparation (Ongoing).

Feedback

Feedback to Fed4FIRE+ (1/4)

PROCEDURE / ADMINISTRATION

- The administration procedures including writing documents, feedback, and performing experimentation in Fed4FIRE+ infrastructure have been apt in terms of the timeframe of the experiment.
- Suggestion
    - DT would like to have an opportunity to present the experiment in FEC5/FEC6 for a wide dissemination.

Feedback to Fed4FIRE+ (2/4)

EXPERIMENT SETUP

- Very minimal effort required to set up and run the experiment for the first time.
- **Excellent assistance from Ugent.be (Brecht Vermeulen) during the experiment.**
- Documentation in Fed4FIRE+ website are covering all aspects relevant for the experiment.
- Issue – Technical challenges with creating virtual devices, NAT.
    - Solved with technical help.

Feedback to Fed4FIRE+ (3/4)

TESTBED CAPABILITIES

- The Testbed capabilities are sufficient to run the CReAT experiment.
- Virtual Wall is relevant as other Testbed devices only allow «reading» measurements using APIs.
    - **Virtual Wall** allows creating virtual IoT devices which are essential to push data to the Paradise IoT Platform.

Feedback to Fed4FIRE+ (1/4)

SUPPORTING SMES

- Such Testbeds are ideal for early stage companies and SMEs who can validate many prototypes, protocols, security aspects before commercializing a technology.
- Even if Fed4FIRE+ is charging a fee to utilize the Testbeds, DT will continue to utilize them.

Conclusion

Conclusion

CREAT HAS BOTH TECHNICAL AND BUSINESS IMPACTS

- Upgraded Cloud based Paradise IoT Platform
- Business development with new customers and revenues
- Help building an ecosystem around Paradise
- DT to continue to utilize Fed4FIRE+
- Ongoing – preparation for Stage 2

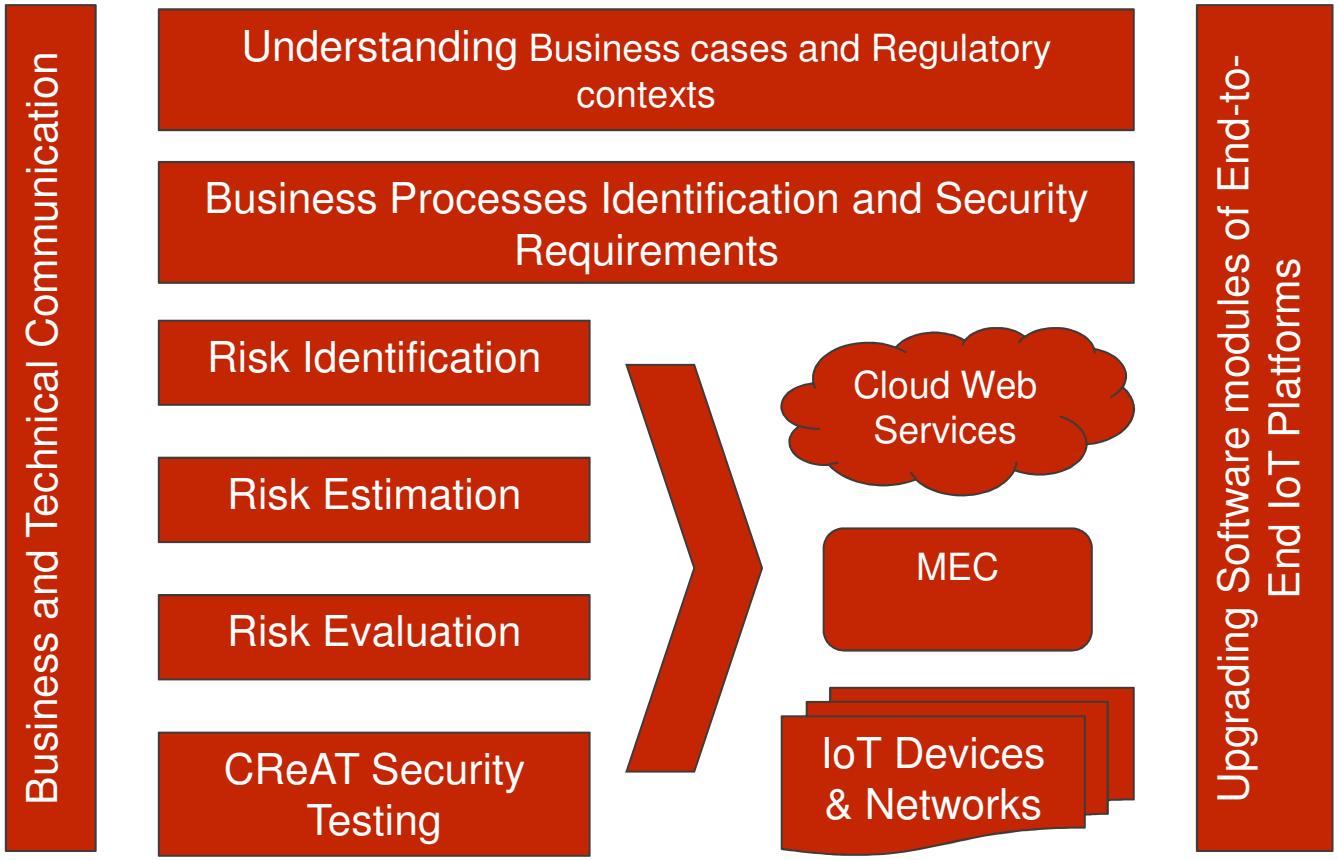

Co-funded by the European Union


Co-funded by the Swiss Confederation

This project has received funding from the European Union's Horizon 2020 research and innovation programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under grant agreement No 732638.

THANK YOU

WWW.FED4FIRE.EU


Business and Technical Communication
Understanding Business cases and Regulatory contexts
Business Processes Identification and Security Requirements
Risk Identification
Risk Estimation
Risk Evaluation
CReAT Security Testing
Cloud Web Services
MEC
IoT Devices & Networks
Upgrading Software modules of End-to-End IoT Platforms