manySECURED

Collaborative Intelligent IoT Gateway

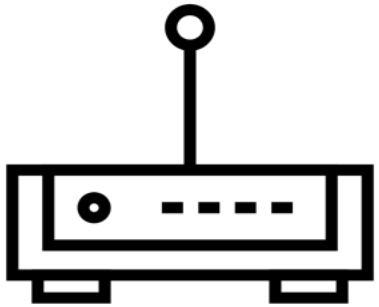
Duncan Purves & Nick Allott

https://manysecured.net/

COLLABORATIVE INTELLIGENT GATEWAY

Innovation at the Gateway

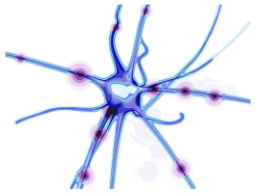
ManySecured's aim is to secure the Internet of Things through security innovation at the gateway.



To better protect consumers and enterprise from the security risks posed by IoT devices

MANYSECURED PROJECT PARTNERS

Security innovation at the gateway



nquiringminds

ai • security • iot

CISCO

IoT Security Foundation

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

Supported by

UKRI Innovate UK

A BOLTED HORSE

Looking at the number of insecure devices already out there

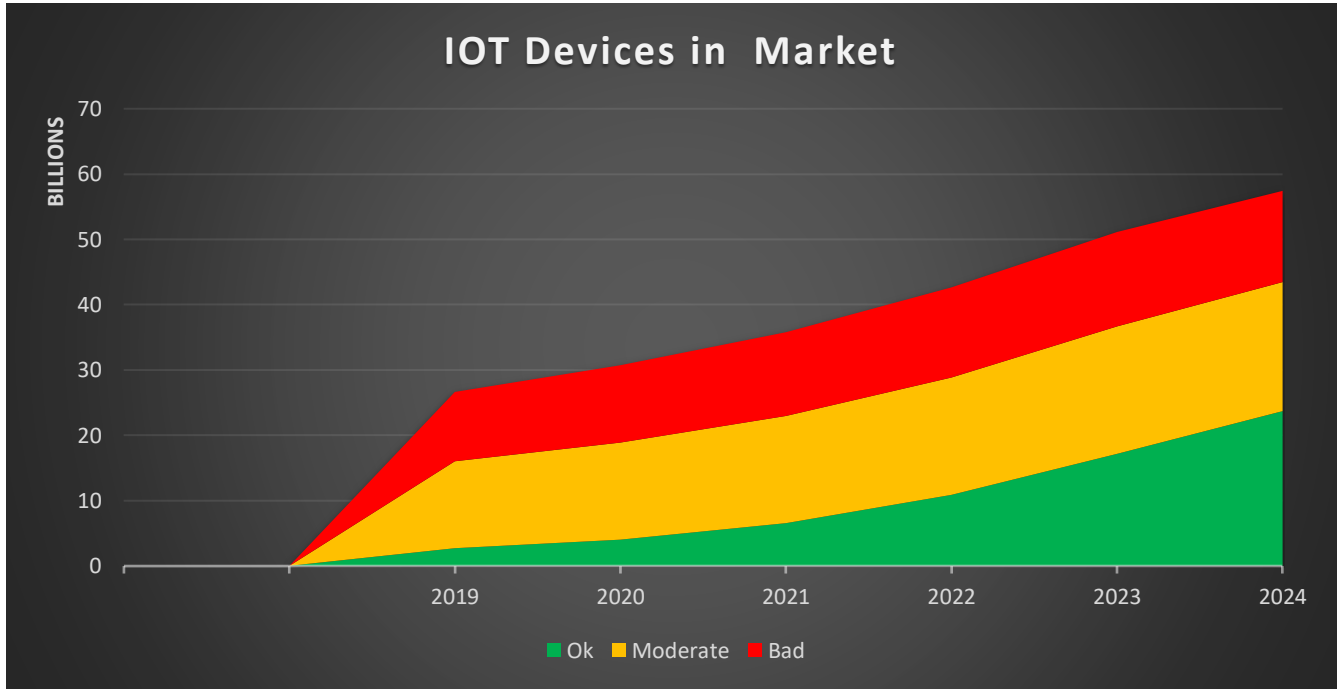
Key assumptions

IOT market growth – **57 Bn** by 2024
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

A spectrum of IOT security quality shifting over time

New device security quality %	2019	2020	2021	2022	2023	2024
Ok	10%	20%	30%	40%	50%	60%
Moderate	50%	45%	40%	35%	30%	25%
Bad	40%	35%	30%	25%	20%	15%

A yearly Churn rate of **20%**



MANYSECURED FEATURES

Key principles

manySECURED

FOUNDATIONS

How do you implement the internals of a secure gateway? Secure storage, secure boot, software verification methods. Defines the underlying foundation security.

SECURE COMMS

How do IOT devices communicate securely on an internal network? Key distribution, user interface, secure local connections.

UPDATE MANAGEMENT

How do you know an IOT device needs updating? How can you manage the process easily. Remote device type identify. Simplified update user interface

THREAT DETECTION

How can you identify threat before or soon after compromise? Defining flexible methods of intelligent detection and subsequent control

MONITORING

How can you monitor IOT activity across IP and NonIP networks? Low level device activity summaries. Creation of behavioural fingerprints.

NETWORK ISOLATION

How can you restrict the IOT attack surface, incoming and outgoing? Define practical methods of segmenting and isolation network activity

SMART CONTROL

How can you locally and dynamically control the internal network? Defining simile interoperable standards for network control to increase security.

COLLABORATION

How do we share information? Smart threat detection needs high quality data in volume. This will only come through industry collaboration on activity and threats.

Ecosystem Initiation Report

Maps out the context in which the ManySecured project will be need to be accepted

- Industry Stakeholders
- Market
- Standards

Makes recommendations as to:

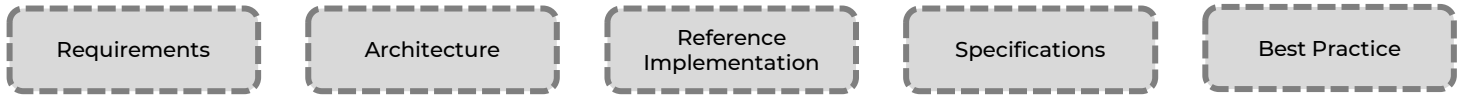
- Best possible approach to adoption/standardisation
- Prioritised set of stakeholders that IoT Security Foundation will need to engage with to ensure project's success

NEXT STEPS

Collaboration, interoperability and engagement are key to success

WHO: Engage with IoT Gateway OEMs, ODMs and Industry Stakeholders

WHAT:



START: with priority areas

- Device activity fingerprinting
- Network isolation
- Threat detection…

MY ASK

Collaboration, interoperability and engagement is key to success

Please contact me if:

You are or have contacts at Gateway OEMs/ODMs

Are interested in and would like to get involved with this project

duncan.purves@iotsecurityfoundation.org

Questions

duncan.purves@iotsecurityfoundation.org