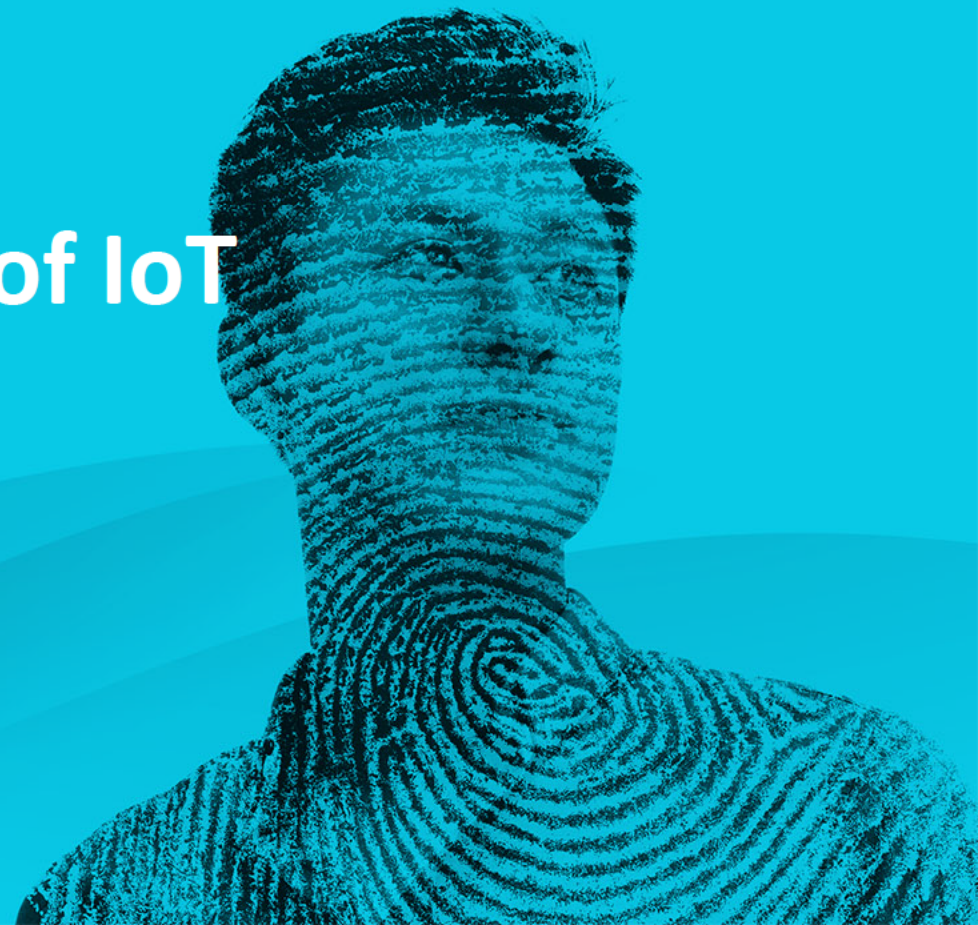
RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: CMI-W02V

20/20 Security Vision: Managing Digital Risk in the Era of IoT



Arthur Fontaine

Solution Strategist
RSA
@arthurfontaine

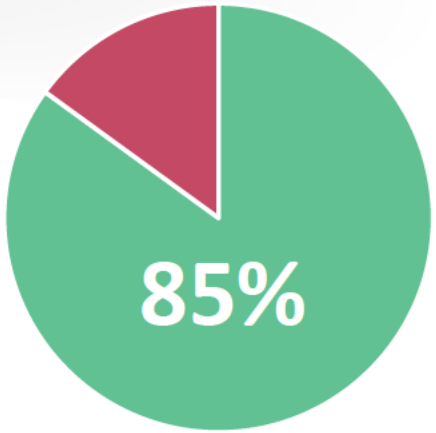
IoT Market Is Exploding

25 billion

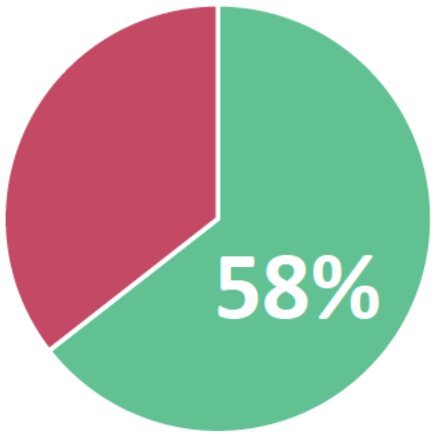
Devices by 2025

$1.1 trillion

IoT Devices Market by 2026



Have IoT project budgets



Report well-developed IoT initiatives

152,200

IoT devices added per minute by 2025

Digital Risk in the IoT

IoT delivers benefits with specific challenges and risks

Breadth of IoT Categories

- **Industrial Internet of Things (IIoT)**
  Networked machines in a production facility to improve efficiency, productivity, and performance
- **Internet of Medical Things (IoMT)**
  Collect and send patient health statistics to health care providers for monitoring, analysis, and remote configuration
- **Smart Cities**
  Central control system to optimize production and distribution to meet demand in real time
- **Smart Homes**
  Smart appliances, TVs, entertainment systems, thermostats, and network connected light bulbs, outlets, door locks, door bells, and home security systems

Policy Issues

- **Regulatory Issues**
  Regulation of IoT may entail policies for deconfliction, harmonization, and/or expansion of agency jurisdictions
- **Digital Privacy Issues**
  Increased data collection and usage may yield innovation, technological progress, and improved utility, but could also lead to the erosion of privacy and data exploitation without consent
- **Data Security Issues**
  As more devices become connected to one another and to the internet, the risk and impact of a compromise increase, along with the possibility of a cascading cyberattack

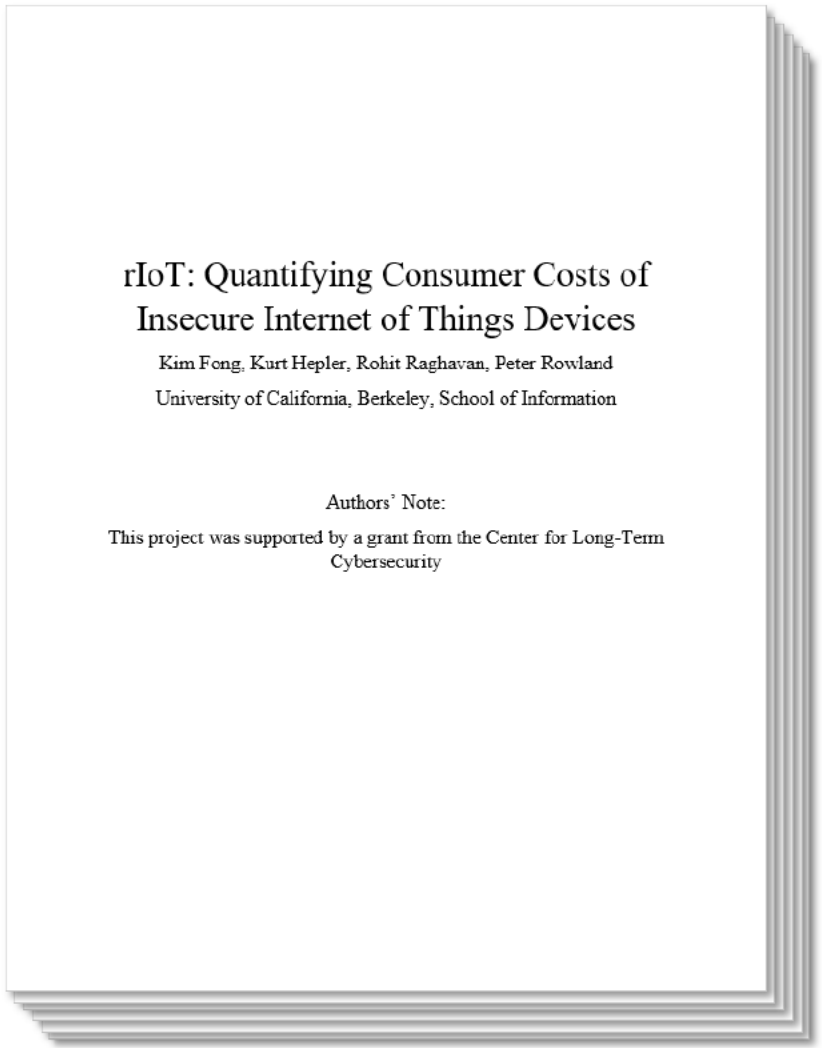
https://crsreports.congress.gov/product/pdf/IF/IF11239

Critical Digital Risks

IoT Digital Risk Impacts

- Mitigate Cyber Attack Risk
- Manage Third Party Risk
- Manage Dynamic Workforce Risk
- Secure Your Cloud Transformation
- Evolve Data Governance & Privacy
- Coordinate Business Resiliency
- Manage Process Automation Risk
- Modernize Your Compliance Program

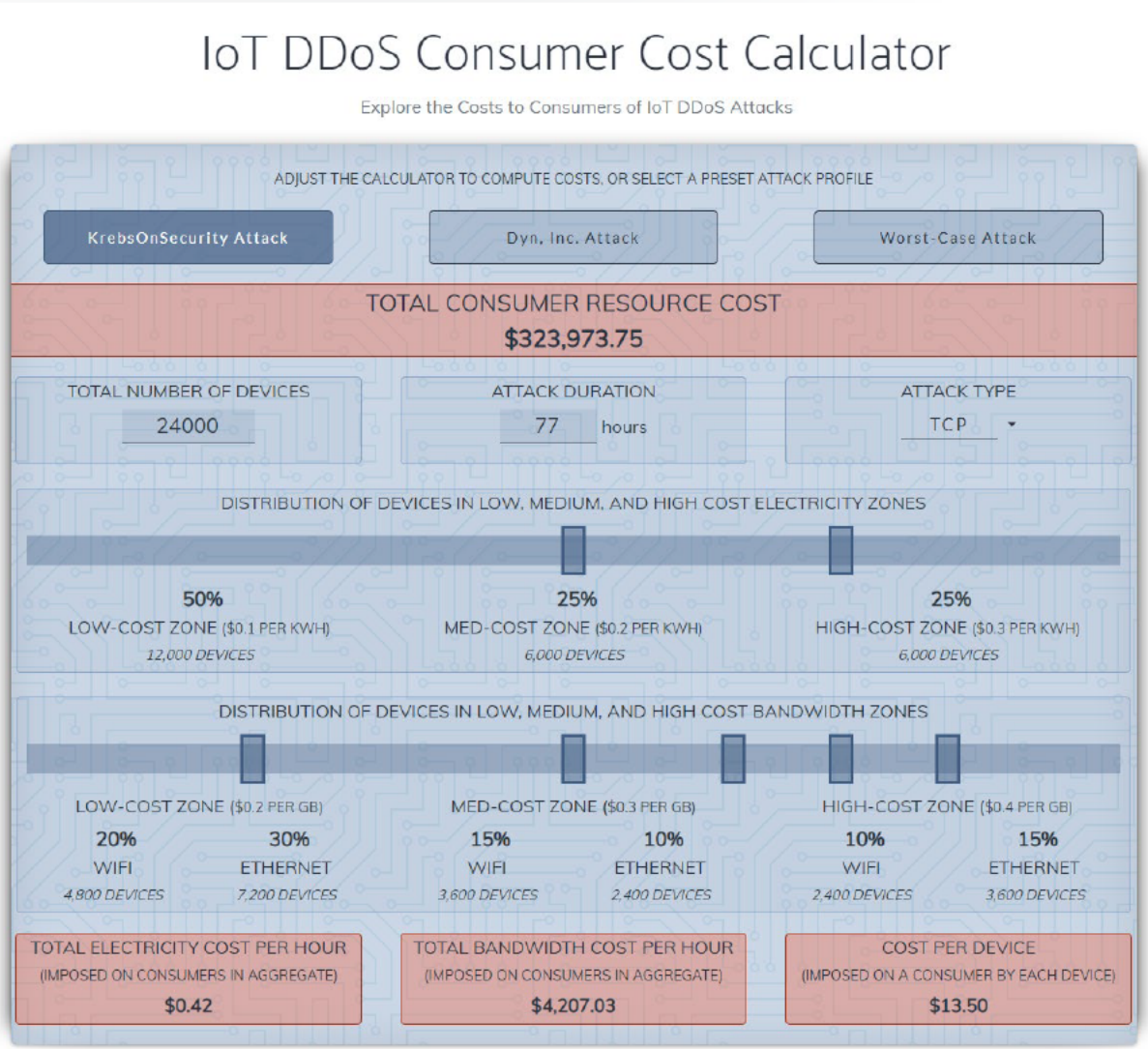
Costs go beyond DDOS targets



rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices

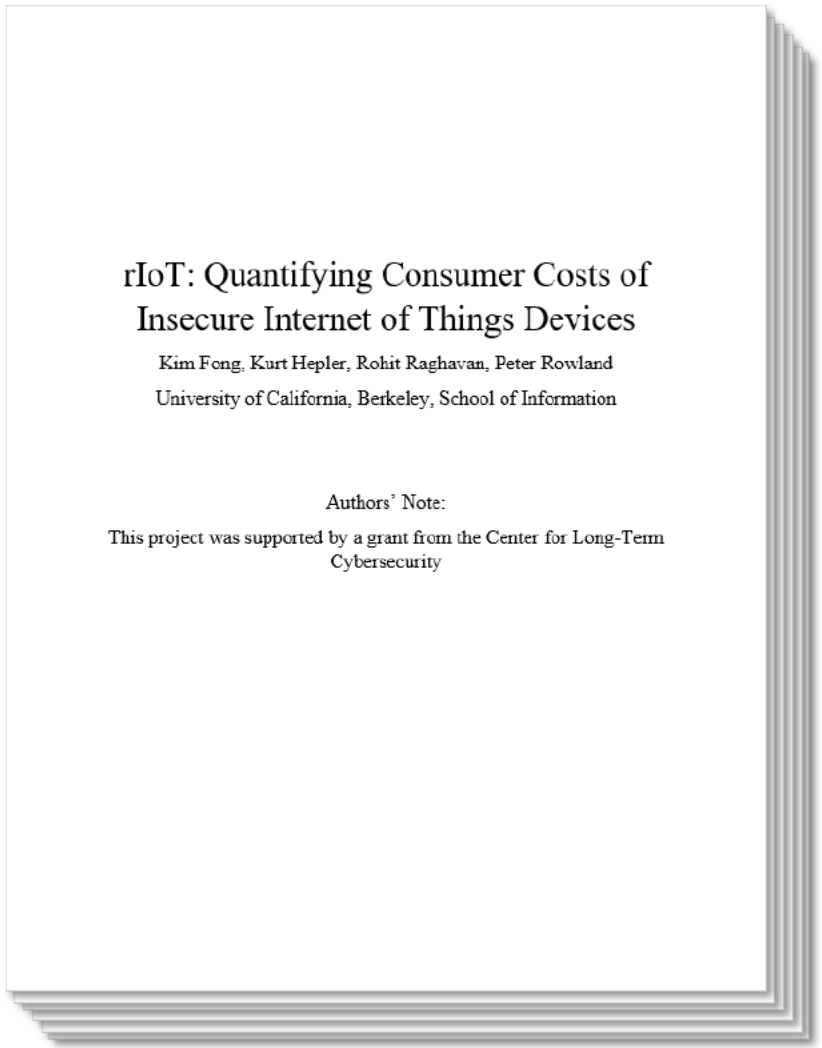
Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland
University of California, Berkeley, School of Information

Authors' Note:
This project was supported by a grant from the Center for Long-Term Cybersecurity



https://groups.ischool.berkeley.edu/riot/

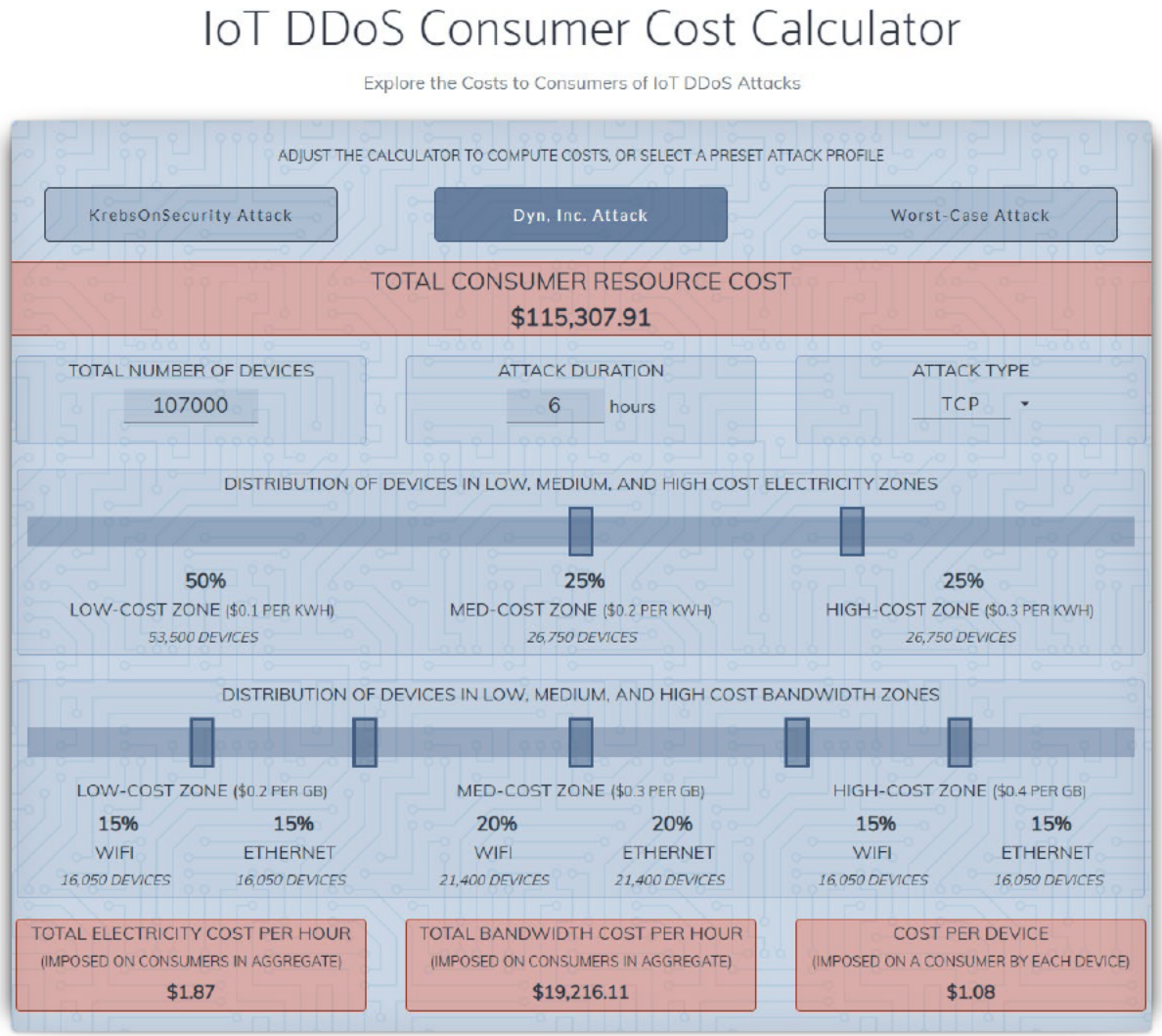
Costs go beyond DDOS targets



rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices

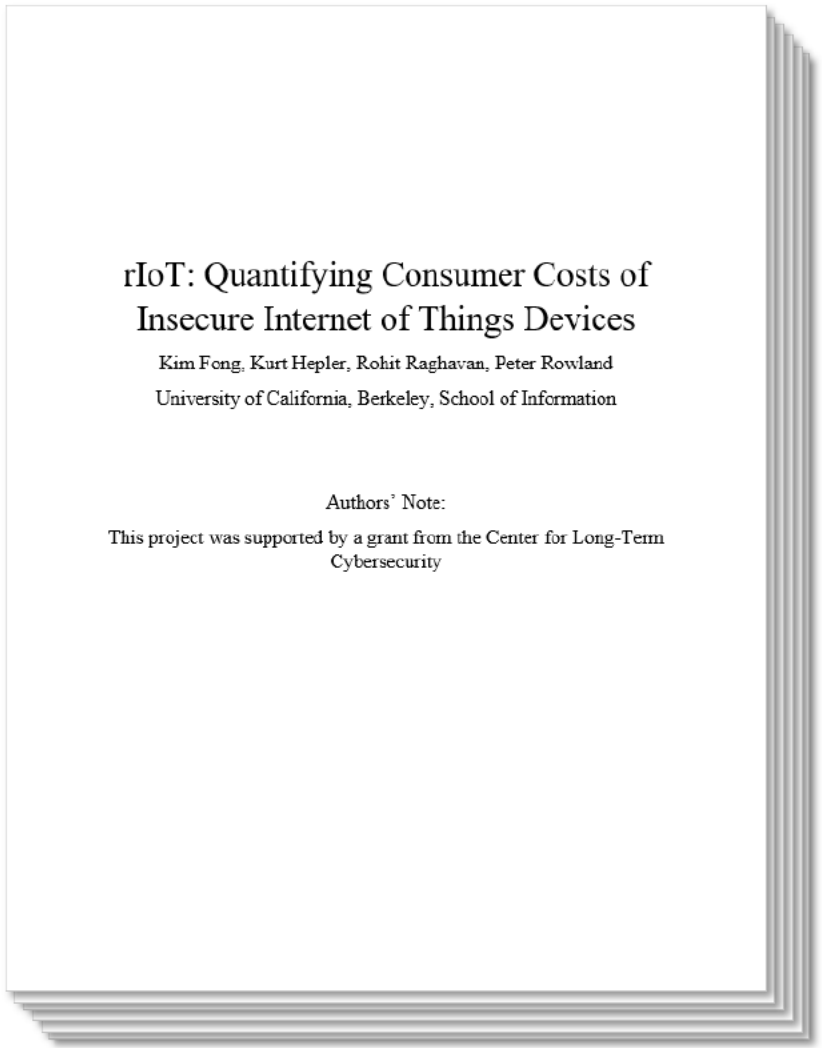
Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland
University of California, Berkeley, School of Information

Authors' Note:
This project was supported by a grant from the Center for Long-Term Cybersecurity



https://groups.ischool.berkeley.edu/riot/

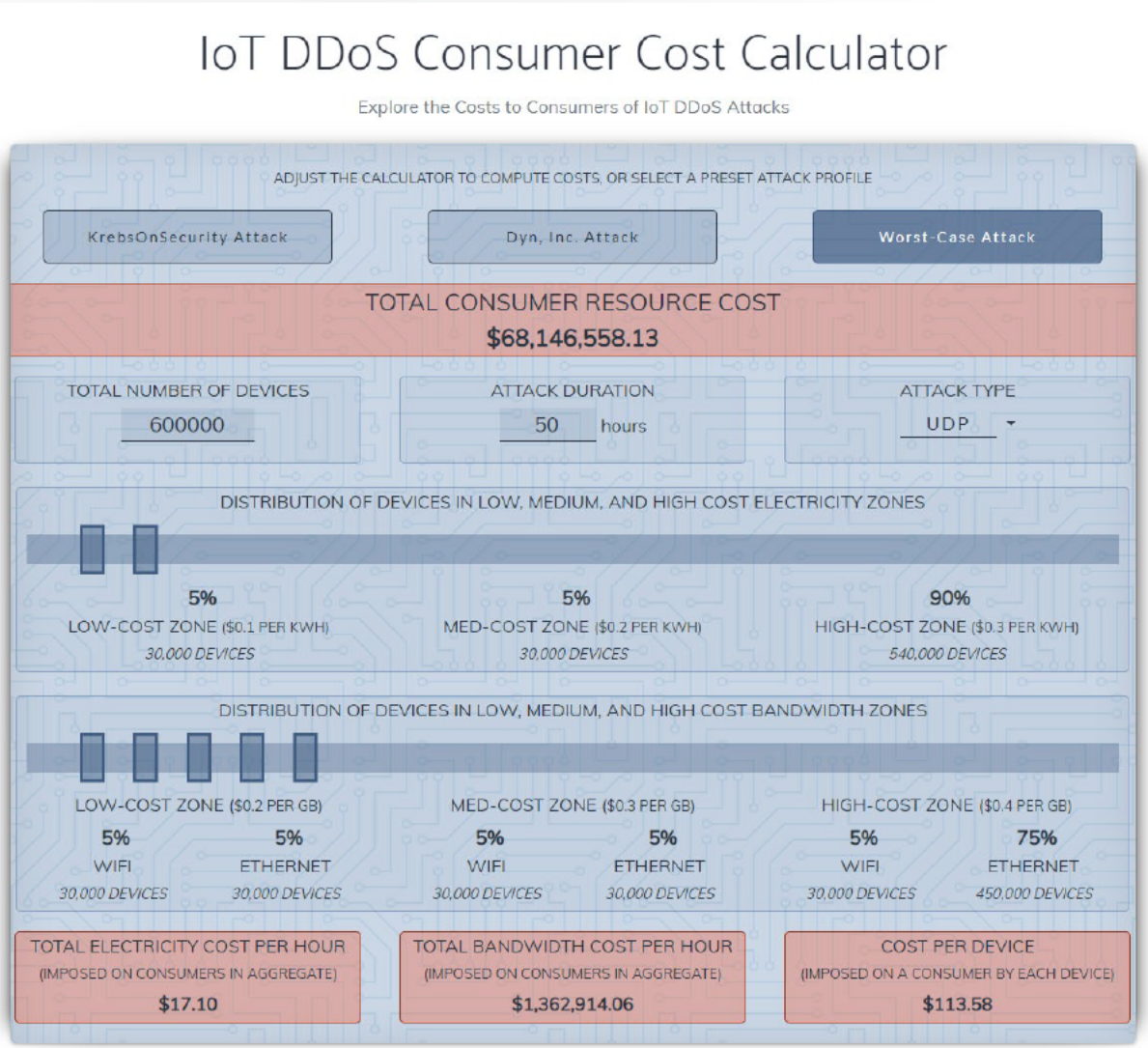
Costs go beyond DDOS targets



rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices

Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland
University of California, Berkeley, School of Information

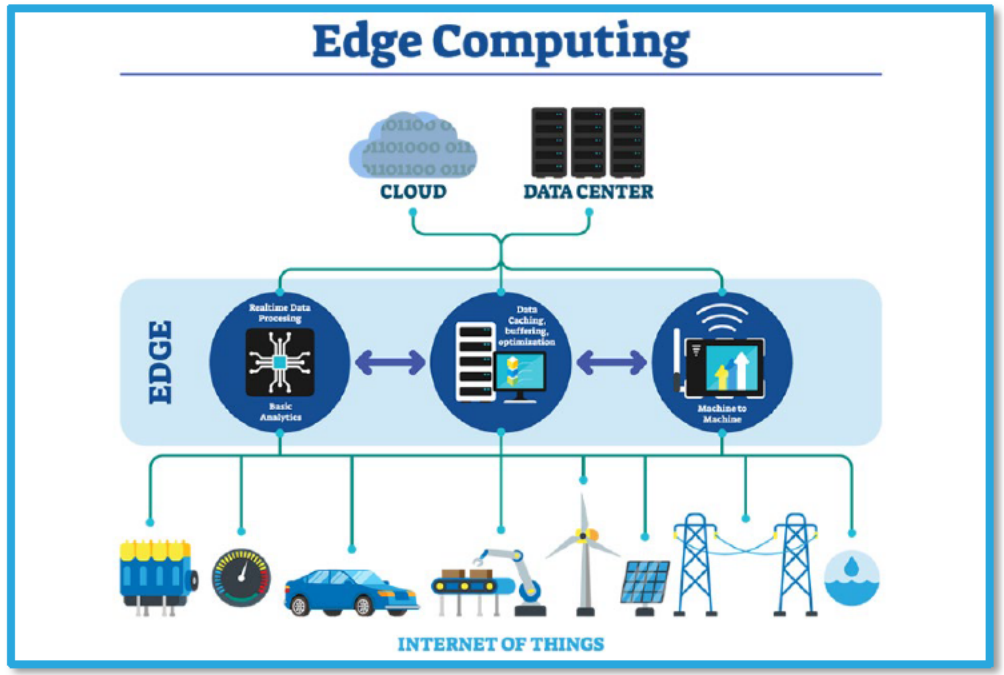
Authors' Note:
This project was supported by a grant from the Center for Long-Term Cybersecurity



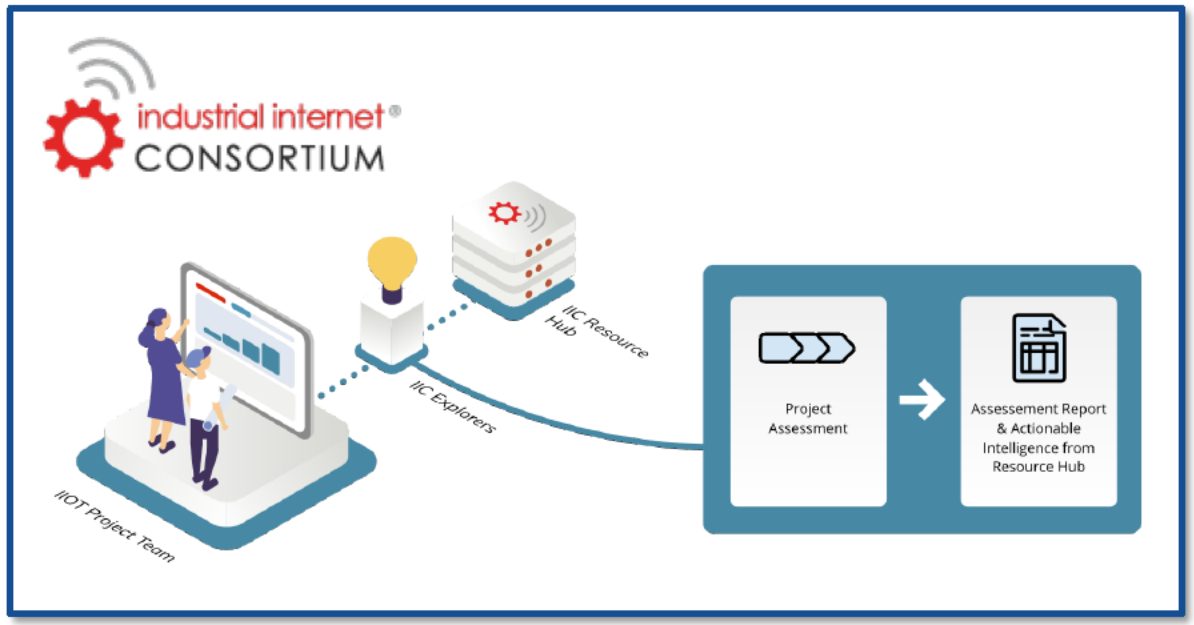
https://groups.ischool.berkeley.edu/riot/

Two Critical IoT Evolutions

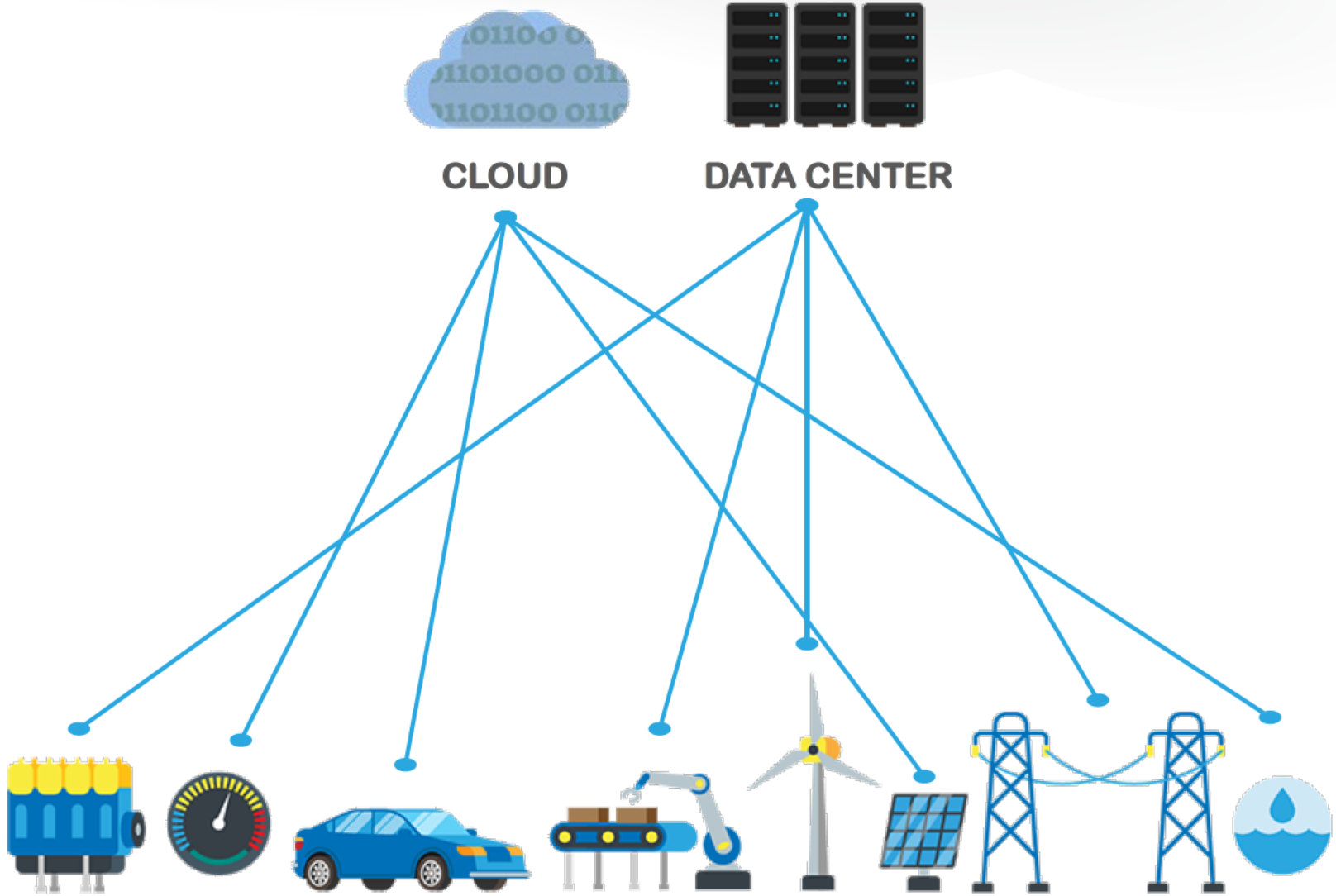
Edge Computing



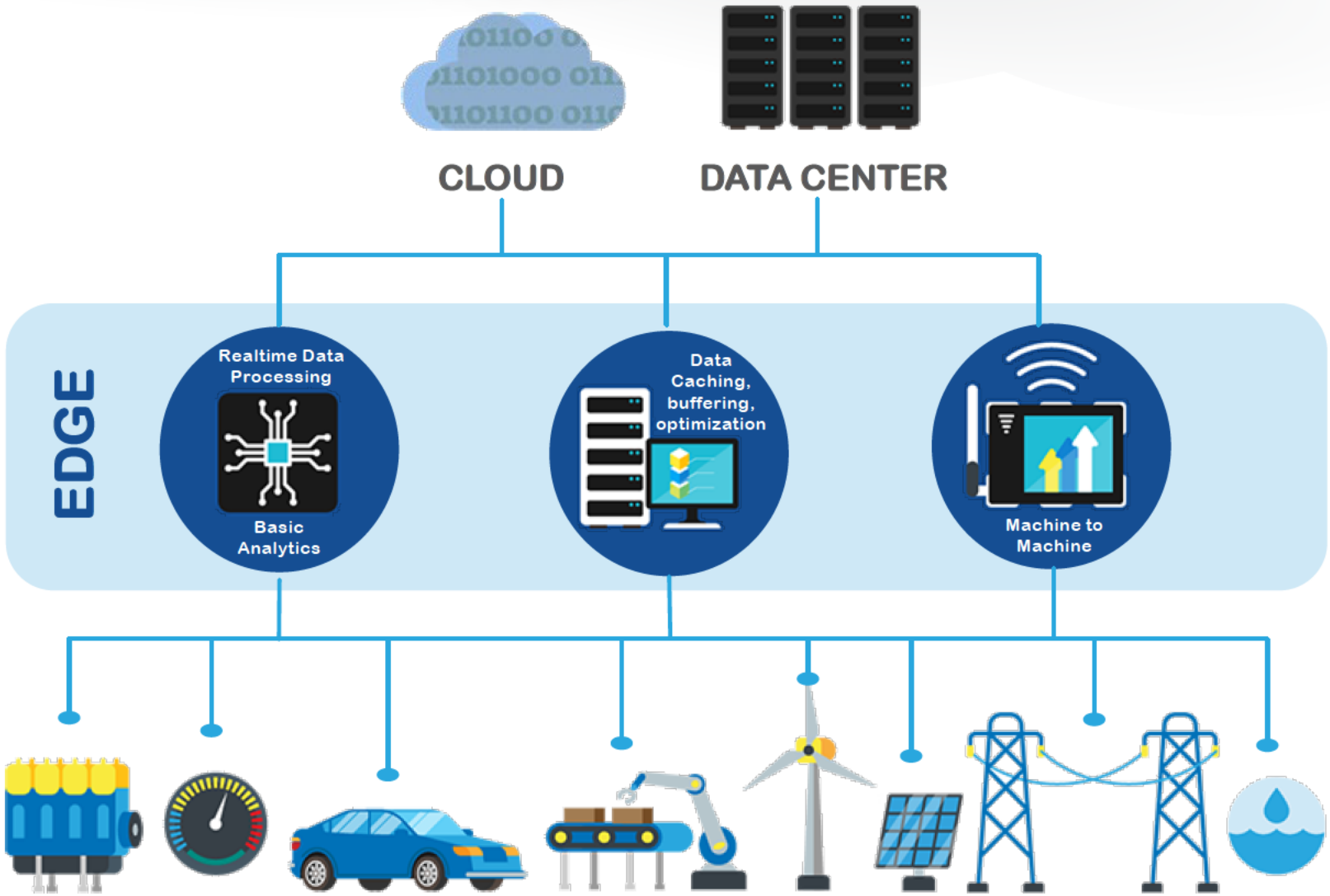
Standards and Frameworks



Edge Computing



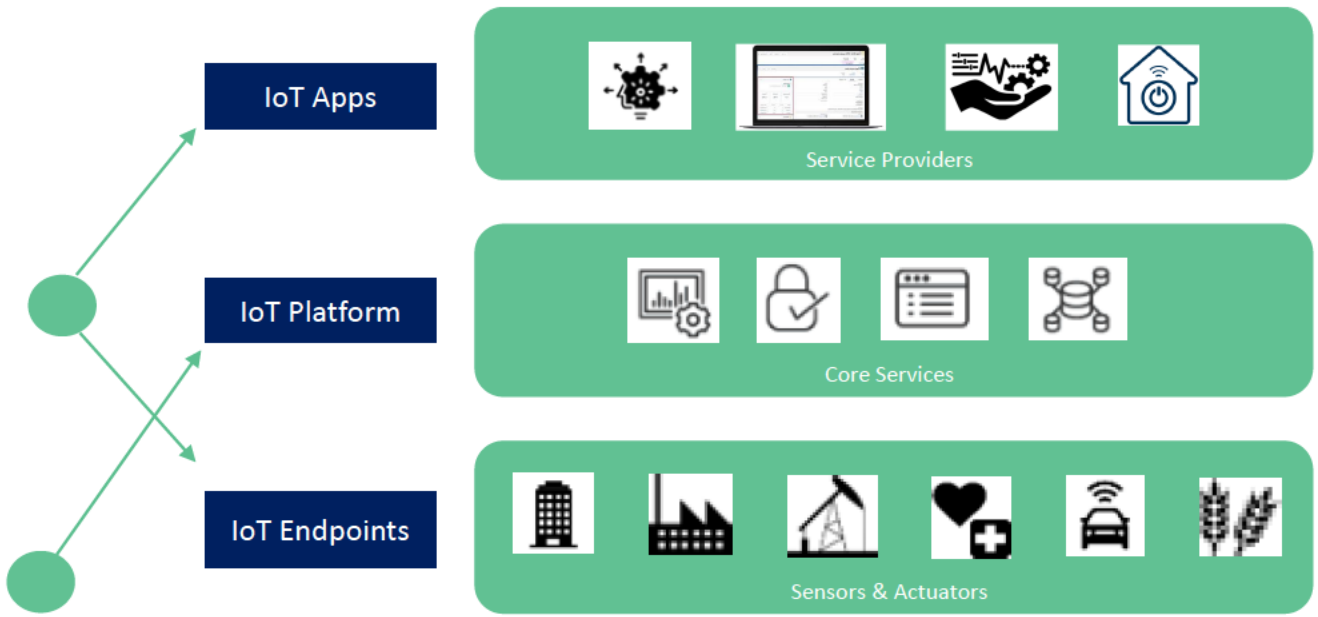
Edge Computing

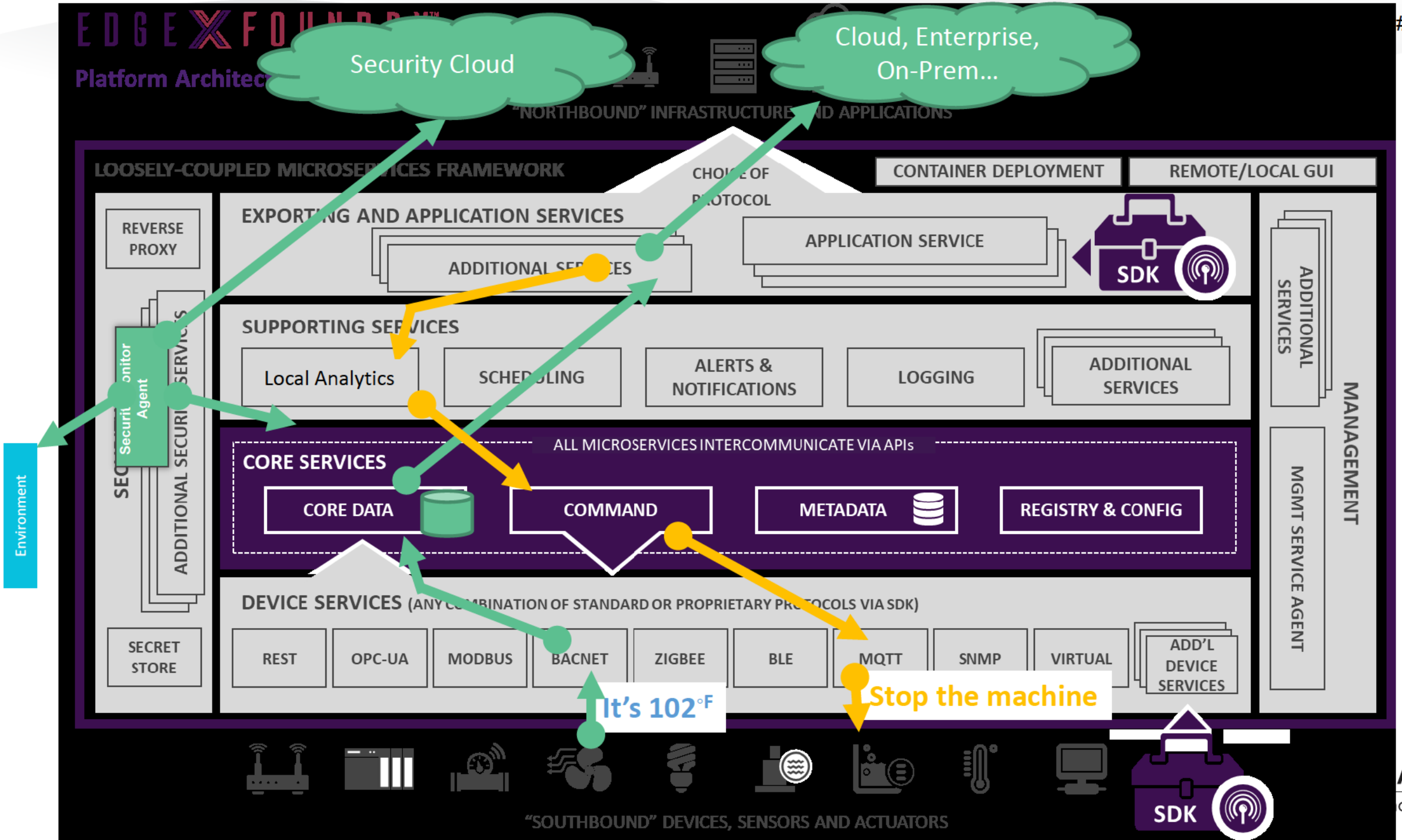


The Anatomy of an IoT Solution

What is an IoT Platform?

- IoT is a transformative force driven by convergence of the physical and digital worlds, bridging Operational Technology (sensors, actuators) and Information Technology
- An IoT Platform provides the critical middle layer, enabling core services such as data management, device management, security, etc.
- Partnerships emerge between OT experts, such as IoT platform vendors and specialized vendors to fill out feature/function and security




EDGE X FOUNDRY™
Platform Architecture
Security Cloud
Cloud, Enterprise, On-Prem…
"NORTHBOUND" INFRASTRUCTURE AND APPLICATIONS
LOOSELY-COUPLED MICROSERVICES FRAMEWORK
CONTAINER DEPLOYMENT
REMOTE/LOCAL GUI
REVERSE PROXY
EXPORTING AND APPLICATION SERVICES
CHOICE OF PROTOCOL
ADDITIONAL SERVICES
APPLICATION SERVICE
SDK
SUPPORTING SERVICES
Local Analytics
SCHEDULING
ALERTS & NOTIFICATIONS
LOGGING
ADDITIONAL SERVICES
Security Agent
ADDITIONAL SECURITY SERVICES
ALL MICROSERVICES INTERCOMMUNICATE VIA APIs
CORE SERVICES
CORE DATA
COMMAND
METADATA
REGISTRY & CONFIG
Environment
DEVICE SERVICES (ANY COMBINATION OF STANDARD OR PROPRIETARY PROTOCOLS VIA SDK)
SECRET STORE
REST
OPC-UA
MODBUS
BACNET
ZIGBEE
BLE
MQTT
SNMP
VIRTUAL
ADD'L DEVICE SERVICES
ADDITIONAL SERVICES
MGMT SERVICE AGENT
MANAGEMENT
It's 102°F
Stop the machine
SDK
"SOUTHBOUND" DEVICES, SENSORS AND ACTUATORS

Standards and Frameworks

Standards and Frameworks

NISTIR 8259A
IoT Device Cybersecurity Capability Core Baseline
Identifies a core baseline of IoT device cybersecurity capabilities for manufacturers

NISTIR 8259
Foundational Cybersecurity Activities for IoT Device Manufacturers
Specific activities to help manufacturers address customer IoT cybersecurity in product development processes.

Standards and Frameworks

MQTT (MQ Telemetry Transport)

A machine-to-machine (M2M) IoT connectivity protocol

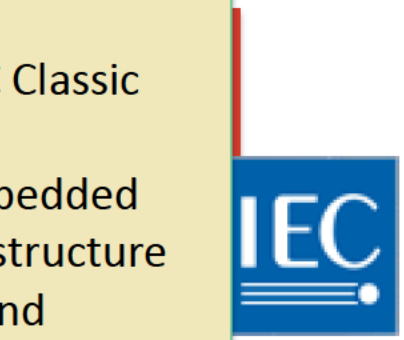
- Extremely lightweight publish/subscribe messaging transport
- Useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium
- Ideal for mobile applications because of its small size, low power usage, minimised data packets, and efficient distribution of information to one or many receivers

Standards and Frameworks

OPC UA (OPC Unified Architecture)

A platform independent service-oriented architecture that integrates all the functionality of the OPC Classic specifications into one extensible framework.

- **Functional equivalence:** all COM OPC Classic specifications are mapped
- **Platform independence:** from an embedded micro-controller to cloud-based infrastructure
- **Secure:** encryption, authentication, and auditing
- **Extensible:** ability to add new features without affecting existing applications
- **Comprehensive information modeling:** for defining complex information



Standards and Frameworks

EdgeX Foundry

A common open platform unifying the IoT Edge

- An open source project hosted by the Linux Foundation that is building a common open platform for IoT edge computing.
- Enables an ecosystem of plug-and-play components that unifies the marketplace
- Unique in scope, with broad industry support, credibility, investment, vendor-neutrality
- Apache 2.0 open source licensing model
- Community of developers or companies that collaborate on IoT solutions using standards combined with proprietary innovations

Standards and Frameworks

IEEE P2413

Draft Standard for an Architectural Framework for the Internet of Things

- Defines an architectural framework for the Internet of Things (IoT)
- Descriptions of various IoT domains, IoT domain abstractions, commonalities between different IoT domains

IEEE P2413.1

Standard for a Reference Architecture for Smart City (RASC)

IEEE P2413.2

Standard for a Reference Architecture for Power Distribution IoT (PDIoT)

Standards and Frameworks

Industrial Internet Security Framework (IISF)

Comprehensive resource for understanding Industrial Internet of Things (IIoT) security considerations

- Promotes IIoT security best practices and accelerates their adoption
- Explains how security fits within the business of industrial operations
- Defines functional building blocks for addressing security concerns
- Provides implementation guidance and practical techniques for IIoT security

IoT Security Maturity Model (SMM)

Builds on IISF to help organizations assess and plan for IoT maturity

- Path for IoT providers to understand where they need to be
- Enables intelligent choices about which mechanisms to use and how to invest in them

Standards and Frameworks

FIDO IoT

Technical Working Group develops use cases, target architectures and specifications

- IoT device attestation/authentication profiles to enable interoperability between service providers and IoT devices
- Automated onboarding, and binding of applications and/or users to IoT devices
- IoT device authentication and provisioning via smart routers and IoT hubs

NIST National Institute of Standards and Technology U.S. Department of Commerce

IETF

industrial internet CONSORTIUM

ISO IEC

ETSI

DDS

EDGE X FOUNDRY™

fido ALLIANCE

S…works

OMG DDS

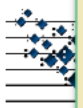
Data-Distribution Service for Real-Time Systems

- A virtual Global Data Space where applications can share
- QoS parameters including reliability, bandwidth, delivery deadlines, and resource limits
- Supports the construction of local object models on top of the Global Data Space

ETSI M2M

Radio standards for machine-to-machine (M2M) real-time communications

- OneM2M standards initiative
- Requirements (ETSI TS 102 689)
- Functional architecture (ETSI TS 102 690)
- Interface descriptions (ETSI TS 102 921)



NIST National Institute of Standards and Technology U.S. Department of Commerce

IETF®

industrial internet® CONSORTIUM

ISO IEC

ETSI DDS™

tido™ ALLIANCE

Standards and Frameworks

ISO/IEC

Global standards and frameworks for IoT

- ISO/IEC 20924:2018
  Information technology — IoT — Vocabulary
- ISO/IEC 21823-1:2019
  IoT — Interoperability for IoT systems — Part 1: Framework
- ISO/IEC 21823-2:2020
  IoT — Interoperability for IoT systems — Part 2: Transport interoperability
- ISO/IEC TR 22417:2017
  Information technology — IoT use cases
- ISO/IEC TR 30164:2020
  IoT — Edge computing
- ISO/IEC TR 30166:2020
  IoT — Industrial IoT

Standards and Frameworks

IETF

RFC 8576 -- IoT Security: State of the Art and Challenges

- Document for use by implementers and authors of IoT specifications as a reference for details about security considerations while documenting their specific security challenges, threat models, and mitigations

IoT for Security and Risk Managers

- Make IoT part of your risk and security plans
  - Treat it like any other digital risk
  - Engage the right functional areas
  - Address the “kudzu” of freely deployed devices

- Empower IoT use with risk and security controls
  - Encourage use of IoT when appropriate, but require security and risk review
  - Create a playbook for deployment and management of IoT devices and systems

De-Risking IoT

Questions to ask:

- Do we have a handle on current IoT deployments?
  - Where do challenges exist in brownfield devices?
  - Are there proprietary/siloed systems to integrate?
  - Do we know what's really out there in our environment?

- Do we have a strategy for future IoT deployments?
  - Have we implemented an edge architecture to plug everything into?
  - Are we able to track and prove conformance to standards and frameworks?

RSAConference2020 APJ

A Virtual Learning Experience

Thank you!

Arthur Fontaine
RSA
@arthurfontaine