Hewlett Packard
Enterprise

Enhanced IoT security through orchestrated policy enforcement gateways

Hamza Attak, Research Engineer

C&ESAR conference, November 23rd 2016, Rennes

Introduction

IoT devices need to be secure:

- Data privacy concerns
- Hijacking devices to higher ends
- Becoming responsible of public safety

IoT fleet constitutes a case separated from the device-centric scenario:

- A local packet that seems legit, might have a different meaning when sent to a set of devices on the network
- Security flexibility at scale is a challenge by itself

Problems

- **Multiplicity**: Huge and growing number of devices to be secure (~40B estimation by 2020)
- **Heterogeneity**: Each device has its own way to be configured (inducing high costs)
- **Non-extensibitlity**: Being constrained in memory, computing power or even in capability, extensibility is optional on most of IoT devices
- **Non-configurability**: worse version of non-extensibility (most ‘On-Only’ devices)
- **Attack patterns:** Individual devices traffic seemingly legit but actually looks harmful at the IoT fleet level

Most of these constraints are direct characteristics of IoT devices…

-> Should the security features really be on the IoT device then?

Also:

-> Could the different types of attacks be detected at the infrastructure level?

Plan

I SECURED: SECurity at the network Edge

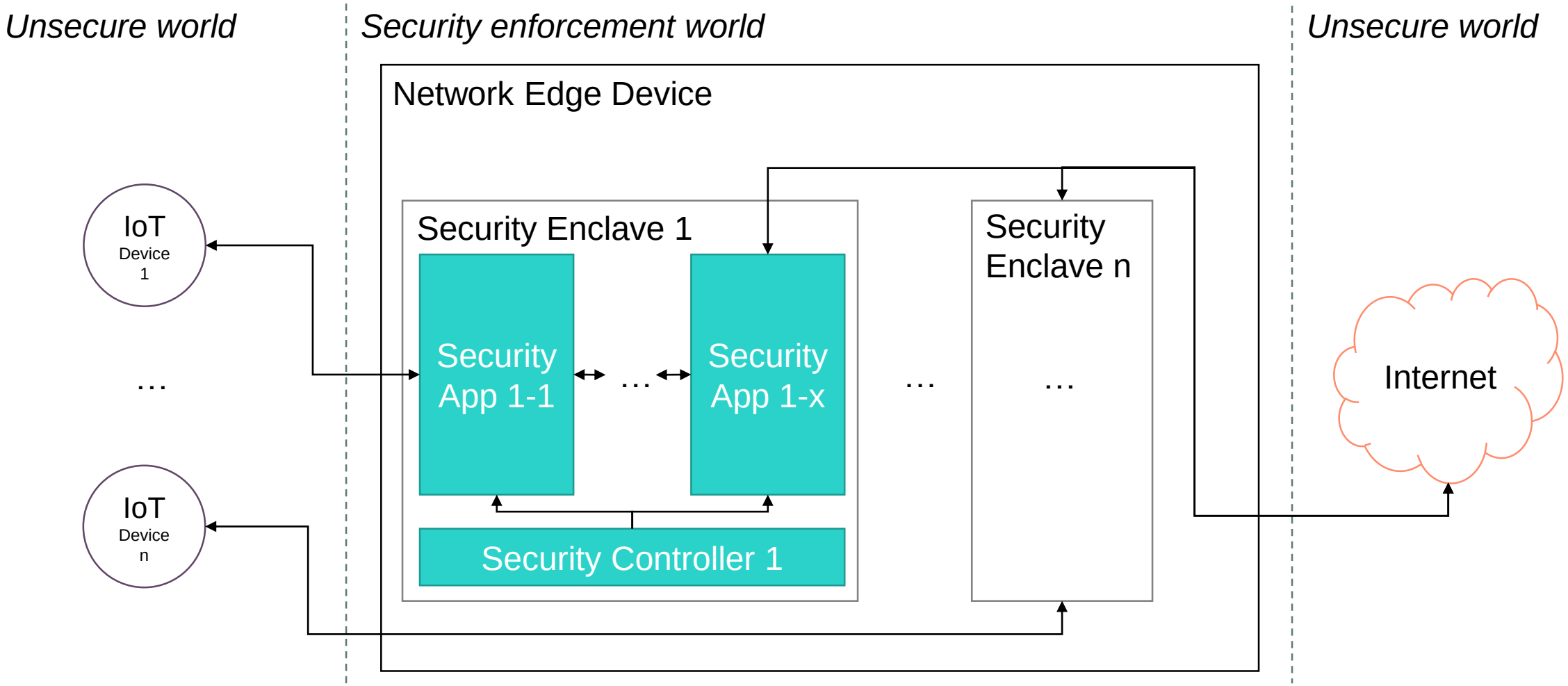
II SHIELD: Leveraging big-data analytics for flexible security

Conclusion

I - SECURED

SECurity at the network EDge

1 – Architecture and Design



Hewlett Packard Enterprise

Available Security Applications

– Intrusion Detection (Bro NSM)

– Re-encryption (MITMproxy)

– Anti-phishing (DansGuardian)

– Transparent VPN (StrongSwan)

– L4 Firewall (IPtables)

– L7 Firewall (Squid)

– Anonymity (OpenVPN)

– Bandwidth Control (‘tc’ command)

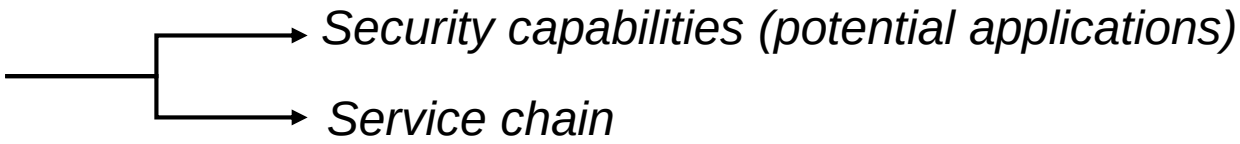
Hewlett Packard Enterprise

2 – Policy Model

Three abstraction levels for configuring the solution:

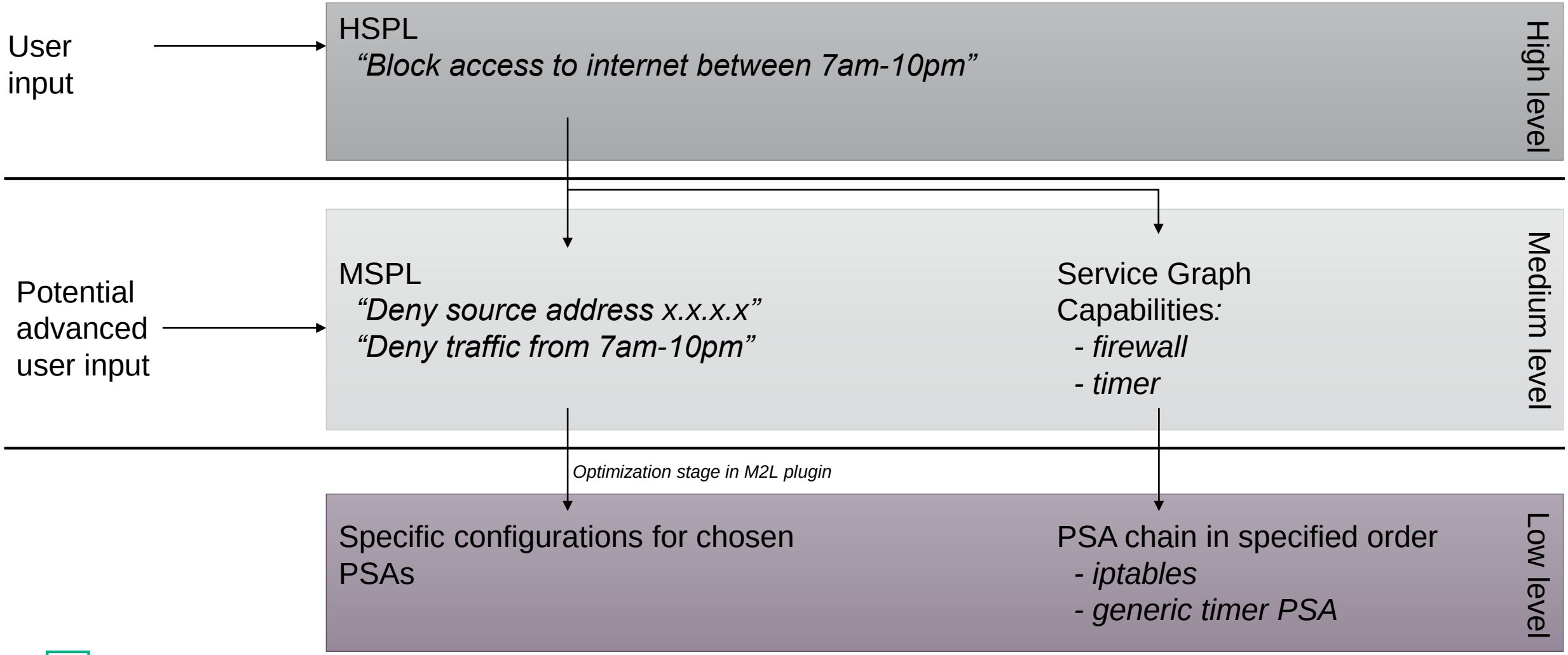
High level language: for non-technically savvy users

Medium level language: for administrators and simply intermediate translation of the high level language

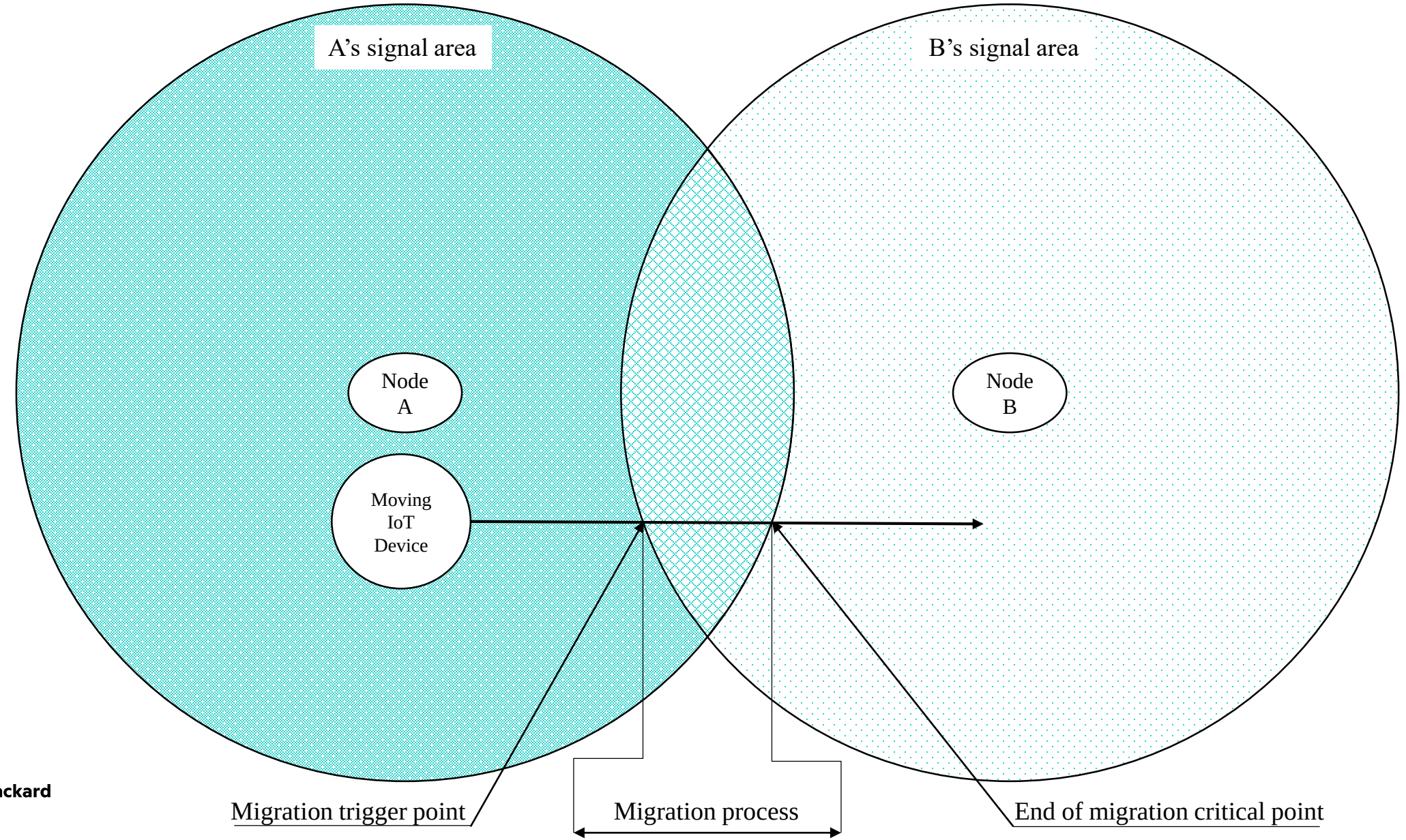


Low level language: not configurable, translation plugin is provided by the security application developer

2 – Policy Model Example



3 – Mobility Scenario

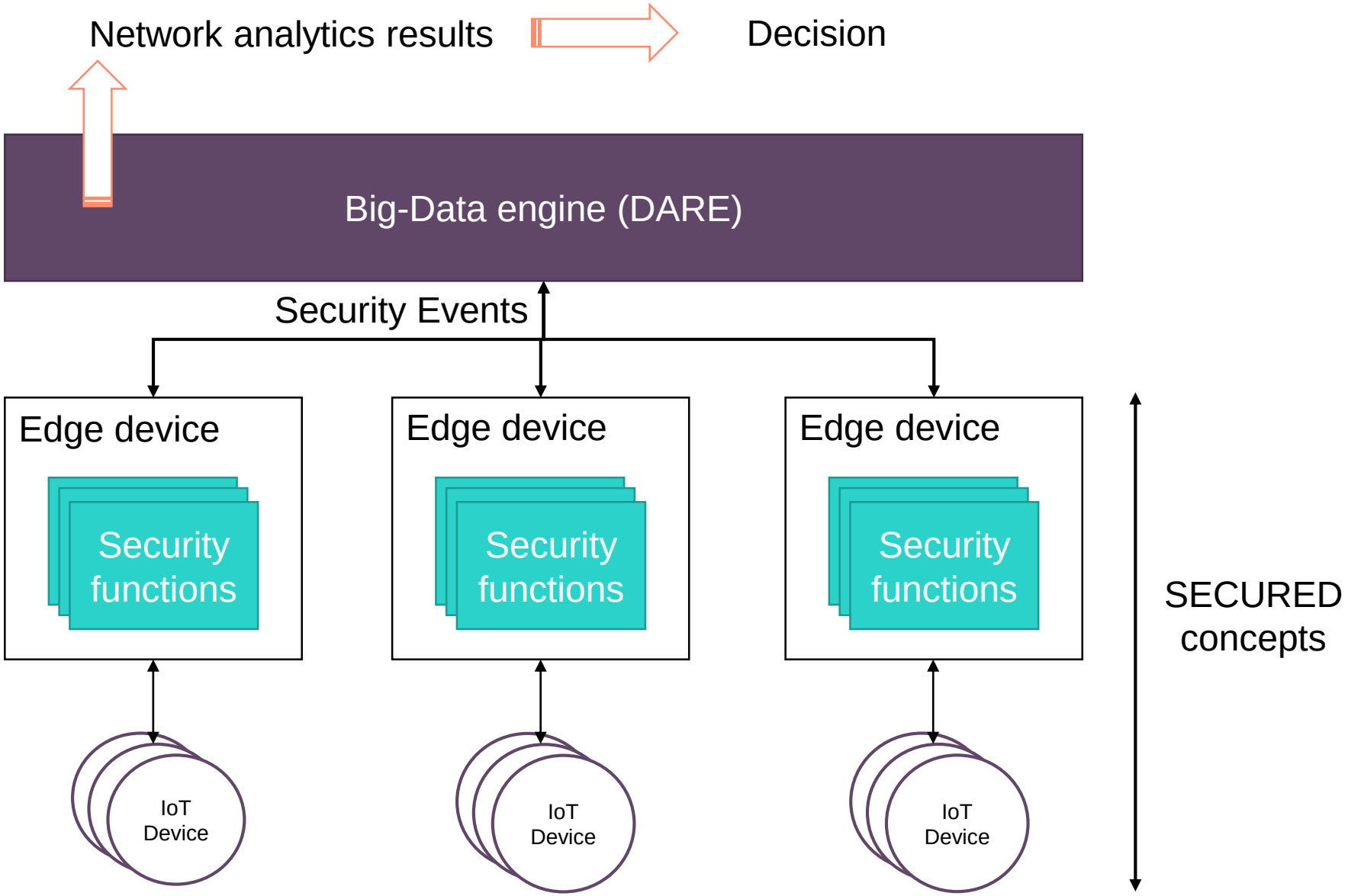


Hewlett Packard Enterprise

II - SHIELD

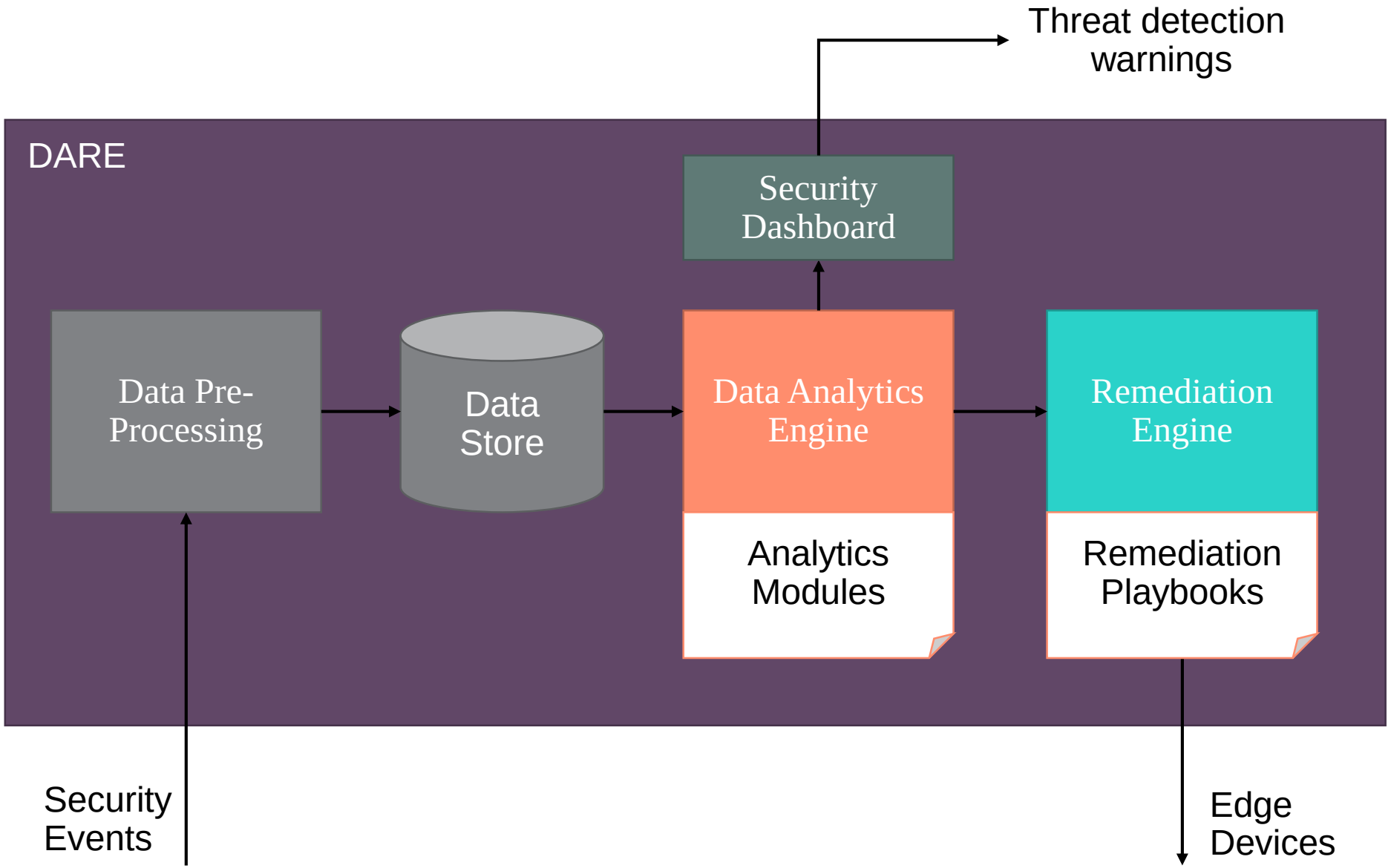
Leveraging big-data analytics for flexible security

Architecture overview



Hewlett Packard Enterprise

Data Analytics and Remediation Engine (DARE)



Hewlett Packard Enterprise

Conclusion

SECURED

– Full solution for securing **IoT devices**

– **Enforced security**, between the device and outer – unsecure – resource

– Project is finished, after 2.5 years with 7 European partners

– Project website accessible at: https://www.secured-fp7.eu/

– Source code available at: https://github.com/secured-fp7

SHIELD

– Full solution for securing **IoT fleets**

– **Extensible** with new attack recognition moduls

– Project has just begun, for 3 years with 11 partners

– Project website accessible at: https://www.shield-h2020.eu/

Full picture

– Effectively protects **individual** devices and at the **infrastructure** level

– Respective of IoT constraints, especially **non-extensibitlity** and **non-configuration**

– Fully compatible with current devices, **no modifications needed** (except for mobility proposal)

Hewlett Packard
Enterprise

Thank you

hamza@hpe.com