



UNIK4750 - Measurable Security for the Internet of Things

L3 – Security of the Internet of Things

György Kálmán,
Mnemonic/CCIS/UNIK
gyorgy@unik.no

Josef Noll
UiO/UNIK
josef@unik.no

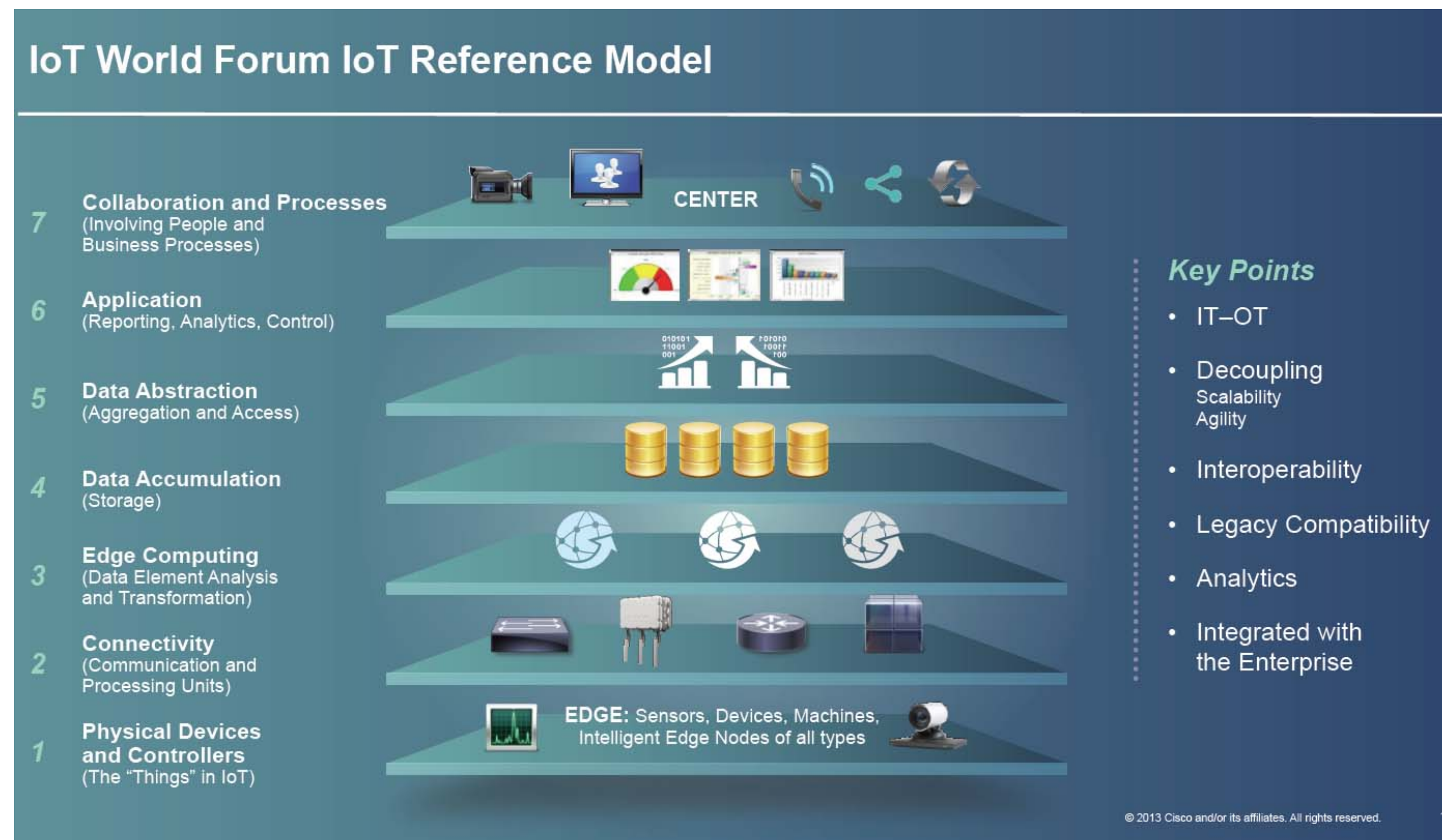
Overview



- Recap: IoT
- Resources and Converged infrastructure
- Threat landscape and surface
- Security challenges and needs
- Security life cycle
- Privacy
- Conclusion

Internet of Things - recap

- Heading toward a fully connected world
- The substantial difference is, that these systems have a physical dimension
- Integration of a wide variety of devices with very different capabilities and tasks
- Security is an enabler
- Life-cycle of devices is very different than typical IT
- The attack surface grows



Current situation of IoT

- IoT is not necessarily something big: an IP camera, smart thermostat, door opener, remote controlled power outlet, all is part of the IoT.
- Problems:
 - ➔ Privacy: many of the devices require e.g. to use a Google account for setup
 - ➔ Lack of resources also results in e.g. weak password policies
 - ➔ Confidentiality: using no security is the widest adapted method
 - ➔ Outdated solutions: UI is poorly implemented and is prone to vulnerabilities several years old

Resource-related challenges

- Limited bandwidth
- Latency
- Reliability

- Not feasible to create a "perfect" system: be prepared to be compromised
 - ➔ Redundancy, reconfiguration, backup
- Security focus points:
 - ➔ Gateway/router
 - ➔ Cloud services

Converged IoT infrastructure

- End-to-end support of processes
- Priority on availability and reliability
- Scalable, efficient
- Globally identifiable things – have both a dimension in the physical and in the logical world
- Consistent security in the whole value chain
- Deterministic operation (on the scale of the processes running on it)
 - ➔ Machine lines with hundreds of axes, transportation, critical infrastructure
- Management of assets

Converged IoT infrastructure-related challenges

- From closed networks to cloud computing. Not only new possibilities, but also new threats
- Heterogenous infrastructure connects a wide range of devices with a life-cycle mismatch
- Opens up new interfaces to attack
 - ➔ Risk for loss of privacy, functionality, fraud
 - ➔ Physical consequences
- Security measures shall be budgeted in accordance with the possible damage, not with the price of the asset
- IoT devices can introduce unexpected traffic into corporate networks (e.g. IPv6), which can be a challenge for the IDS system (if e.g. rules include IPv4 parameters) – one should enforce security controls both on IPv6 native and IPv6 tunneled traffic

Threat landscape

- Vectors:
 - ➔ Physical access (e.g. USB drive – Stuxnet)
 - ➔ Authenticated attacks
 - ➔ Unauthenticated attacks
 - ➔ Trivial access
- Types of attackers
 - ➔ Hack – typically exploits vulnerability in the system
 - ➔ System analysis – side channel attacks, analysis of the running environment and runtime
 - ➔ Lab-based attack – highly skilled attacker supported with special equipment
- Types of attacks
 - ➔ DDoS, botnet, malware, perimeter weakening, data breach
- Defense:
 - ➔ Tamper resistance
 - ➔ Monitoring of equipment status



Security challenges

- IoT intrudes a dramatically larger attack surface
- Wide range of technologies involved:
 - ➔ Sensors: AV, positioning, acceleration, temperature, proximity
 - ➔ Communication: cellular, wireless, wired, light
 - ➔ Identification: rfid, barcodes, tags, biometry
 - ➔ Localization: gps, indoor solutions
- From closed networks to cloud computing:
 - ➔ Security solutions should not build on and depend on to the network technology (heterogeneous infrastructure)
- Cost of security:
 - ➔ Possible mismatch between the value of the device and the data handled
- Misconception: device focus. IoT has many attack surfaces, each of these shall be evaluated.
- All elements of the system have to be considered:
 - ➔ End devices, cloud infrastructure, the application, network interfaces, software environment, use of crypto
- Public acceptance of IoT depends on security of the systems

- It's not about the device. One shall see the big picture
- Structured approach with well-known steps: e.g. securing a web interface, analysis and setup of protocol parameters (avoid fallback to weak crypto), analysis of data to select correct protection
- Insecure network services: unfortunately, typical for industrial applications
- Transport encryption: use appropriate technological solutions
- Cloud interface
- Mobile interface
- Appropriate granularity in security configuration: e.g. monitoring, logging, password and lockout parameters
- Insecure software
- Physical security

Security needs of IoT

- User identification
 - Identity management
 - Tamper resistance
 - Secure storage
 - Secure content
 - Secure software execution
 - Secure communication
 - ➔ Over-the-air updates
 - Secure network access
-
- Gateway as a key customer component: edge device for the LAN, concentrator

Security needs of IoT

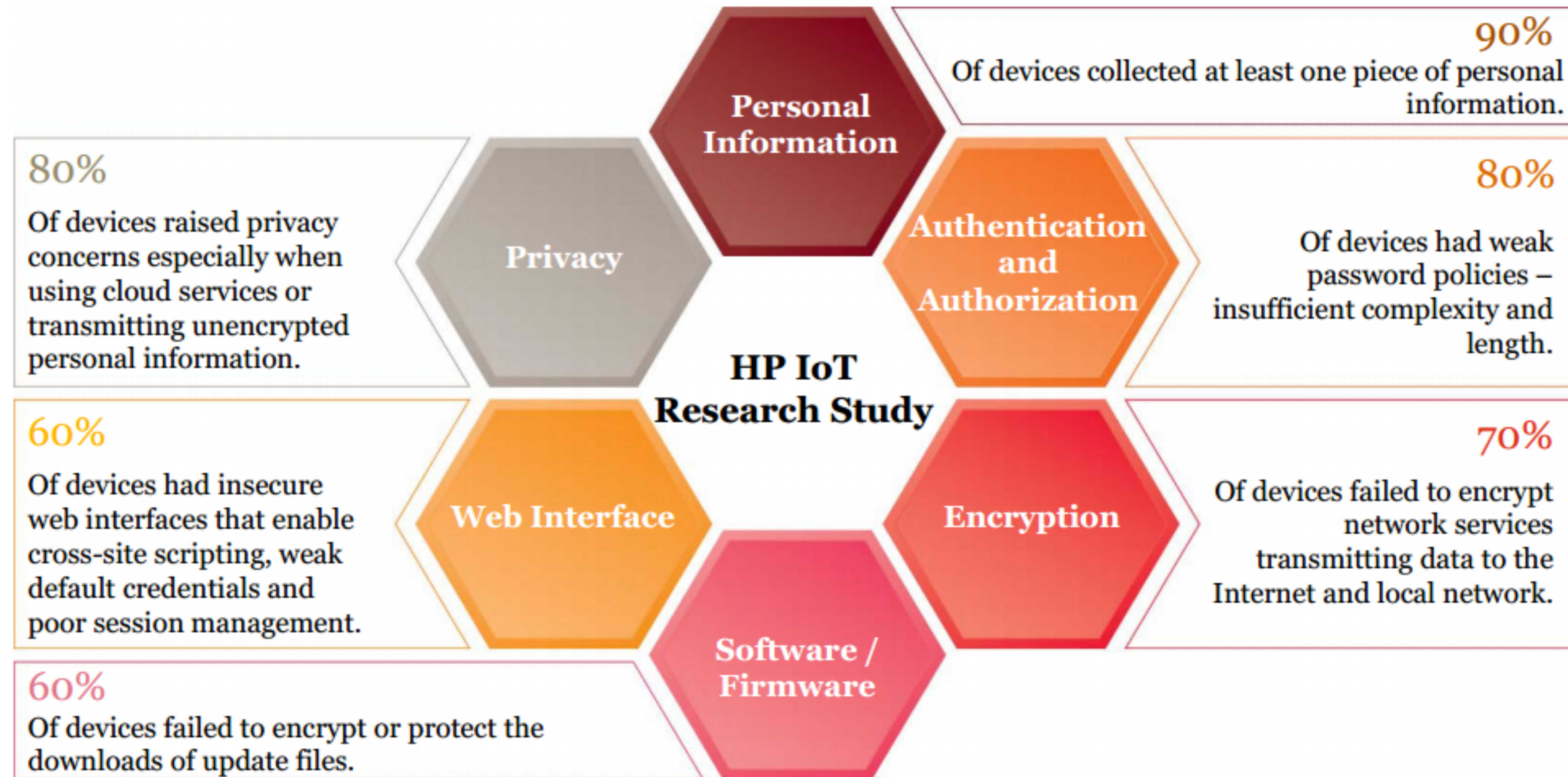


Figure from PwC, data from HP

Threat vectors

- Gateway:
 - ➔ physical access,
 - ➔ authenticated attacks,
 - ➔ Unauthenticated attacks,
 - ➔ Trivial access
 - ➔ Other problems from the fact, that the gateway has at least two interfaces, one LAN and one WAN.
- Security features for embedded devices (more or less true for the whole LAN ecosystem)
 - ➔ Integrated crypto hardware
 - ➔ Firmware protection,
 - ➔ Tamper resistance
 - ➔ Vertical integration of security functions
 - ➔ Trivial access throughout the vertical

- Computational capabilities and permanent internet connectivity
- Can be used to:
 - ➔ Send spam
 - ➔ Coordinated attack against e.g. Critical infrastructure
 - ➔ Act as server for malware
 - ➔ Entry point into an other network (e.g. Corporate)
- Example:
 - ➔ Spike botnet: DDoS attacks, ARM platform, infected devices included routers, smart thermostats, dryers, freezers, raspberry pi appliances.
 - ➔ Control systems, vehicles, and even the human body can be accessed and manipulated causing injury or worse
 - ➔ Health care providers can improperly diagnose and treat patients
 - ➔ Loss of vehicle control
 - ➔ Critical infrastructure damage
 - ➔ Safety-critical information such as warnings of a broken gas line can go unnoticed

- Object privacy
 - ➔ Eavesdropping, tracking and stealing data
- Location privacy
 - ➔ Tracking, monitoring, revealing data
- Devices shall:
 - ➔ Only collect data, which is necessary for the functionality
 - ➔ Try to avoid collection of sensitive data and de-identify or anonymize as early as possible

Security profiles



- Authentication, Confidentiality and integrity in relation with the application
- Constrained sub-environments: lightweight protocols and the role of the gateway or concentrator
- Self-healing and resiliency
 - ➔ Make sure, that software updates are possible remotely
 - ➔ Protect and verify the update file
- Actual security functions in relation with the application

L3 Conclusions



- Converged infrastructure
- IoT expands the attack surface
- Security requirements do also depend on type of data processed
- Devices with multiple interfaces present a risk
- End-to-end security and life-cycle support is key
- Privacy
- Why is this all good for the user?