UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L3 – Security of the Internet of Things

György Kálmán,
ITS@UiO

Josef Noll
ITS@UiO
josef.noll@its.uio.no

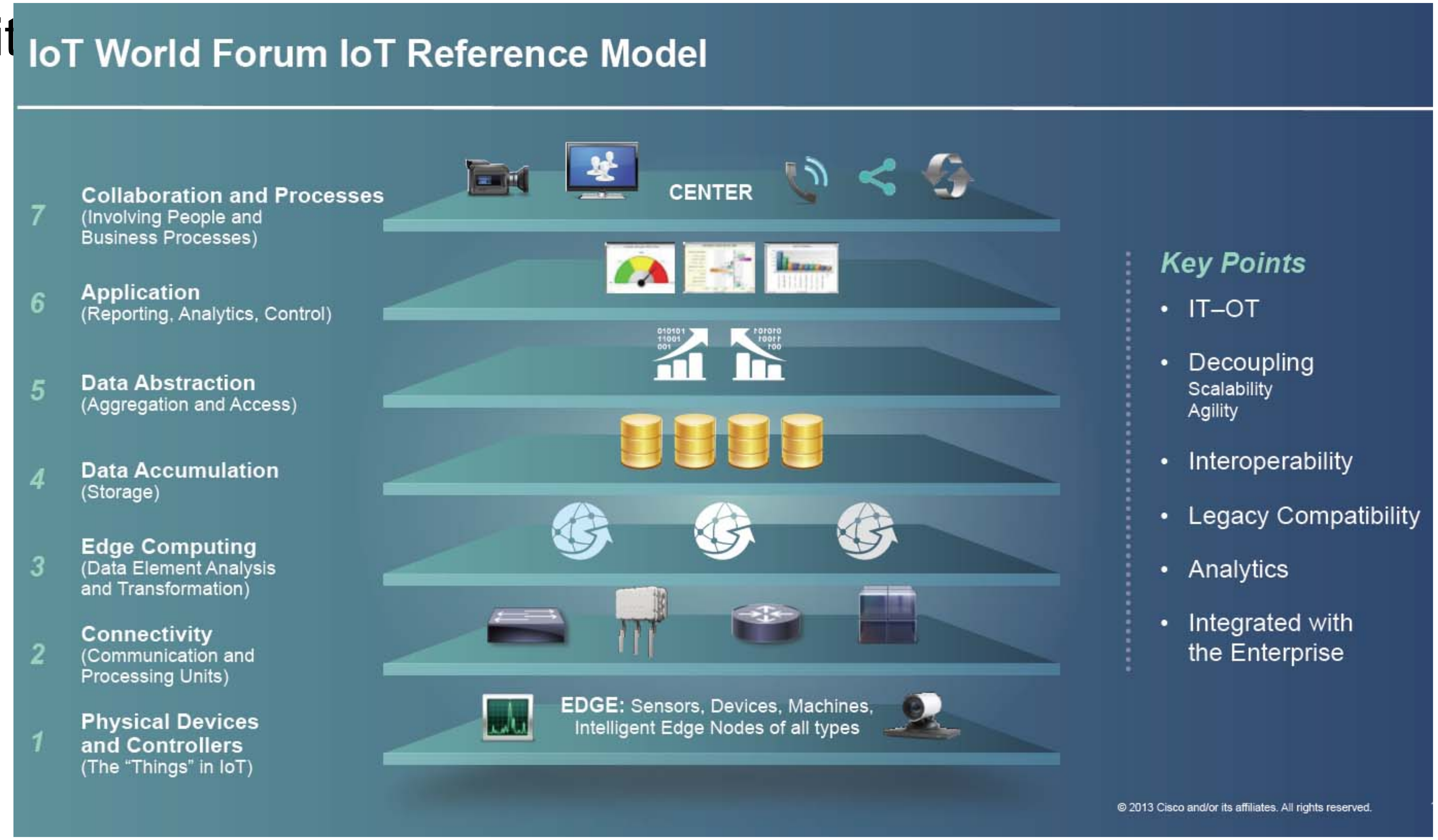
http://IoTSec.no , #IoTSec, #IoTSecNO

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 wit
- 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 necessarely 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 amongst other factors may lead weak password policies
  - Confidentiality: using no security is the widest adapted method
  - Outdated solutions: UI is poorly implemented and is prone to vulnerabilities found several years ago

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: the edges:
  - Gateway/router
  - Cloud services

Converged IoT infrastructure

- End-to-end support of processes
- Pirority 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 possiblities, 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
  - Phyisical 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 – http Basic Auth, no access control at all
- Types of attackers
  - Hack – typically exploits vulnerability in the system (might be trivial)
  - System analysis – side channel attacks, analysis of the running environment and runtime
  - Lab-based attack – highly skilled attacker supported with special equipment
  - Inside job
- Types of attacks
  - DDoS, botnet, malware, perimeter weakening, data breach, just for fun
- Defense:
  - Tamper resistance
  - Monitoring of equipment status

Security challenges

- IoT introduces 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 intefaces, software environment, use of crypto
- Public acceptance of IoT depends on security of the systems

Security analysis

- 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
- Phyisical 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

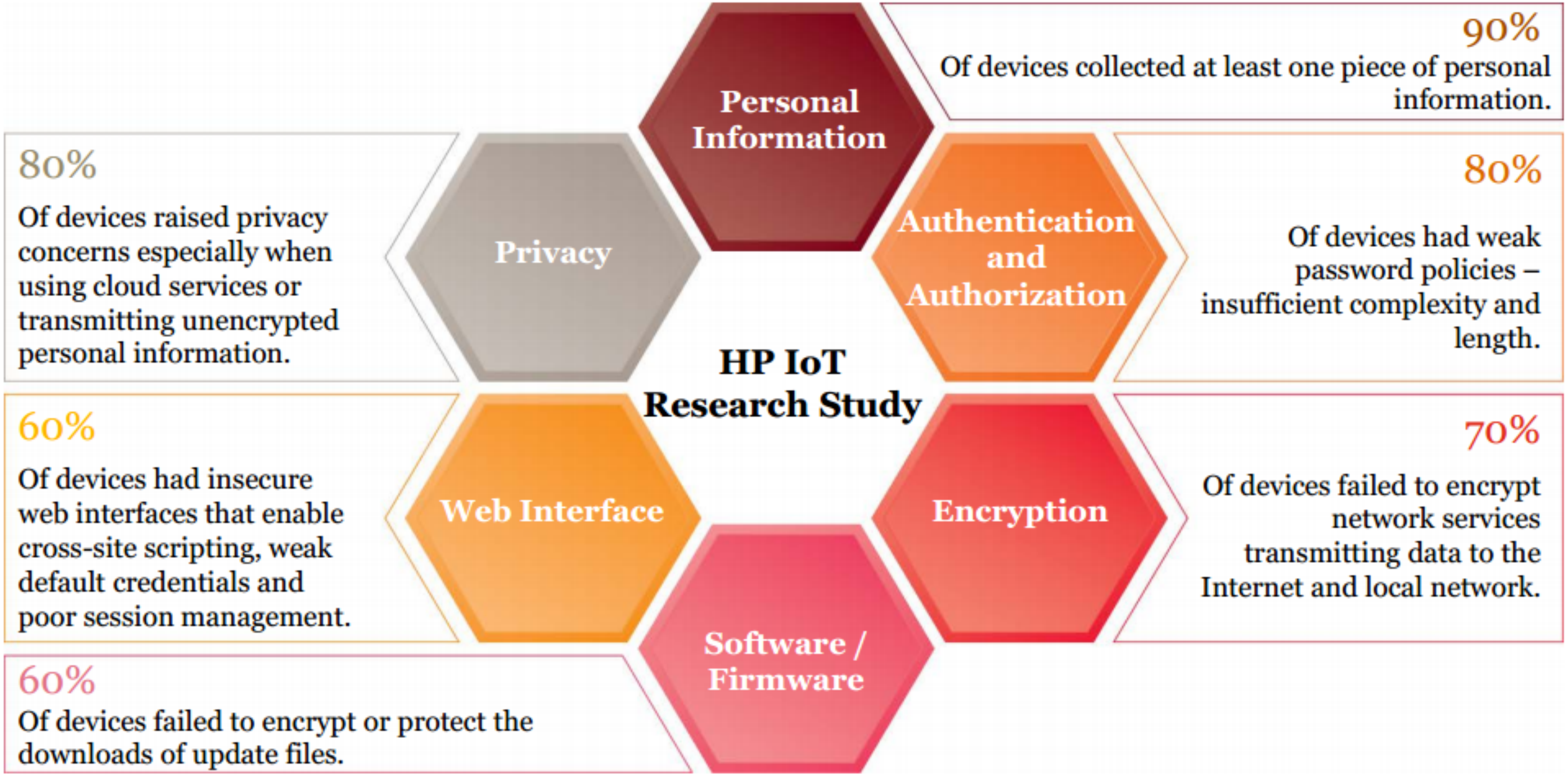


Figure from PwC, data from HP

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

An example – Secure gateway vulnerability

- **eWON Reference: Password visibility (https://ewon.biz/support/news/support/ewon-security-enhancement-7529-01)**
- **Affected devices:** eWON Flexy/CD
- **Affected versions:** All firmware versions
- **Impact/description:**
- It is possible to "sniff" passwords when the firmware website is accessed through standard non-secure HTTP.
- Furthermore the autocomplete feature integrated with the evergreen browsers might suggest in clear text previous passwords in the eWON User Setup creation/edition page.
- **Mitigating factors:**
- Connections to eWON devices should only be done through a point-to-point LAN, a secured LAN or a secured VPN. Sniffing is thus not a valid attack use case as it concerns closed work environment (limited connectivity) or secure environment.
- Regarding the second issue the internet browser is supposed to be manipulated by the eWON administrator only as the page that leaks passwords requires configuration management right.
- **Solution / Advice:**
- Always connect to eWON using a closed work environment (limited connectivity) using a point-to-point LAN, a secured LAN or a secured VPN (for instance using Talk2M).
- Since eWON firmware version 10.1s0 we disable password fields auto completion.

An example – glibc vulnerability affecting ICS

Embedded devices also use code from other IT systems

Vulnerabilities can be valid across platforms

Technical FAQs

Question	Moxa Statement on "GHOST" Vulnerability (CVE-2015-0235)
Question Type	Other
Updated	6/1/2016 1:54:36 PM
Hits	1
Products	

Suggestions

Background and Impact
According to ICS-CERT, the "GHOST" vulnerability (CVE-2015-0235) in the "glibc" library could affect industrial systems. An authenticated local administrator could cause a denial of service of the targeted system by exploiting this vulnerability. ICS-CERT recommends the three following general defensive measures to protect against this and other cybersecurity risks:

"Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices."

Impacted Products
Some Moxa devices are impacted by the "GHOST" vulnerability. Refer to the table below for a list of impacted products.

Category	Industrial Ethernet	Serial Connectivity	Industrial Computing	Remote Automation	IP Surveillance
Impacted Products	EDR-810 Series EDR-G900 Series	W2X50A, W1 MGate 5101-PBM-MN MGate 5101-PBM-PN MGate 5101-MB-EIP	UC-8100 X86, IA240, IA3341, W315A, W325A, UC-7112 Plus, W311, W321, W341, W327, DA-661/662/663. UC-8430, UC-8481/8486, MAR-2000-LX, RNAS/FLI, UC-7112 Plus, W315, W325, W345, IA241, DA-660, W406, IA261-I/IA262-I, IA260, EM-2260	ioPAC 8500 ioPAC 8600 ioPAC 5500	VPort 06-1MP Series VPort 16-1MP Series VPort 26A-1MP Series VPort 36-1MP Series VPort 56-2MP VPort 66-2MP VPort 36-2MP VPort 461A VPort 06-2MP

Attacks

- 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.
  - Mirai botnet: cameras (http://www.welivesecurity.com/2016/10/24/webcam-firm-recalls-hackable-devices-mighty-mirai-botnet-attack/)
  - 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

Privacy

- 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
- Constratined 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 funcions 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 intefaces present a risk
- End-to-end security and life-cycle support is key
- Privacy
- Why is this all good for the user?