Privacy Labelling, Security Metrics, Roadmap towards a more secure and privacy-aware society

Josef Noll (Movation)

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

SCOTT today

- Expectations when visiting our site:

- Security - “SCOTT will present a framework for security”
- Safety - “The link between Safety and Security”
- Privacy - “Privacy label? - changing the rules of the game?”
- Usability - “Are solutions really useable?”
- Trustability - “Can I trust sensors to speak Norwegian?”

- Reality:
- 16 use cases
- >40 Building Blocks
- >600 Requirements

List of Building Blocks in SCOTT [edit]

The Building Blocks are sorted along WP 22: Technology Lines. These Technology Lines are:

- WP23: **Security & Safety**
- WP24: **Distributed Cloud Integration**
- WP25: **Autonomy of Devices/Energy Efficiency of WSN**
- WP26: **Reference Architecture/Implementation**

[hide]

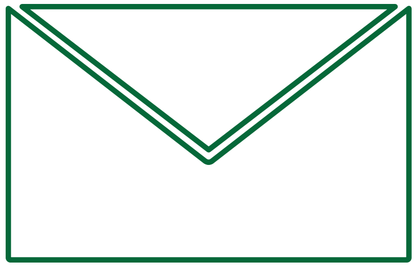
1 List of Building Blocks in SCOTT
1.1 Semantic Relations
2 Building Blocks involved from Norway

List of Building Blocks in SCOTT

- BB23.A Dependable Wireless Sensor Network, Leader: **Teresa Riesgo**, partners: INDRA, Universidad Politécnica de Madrid, Telenor, Wolffia (BB23.A)
- BB23.B End-to-end assured QoE, Leader: **Xavier Alberti**, partners: INDRA, CIT, KLAS, VEMCO (BB23.B)
- ~~BB23.E Safety-critical applications via Satcom~~, Leader: **Xavier Alberti**, partners: INDRA (BB23.E)
- BB23.I Reinforcement of safety for traffic infrastructures, Leader: **Francisco Parrilla**, partners: INDRA, Universidad Politécnica de Madrid, Instituto Tecnologico de Informatica, IK4-TEK, SAGOE (BB23.I)
- BB23.K Realiable Wireless PHY and MAC, Leader: **Egoitz Arruti**, partners: INDR
- BB23.R Trust Trust Anchor and Trust Indicators, Leader: **Marco Steger**, partners SECURE, AIT, IMEC, Johannes Kepler Universität, SBA, Nokia, Virtual Vehicle R
- BB3.1.B Dependable, Leader: **Thuan**, partners: UiO, Wolffia (BB24.A)
- BB24.A Remote Configuration of Infrastructure, Leader: **Linda Firveld**, partners: (BB24.A)
- BB24.B Addressing and Mobility Management of Devices, Leader: **Joachim Hille** Nokia, Virtual Vehicle Research Center (BB24.B)
- BB24.C Application Layer Protocols and Cloud Architectures, Leader: **Pedro Rui** (BB24.C)
- BB24.D Big Data Analytics, Leader: **Antonio Lagarda**, partners: Instituto Tecnol
- BB24.E Cloud computing services for mobility applications, Leader: **N.n.**, partner University College Cork, VTT, VEMCO, SICS, Virtual Vehicle Research Center (B
- BB24.F Cross-technology synchronisation, Leader: **Peter Priller**, partners: UiO (B
- BB24.G Mobile Edge Computing, Leader: **Lucasz Kawolski**, partners: PRE, Tele
- BB24.I Semantic Attribute Based Access Control (S-ABAC), Leader: **Christian J** Norway (BB24.I)
- BB24.J Wireless Vehicle Interface, Leader: **Pawel Czernecki**, partners: FEV PL,
- BB24.K Trustable Passenger Vehicle Data Logging System, Leader: **Alexander** Research Center (BB24.K)
- BB24.L Adaptable network slicing, Leader: **Do van Thanh**, partners: Telenor, HiO
- BB26.A Autonomous Wireless Network, Leader: **Francisco Parrilla**, partners: IN KLAS, Universidad Politécnica de Madrid (BB26.A)
- BB26.B Cloud computing service platform, Leader: **N. n.**, partners: AIT, AVL, CIS Cork, Nokia, Virtual Vehicle Research Center (BB26.B)
- ~~BB26.C Smart routing for WSN on trains~~, Leader: **Xavier Alberti**, partners: INDR
- BB26.D Infrastructure design and security threat analysis, Leader: **Ramiro Roble**
- BB26.E Interoperability and secure cross-domain application development, Lead
- BB26.F Measurable security and privacy, Leader: **Toktam Ramezani**, partners:
- BB26.G Privacy labels (A-F), Leader: **Christian Johansen**, partners: UiO (BB26.G
- BB26.H Methods for wireless vehicular data links, Leader: **Thomas Zemen**, part Research Center (BB26.H)
- BB26.I Ontology for secure wireless data transfer, Leader: **Ramiro Robles**, partners: ISEP (BB26.I)
- BB3.1.C HW supported security mechanisms, Leader: **Marco Steger**, partners: VTT, AVL, Johannes Kepler Universität, TUG, UiO, F-SECURE, TU Delft, IMEC, AIT, FEV, Nokia, Virtual Vehicle Research Center (BB3.1.C)
- BB3.1.D Integrated Safety&Security Development, Leader: **Silke Holtmanns**, partners: AVL, KTH, INDRA, VEMCO, Universidad Politécnica de Madrid, Politechnika Gdanska, IT, Nokia, Virtual Vehicle Research Center (BB3.1.D)
- BB3.1.F Out of Band Security, Leader: **Achim Berger**, partners: AVL, Johannes Kepler Universität, SBA (BB3.1.F)
- BB3.1.G PHY layer security, Leader: **Andreas Springer**, partners: Johannes Kepler Universität, Linz Center of Mechatronics GmbH, AVL, Politechnika Gdanska (BB3.1.G)
- BB3.1.H Real-time configuration of secure zones, Leader: **Ken Brown**, partners: University College Cork, Tyco, VEMCO, Politechnika Gdanska (BB3.1.H)
- BB3.1.J Reliable Wireless Multi-hop Communications, Leader: **Salvador Santonja**, partners: Instituto Tecnologico de Informatica, AVL, INDRA (BB3.1.J)
- BB3.1.L Routing and scheduling in real-time WSN, Leader: **Rafael C. Socorro Hernández**, partners: Tecnalia, Acciona (BB3.1.L)
- BB3.1.M Safety WSN Adapter, Leader: **Salvador Santonja**, partners: Instituto Tecnologico de Informatica, INDRA (BB3.1.M)
- BB3.1.N SCOTT Security Library, Leader: **Marco Steger**, partners: AVL, VEMCO, Politechnika Gdanska, INDRA, UiO, TUG, Johannes Kepler Universität, F-SECURE, SBA, HiOA, TU Delft, Virtual Vehicle Research Center, EyeNetworks (BB3.1.N)
- BB3.1.O Security Core - Identification, Authentication and Communication, Leader: **Silke Holtmanns**, partners: CISC, EAB, F-SECURE, Linz Center of Mechatronics GmbH, PRE, UiO, SBA, VTT, VEMCO, Nokia, Virtual Vehicle Research Center (BB3.1.O)
- BB3.1.P Spatial-based authorization and authentication, Leader: **Mateusz Rzymowski**, partners: VEMCO, Politechnika Gdanska, PRE, TYCO, University College Cork (BB3.1.P)
- BB3.1.Q Towards a Safe Virtual Coupling, Leader: **Francisco Parrilla**, partners: INDRA, Universidad Politécnica de Madrid, SAGOE (BB3.1.Q)
- BB3.2.H Mobility Prediction, Leader: **Ken Brown**, partners: University College Cork, Tyco (BB3.2.H)
- BB3.3.A Energy efficient security implementation in WSNs, Leader: **Andreas Springer**, partners: Johannes Kepler Universität, AVL, Linz Center of Mechatronics GmbH, SBA (BB3.3.A)
- BB3.3.B Energy efficient & resource optimized component concepts for WSNs, Leader: **Stefan Drude**, partners: NXP NL, NXP AT, AVL (BB3.3.B)
- BB3.3.C Energy storage for WSNs, Leader: **Rafael C. Socorro Hernández**, partners: UiO, Acciona, Tecnalia (BB3.3.C)
- BB3.3.D Energy supply to on track segment, Leader: **Javier Uceda**, partners: Universidad Politécnica de Madrid, INDRA (BB3.3.D)
- BB3.3.E Improved energy harvesting, Leader: **Rafael C. Socorro Hernández**, partners: Acciona, Tecnalia (BB3.3.E)
- BB3.3.F In-vehicle WSN, Leader: **Achim Berger**, partners: Linz Center of Mechatronics GmbH, AVL, Johannes Kepler Universität, SBA (BB3.3.F)
- BB3.3.G System level availability, Leader: **Willem van Driel**, partners: NXP AT, HH, VEMCO, Instituto Tecnologico de Informatica, Politechnika Gdanska, AVL, Tecnalia, Acciona, CISC, VTT, Philips Lightning, Nokia (BB3.3.G)
- ~~BB26.J - IoT/M2M over satellite~~, Leader: **Xavier Alberti**, partners: INDRA (BB36.J)

SCOTT - our current message

- We don’t have the message for the project
  - how are our keywords answered?
- Our presentations are bin counting
  - e.g. >600 requirements
  - average 11,4 requirements per use case
- Our goals with respect to impact are not clear
  - change something in Europe?
  - key selling argument for European industry?



Use Cases

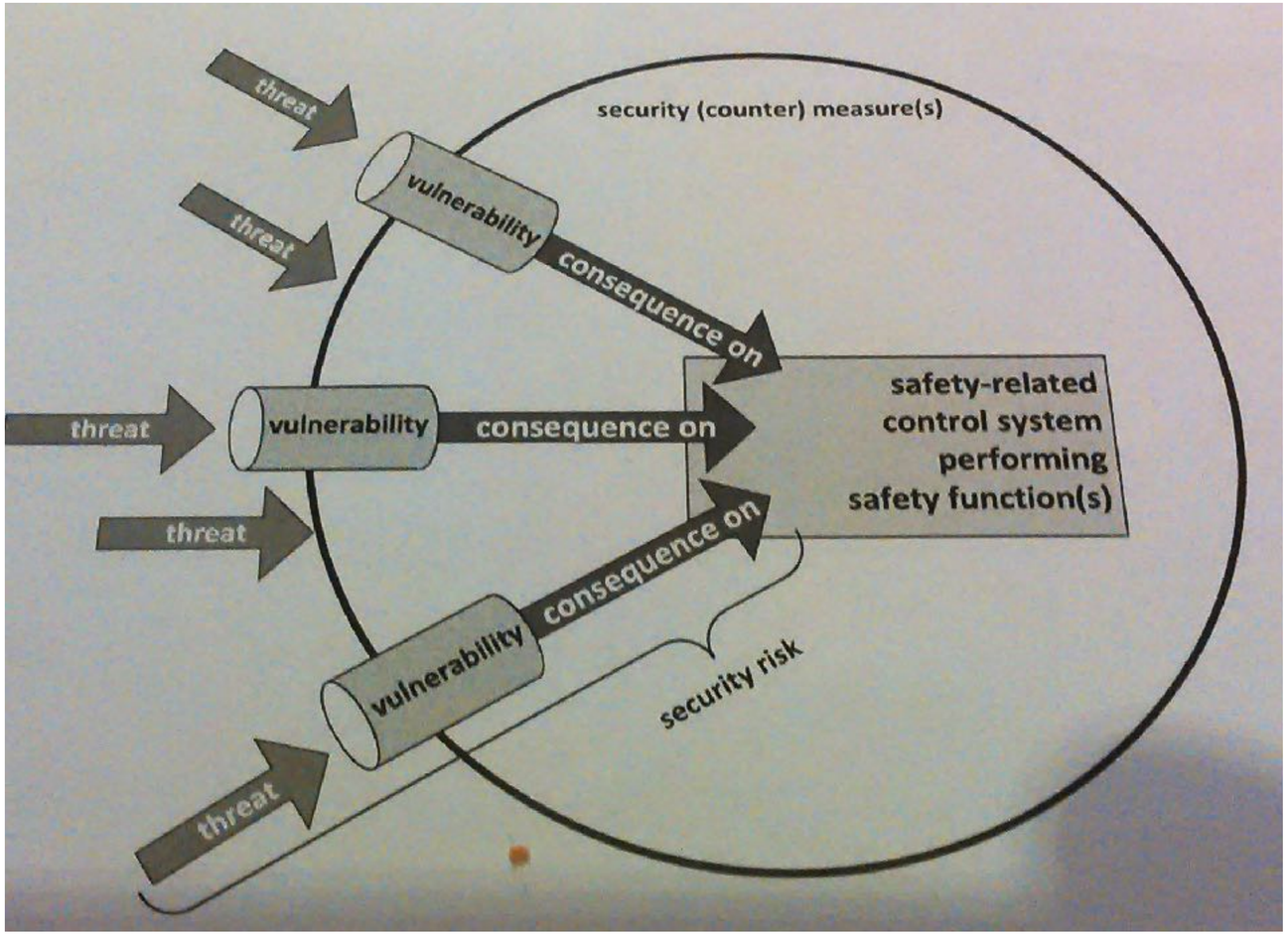
SCOTT

- See Excel sheet

- Attraction for SMEs?
  - our offer?

Roadmap for a more secure and privacy-aware society?

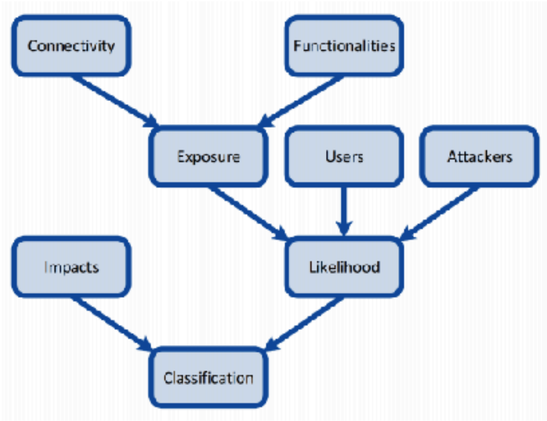
- We have collected the brightest minds in security and safety to answer:
  - Shall we continue “business as normal”?
  - Is “addressing vulnerability” the right answer for the security threats in the IoT domain?
  - “What could be a business advantage for European industries?”

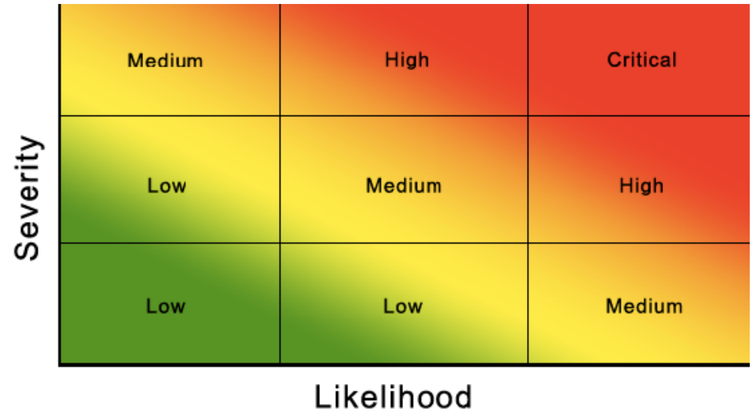


a “more secure society”

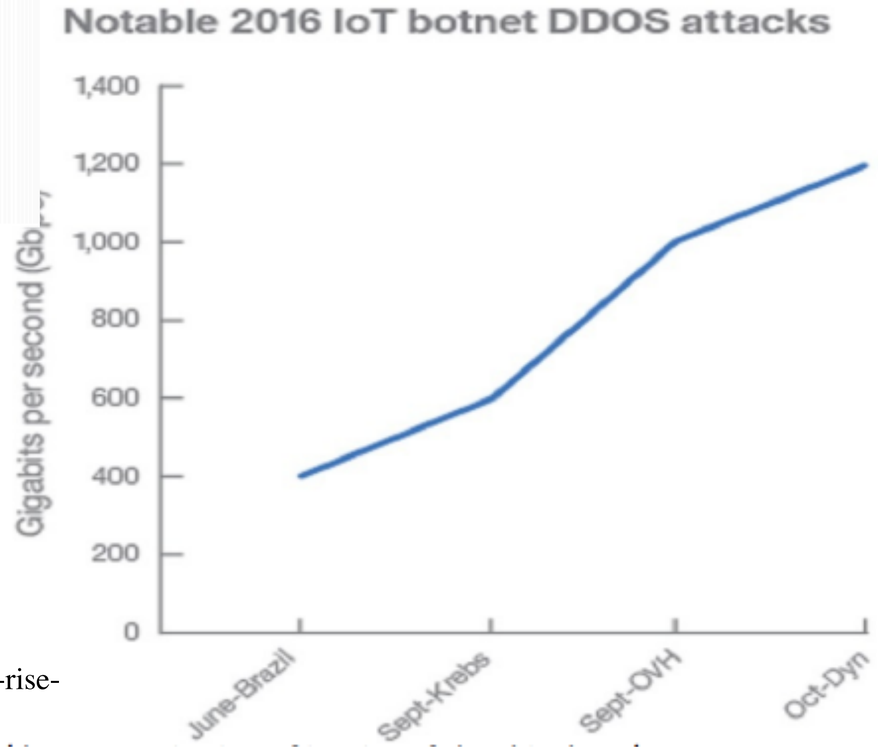
- Do we need a risk analysis?

ANSSI Security Classification for ICS





- IoT threats
  - significantly different
  - DDoS 3x in 2016
  - Botnet(?)

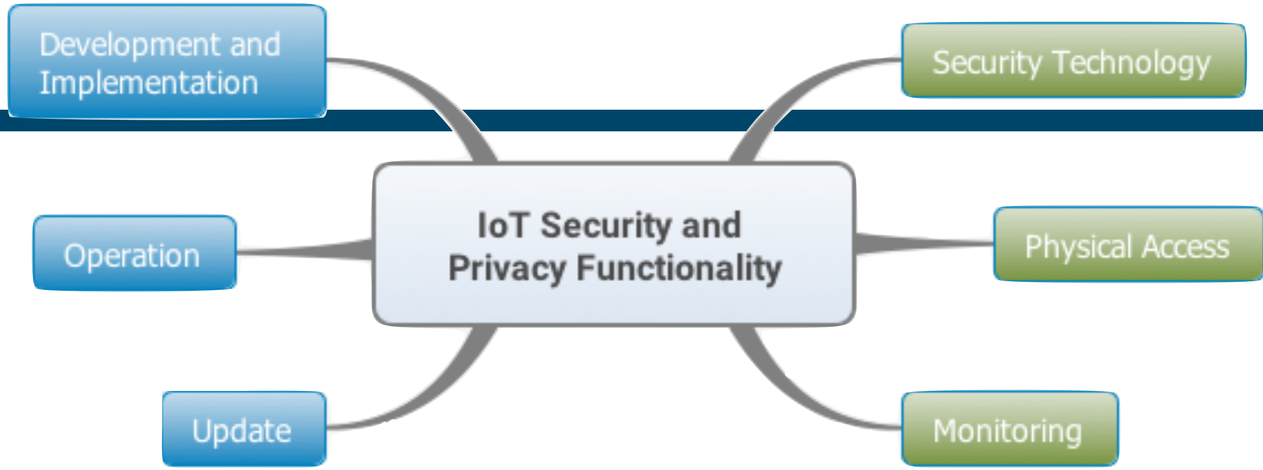


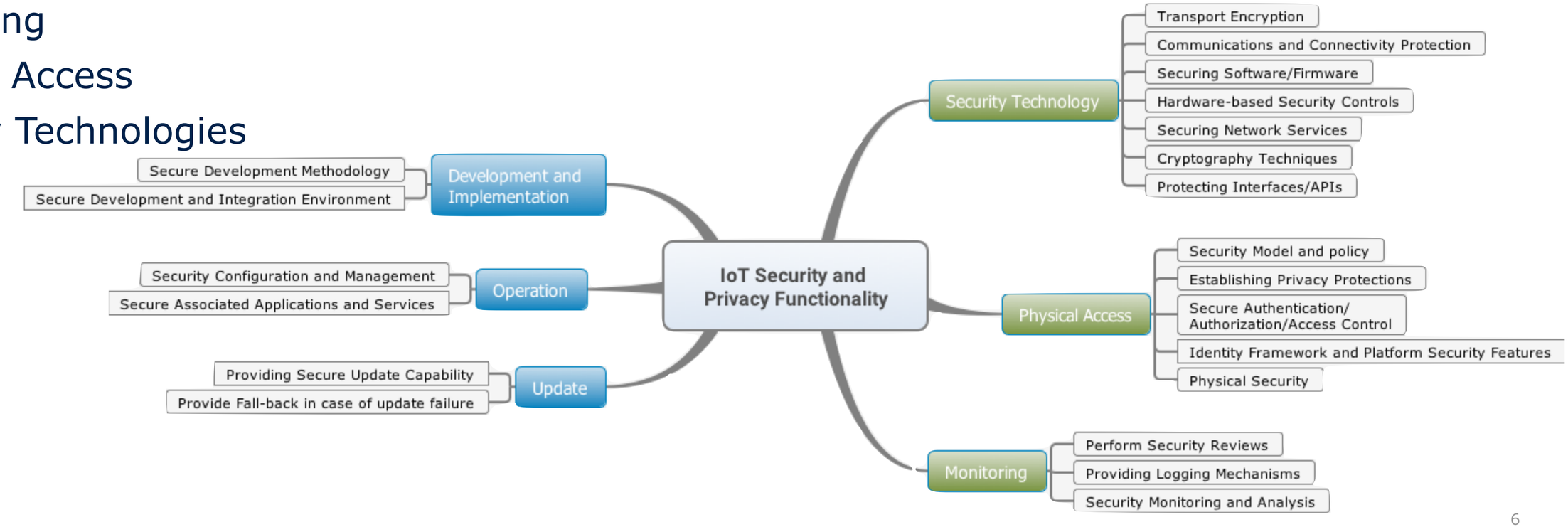
- SCOTT
  - Security classes
  - Measurable security
  - Security metrics
  - applied where?
    - discussion: Technical board?

. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

IoT security roadmap

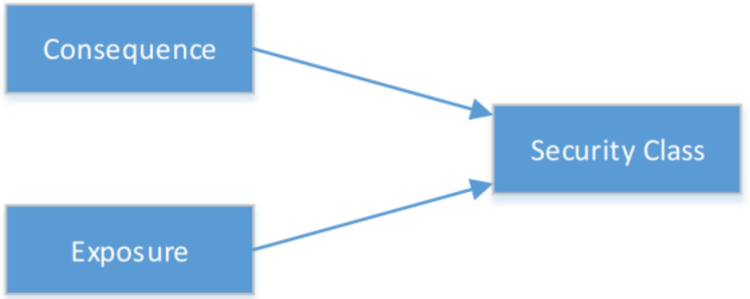
- Live-cycle of IoT
  - Development
  - Operation
  - Update
- Other aspects
  - Monitoring
  - Physical Access
  - Security Technologies





Security Classes and measurable security

- Security Class in IoT
  - Consequence
  - Exposure
- Consequence
  - as in risk map
- Exposure
  - Physical exposure
    - people, building, physical ports,…
  - IT exposure
    - ports, firewall, connectivity



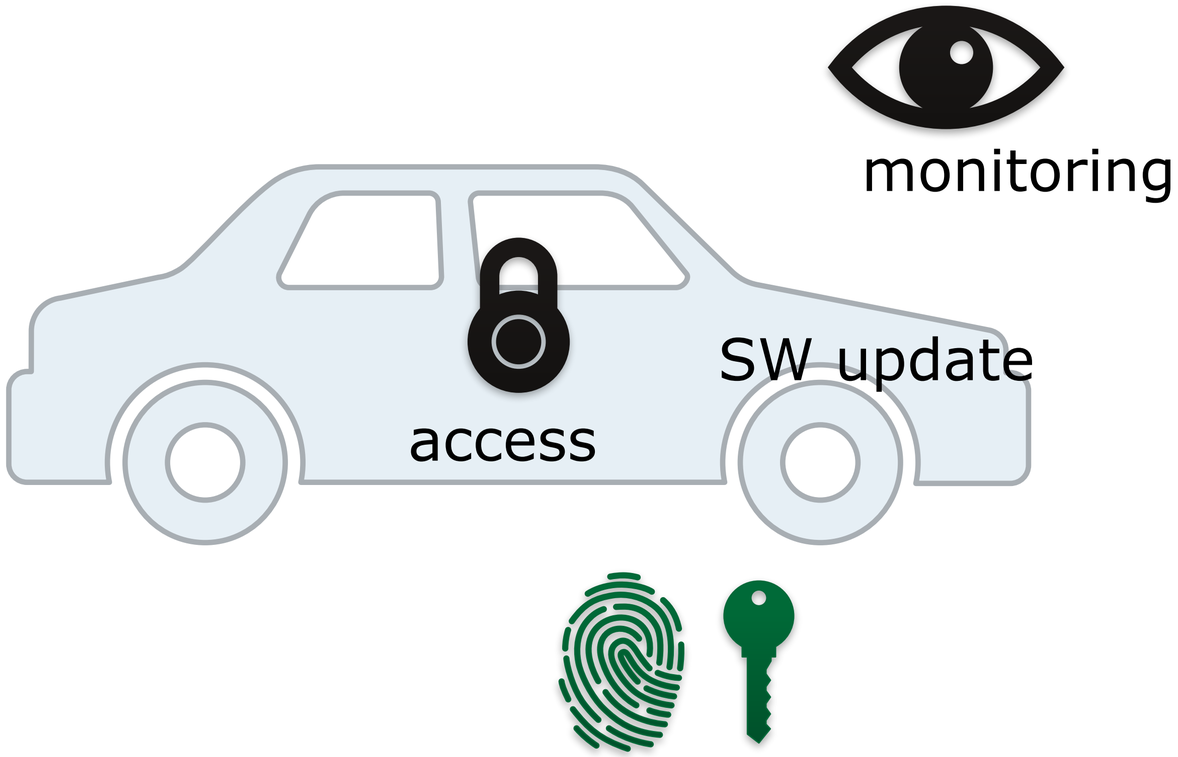
New postulate of security class

5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Class 4	Class 4	Class 5
3	Class 3	Class 4	Class 4	Class 4
2	Class 1	Class 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

Domain specific applicability: Automotive

- Suggested methodology:
- The car as a system of systems

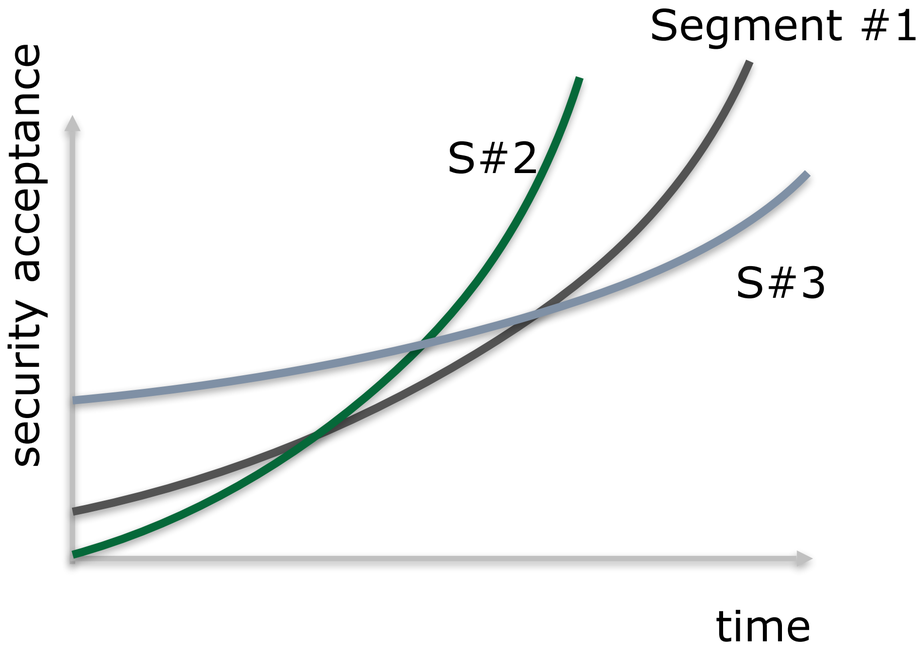
- For each subsystem, perform
- Security classes: 1-5
  - Exposure analysis of components
  - Impact analysis



Required: Roadmap for technologies

- Technology Roadmap for uptake
  - Segment specific (car, home, cloud, ….)
  - best praxis
  - obstacles

- Expected outcome from SCOTT
  - Privacy labelling
  - Security classes
  - increased Trust



Answer the Challenges addressed by the EU

DIGITALEUROPE

Our Work | Press Room | Services | Events | About Us | Why Join Us | A A

D

DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes

Brussels, 23 March 2017

RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security **certification framework for ICT products** and 2) a **"Trusted IoT label"** giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

2. Trusted IoT Label

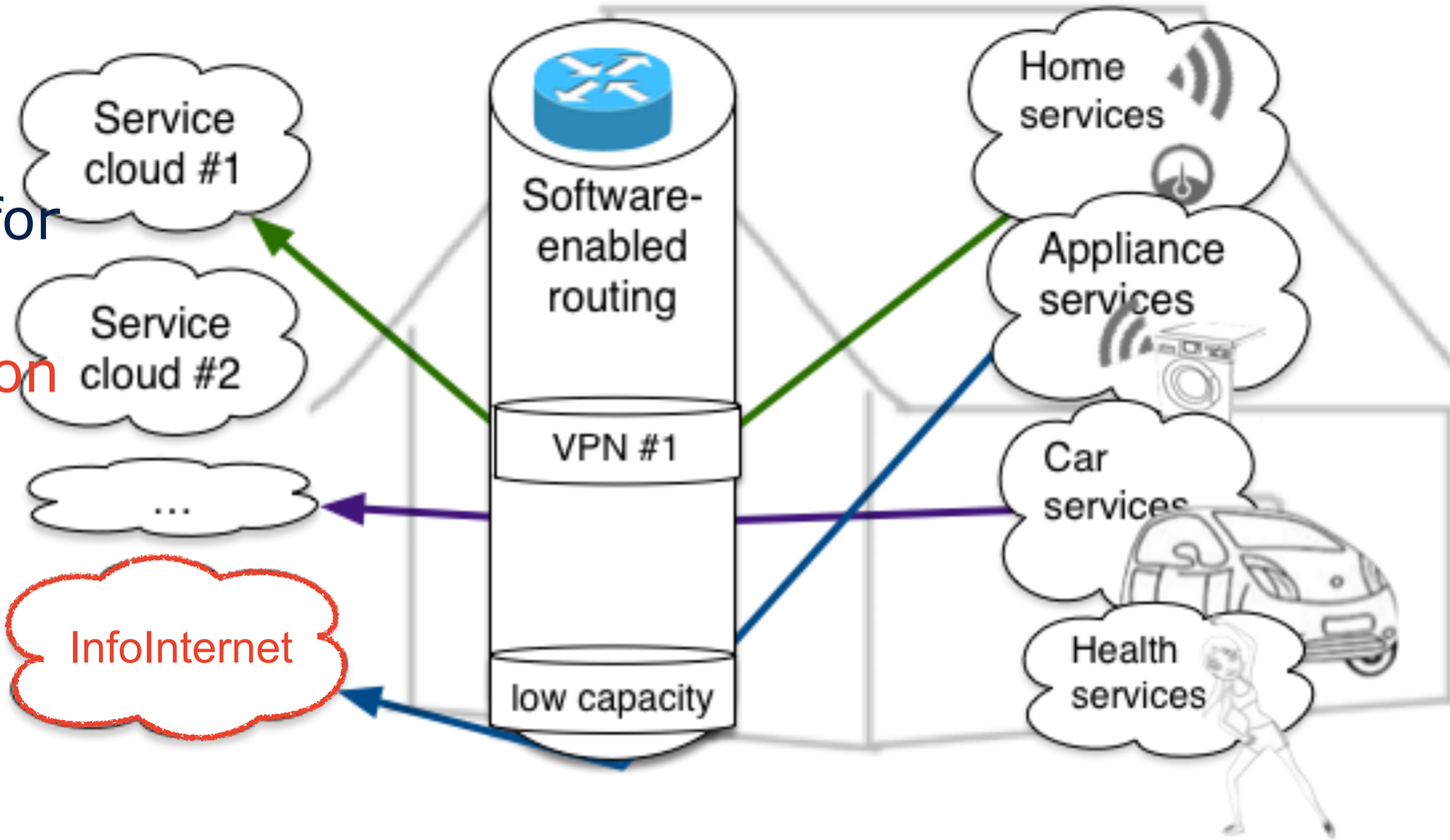
In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.

our contribution: privacy label?

Suggestion:
High-level vision for each domain

- Home/Infrastructures: Cost-efficient monitoring and management for trusted services
- Mobile: Configurable networks providing reliable services
- Automotive: Security architecture for accident-free transport
- Rail: Highly flexible train composition
- …
- Support vision through
  - showcases
  - common security assessment
  - highlights, e.g. “InfoInternet: free access to Information for all”

Example: Home

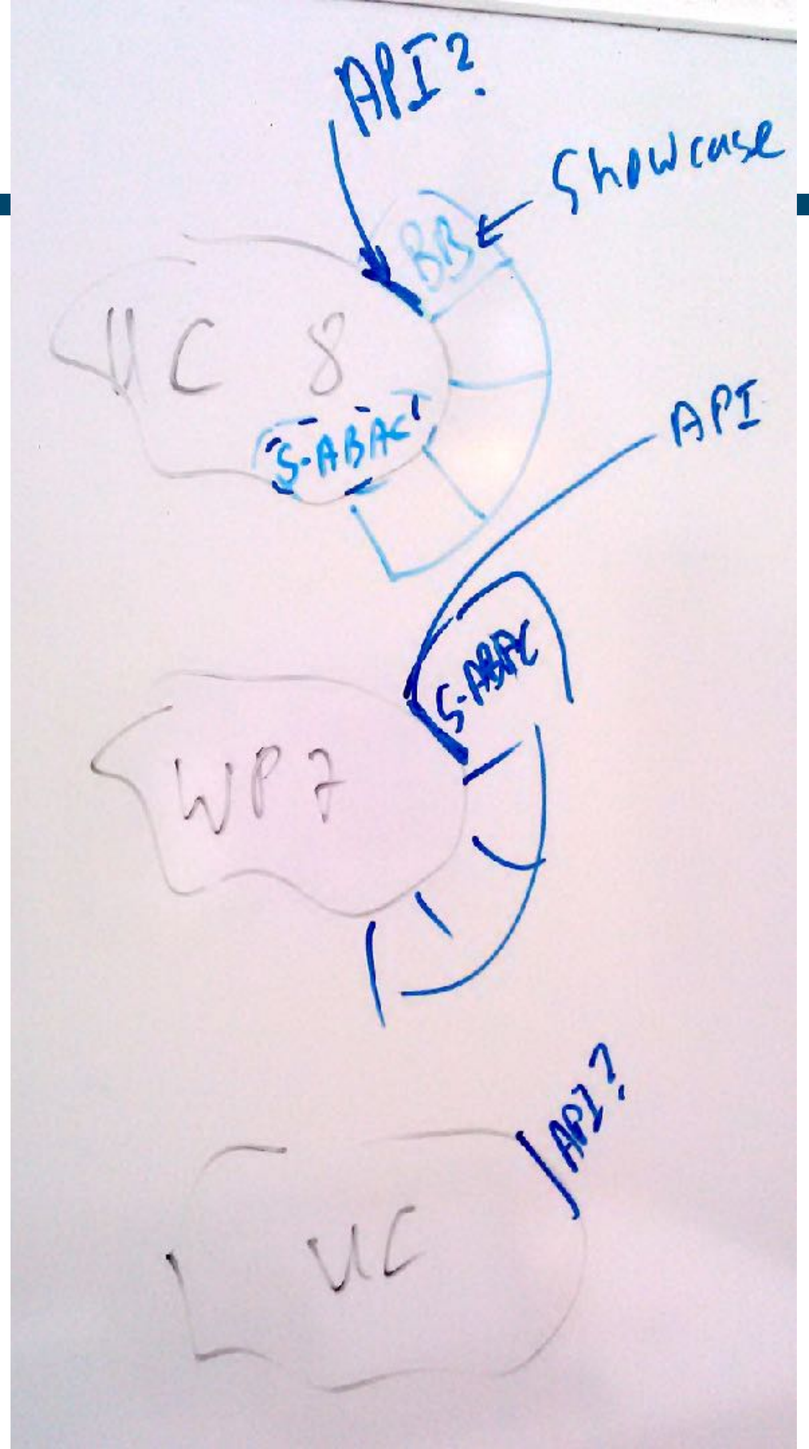


Suggestion:
Showcases for each domain

- Challenge
  - use cases have variety of building blocks
    - e.g. WP11 - 27+ Building Blocks involved
  - Implementation not clarified

- Showcase implementation
  - specific (limited) building blocks
  - focus on information exchange (API)

- Building blocks
  - describe how BB contributes to use cases (high level)
  - demonstrate on limited scales
  - concentrate on APIs



Conclusions

- SCOTT is needs the helicopter perspective
  - overall vision broken down into showcases
  - interconnected activities
  - create the discussion forum

- EU-wide impact
  - competitive advantage, e.g.:
    - privacy label
    - security classes
    - security and privacy ontology
    - reference architectures for sectors

New postulate of security class

5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Class 4	Class 4	Class 5
3	Class 3	Class 4	Class 4	Class 4
2	Class 1	Class 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+