Security and Privacy Challenges in the Internet of Things

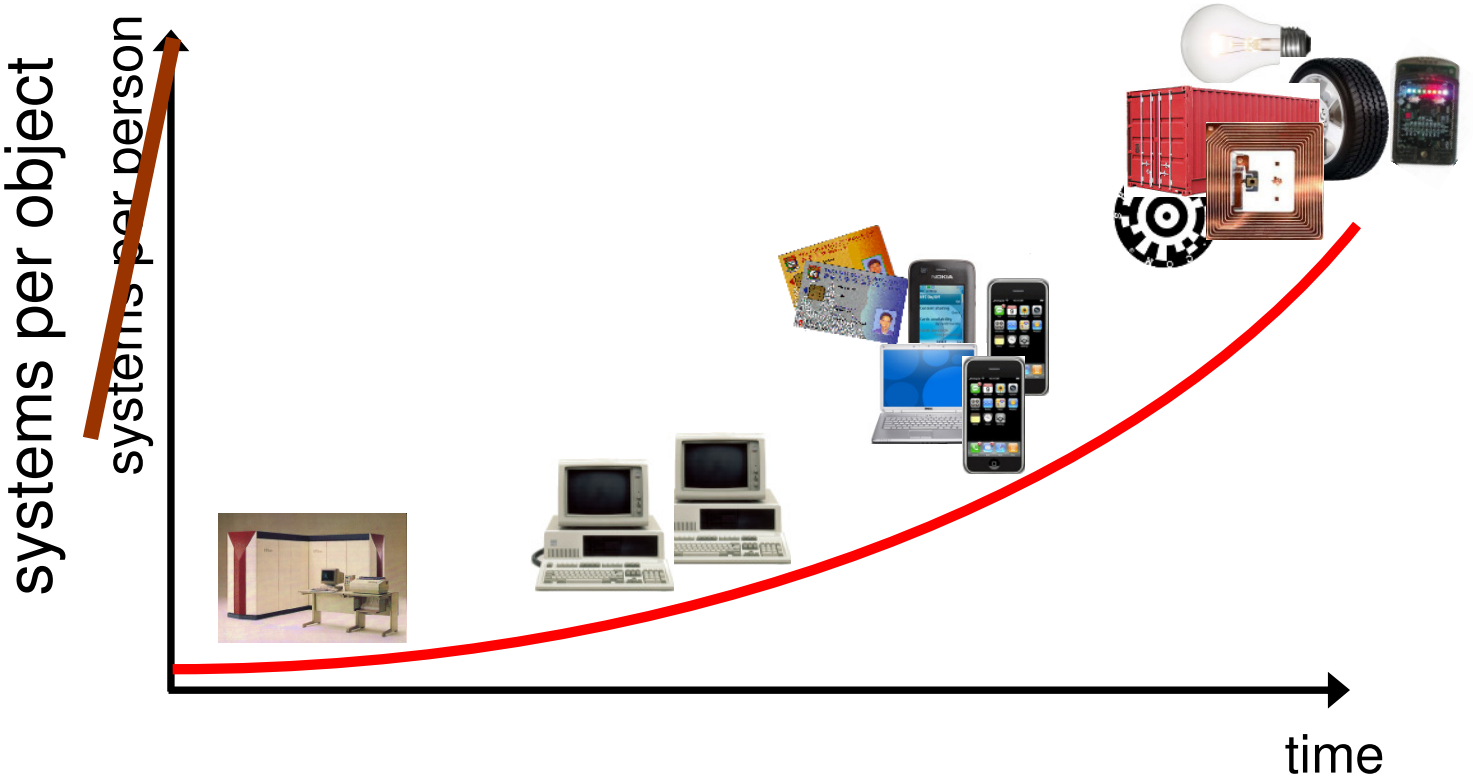
Christoph P. Mayer

6. Mar 2009 - KiVS Workshop on Global Sensor Networks (GSN09)

Institute of Telematics, University of Karlsruhe (TH)
Karlsruhe Institute of Technology (KIT)

Internet of Things … a new Era

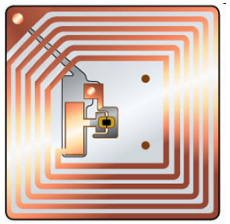
- Evolution of our technological environment



Every object has an identity
→ lives in the physical *and* in the digital world

Is the Internet of Things here already?

- Wall-Mart uses RFID heavily in supply chain
  - forced suppliers to use RFID tags
  - faster handling
    → scan pallet of goods
  - general: 1.8bn RFID tags produced 2005, 33bn forecast 2010



identity linking

- Tagging the physical environment with 2D barcodes
  - 2D barcodes encode (e.g. URL, vCard, Code)
  - attach *digital information to physical objects*
  - physical world enters the digital world

www.tm.uka.de/~mayer

identity linking

- Monitoring environment
  - sensor nodes for e.g. volcano activity

environmental property linking

Integration of different technologies will spawn great value → physical-digital world mashups

RFID ⊂ Internet of Things

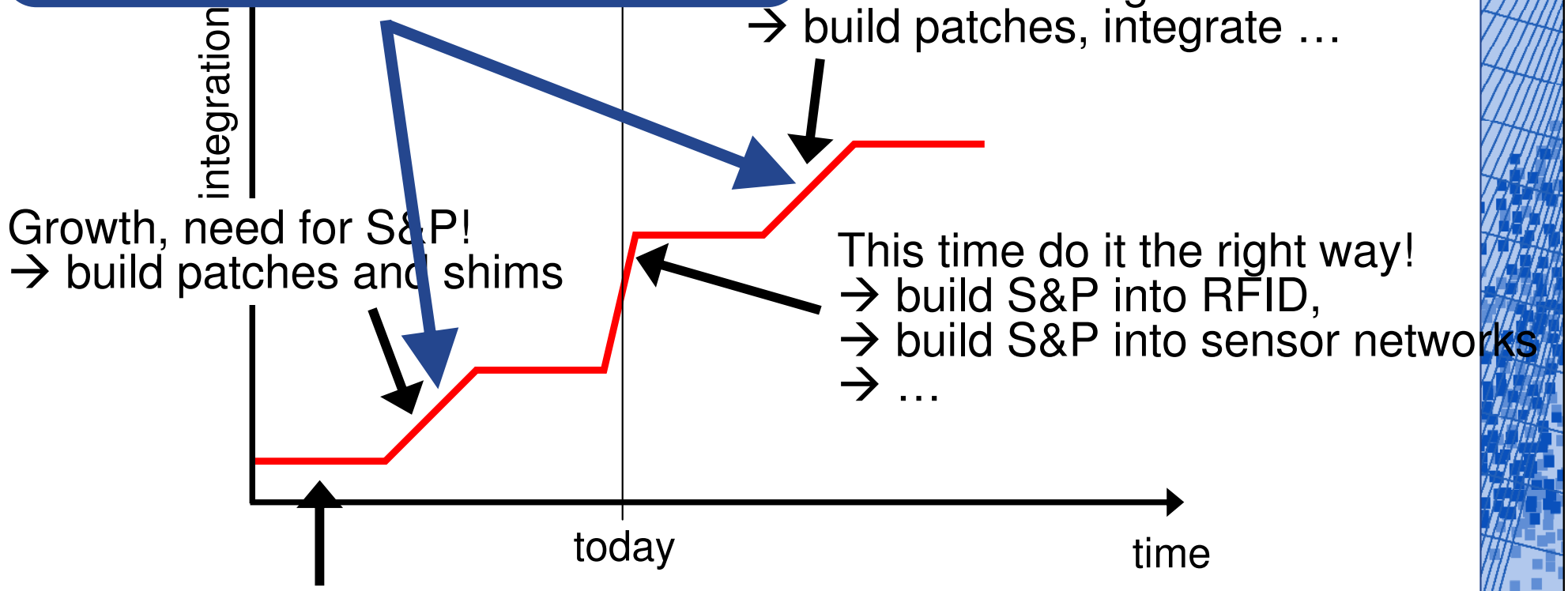
- RFID is *not* the Internet of Things
  - one of many enablers for the Internet of Things
  - currently the most popular with large number of deployments

  → looking at security and privacy only from the RFID perspective is wrong!
- Pitfalls from thinking RFID is all
  - Evolution of an RFID object name service (ONS)
    - other identification techniques need object registries, too
    - what about 2D barcodes, sensor nodes, etc.
    - ONS should be about identities, not bound to identification technology
  - Broken Security&Privacy model for Internet of Things
    - S&P research in RFID, in sensor networks, in …
    - think of a system that uses RFID, sensor networks, mobile phones … how to integrate? RFID tag and 2D barcode attached to sensor node?
    - will seperate security models prevent a system model?

→ Thinking of the Internet of Things in more general may yield a better security and privacy model

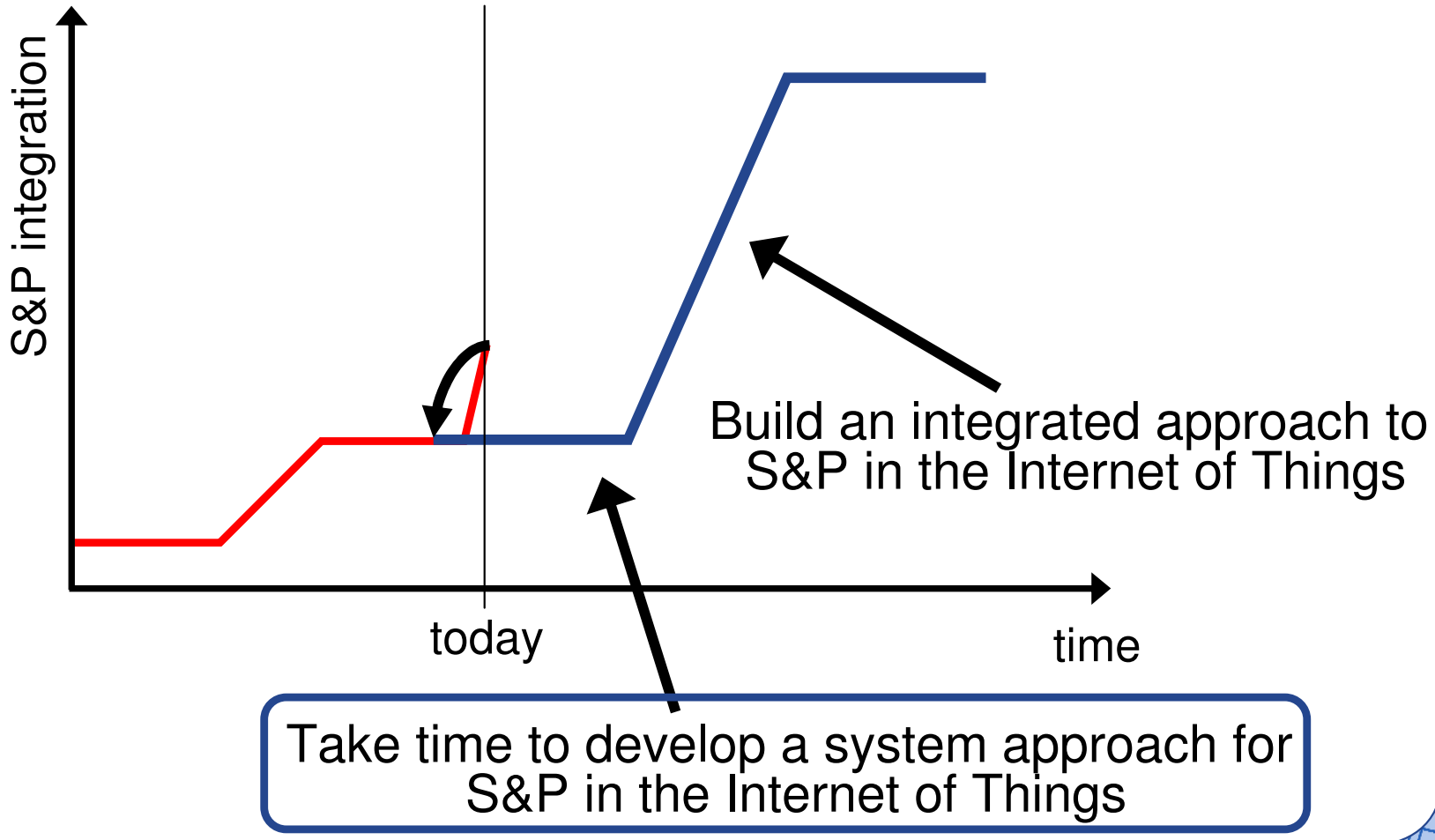
Evolution of Security&Privacy

Did we really learn from the past?



Evolution of Security&Privacy

- Is there a better evolutionary road?



Systematic Approach to Security&Privacy

- First small steps towards systematic approach

1. Categorization of topics in the Internet of Things
   - Take a step back from the technical perspective
   - What are the generic topics taking part?

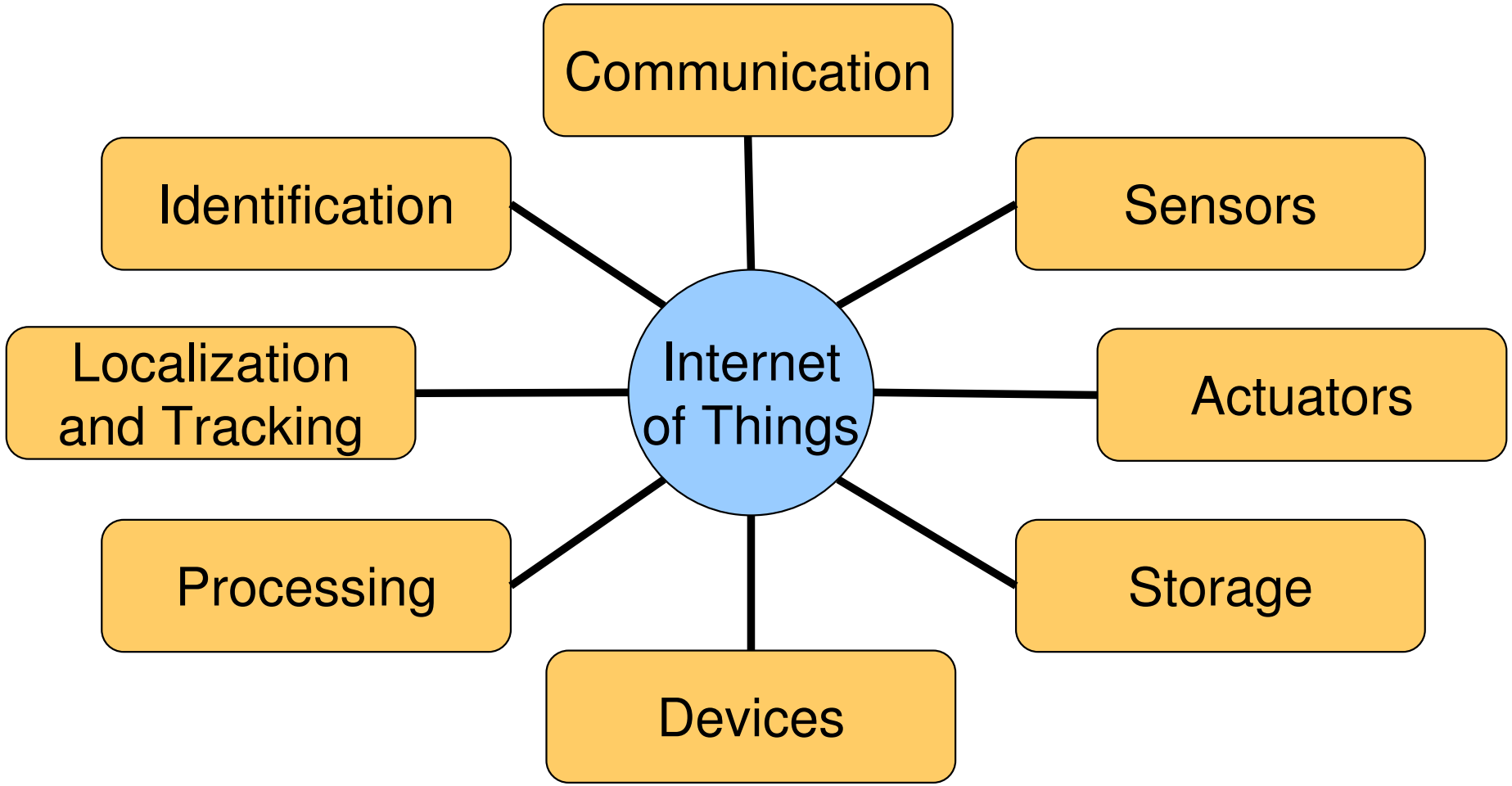
2. Assign technologies to topics
   - What technologies fall into which topics?
   - Do technologies appear in several topics?

3. Analyze sensitivity of topics to S&P
   - See how sensitive topics are to S&P properties?
   - Don‘t analyze technologies, analyze topics!

4. Analyze state of research in topics
   - How much research has been done for the S&P properties?
   - Has something been neglected?

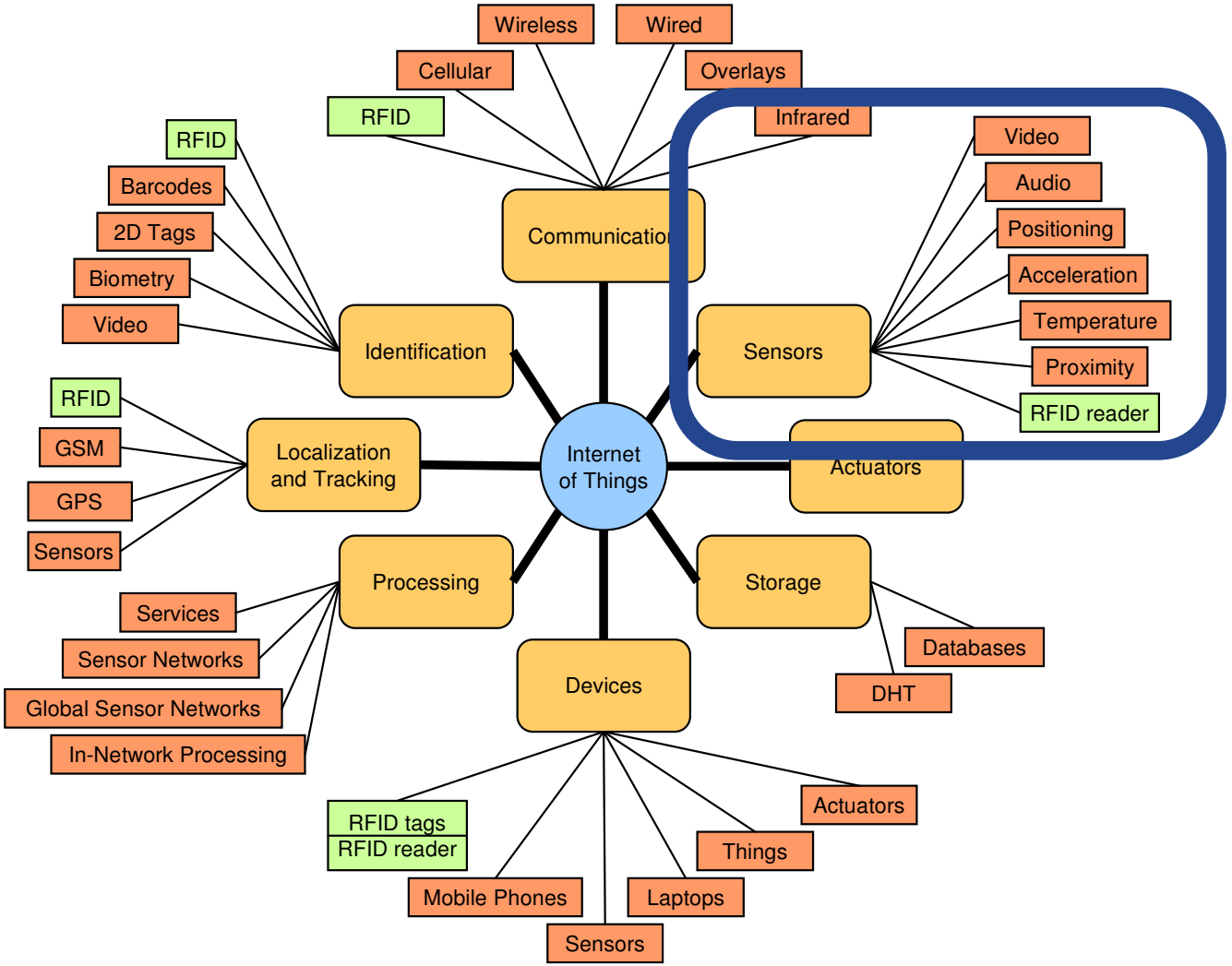
Categorization of the Internet of Things

- What topics make up the Internet of Things



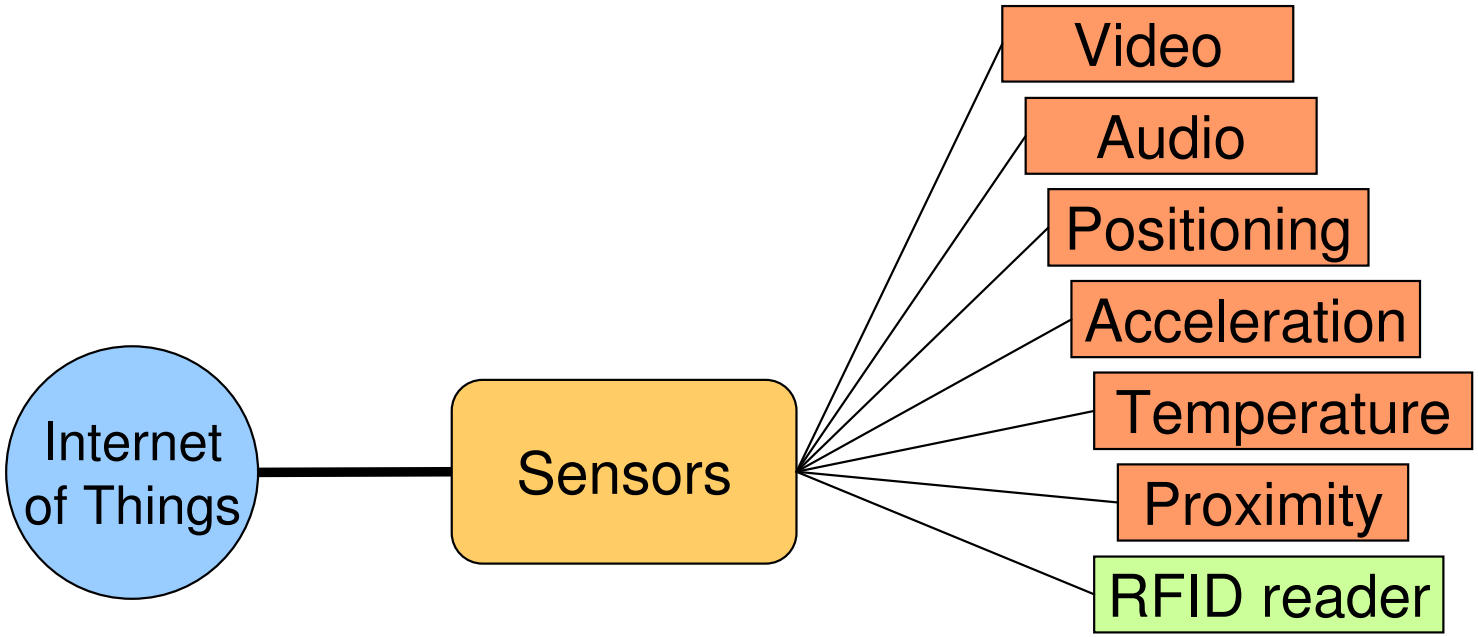
Categorization of the Internet of Things

- What technologies are attached to the topics



Categorization of the Internet of Things

- What technologies are attached to the topics

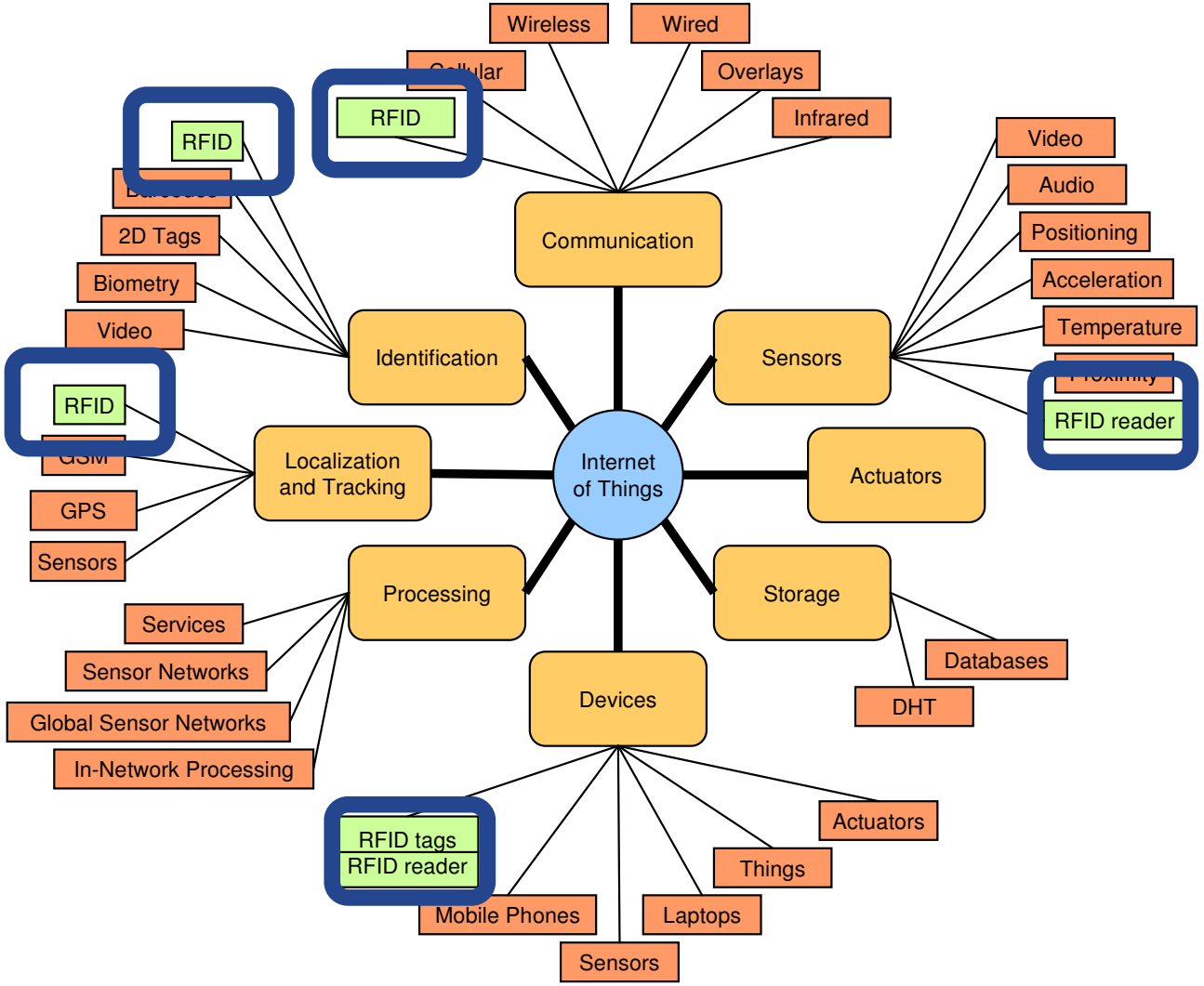


- Definitely not complete, needs more work
  - but completeness it not the point here!

  → providing a first approach to categorization

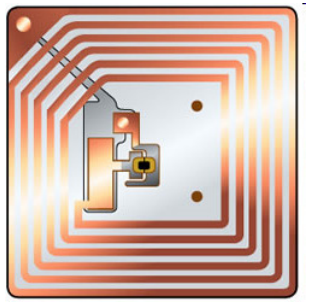
The Role of RFID

- Important point: RFID spans several topics



The Role of RFID

- Important point: RFID spans several topics
  - Communication
    - between tag and reader
  - Sensors
    - the reader senses the tag
  - Devices
    - reader and tag are devices
  - Localization/Tracking
    - if you know the reader location, you roughly know the tag and therewith object location
  - Identification
    - the unique identification of the tag through the reader



Categorization of the Internet of Things

- Mid summary: takeaway points from last slides
  - RFID is assigned to several topics
  - Being unaware of this dual-use can end up badly
    - Same with IP addresses! Used as locator and identifier. Now research into ID/Locator split
  - Point is not to take RFID apart technically, but be aware of the multi-use when developing protocols
  - S&P currently done per technology, not per topic

Key question

Is it possible to design generic S&P mechanisms for a *topic* rather than for a *technology*?

Sensitivity to Security&Privacy

- Now that we have the general topics
  → how sensitive are they to S&P properties?

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	+++	+++	+++	++	+++	+
Sensors	+++	++	+	+++	+	+++
Actuators	+	+	+		+	++
Storage	+++	++	+++	+++	+	+++
Devices	+++	+	+	++	++	++
Processing	++	+	+	+++	+	+++
Localization/Tracking	+	+	+++	+++	+++	+++
Identification	++	+	+++	+++	+++	+++

- Example
  - Communication has high sensitivity to confidentiality
    - don‘t want others to read my data
  - Sensors have low sensitivity to confidentiality
    - can always place my sensor near and sense the same physical property, therefore *sensing in itself* is not confidential

State of Research

- State of research in areas highly sensitive
  → research areas that have been neglected?

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability
Communication	2	2	3		1
Sensors	2			1	
Actuators					
Storage	3		3	1	
Devices	1				
Processing				1	
Localization/Tracking			3	1	2
Identification			3	1	2

- Example
  - Devices highly sensitive to integrity but few research
    - devices that can affect to the physical world
    - physical world DDoS from digital systems

Generic Security&Privacy

- And what now?
  - categorization and analysis is a first step towards understanding the Internet of Things
  - need to work out details

- Develop generic S&P mechanisms
  - that work on a topic, not on a technology
    - similar to privacy preserving data-mining
    - makes interworking between technologies easier
  - generic mechanisms with specializing properties
    - can't deploy protocol for RFID and WLAN communication, but what about RFID and 2D barcodes?
    - what are the common, what is different?
    - proving properties of the protocol can be easier

→ Enables to develop an integrated S&P approach for the Internet of Things

Conclusions

- Summary
  - RFID ≠ Internet of Things, need more generic S&P approach
  - looking at topics, not directly at technologies can make it easier to develop a S&P model
  - generic S&P mechanisms can provide better interworking that is required for the Internet of Things
- Outlook
  - categorization, sensitivity etc. only reflect my opinion, need discussion about these
  - try to develop generic mechanisms, is it possible, is it better?
  - learn from others
    - cryptographic identifiers, privacy preserving data mining, …
    - multi-channel protocols (difference between RFID and 2D barcodes? → mainly the channel)

Thank you!
Question?