ITU-SUDACAD Regional Forum on Internet of Things for Development of Smart and Sustainable Cities

Khartoum, Sudan 13-14 Dec 2017

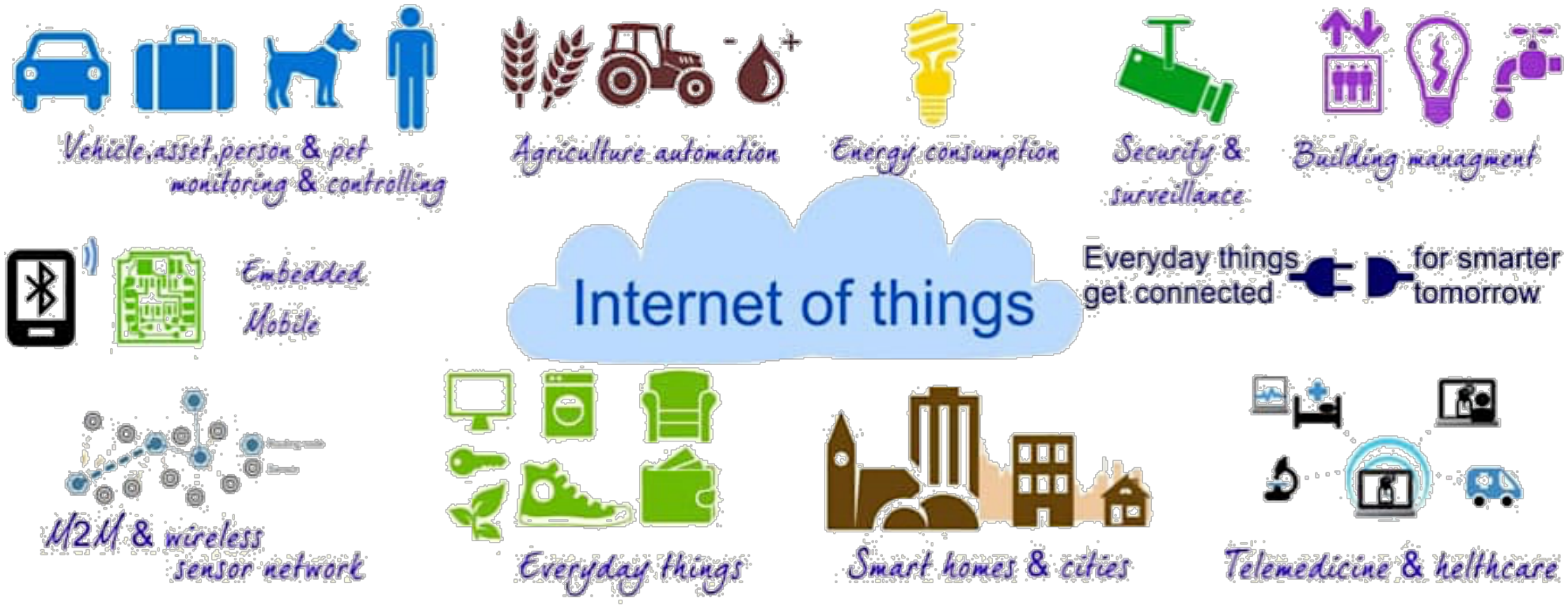
Privacy and trust in IoT

Gopi Garge

Agenda

- The context of SSC
- Trust & Privacy – Some thoughts
- Technology for Trust?
- Privacy
- Conclusion

Enablers of SSC



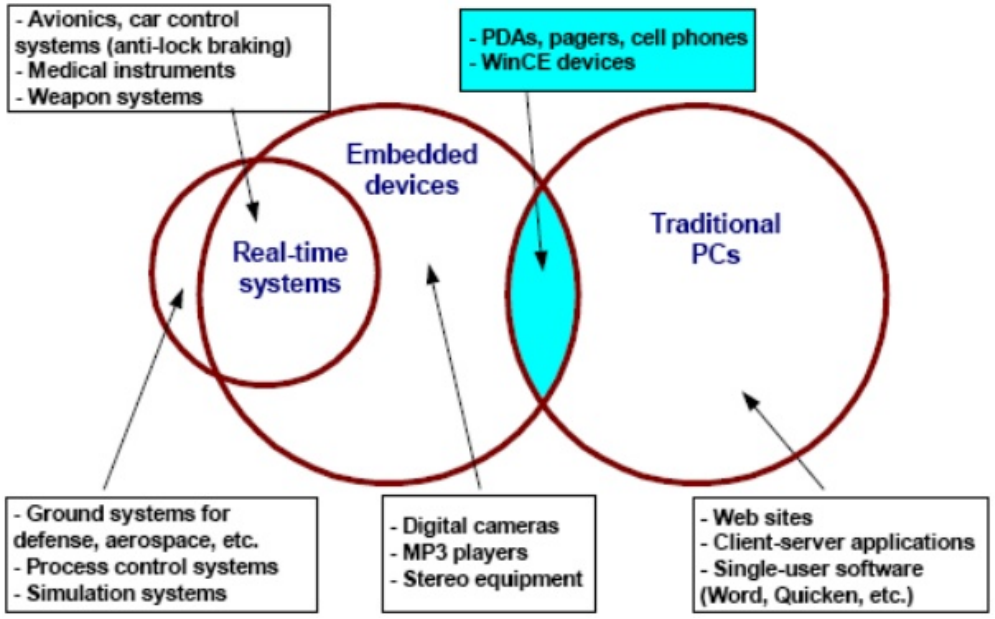
Source: https://disruptionhub.com/wp-content/uploads/2014/11/internet-of-things.jpg

SSC evolves into

Source: http://www.embedded-computing.com/embedded-computing-design/security-for-iiot-embedded-devices-a-platform-based-approach#

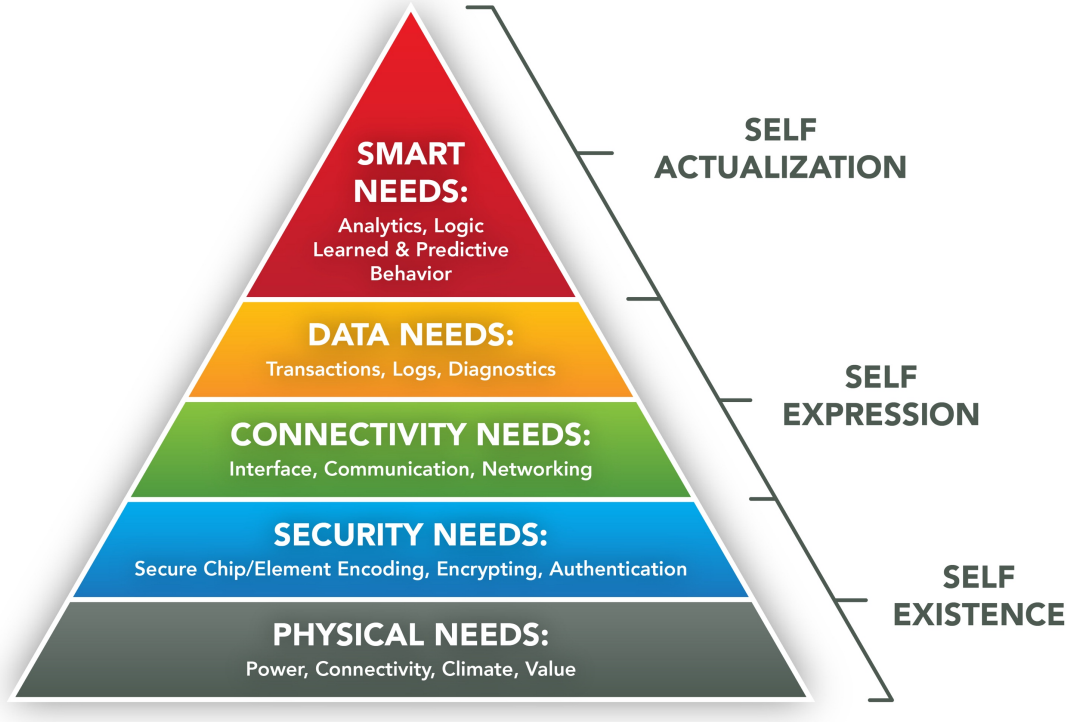
The SSC Context

- Interconnectivity
  - Layered and complex
- Devices
  - Wide variety of capabilities and application contexts
  - Independently powered, Embedded, Autonomous
- Networks
  - Dense at the edge
  - Converging traffic towards gateways
  - Substantially wireless; Guaranteed delivery?
  - Infrastructure
    - Single network, multiple services? (SoA, SDN, ..?)
    - Single backbone, multiple edge networks?
    - Multiple networks?



The SSC Context - 2

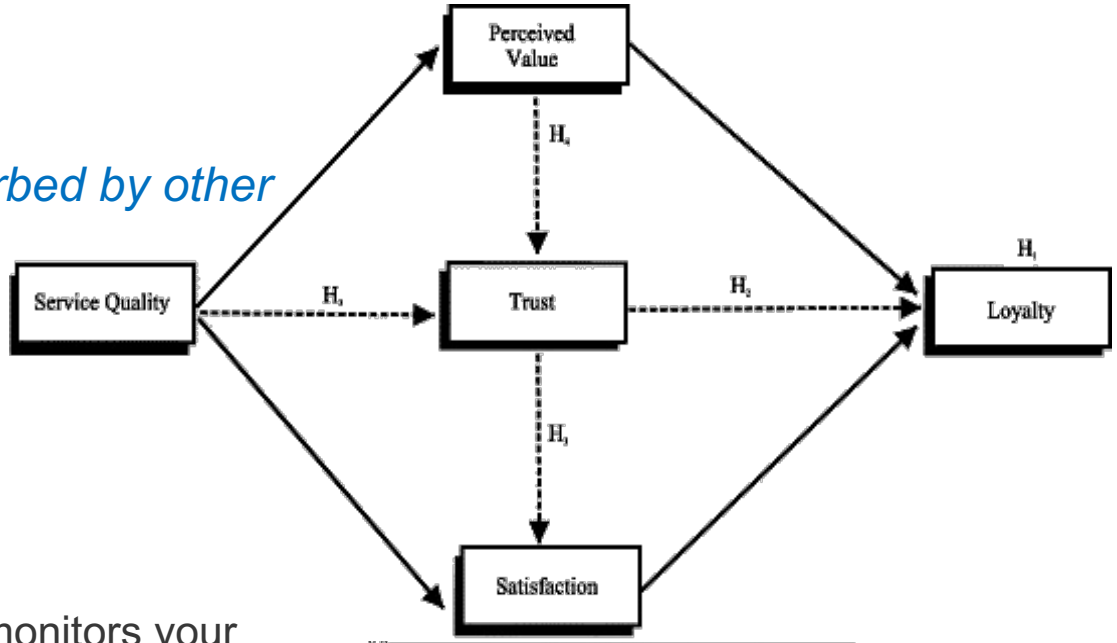
- Data Generated
  - Volumes, storage, archives
  - Ownership
  - Sharing, Open data
- Services
  - Interactions between services
    - For data exchange
    - For information extraction
  - Common point of service delivery
    - Each service with a different app? NO!
    - Multiple authentications? NO
- How would arbitration work?

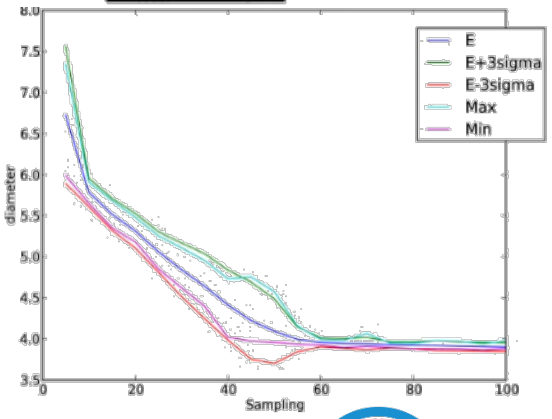


Source: https://techcrunch.com/2015/09/05/the-hierarchy-of-iot-thing-needs/

Trust and Privacy

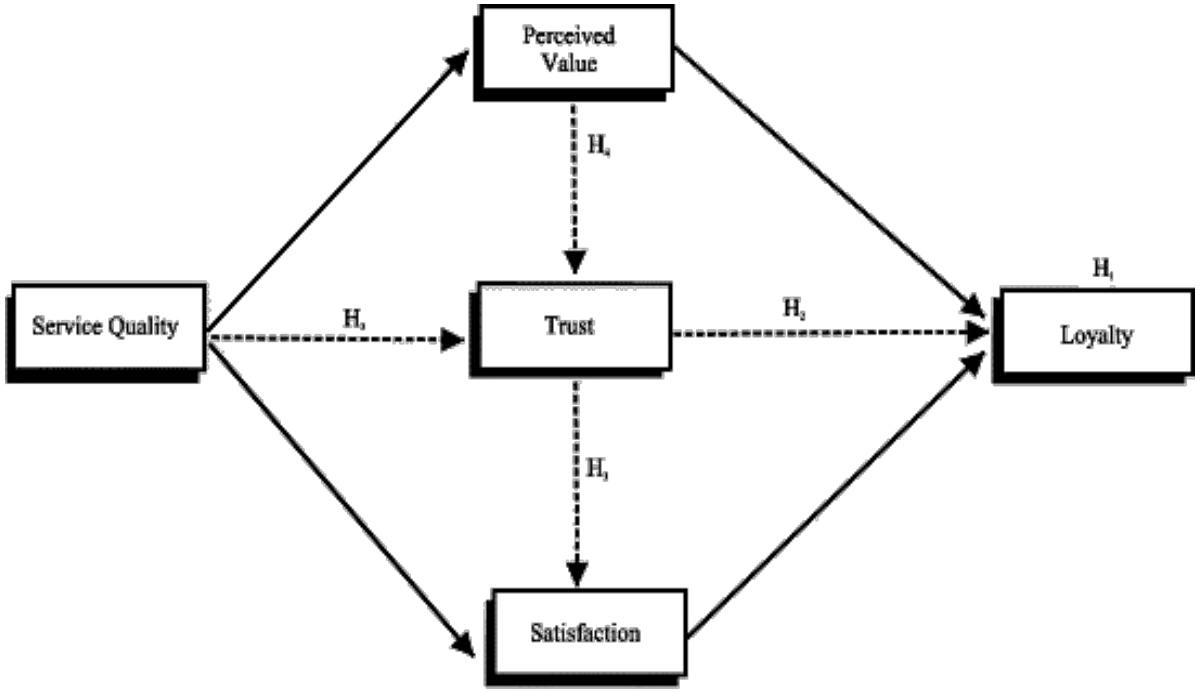
- Privacy – "*a state in which one is not observed or disturbed by other people; the state of being free from public attention*"
  - Data
  - Information
  - Individual
- Data
  - Who owns it? Users?
  - Is it shared? Who authorizes it?
  - Eg: The highways authority monitoring traffic effectively monitors your movement!
- Trust - *firm belief in the reliability, truth, or ability of someone or something*
  - Devices – their presence and location, the data they generate, their functions and interaction
- Levels of Trust?
- Trust Networks? Is a zero trust architecture feasible?

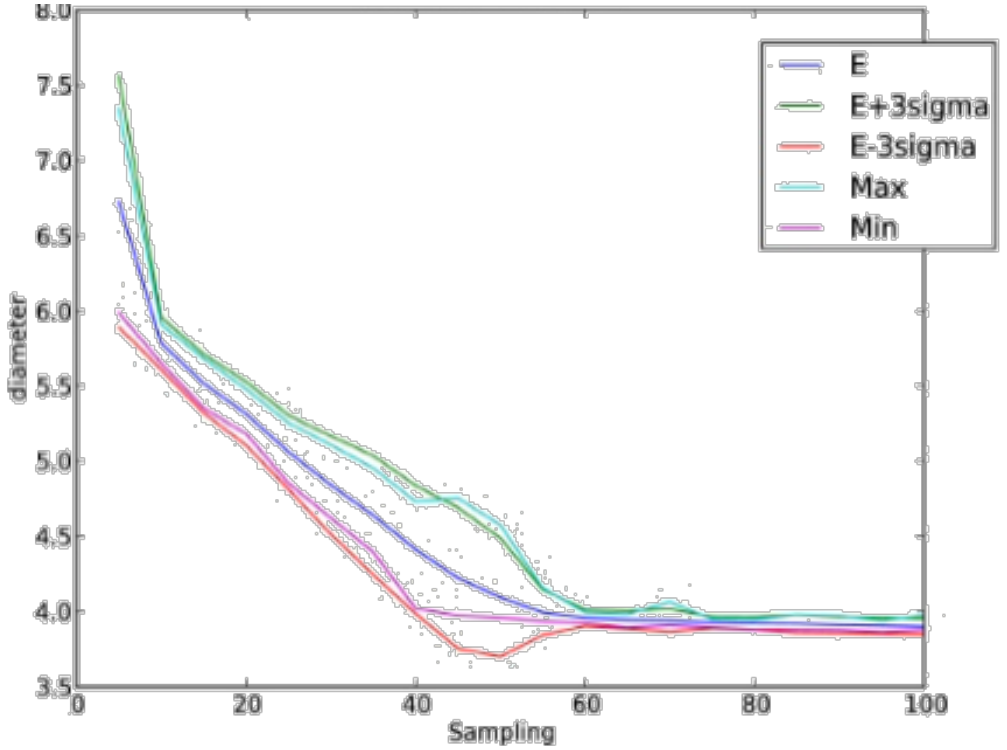




Source: Harris, L.C. and Goode, M.M., 2004. The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of retailing*, *80*(2), pp.139-158.

Trust & Privacy



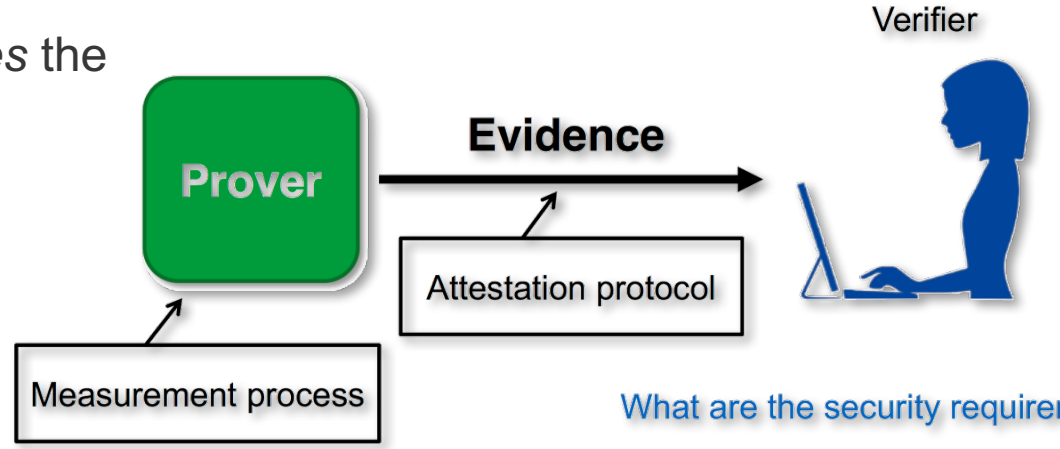


Source: konegis@uni-koblenz.de

There is a lot of housekeeping required. How will it be done? Centralised or Distributed?

Trust

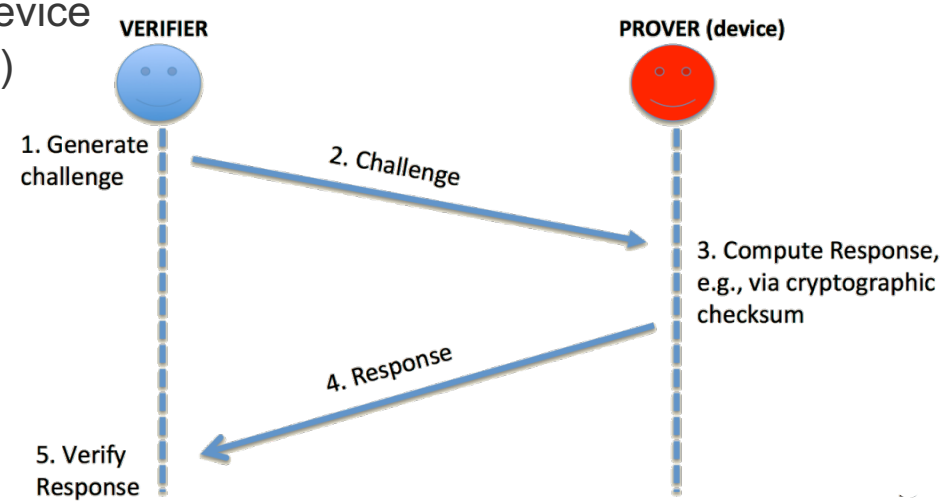
- Number of IoT devices *broadens and amplifies* the attack surface
  - Network
  - Software
  - Physical
- Are the devices trustworthy?
  - Do they behave as expected?
  - Are they in specific states - pre-defined/well-known states?
- Remote attestation is used for verifying states
  - Authenticate the hardware and software to a remote server



What are the security requirements?

Remote Attestation

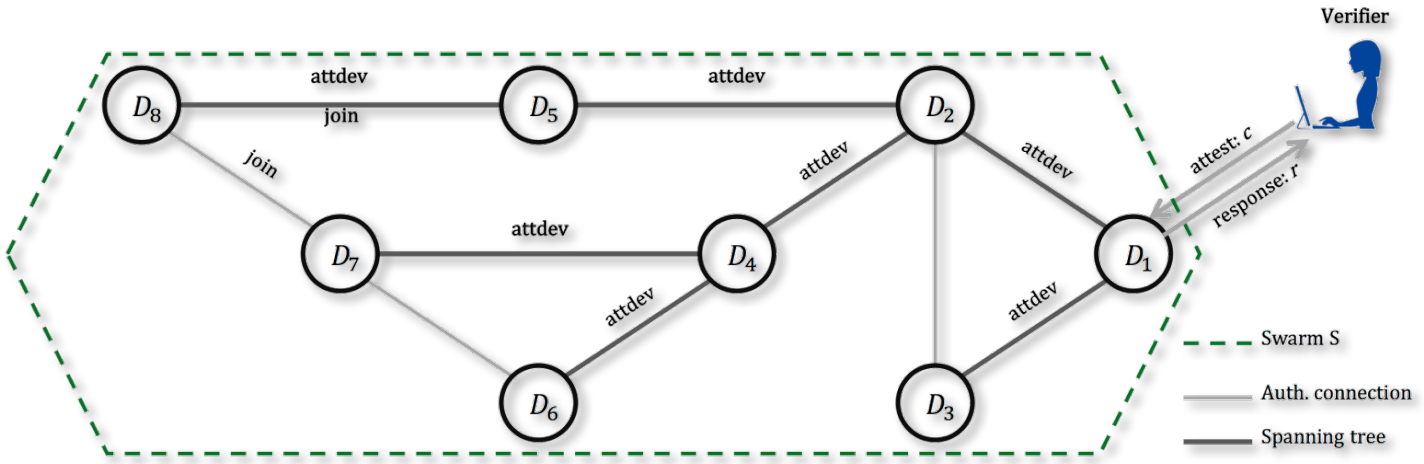
- Remote Attestation - *2-party security protocol between trusted Verifier and untrusted Prover*
  - Prover – **untrusted** (possibly compromised/infected) embedded device
  - Verifier–**trusted** reader/controller/base-station (not always present)
  - Internal state of Prover composed of:
    - Code, Registers, Data Memory (RAM), I/O, etc.
- Attestation requires:
  - Authenticity – representing the real state of the system
  - Freshness – represent the current state
- Types
  - Hardware – Trusted Platform Module (TPM)
  - Software – computes a time-optimal checksum of the verifier; “time” is limiting!
  - Hybrid



Source: gene.tsudik@ucl.edu

Implementation?

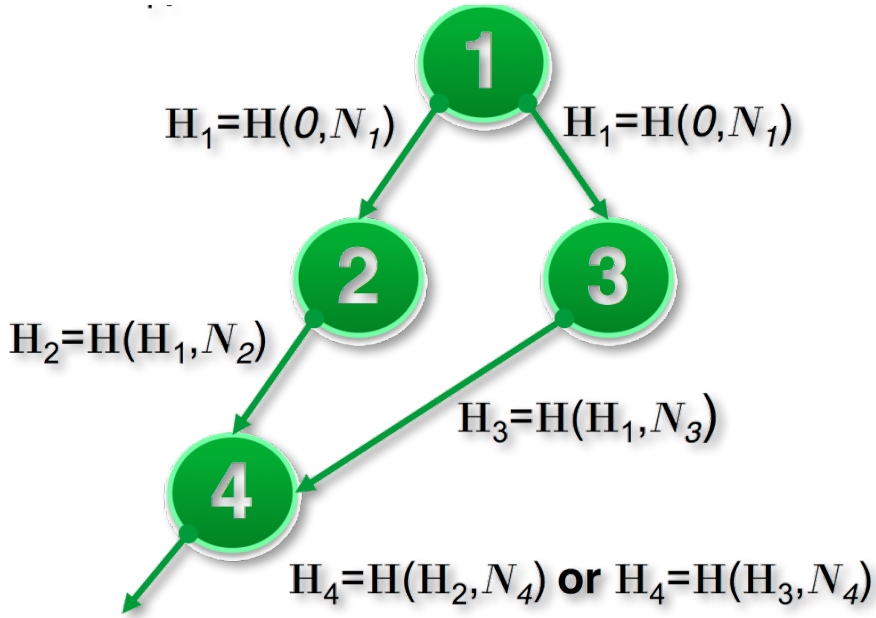
- Attestation protocols assume a single prover
  - IoT scenarios involve groups of devices (swarms) as provers
- Groups / Swarms
  - Devices can move within groups – varying topology
  - Devices can join or leave the group – dynamic membership
- SEDA: Scalable Embedded Device Attestation



Source: Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.R., Schunter, M., Tsudik, G. and Wachsmann, C., 2015, October. Seda: Scalable embedded device attestation. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 964-975). ACM.

Attestation

- Attestation schemes, currently
  - Improve security, performance and functionality
- Attestation measures binaries at load time
- Run-time attacks are not addressed
  - Control-flow attestation (C-FLAT)
  - Handles control loops too
- Property based attestation



Source: Abera, T., Asokan, N., Davi, L., Ekberg, J.E., Nyman, T., Paverd, A., Sadeghi, A.R. and Tsudik, G., 2016, October. C-FLAT: control-flow attestation for embedded systems software. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 743-754). ACM.

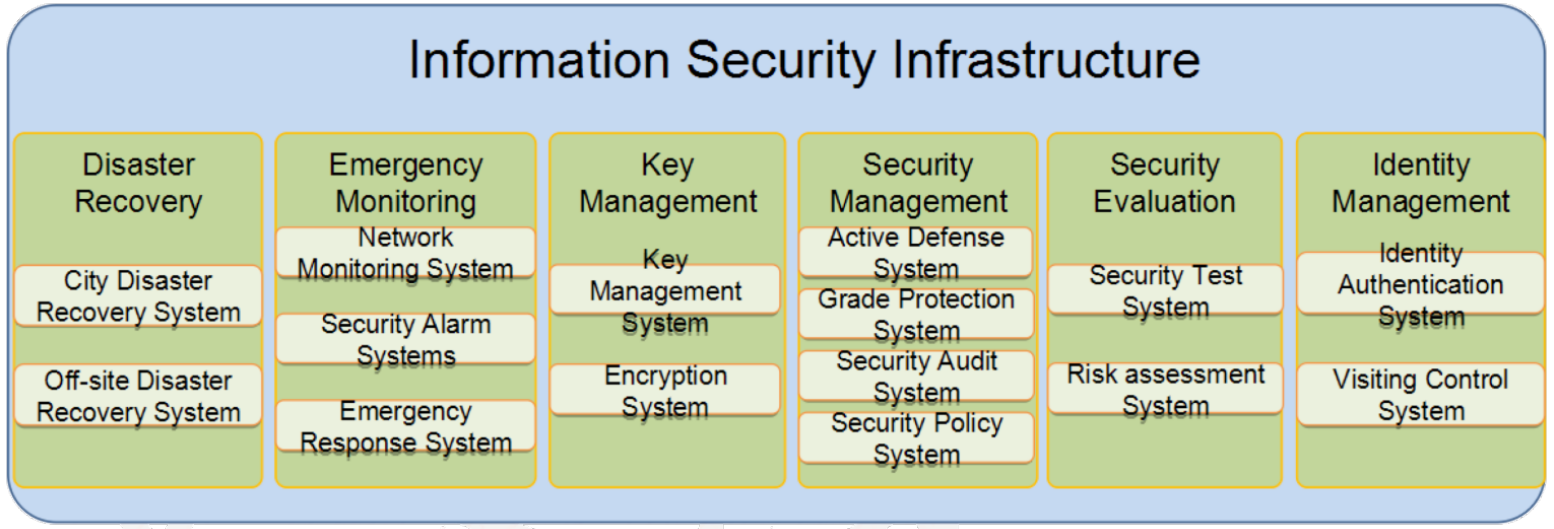
Privacy

- Privacy forms are highly inter-related
  - identity privacy (to protect personal and confidential data);
  - bodily privacy (to protect the integrity of the physical person);
  - territorial privacy (to protect personal space, objects and property);
  - locational and movement privacy (to protect against the tracking of spatial behaviour);
  - communications privacy (to protect against the surveillance of conversations and correspondence); and
  - transactions privacy (to protect against monitoring of queries/searches, purchases, and other exchanges).
- IoT and SSC touch all of these!

Kitchin, R. (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland

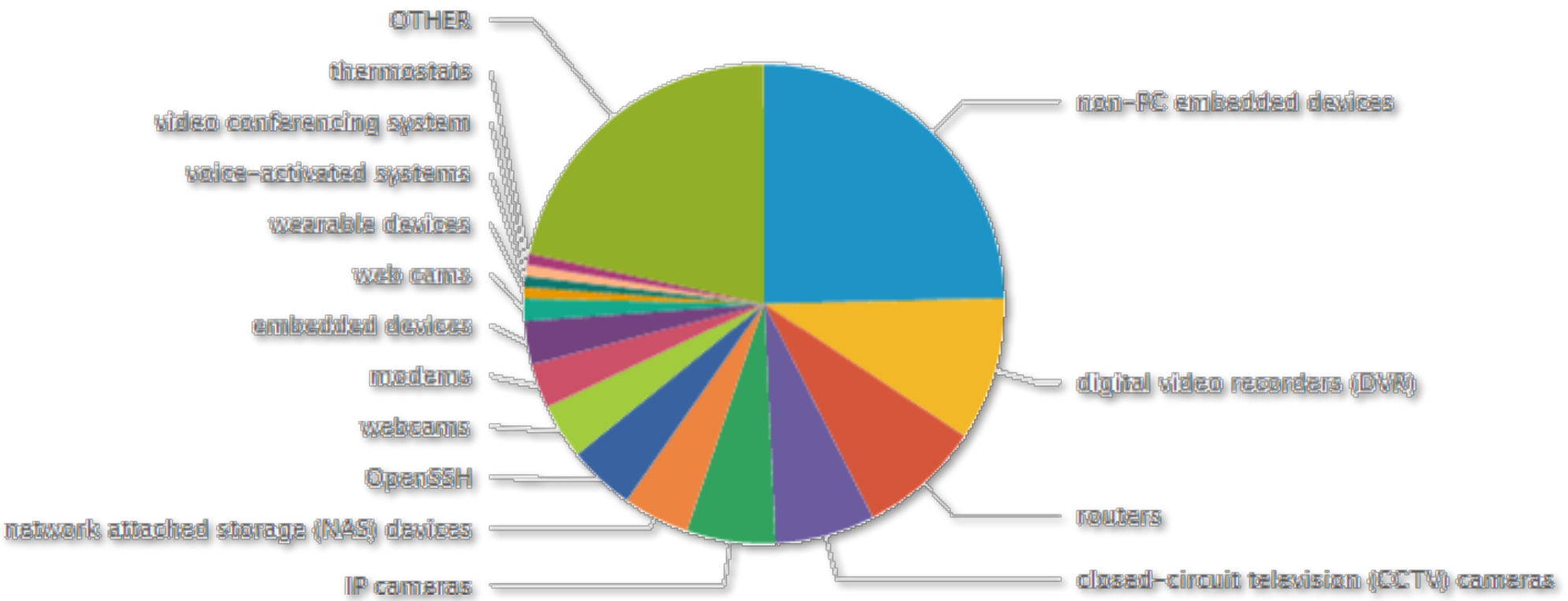
Privacy

- Data privacy
  - Fairly well addressed in the context of storage and data transport
- Information privacy
  - Connotations not fully understood in the context of IoT/SSC; easy to derive behavioural patterns
  - Several personal spaces would have personal information stored on devices
  - Seclude from public scrutiny
- Legislation



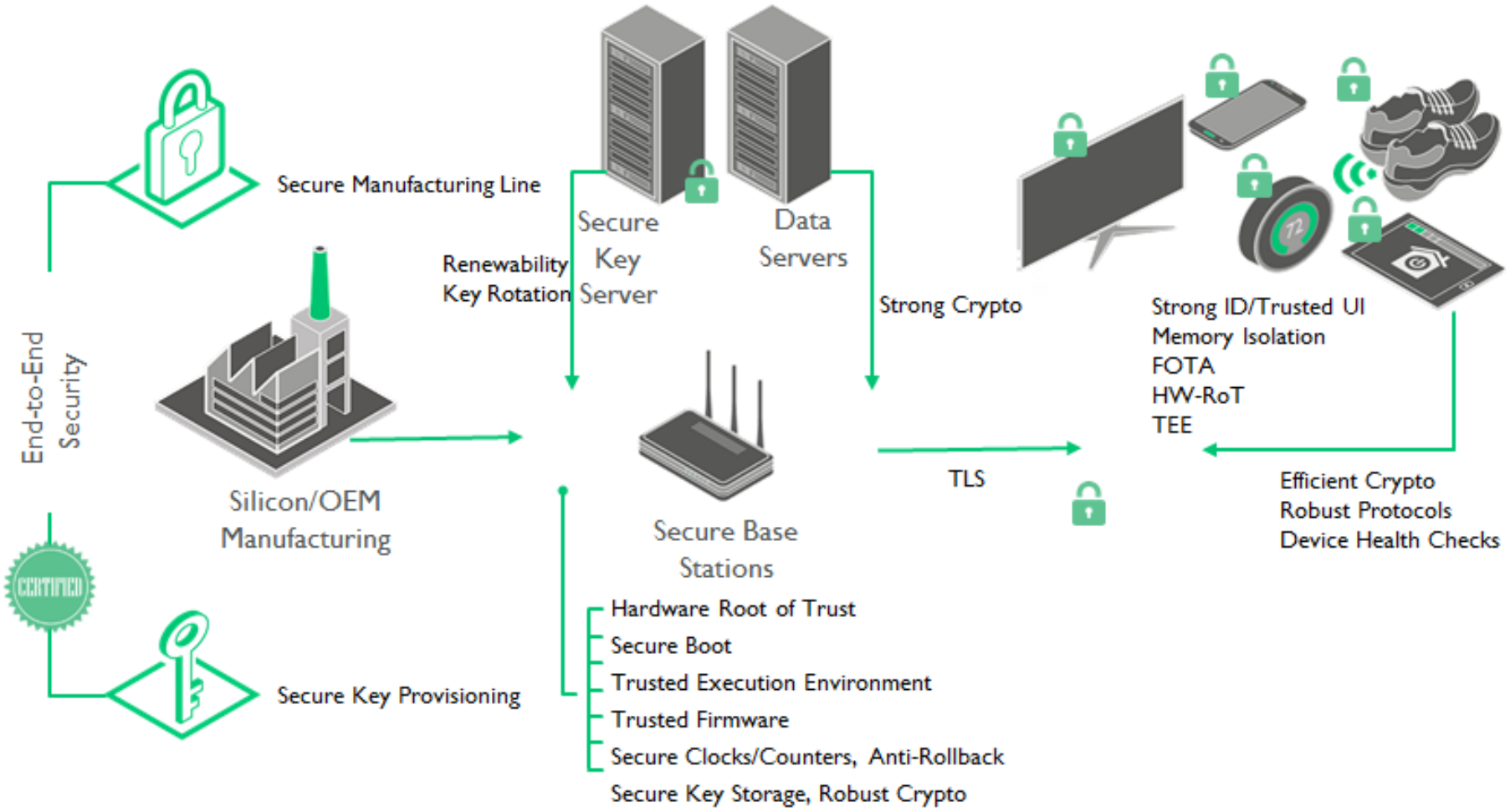
Source: FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustaintable Cities", page 16

Attack Targets



Source: https://blog.surfwatchlabs.com/2017/03/24/webinar-iot-devices-expanding-digital-footprints-security-issues/

Pervasive Security?



Source: https://community.arm.com/iot/embedded/b/embedded-blog/posts/securing-the-embedded-iot-world

The need for enforcement policies

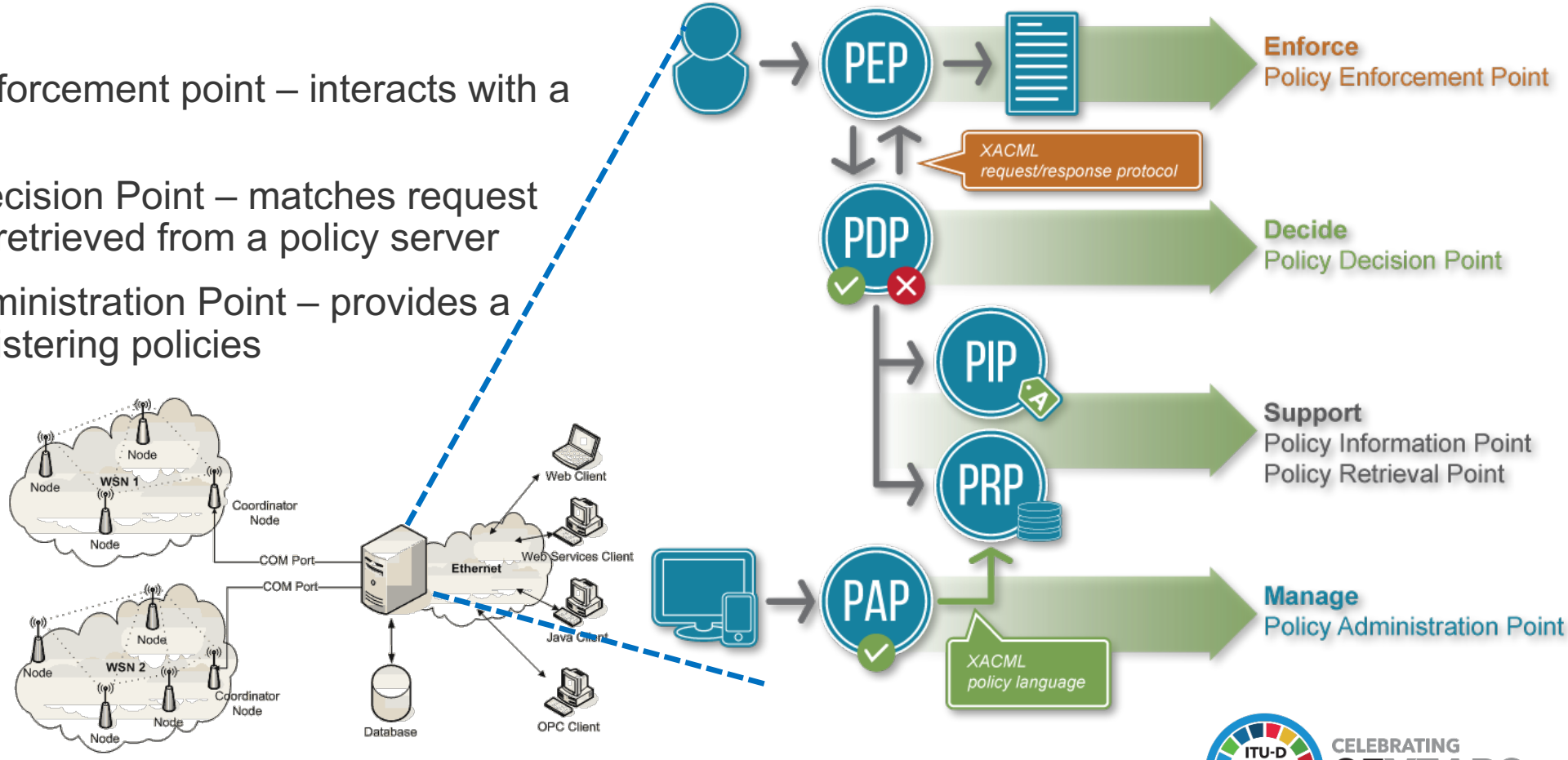
Policies, in general

- Policy - *a course or principle of action adopted or proposed by an organization or individual*
  - Designed, not just conceived
  - Often, determined by events
  - Policy effects must be direct and immediate – not all should be long-term
- Usually, bottom up
- Evolutionary process
- Asset/system analysis must not be extended to sectors and jurisdictions

Source: Australian Government Protective Security Policy https://www.protectivesecurity.gov.au/overarching-guidance/Pages/default.aspx

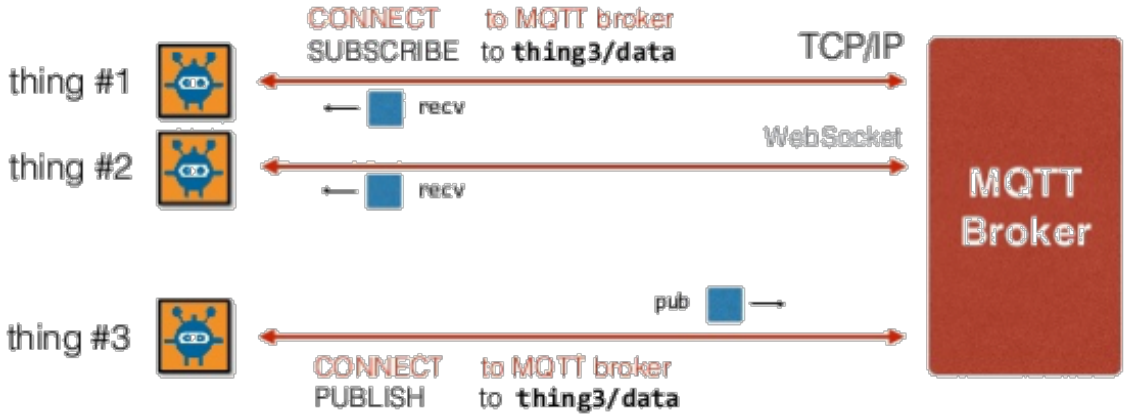
Policy Enforcement

- PEP – Policy enforcement point – interacts with a request, Y/n
- PDP – Policy Decision Point – matches request with policy data retrieved from a policy server
- PAP - Policy Administration Point – provides a means of administering policies

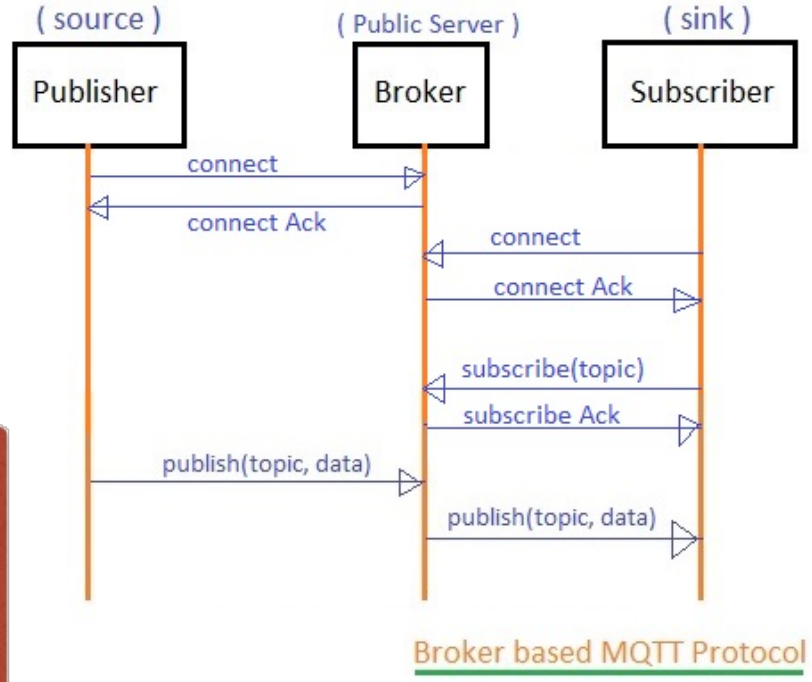


Policy Enforcement

- Working protocol is MQTT
- Publish, subscribe features
- Requires additional support for policy enforcement
- Middleware option ? SecKit[1], NOS v1, NOS[2] v2



Source: https://www.slideshare.net/BryanBoyd/mqtt-austin-api



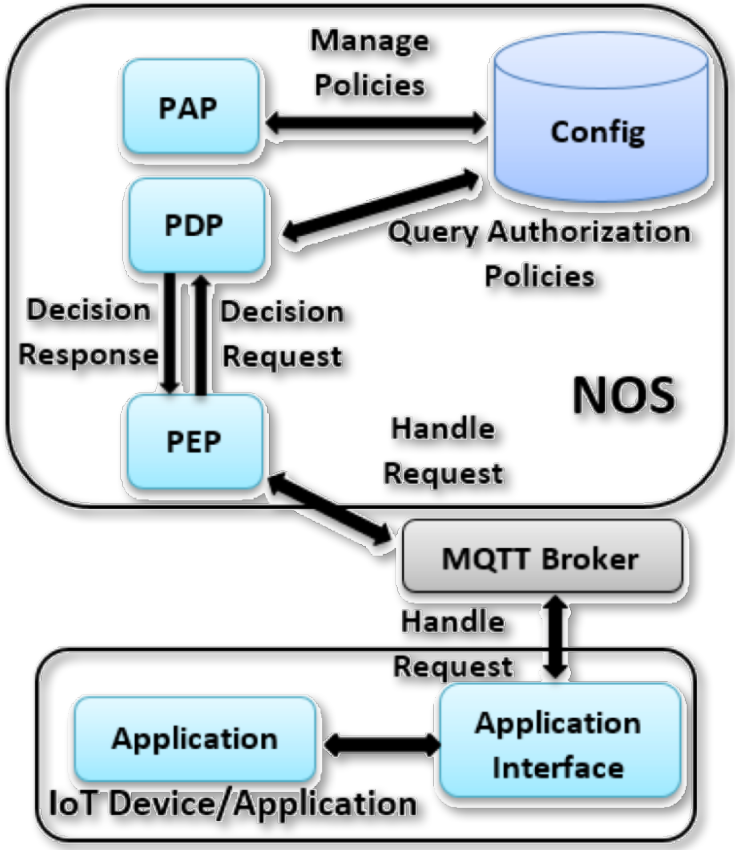
Source: rf-wirelessworld.com

1 - Neisse, R., Steri, G. and Baldini, G., 2014, October. Enforcement of security policy rules for the internet of things. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on* (pp. 165-172). IEEE.

2 - Sicari, S., Rizzardi, A., Miorandi, D. and Coen-Porisini, A., 2017. Dynamic Policies in Internet of Things: Enforcement and Synchronization. *IEEE Internet of Things Journal*.

Policy Enforcement

- Networked Smart Objects (NOS) – middleware on gateways
- Monitor more than data and health of device
  - enforcement when a message is delivered to a client in addition to enforcement when a client subscribes to a topic;
  - support for reactive rules to notify, log, or request user consent;
  - misbehavior checking rules, for Denial-of-Service (DoS) attack detection.
  - modification of messages and identity obfuscation in addition to simply allow or deny;
  - delaying of messages to prevent real-time tracking of devices and users;
  - Multiple NOSs communicate and synchronise – topic creation, policy updates. Leader election among the group of gateways for periodical change.



Questions…

- How will such enforcement scale across the infrastructure?
  - Distributed approach? Policy synchronisation, context dependency (entry into campus vs. entry into a lab), Size of the policy dB, Performance – with actuation, ….
- How vulnerable will the PEPs be?
- Enforcement on a common infrastructure?
- Policy administration?
- Policy design?

References

Kitchin, R. (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Minelli, M., Chambers, M. and Dhiraj, A. (2013) Big Data, Big Analytics. Wiley, Hoboken, NJ

OECD (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Thank You