Cybersecurity for IoT – Security in IoT devices

Department of Electrical, Computer and Biomedical Engineering of University of Pavia

Master of Science Program in Computer Engineering

Instructor: Paris Kitsos

http://diceslab.cied.teiwest.gr

E-mail: pkitsos@teimes.gr

Pavia 2018

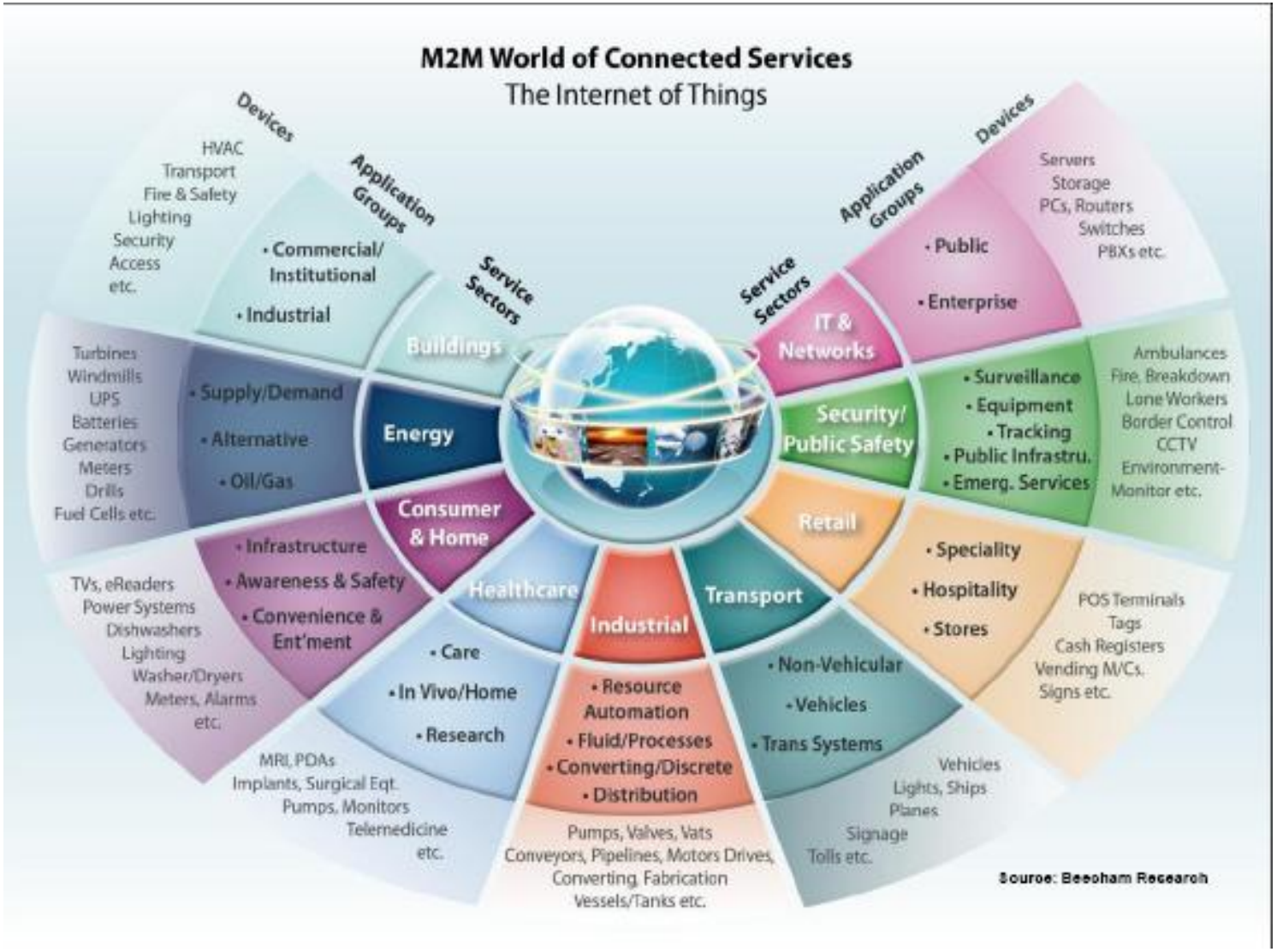
What is Internet-of-Things (IoT)

- The **Internet of Things (IoT)** is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data. [Wikipedia]

Other Names

- M2M (Machine to Machine)
- “Internet of Everything” (Cisco Systems)
- “World Size Web” (Bruce Schneier)

The Internet-of-Things



IoT Characteristics

- Heterogeneous entity
  - High-end devices (laptop, smartphone, tablets)
  - Low-end devices (sensors, actuators)
  - Passive entities (barcode, QR-code, RFID)
- Heterogeneous communication
  - Wired communications (ethernet)
  - WiFi / 3G / 4G
  - Bluetooth (LE) / Zigbee / 6LoWPAN
- Highly personal data
- Device manufacturers are not security expert

[Corvington and Carskadden “Threat Implications of the Internet of Things”, 2013]

Node Constraints

- Maximum code complexity (ROM/Flash)
- Size of state buffers (RAM)
- Amount of computation feasible in a period of time (processing capabilities)
- Available power
- User interface and accessibility in deployment (set keys, update software)

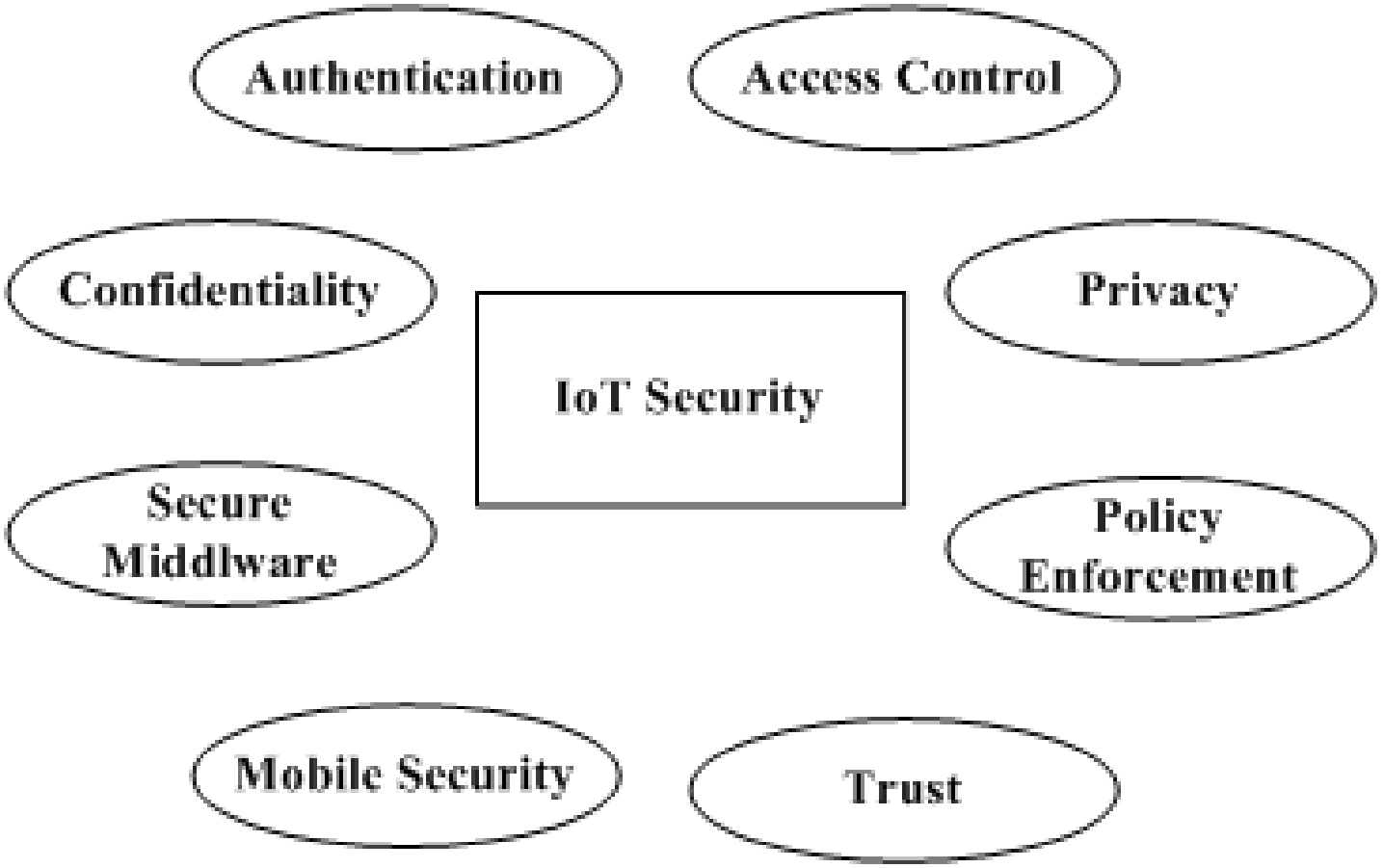
RFC7228 “Terminology for Constrained-Node Networks” https://tools.ietf.org/html/rfc7228)

Network Constraints

- Low achievable throughput
- High packet loss
- Asymmetric link characteristics
- Penalties for using large packets (e.g. high packet loss due to link layer fragmentation)
- Reachability over time (wake-up and sleeping time of devices)

RFC7228 “Terminology for Constrained-Node Networks” https://tools.ietf.org/html/rfc7228)

Security of the IoT

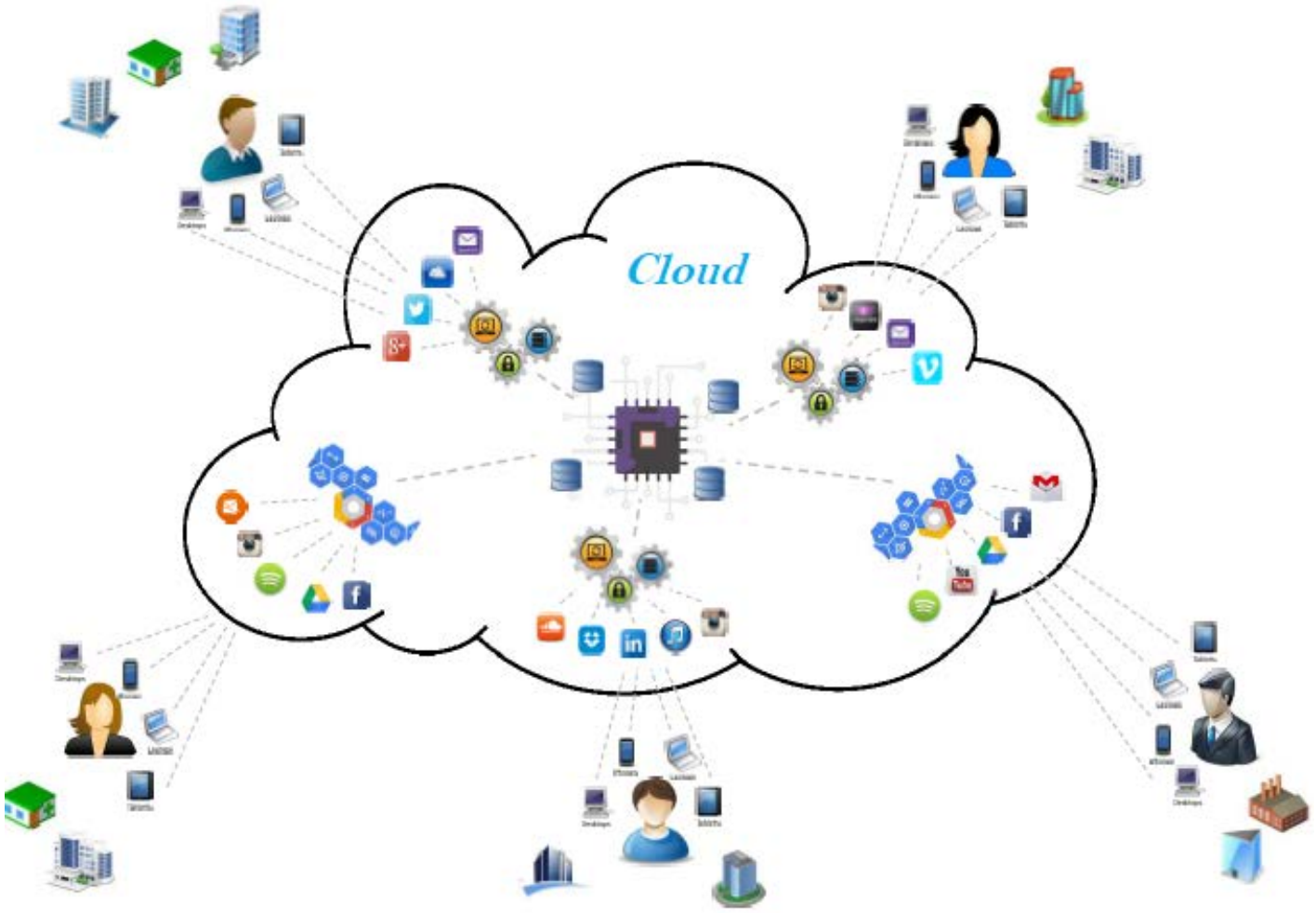


IoT Security Requirements

- IoT enables a constant transfer and sharing of data among things and users.

- In such a sharing environment, **authentication**, **authorization**, **access control** and **non-repudiation** are important to ensure secure communication.

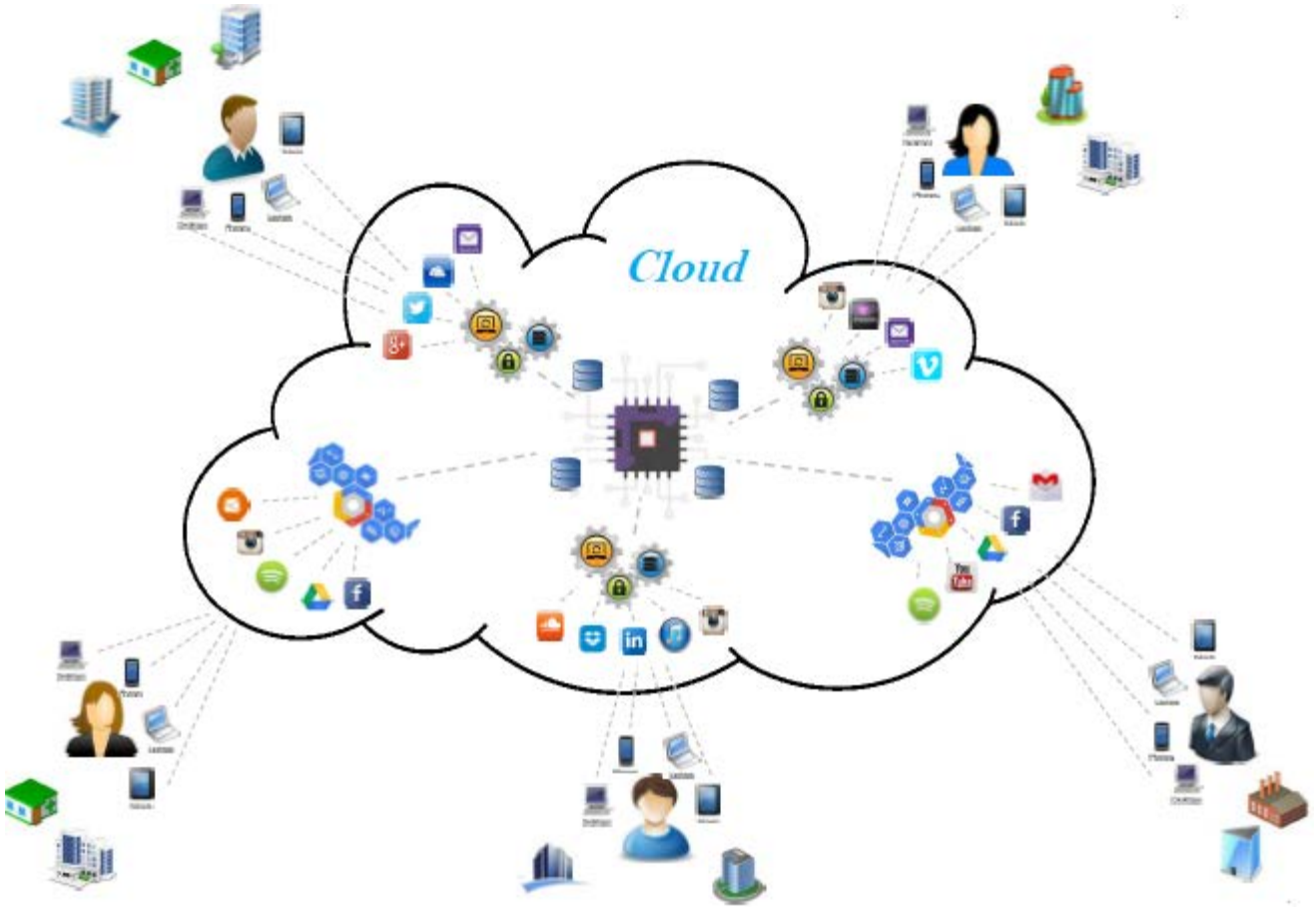
IoT Cloud…



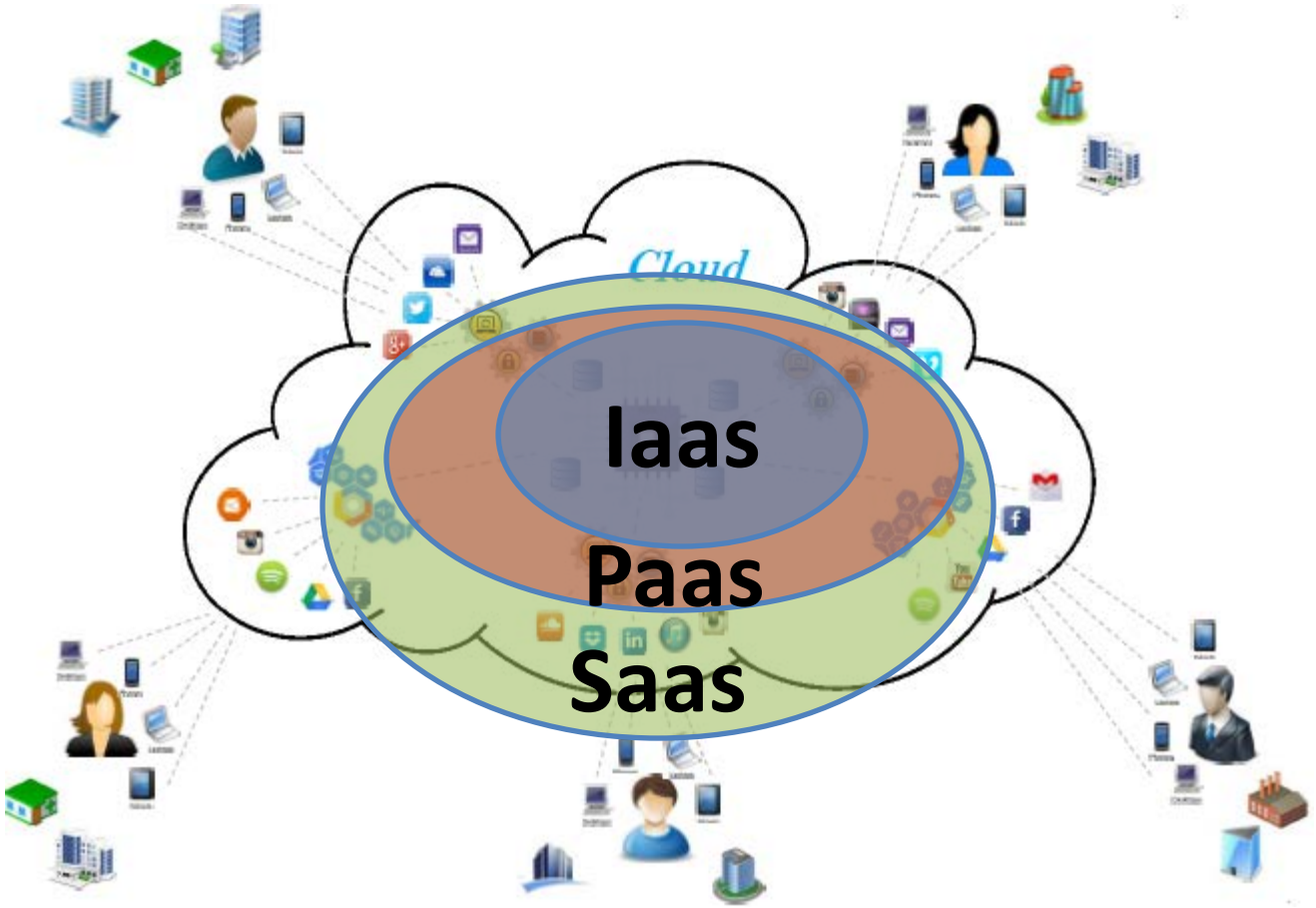
…IoT Cloud

- IoT Cloud is a platform that is designed to store and process Internet of Things (IoT) data.
- The platform is built to take in the massive volumes of data generated by devices, sensors, websites, applications, customers and partners and initate actions for real-time responses

Cloud Computing…



…Cloud Computing…



…Cloud Computing

- ***Software-as-s-Service (SaaS):*** Applications designed for end-users, run on someone else's system, delivered over the web
- ***Platform-as-s-Service (PaaS):*** It is a computing platform (a set of tools and services) that allows the creation and deployment of web applications quickly and easily
- ***Infrastructure-as-s-Service (IaaS):*** Hardware and software that powers it all – virtual server space, network connections, bandwidth, IP addresses and load balancers, storage

Cloud Security

- Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing
- It is a sub-domain of computer security, network security, and, more broadly, information security

Trusted Computing

- Trusted system
  - A system whose failure may break a specified security policy
- Trusted Computing (TC)
  - Specified by Trusted Computing Group (TCG)
  - (*In year 2007, the leading companies in the computing world such as AMD, Hewlett-Packard, IBM, Intel and Microsoft have created the not-for-profit Industry Security Standard Consortium known as the* ***Trusted Computing Group (TCG))***
  - Technologies and standards intended to make computers safer, more reliable and less prone to viruses, through **hardware** enhancements supported by software

Trusted Platform Module (TPM)…

- Specialized security chip *on an endpoint device/system*
  - Stores RSA keys *specific to the endpoint system*
  - vTPM for virtualized environments

- Tamper resistant
  - To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software with the appropriate security measures

…Trusted Platform Module (TPM)…

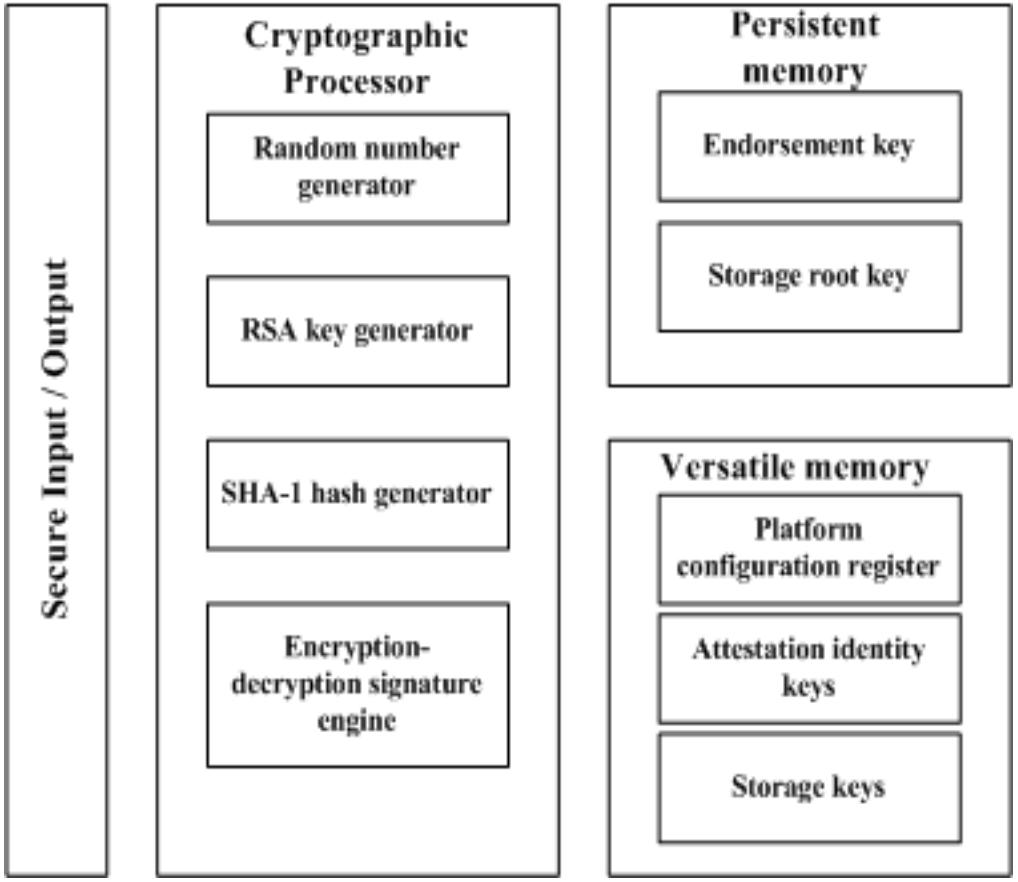
- Secure random number generation
- Keys storage and derivation
- Used for:
  - Data encryption
  - Secure/authenticated boot and root of trust
  - Hardware/platform authentication
  - Should be added at the beginning (Design-for-security)

…Trusted Platform Module (TPM)…

- Offers at least three trusted computing primitives:
  - secure measured boot: - ensures that the machine can only boot a certain hardware and software configuration
  - remote attestation - enables users to remotely attest that a machine booted a certain hardware and software configuration
  - sealed storage - protects data by binding it to a particular TPM and software configuration in a way that can only be accessed by the same combination of hardware and software.

…Trusted Platform Module (TPM)

- In TPM there are three separate domains:
  - Security – functions that protect the security of the user;
  - Privacy – functions that expose the identity of the platform/user ;
  - Platform – functions that protect the integrity of the platform/firmware services



Hardware Security Module (HSM)…

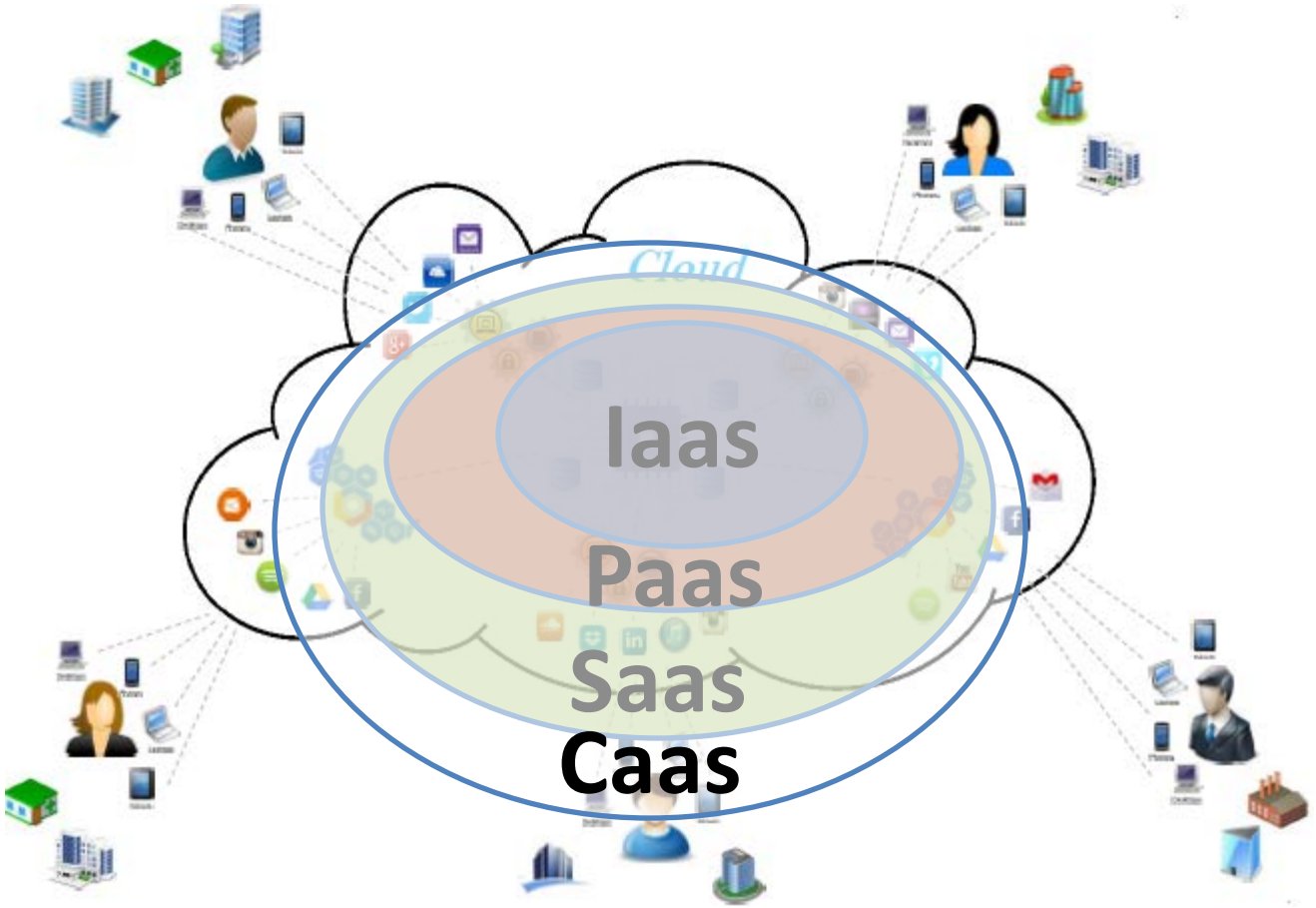
- Specialized security HW (e.g., plug-in card)
  - vHSM for virtualized environments
  - CloudHSM for cloud setups
  - Dongle HSM for mobility solutions
- Tamper resistant

…Hardware Security Module (HSM)

- Function
  - Secure random number generation
  - Securely generates, stores and manages cryptographic keys and material for strong authentication and encryption
  - Performs symmetric and asymmetric encryption/decryption

- Can be added later, easy to scale

Cloud Computing: Revisited



Cryptography as a Service (CaaS)…

- Cryptographic operations performed by a CaaS provider on behalf of a device-at-risk via web services APIs
  - Cryptographic keys are stored within the CaaS provider
  - Devices do not possess these keys at any time → much lower benefit for attacker

- Can be Software-only (riskier)
- Or, Hardware-enhanced (safer, higher security, higher costs)

…Cryptography as a Service (CaaS)…

- Advantages
  - Improved security
  - No important key or data on end points
  - Important key and data securely stored and managed by HSM
- Performance
  - Offload crypto-processing to dedicated HSM hardware

…Cryptography as a Service (CaaS)

- Disadvantages
  - All end nodes must authenticate to CaaS first
  - Requires network connectivity
  - Certain scenarios do not allow connectivity
    - DoS on the Trusted Cloud Hardware provider
    - More complex of the architecture
  - Higher costs and hardware requirements
  - Latency and performance penalty/overhead due to web

Questions??