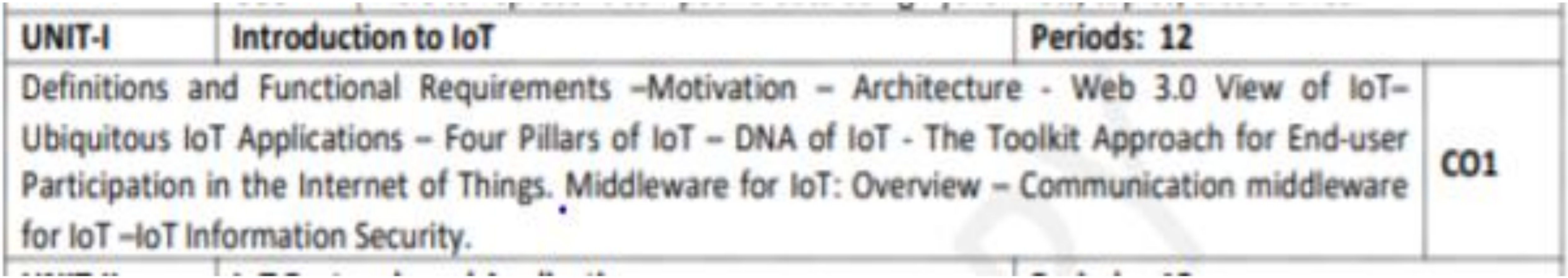
ITY10
Internet of Things

UNIT - I



UNIT-I	Introduction to IoT	Periods: 12
Definitions and Functional Requirements –Motivation – Architecture - Web 3.0 View of IoT– Ubiquitous IoT Applications – Four Pillars of IoT – DNA of IoT - The Toolkit Approach for End-user Participation in the Internet of Things. Middleware for IoT: Overview – Communication middleware for IoT –IoT Information Security.		CO1

Introduction to IoT

(International Telecommunication Union)ITU Definition for IoT

“The IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT).”

Why IoT now?

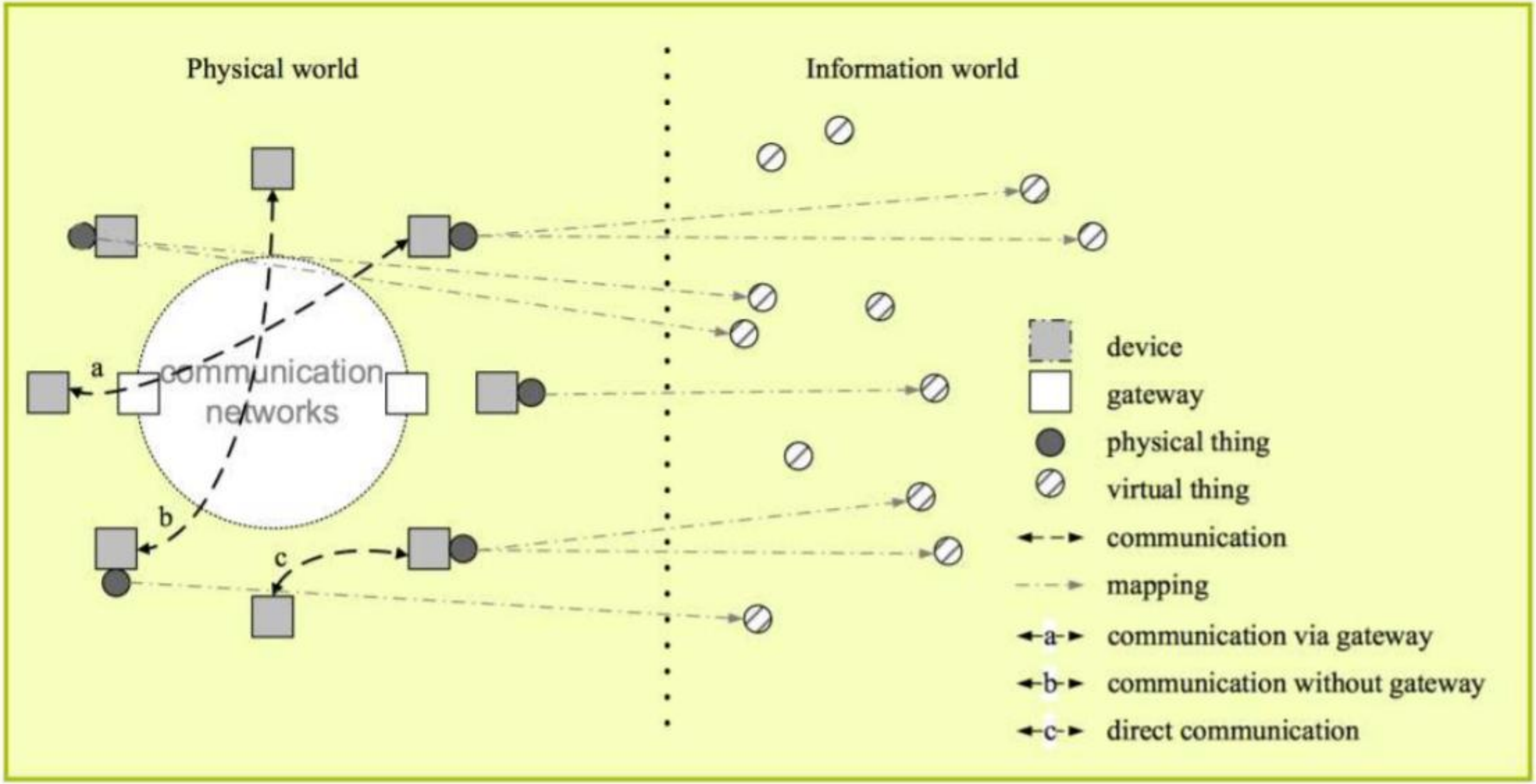
- Ubiquitous Connectivity
- Widespread Adoption of IP
- Computing Economics
- Miniaturization
- Advances in Data Analytics
- Rise of Cloud Computing

Things

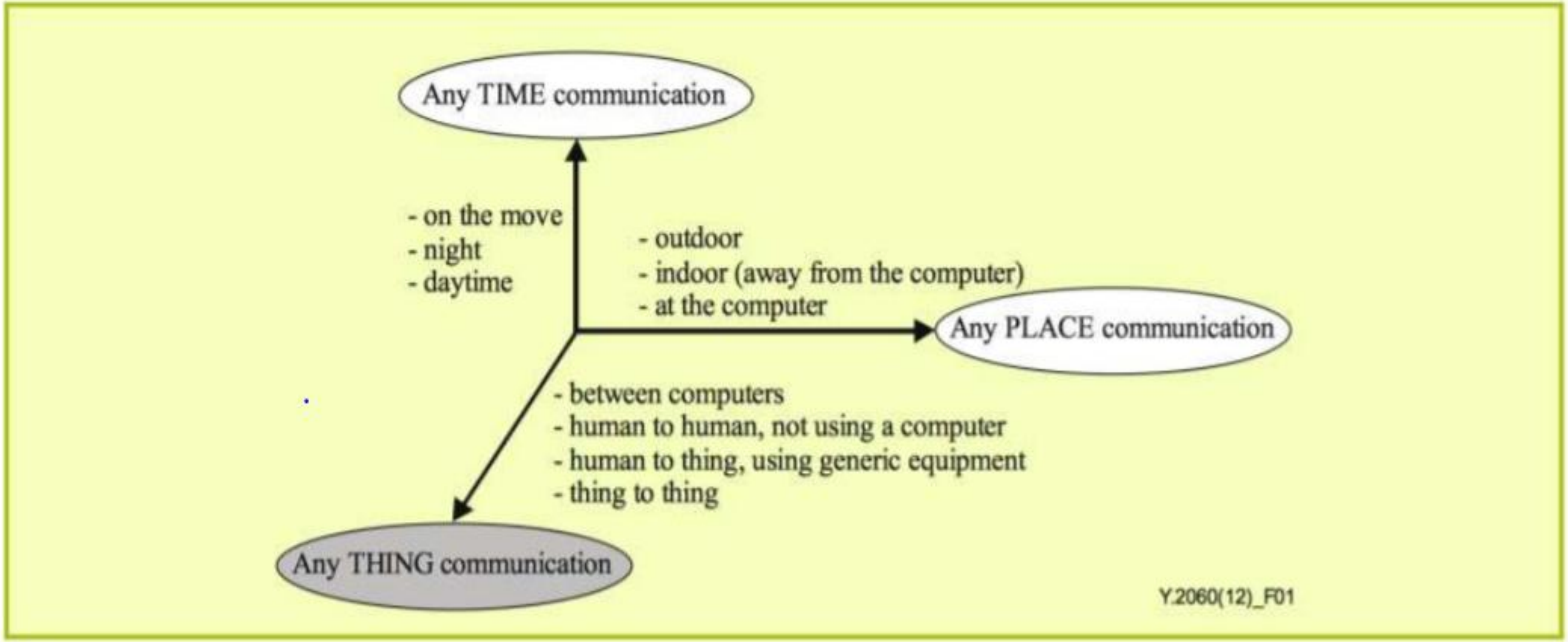
Things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic.

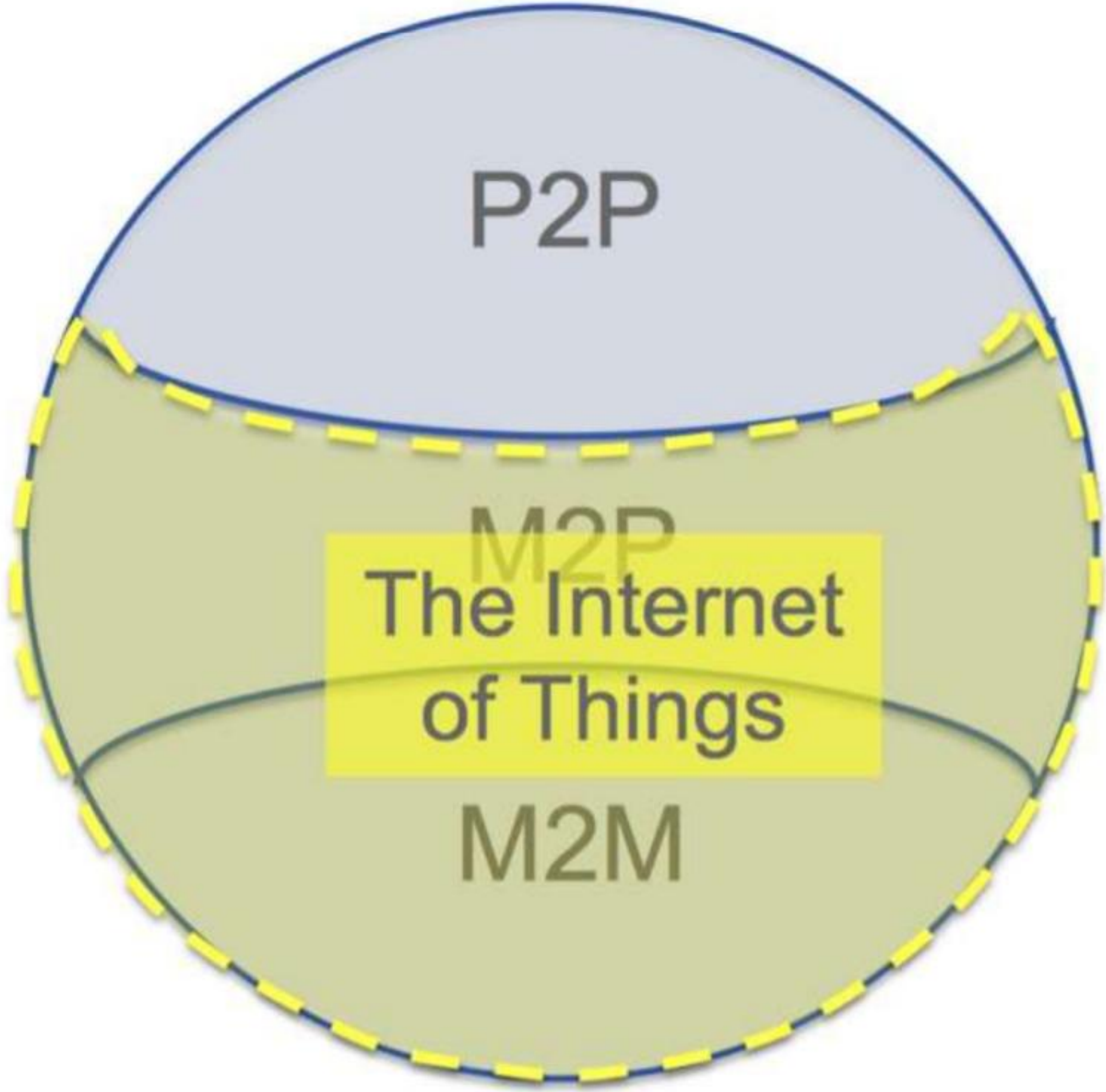
Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment and human beings.

Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.


Physical world
Information world
communication networks
a
b
c
device
gateway
physical thing
virtual thing
communication
mapping
a communication via gateway
b communication without gateway
c direct communication

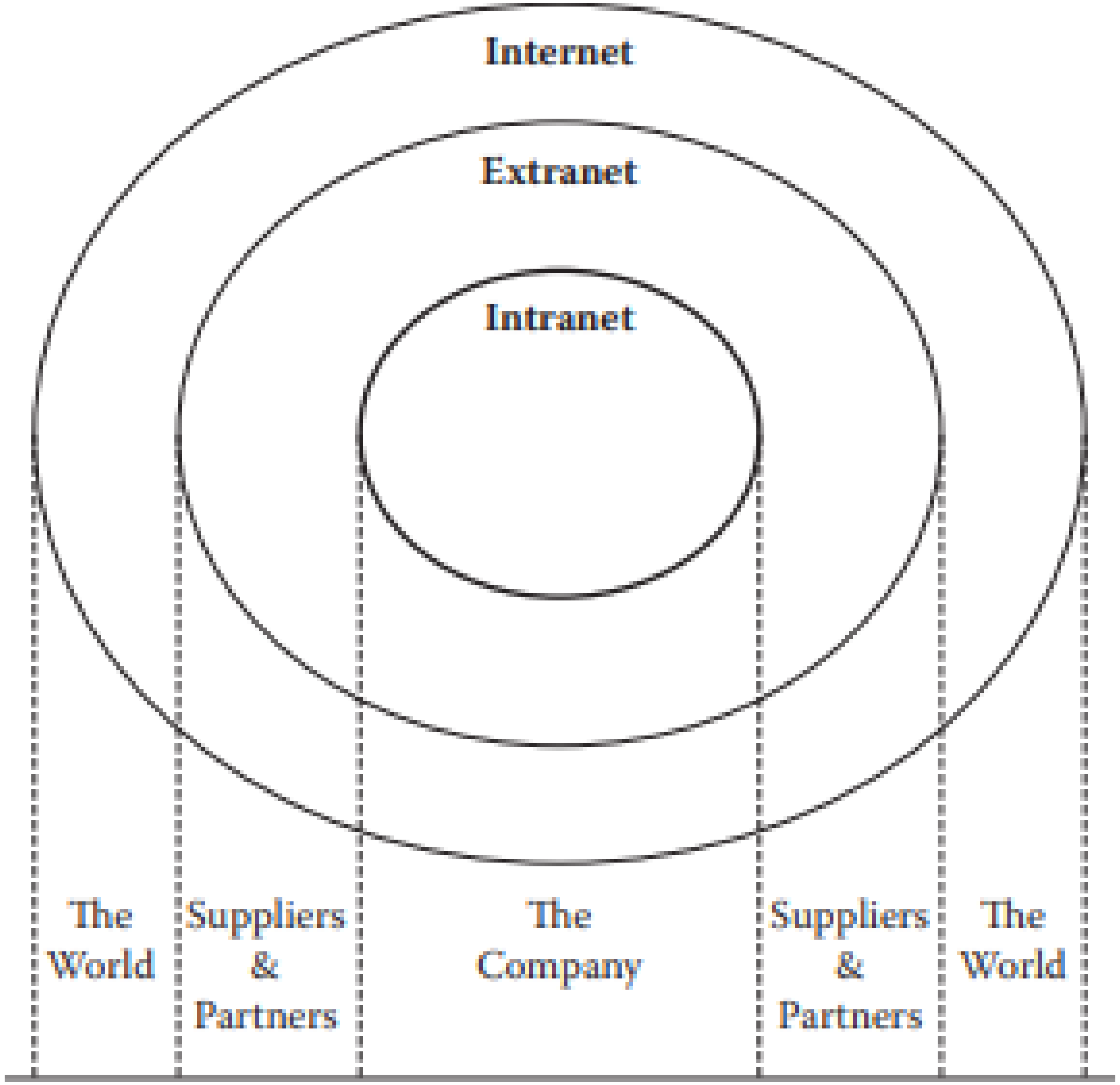
Any-Time/Place/Thing




P2P
M2P
The Internet of Things
M2M

ITU Definition for Device

- A device is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing.
- The devices collect various kinds of information and provide it to the information and communication networks for further processing.
- Some devices also execute operations based on information received from the information and communication networks.


Internet
Extranet
Intranet
The World
Suppliers & Partners
The Company
Suppliers & Partners
The World

Goals of IoT

- The immediate goal is to achieve pervasive M2M connectivity and grand integration and to provide secure, fast (real time), and personalized functionalities and services such as (remote) monitoring, sensing, tracking, locating, alerting, scheduling, controlling, protecting, logging, auditing, planning, maintenance, upgrading, data mining, trending, reporting, decision support, dashboard, back office applications, and others.
- The ultimate goal is to build a universally connected world that is highly productive, energy efficient, secure, and environment friendly.

Fundamental Characteristics

- **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- **Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
- **Dynamic changes:** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- **Enormous scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device triggered communication.

Functional Requirements

- **Diverse Connectivity**: Probably the most familiar form of connectivity for the internet, and for IoT, is Ethernet. In addition to Ethernet, IoT devices can connect using a wide variety of other technologies. The connectivity objective is that an IoT platform support as many modes of connection — wired and wireless — as possible. Wireless options include ANT+, Bluetooth, EDGE, GPRS, IrDA, LTE, NFC, RFID, Weightless, WLAN, ZigBee, and Z-Wave.

- **Leverage Applications**: IoT software applications are emerging for businesses in virtually every industry as well as for home users. These applications provide much of the automation capabilities that make IoT solutions so valuable. These software and middleware applications help businesses drive down costs, increase efficiency, and improve regulatory compliance. To achieve these goals, an IoT platform should be compatible with applications specific to your industry.

Functional Requirements (Contd.)

- **Range of Devices:** The number of devices connected to IoT will soon reach anywhere from 28 billion to 50 billion, depending on who you ask. IoT sensors gather information about conditions in their vicinity, such as temperature or moisture level. IoT actuators perform specific tasks, such as turning things on or off, and recording information about its triggers and subsequent reactions. In addition, IoT wearables of various kinds, like a health-tracking bracelet, can record your health statistics and other data such as your location. In essence, the functional requirement for an IoT platform is that it has the ability to manage a heterogeneous set of devices.

- **Massive Amounts of Data:** Devices don't just perform tasks. In most cases, they will also report on the tasks they perform. Through their connection to an IoT platform and to each other, they will transmit detailed data about their actions. Typically, there will be no need for human intervention in the process. The devices will simply send data, potentially in real-time, for storage and analysis. To give you an idea of just how much data is involved, one estimate foresees the IoT generating around 400 ZB (zettabytes) by 2018. Functionally, therefore, an IoT platform must be able to support storing massive amounts of data.

Functional Requirements (Contd.)

- **Powerful Analytics**: The vast volumes of data discussed above have the potential to provide unprecedented insights into consumer behavior and preferences. Unlocking those insights, however, requires powerful analytics tools. A key IoT platform functionality, therefore, is that it is capable of either incorporating — or offering compatibility with — analytics solutions that will translate significant amounts data into useful and actionable insights.

Non-functional Key Requirements

1. Meet key societal needs for the Internet of Things including open governance, security, privacy and trustworthiness.
2. Bridge the gap between B2B, business-to-consumer (B2C) and machineto-machine (M2M) requirements through a generic and open Internet of Things infrastructure.
3. Design an open, scalable, flexible and sustainable infrastructure for the Internet of Things.
4. Develop migration paths for disruptive technological developments to the Internet of Things.
5. Excite and enable businesses and people to contribute to the Internet of Things.

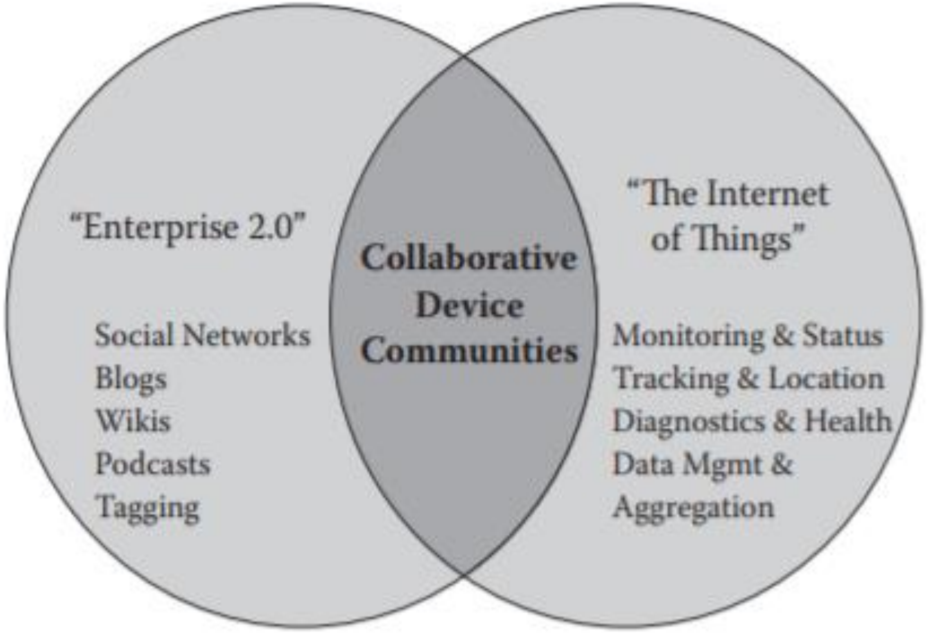
6. Enable businesses across different industries to develop high added value products and services.
7. Encourage new market entrants, such as third party service and information providers, to enter the Internet of Things.
8. Provide an open solution for sharing costs, benefits and revenue generation in the Internet of Things.
9. Public initiatives to support the usage of the Internet of Things for social relevant topics. L
10. Enable people to seamlessly identify things to access as well as contribute related information.

Web 3.0 View of IoT

- The Internet (network) and the web (application) are two sides of a coin.
- The Internet (hardware) is the infrastructure and the web (software) is the application everybody uses.
- In the Internet of Things, web-based applications and software (the supporting data representation and middleware) are the keys.
- The key application functionalities of IoT systems:
  1. Information and analysis
     a. Tracking behavior
     b. Enhanced situational awareness
     c. Sensor-driven decision analytics
  2. Automation and control
     a. Process optimization
     b. Optimized resource consumption
     c. Complex autonomous systems

- The web-based applications, systems, and networked services of IoT are expanding more rapidly than the hardware and infrastructure.
- Hence the software (middleware and web-based integrated applications) market will play a pivotal role in the IoT business.
- Web 1.0 is about publishing and pushing content to the users. It’s mostly a unidirectional flow of information.
- Web 2.0 can be seen as a result of technological refinements as well as the behavior change of those who use the World Wide Web, from publishing to participation.
- Web 2.0 is about two-way flow of information and is associated with web applications that facilitate participatory information sharing, interoperability, user-centered design, and collaboration.
- Example applications of Web 2.0 include blogs, social networking services (SNSs), wikis, mashups, folksonomies, video-sharing sites, massive multiplayer online roleplaying games, virtual reality, and so on

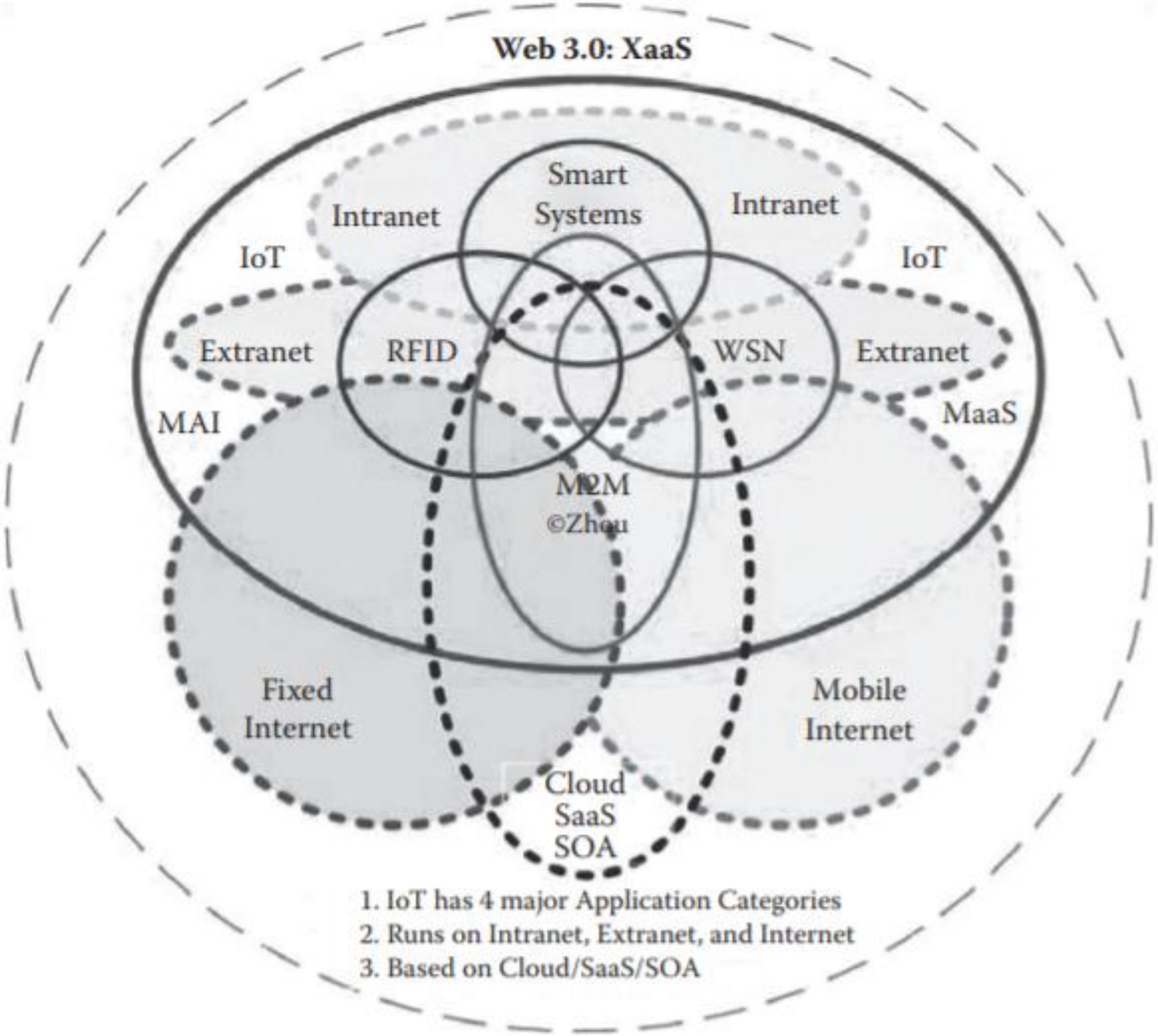
- Enterprise 2.0 is the use of Web 2.0 technologies within an organization to enable or streamline business processes while enhancing collaboration.
- It is the extension of Web 2.0 into enterprise applications.
- IoT technologies and applications can be integrated into Enterprise 2.0 for enterprises that need to monitor and control equipment and facilities and integrate with their ERP and CRM back office systems.



Blending of IoT and Enterprise 2.0.

- Web 3.0 is about Semantic Web.
- The Semantic Web is a vision of information that can be readily interpreted by machines, so machines can perform more of the tedious work involved in finding, combining, and acting upon information on the Web.
- A fundamental difference between the Internet of People (Web 1.0 and Web 2.0) and the Internet of Things is that in the former, data are generated by people (keyed in by hand, photographed by hand, etc.); in the latter, data are generated by machines, not humans.
- The data are generated by things and consumed by people and machines via SaaS or XaaS (Everything as a Service), and this model constitutes the basis of Web 3.0

Web 3.0: The Internet of Things



Ubiquitious IoT Applications

- The arrival of the IoT concept and its worldwide attention is closely relevant to environmental, societal, and economic challenges such as climate change, environment protection, energy saving, and globalization.
- For these reasons the IoT is increasingly used in a large number of sectors.
- Key sectors in this context are transportation, healthcare, energy and environment, safety and security, logistics, and manufacturing.
- M2M and embedded mobile devices are sending mobile data to servers that are increasingly useful and valuable to ERPs

Harbor Research segments the IoT/M2M market into 10 key sectors [, 30+ subsectors, and countless systems and devices:

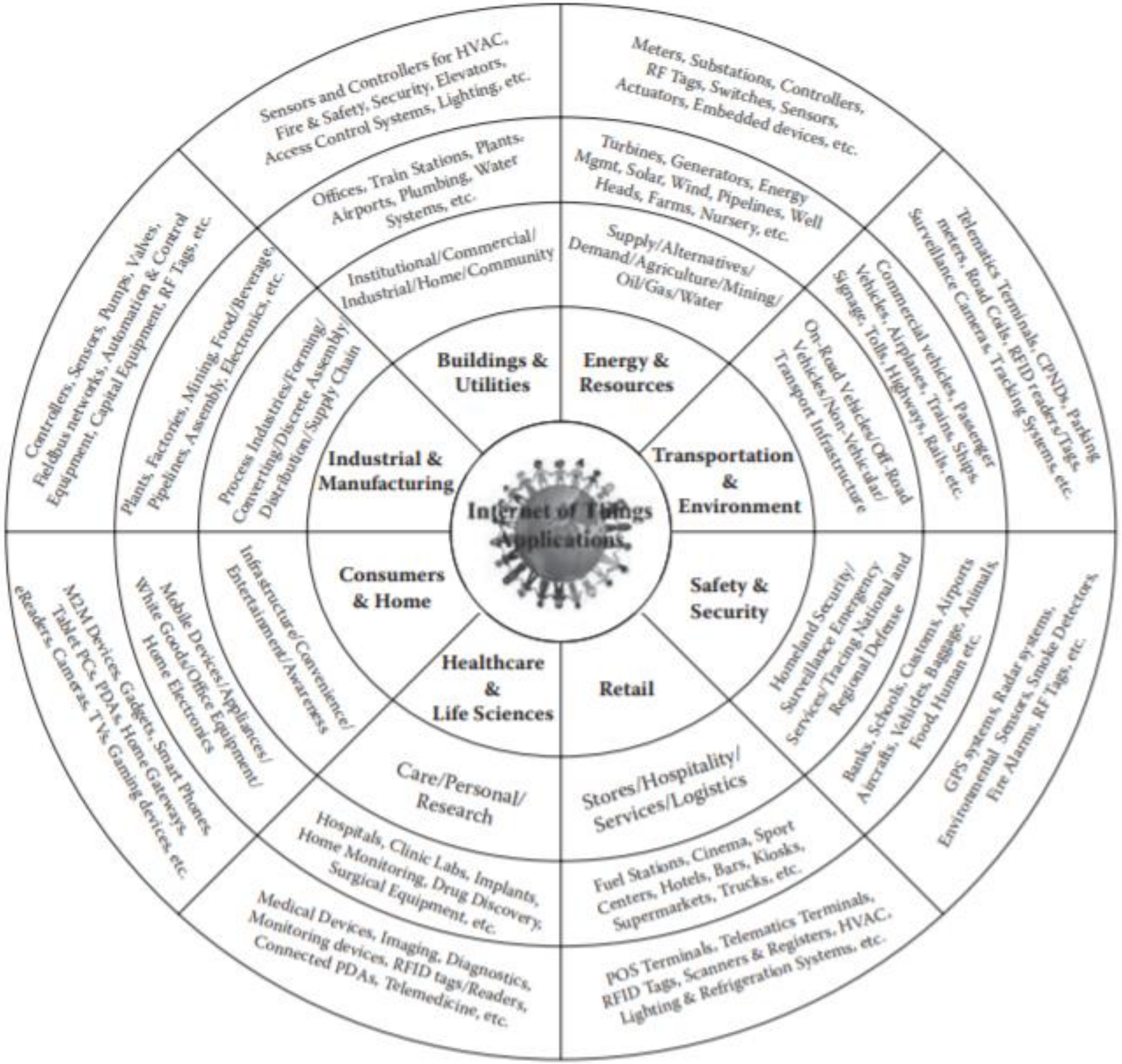
- **Buildings**: Institutional/Commercial/Industrial/Home. HVAC, fire and safety, security, elevators, access control systems, lighting
- **Energy and Power**: Supply/Alternatives/Demand. Turbines, generators, meters, substations, switches
- **Industrial**: Process Industries/Forming/Converting/ Discrete Assembly/Distribution/Supply Chain. Pumps, valves, vessels, tanks, automation and control equipment, capital equipment, pipelines
- **Healthcare**: Care/Personal/Research. Medical devices, imaging, diagnostics, monitor, surgical equipment
- **Retail**: Stores/Hospitality/Services. Point-of sale terminals, vending machines, RFID tags, scanners and registers, lighting and refrigeration systems

- **Security and Infrastructure**: Homeland Security/Emergency Services/National and Regional Defense. GPS systems, radar systems, environmental sensors, vehicles, weaponry, fencing
- **Transportation**: On-Road Vehicles/Off-Road Vehicles/ Nonvehicular/Transport Infrastructure. Commercial vehicles, airplanes, trains, ships, signage, tolls, RF tags, parking meters, surveillance cameras, tracking systems
- **Information Technology and Network Infrastructure**: Enterprise/Data Centers. Switches, servers, storage
- **Resources**: Agriculture/Mining/Oil/Gas/Water. Mining equipment, drilling equipment, pipelines, agricultural equipment
- **Consumer/Professional**: Appliances/White Goods/Office Equipment/Home Electronics. M2M devices, gadgets, smartphones, tablet PCs, home gateways

Machina Research classified the IoT/M2M market into 3 categories and 11 segments

- **Intelligent Environment**: Intelligent buildings/smart cities and transportation
- **Intelligent Living**: Automotive/consumer electronics
- **Intelligent Enterprise**: Health/utilities/manufacturing/ retail and leisure/construction/agriculture and extraction/ emergency services and national security

A panoramic view of IoT applications



Internet of Things
Applications

Buildings &
Utilities

Institutional/Commercial/
Industrial/Home/Community

Offices, Train Stations, Plants,
Airports, Plumbing, Water
Systems, etc.

Sensors and Controllers for HVAC,
Fire & Safety, Security, Elevators,
Access Control Systems, Lighting, etc.

Energy &
Resources

Supply/Alternatives/
Demand/Agriculture/Mining/
Oil/Gas/Water

Turbines, Generators, Energy
Mgmt, Solar, Wind, Pipelines, Well
Heads, Farms, Nursery, etc.

Meters, Substations, Controllers,
RF Tags, Switches, Sensors,
Actuators, Embedded devices, etc.

Transportation
&
Environment

On-Road Vehicles/Off-Road
Vehicles/Non-Vehicular/
Transport Infrastructure

Commercial vehicles, Passenger
Vehicles, Airplanes, Trains, Ships,
Signage, Tolls, Highways, Rails, etc.

Telematics Terminals, CPNDs, Parking
meters, Road Coils, RFID readers/Tags,
Surveillance Cameras, Tracking Systems, etc.

Safety &
Security

Homeland Security/
Surveillance Emergency
Services/Tracing National and
Regional Defense

Banks, Schools, Customs, Airports
Aircrafts, Vehicles, Baggage, Animals,
Food, Human etc.

GPS systems, Radar systems,
Environmental Sensors, Smoke Detectors,
Fire Alarms, RF Tags, etc.

Retail

Stores/Hospitality/
Services/Logistics

Fuel Stations, Cinema, Sport
Centers, Hotels, Bars, Kiosks,
Supermarkets, Trucks, etc.

POS Terminals, Telematics Terminals,
RFID Tags, Scanners & Registers, HVAC,
Lighting & Refrigeration Systems, etc.

Healthcare
&
Life Sciences

Care/Personal/
Research

Hospitals, Clinic Labs, Implants,
Home Monitoring, Drug Discovery,
Surgical Equipment, etc.

Medical Devices, Imaging, Diagnostics,
Monitoring devices, RFID tags/Readers,
Connected PDAs, Telemedicine, etc.

Consumers
& Home

Infrastructure/Convenience/
Entertainment/Awareness

Mobile Devices/Appliances/
White Goods/Office Equipment/
Home Electronics

M2M Devices, Gadgets, Smart Phones
Tablet PCs, PDAs, Home Gateways,
eReaders, Cameras, TVs, Gaming devices, etc.

Industrial &
Manufacturing

Process Industries/Forming/
Converting/Discrete Assembly/
Distribution/Supply Chain

Plants, Factories, Mining, Food/Beverage,
Pipelines, Assembly, Electronics, etc.

Controllers, Sensors, Pumps, Valves,
Fieldbus networks, Automation & Control
Equipment, Capital Equipment, RF Tags, etc.

Important Vertical IoT Applications

1. Telematics and Intelligent Transport Systems

- Telematics and intelligent transport system (ITS) have been a kind of IoT application for a long time.
- Telematics, as determined by its name, is any integrated use of telecommunication and informatics. Its application is within any of the following:
  - The technology of sending, receiving, and storing information via telecommunications devices in conjunction with effecting control on remote objects, especially for application in vehicles and with control of vehicles on the move
  - GPS technology integrated with computers and mobile communication technology in automotive navigation systems
  - The use of such systems within road vehicles, including commercial and (particularly) passenger vehicles

- Fleet management, especially GPS-based fleet tracking, is thought by some people as a subsector of telematics known as fleet telematics.
- Fleet management is for commercial vehicles what telematics is for passenger vehicles.
- Fleet management (and also telematics) is a subsector of MRM (mobile resource management), which is itself a subsector of the M2M business.
- Telematics and fleet management–based applications can be extended to enable many innovative capabilities:

- Vehicle relationship management has been designed to utilize a vehicle’s telematics hardware to provide cost reductions, business efficiencies, and enhanced customer service for automobile manufacturers and their affiliated automobile dealerships.
- Interest has increased across the globe in the benefits of usage-based car insurance, also known as PAYD (Pay as You Drive), which enables vehicle owners to pay reduced car insurance premiums based only on the distances that they drive and the way that they drive.
- Vehicle lifecycle management solution aims to improve customer service, optimize operational processes, lower costs, increase vehicle safety, and improve productivity throughout the automotive design process and supply chain, as well as provides telematics services to vehicle consumers, automotive retailers, car companies, and their suppliers.

- The term intelligent transport systems (ITS) refers to information and communication technologies (ICT) applied to transport infrastructure and vehicles that improve transport such as transport safety, transport productivity, travel reliability, informed travel choices, social equity, environmental performance, and network operation resilience.
- Telematics/ITS standards are provided by standard organizations such as,
    - DSRC
    - NGTP
    - GENIVI
    - Automotive Open System Architecture (AUTOSAR)
    - Society of Automotive Engineers (SAE)
    - Automotive Multimedia Interface Collaboration (AMI-C)
    - 3GPP
    - Telecommunications Industry Association (TIA)
    - Automatic Terminal Information Service (ATIS)
    - Communications for Coordinated Assistance and Response to Emergencies (COMCARE)
    - National Emergency Number Association (NENA)
    - ISO
    - IEEE
    - Open Services Gateway Initiative (OSGi)
    - ITU
    - ESTI

2. Smart Grid and Electric Vehicles

- Power SCADA, a technology of IoT characteristics, becoming increasingly complex as new technologies arrive and new issues emerge on the road to a modern electric smart grid.
- SCADA/EMS/GMS (energy management system), (generation management system) supervises, controls, optimizes and manages power generation and transmission systems.
- SCADA/DMS (distribution management system) performs the same functions for power distribution networks.
- Both systems enable utilities to collect, store, and analyze data from hundreds of thousands of data points in national or regional networks, perform network modeling, simulate power operation, pinpoint faults, preempt outages, and participate in energy trading markets.
- These systems are a vital part of modern power networks and are enabling the development of smart grids.

- Smart grid technologies have emerged from earlier attempts at controlling, metering, and monitoring.
- Smart meters add continuous communications so that monitoring can be done in real time and can be used as a gateway to demand response-aware devices and “smart sockets” in the home.
- A power system making use of an integrated electrical and communications systems architecture should be as follows:
  - Self-healing and adaptive, applying automated applications for protection, fault detection, fault location, sectionalization, and automatic service restoration over wide areas of the service territory
  - Interactive with consumers and markets, permitting real-time pricing, energy trading, and load management
  - Optimized to make the best use of aging equipment, personnel from multiple organizations, and other resources in a competitive environment
  - Predictive, scheduling maintenance ahead of time to prevent rather than just react to emergencies
  - Distributed, permitting activities such as generation, metering, load shedding, and others to be easily performed at different locations and by different organizations
  - Integrated, merging the previously separate functions of monitoring, control, protection, maintenance, energy management, distribution management, business, and corporate information technology
  - Secure, protecting vital infrastructure from cyber or physical attack

- A great many smart grid definitions exist: some functional, some technological, and some benefits oriented.
- A common element to most definitions is the application of advanced sensor technologies, two-way communications, and distributed processing to the power grid, making data flow and information management central to the smart grid.
- Smart grid research will have to consider incorporating renewable energies into the power network and the provisioning of electric vehicles.
- In a true smart grid, electric cars will not only be able to draw on electricity to run their motors, but they will also be able to do the reverse: send electricity stored in their batteries back into the grid when it is needed.

- Vehicle-to-grid (V2G) describes a system in which plug-in electric vehicles (EVs), such as battery electric vehicles and plug-in hybrid electric vehicles, communicate with the power grid to sell demand response services either by delivering electricity into the grid or by throttling their charging rate.
- Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities.
- There are three different versions of the vehicle-to-grid concept:

- ***A hybrid or fuel cell vehicle***, which generates power from storable fuel, uses its generator to produce power for a utility at peak electricity usage times. Here the vehicles serve as a distributed generation system, producing power from conventional fossil fuels or hydrogen.
- ***A battery-powered or plug-in hybrid vehicle***, which uses its excess rechargeable battery capacity to provide power to the electric grid in response to peak load demands. These vehicles can then be recharged during off-peak hours at cheaper rates while helping to absorb excess nighttime generation. Here the vehicles serve as a distributed battery storage system to buffer power.
- ***A solar vehicle***, which uses its excess charging capacity to provide power to the electric grid when the battery is fully charged. Here the vehicle effectively becomes a small renewable energy power station. Such systems have been in use since the 1990s and are routinely used in the case of large vehicles, especially solar-powered boats.

3. Smarter Planet and Smart Buildings

- Many of the challenges the planet faces are concentrated in cities.
- Cities struggle with traffic congestion, water management, environment protection, public utility management, smart grids, healthcare solutions, building energy efficiency, and rail transportation issues, to name a few.
- These issues have historically been difficult to manage because of their size and complexity.
- But with new ways of monitoring, connecting, and analyzing the systems, business, civic, and nongovernmental leaders are developing new ways to address those issues.

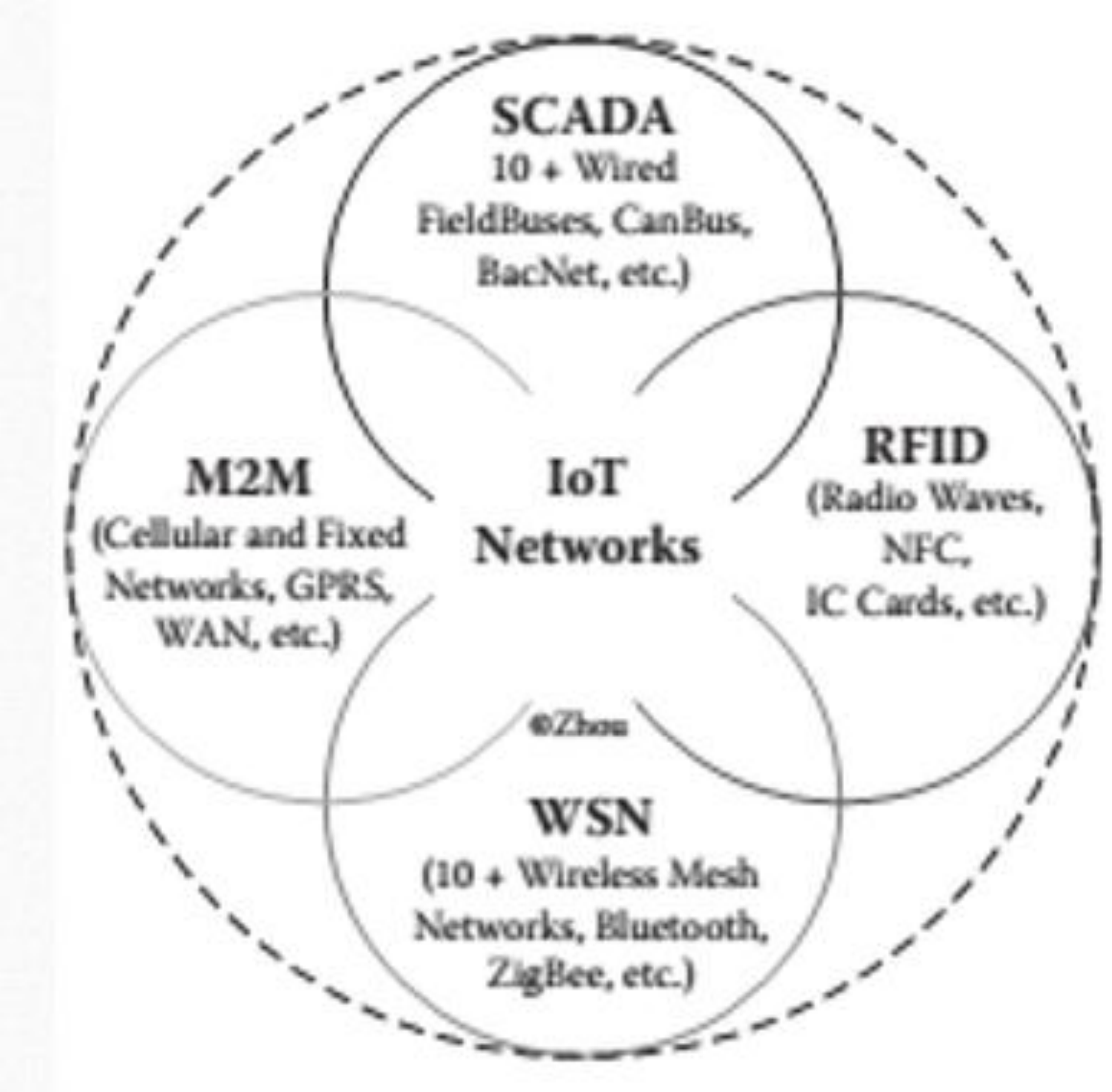
- A smart city is one that “uses information and communications technologies to make the critical infrastructure components and services of a city (administration, education, healthcare, public safety, real estate, transportation, utilities, and so on) more aware, interactive and efficient”
- In building a smart city, ICT has a fundamental role to play.
- The adoption of hardware, software, and services gives way to the creation of a new, holistic, ICT ecosystem which is referred by IDC as “Intelligent X”, that integrates the following three areas,
  - Smart devices involving M2M/telemetry capabilities
  - High-speed ubiquitous communications networks
  - Intelligent software and services to process, consolidate, and analyze data in order to transform industry-specific business processes
- IDC has outlined seven categories of applications for smarter cities: health; home; sports and leisure; education; transport; buildings; and city services, safety, security, and emergency response.

- The Internet of Things plays an important role in building a smarter planet and smarter cities.
- Smart buildings are the building blocks of a smart city, which are building blocks of the smarter planet.
- An intelligent green building is managed by a building management system (BMS) or an interconnected, integrated, and intelligent BMS.
- All four IoT technologies—SCADA, M2M, RFID, and WSN—can be used in a BMS.
- A BMS usually controls and monitors the building’s mechanical and electrical equipment that integrates the BAS (building automation system), security and alerting system, fire alarming system, closed-circuit TV video surveillance system, access control system, power and lighting system, elevator, broadcasting and background music system, parking system, network and cable TV management system, PMS (property management system), and even office automation system.
- Energy efficiency management (power and water usage metering and sub-metering) can also be added into BMS.

- A BMS usually uses higher level Internet and wireless mesh network protocols as well as open standards such as DeviceNet, ZigBee, EnOcean (energy harvesting technology), SOAP, and XML, and builds on top of a middleware platform such as a three-tiered Java application server for web-based access anywhere, anytime.
- A BMS system is an example of a human machine interface (HMI/SCADA);
- A BAS should be part of an integrated BMS.
- A BAS is an example of a distributed control system, which, in most cases, covers the HVAC systems of a building, while a BMS is like an information system that does a grand integration of everything in the building.
- A BAS's core functionality keeps the building climate within a specified range and monitors system performance and device failures.
- A BAS is usually configured in a hierarchical manner using lower level protocols as CAN-bus, Profibus, BACnet, LonWorks, and Modbus.

- A BEMS (Building Energy Management System) is a system that facilitates management and control of building facilities while also realizing energy savings and increasing comfort of building users by making full use of state-of-the-art information technology.
- Another IoT application on buildings is the home automation segment.
- Home automation, also called domotics, is the residential extension of building automation. It is automation of the home, housework, or household activity.
- Home automation may include centralized control of lighting, HVAC, appliances, and other systems to provide improved convenience, comfort, energy efficiency, and security.
- Home automation for the elderly and disabled can provide increased quality of life for people who might otherwise require caregivers or institutional care.

Four Pillars of IoT



SCADA
10 + Wired
FieldBuses, CanBus,
BacNet, etc.)

M2M
(Cellular and Fixed
Networks, GPRS,
WAN, etc.)

IoT
Networks

RFID
(Radio Waves,
NFC,
IC Cards, etc.)

WSN
(10 + Wireless Mesh
Networks, Bluetooth,
ZigBee, etc.)

©Zhou

Four Pillars

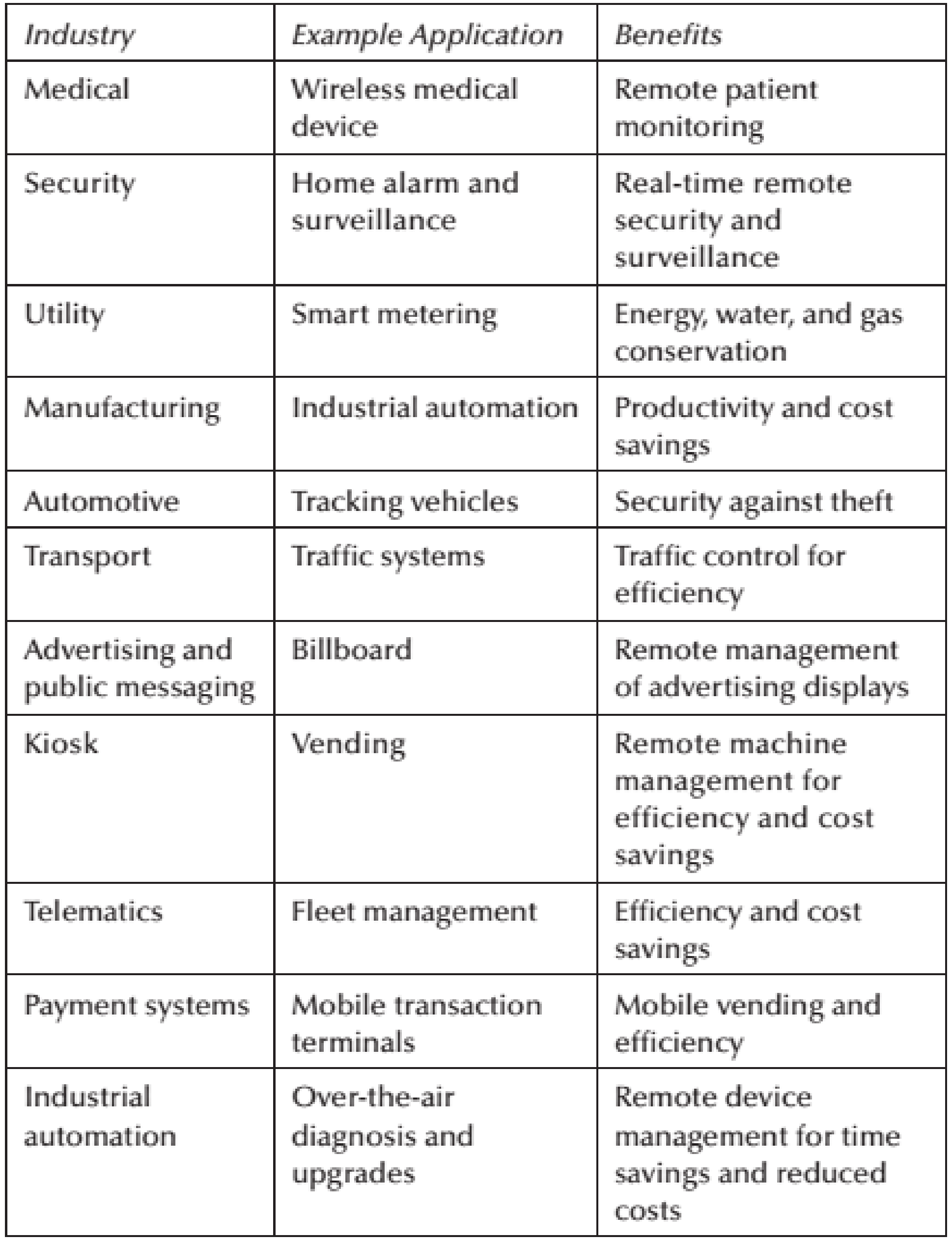
- M2M –Devices to capture events for interpretation

e.g. -vending machine - It automatically sends out information about its inventory to dispatchers.

ATM - which sends information when it's low on cash to the authorities on its own.

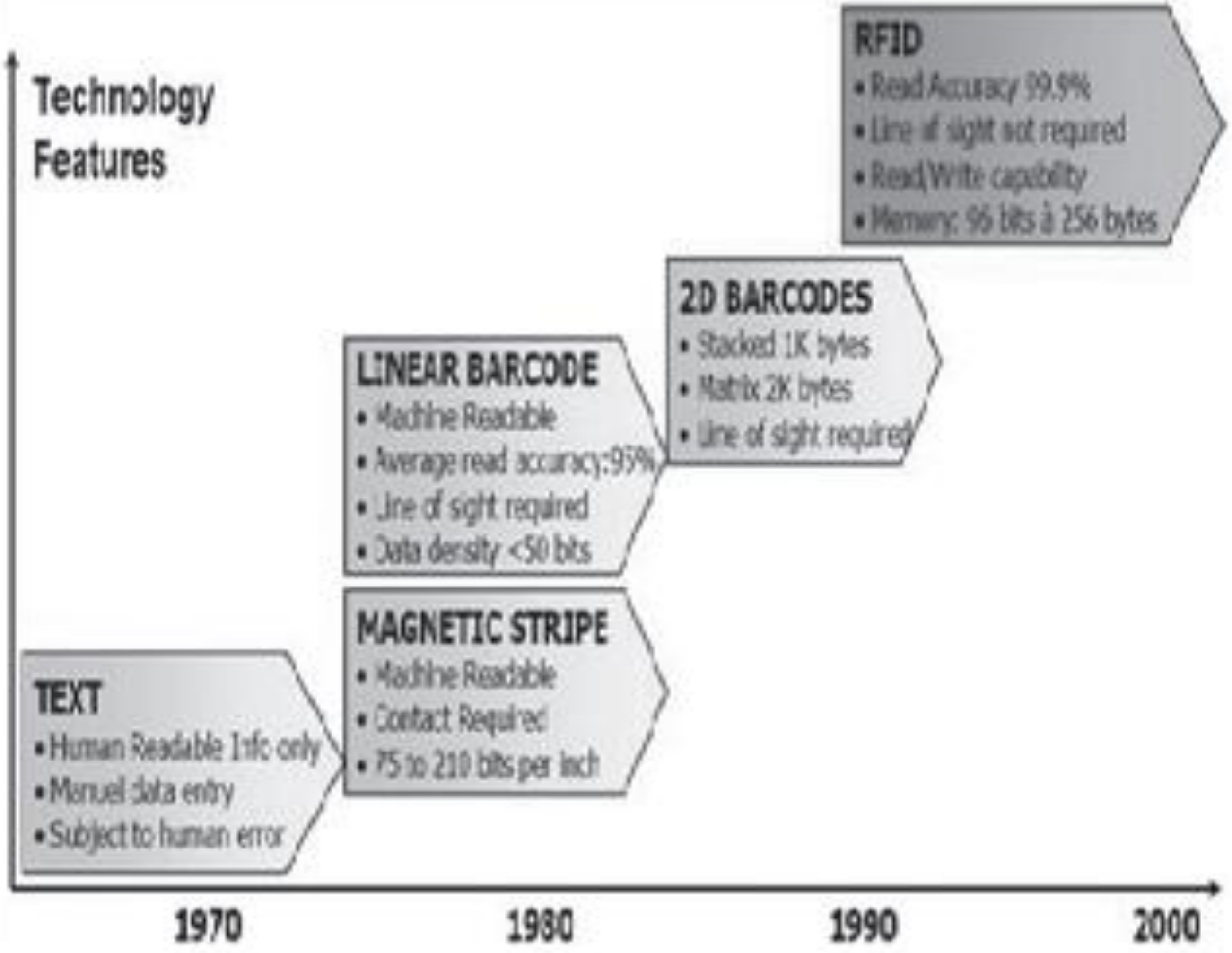
- RFID -uses radio waves to transfer data from an electronic tag for identifying and tracking the object.
- WSN-spatially distributed autonomous sensors to monitor physical or environmental conditions
- SCADA - (supervisory control and data acquisition) is a category of software applications for controlling industrial processes

Applications for M2M



Industry	*Example Application*	*Benefits*
Medical	Wireless medical device	Remote patient monitoring
Security	Home alarm and surveillance	Real-time remote security and surveillance
Utility	Smart metering	Energy, water, and gas conservation
Manufacturing	Industrial automation	Productivity and cost savings
Automotive	Tracking vehicles	Security against theft
Transport	Traffic systems	Traffic control for efficiency
Advertising and public messaging	Billboard	Remote management of advertising displays
Kiosk	Vending	Remote machine management for efficiency and cost savings
Telematics	Fleet management	Efficiency and cost savings
Payment systems	Mobile transaction terminals	Mobile vending and efficiency
Industrial automation	Over-the-air diagnosis and upgrades	Remote device management for time savings and reduced costs

RFID-Auto-Id



TEXT
- Human Readable 1nfo only
- Manuel data entry
- Subject to human error

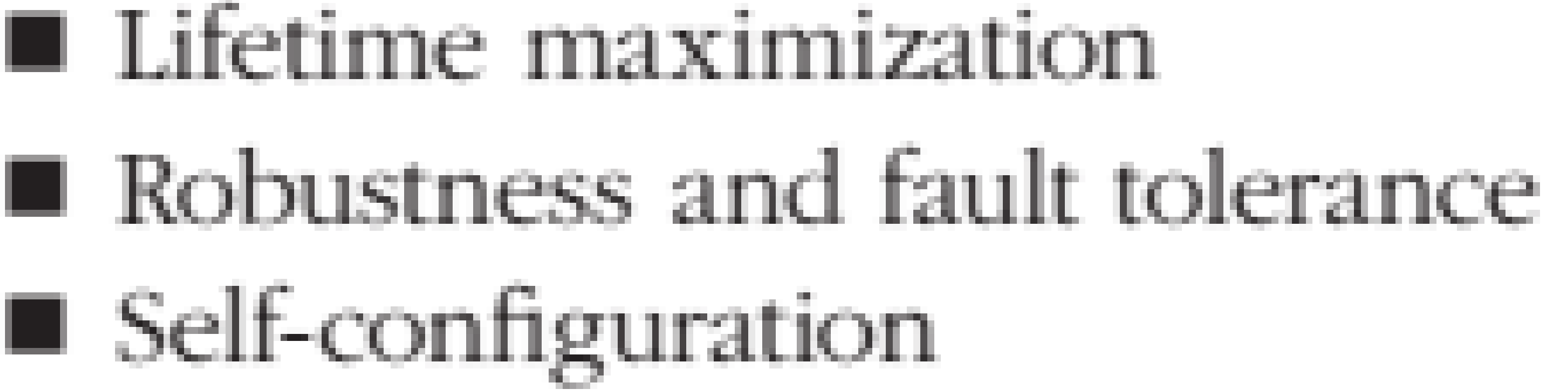
MAGNETIC STRIPE
- Machine Readable
- Contact Required
- 75 to 210 bits per inch

LINEAR BARCODE
- Machine Readable
- Average read accuracy:95%
- Line of sight required
- Data density <50 bits

2D BARCODES
- Stacked 1K bytes
- Matrix 2K bytes
- Line of sight required

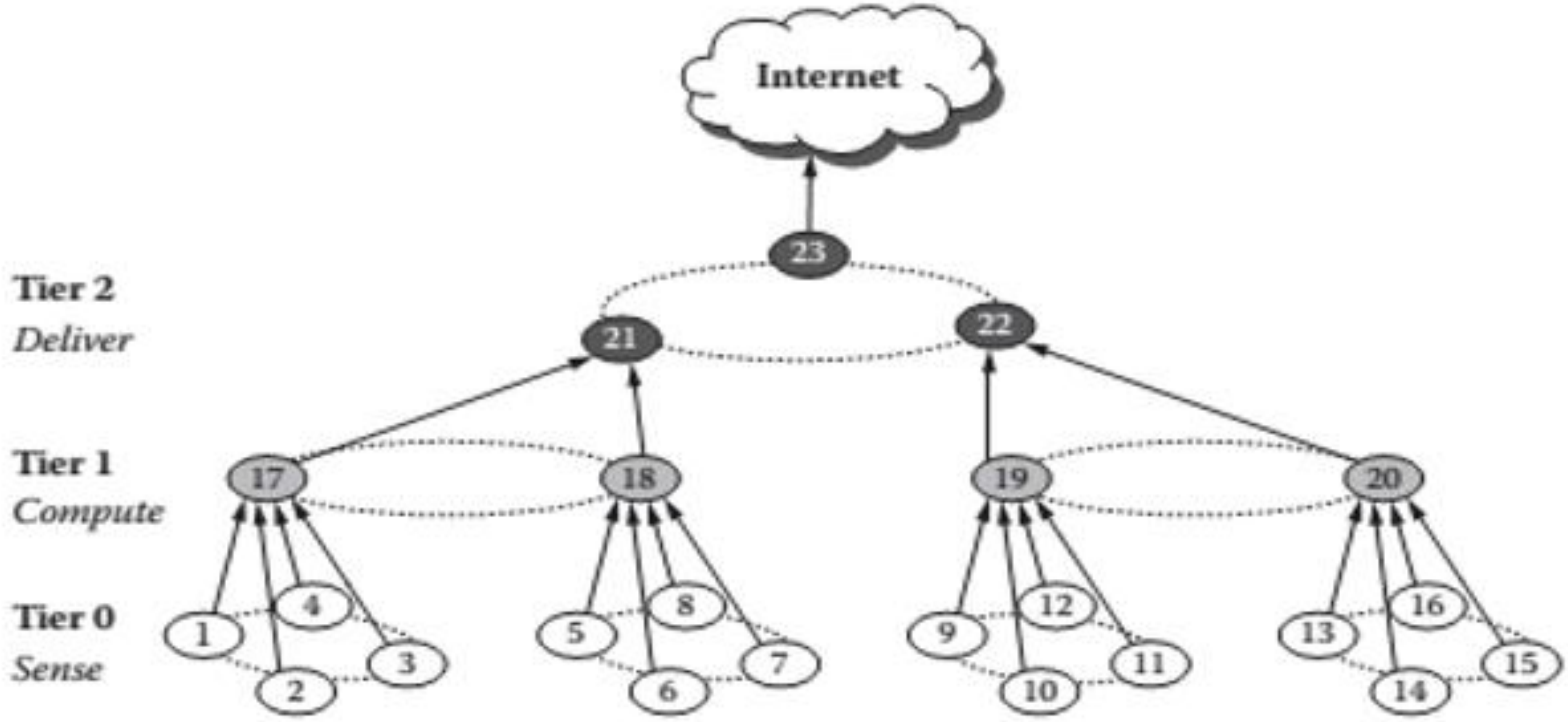
RFID
- Read Accuracy 99.9%
- Line of sight not required
- Read/Write capability
- Memory: 96 bits à 256 bytes

WSN Requirements

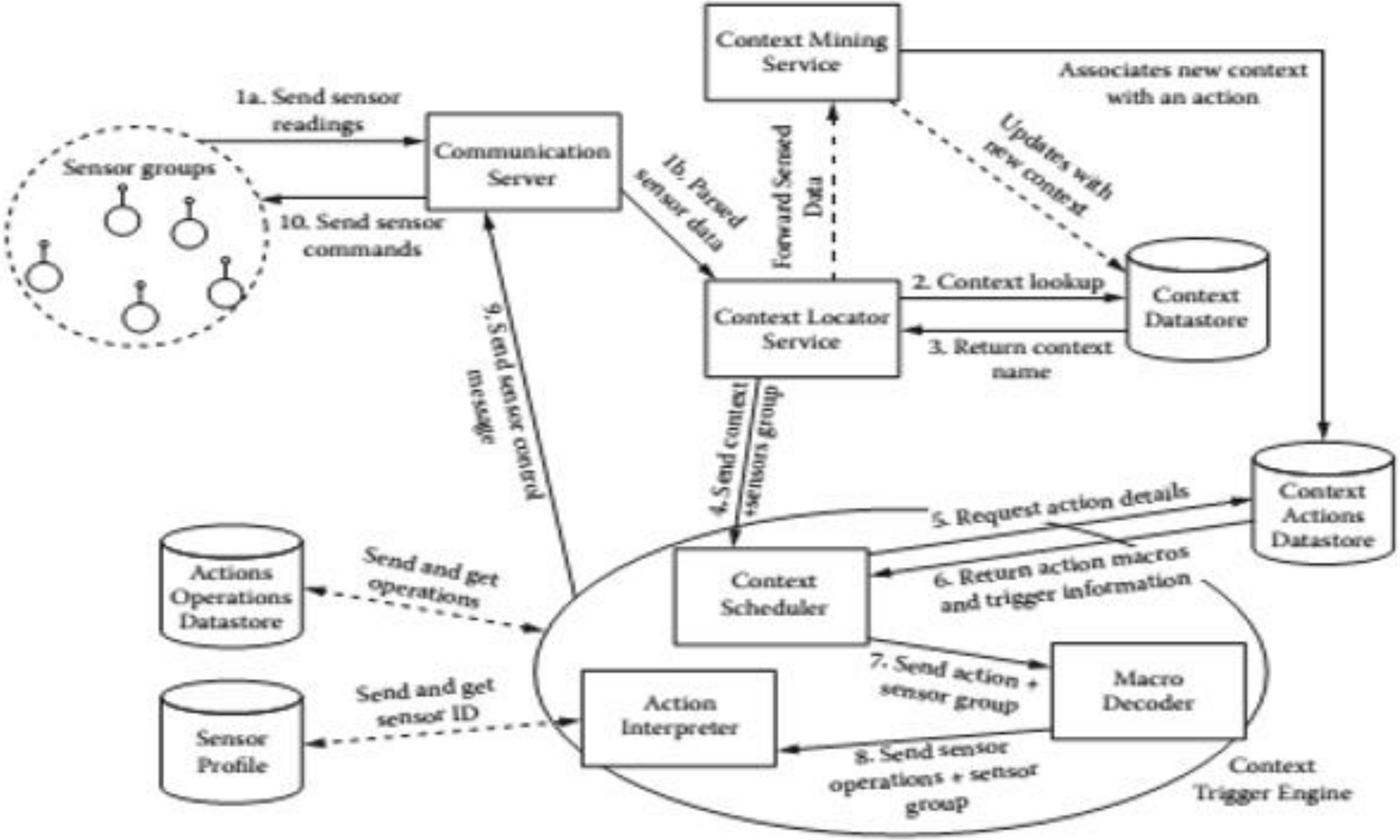


- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Sensor Network Architecture



Context-aware System based on WSN



SCADA: The Internet of Controllers

SCADA (supervisory, control and data acquisition) was generally referring to industrial control systems (ICSs): computer systems that monitor and control industrial, infrastructure, or facility-based processes, as below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defence siren systems, and large transportation systems.
- Facility processes occur in both public and private facilities, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption using PLCs (programmable logic controllers) and DCSs (distributed control systems) via the OPC (OLE for process control) middleware.

An existing SCADA system usually consists of the following subsystems:

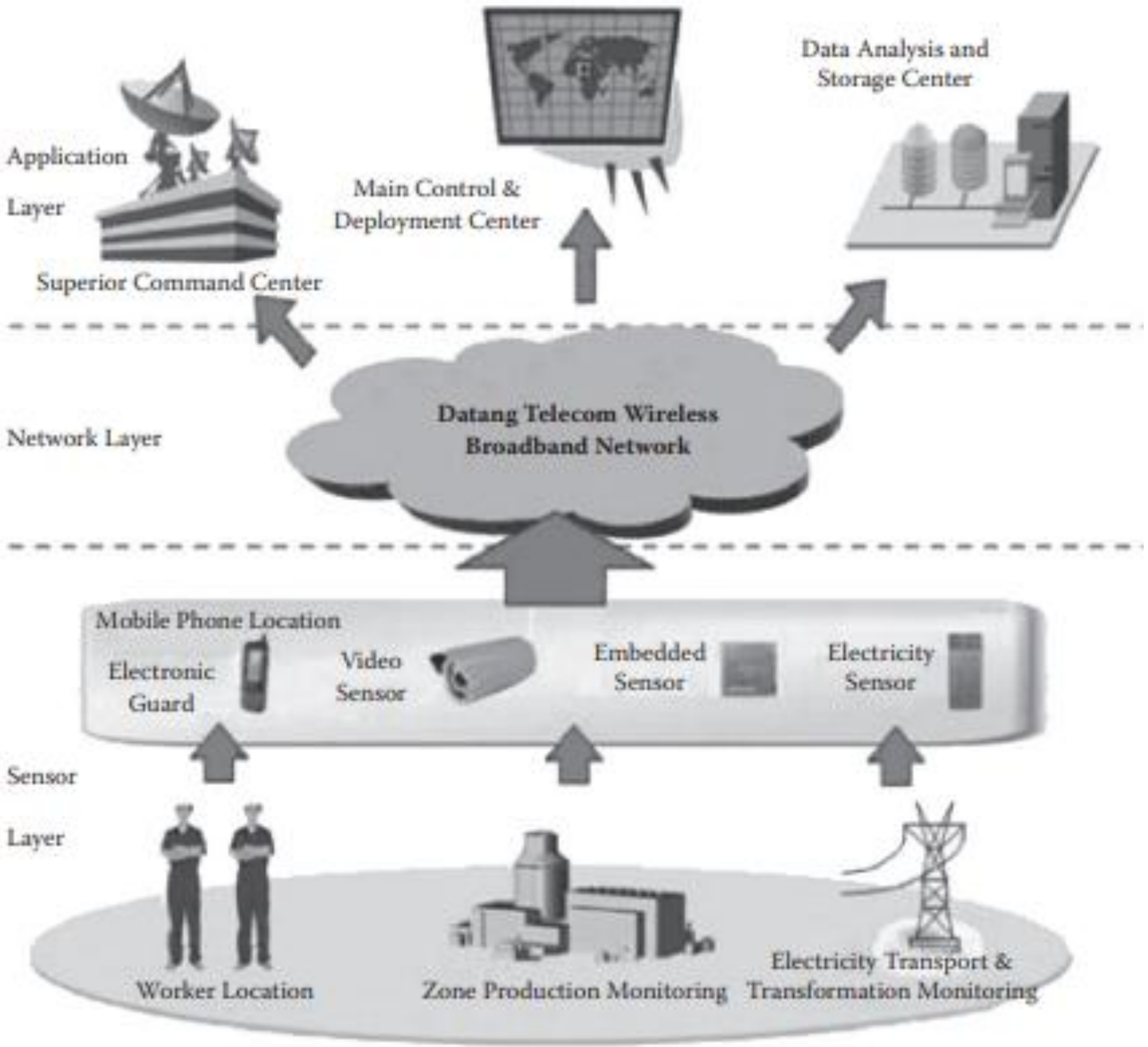
- A human–machine interface (HMI), which is the apparatus that presents process data to a human operator, and through this, the human operator monitors and controls the process.
- Remote terminal units (RTUs) connect to sensors in the process, convert sensor signals to digital data, and send digital data to the supervisory system.
- PLCs are used as field devices because they are more economical, versatile, flexible, and configurable than special purpose RTUs.
- DCSs; as communication infrastructures with higher capacity become available, the difference between SCADA and DCS will fade. SCADA is combining the traditional DCS and SCADA.
- M2M (telemetry), WSN, smart systems, CPS, and others all have overlaps of scope with SCADA, but the extended scope of SCADA is bigger under the IoT umbrella.

- A traditional SCADA system is a client/server system. New technological developments have turned C/S SCADA systems into middleware-backed, web-based, three-tiered open systems with SOA capabilities.
- SCADA systems allow the automation of complex industrial processes where human control is impractical.
- Integrating real-time visual surveillance systems with SCADA systems via IP video technology is now both a viable and an affordable solution for system integrators.
- Many industries are using SCADA as a core technology to link the geographically separated facilities and support new business processes in response to changing industry dynamics.

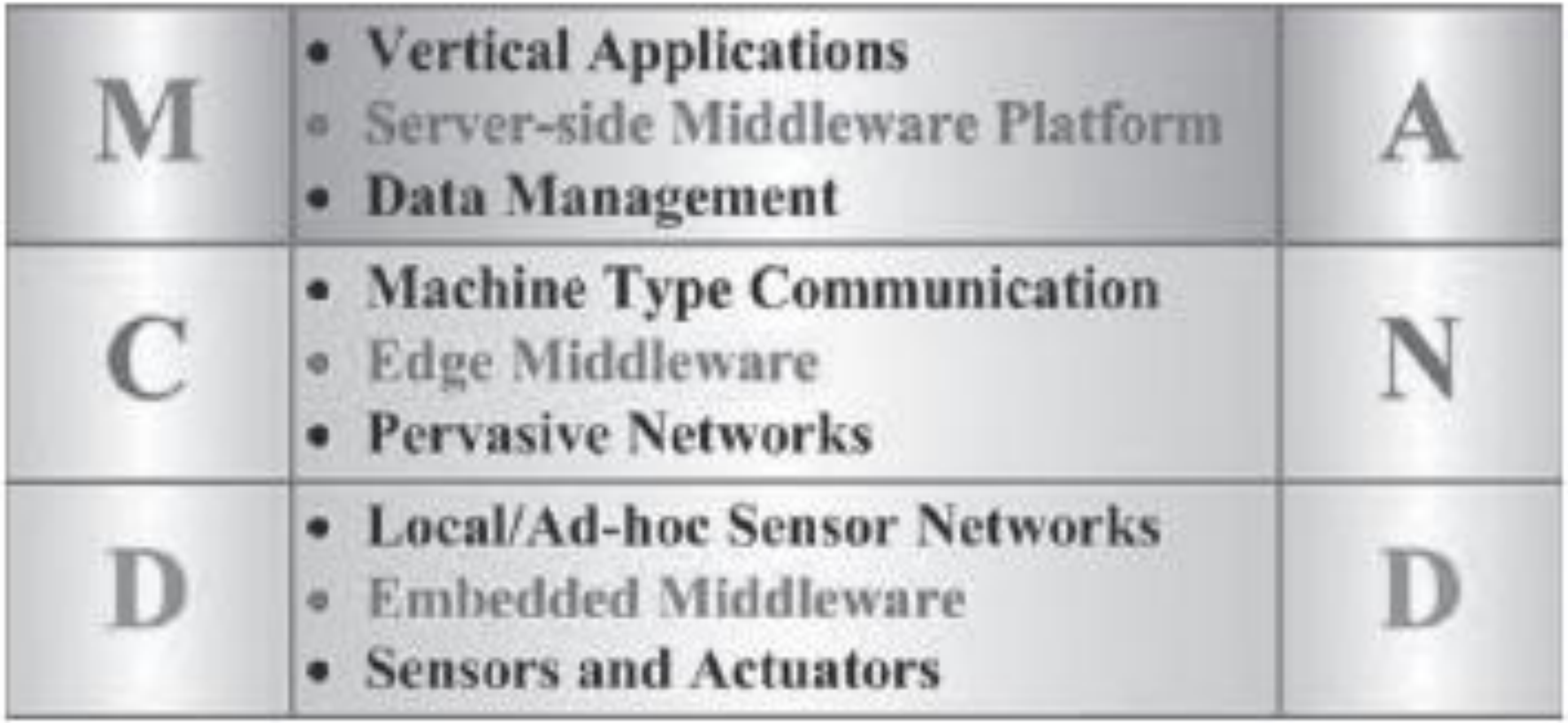
DNA of IoT

- DCM – Device, Connect, Manage
- Three-layer DCM classification is more about the IoT value chain than its system architecture at runtime.
- For system architecture, IoT system is divided into nine layers, from bottom to top: devices, connectivity, data collection, communication, device management, data rules, administration, applications, and integration.
- Large companies such as IBM, Oracle, Microsoft, and others have comprehensive solutions, products, and services that cover almost the entire value chain
- SCM- management of the flow of goods, data, and finances related to a product or service, from the procurement of raw materials to the delivery of the product at its final destination.
- Startups or smaller players in the IoT sector should focus on providing products or services in no more than two components or areas in the value chain

Three layer architecture of IoT - Examples



DCM (DNA) of IoT



M	• Vertical Applications • Server-side Middleware Platform • Data Management	A
C	• Machine Type Communication • Edge Middleware • Pervasive Networks	N
D	• Local/Ad-hoc Sensor Networks • Embedded Middleware • Sensors and Actuators	D

Devices: Things that talk

Two types

- Intelligent Devices - eg: HVAC
- Inert Devices – eg Furniture or Animals, must be enabled to become smart devices (e.g., RFID tagged)

- Sensors are fundamental building blocks of IoT networks
- Sensors are the foundational elements found in smart objects—the “things” in the Internet of Things

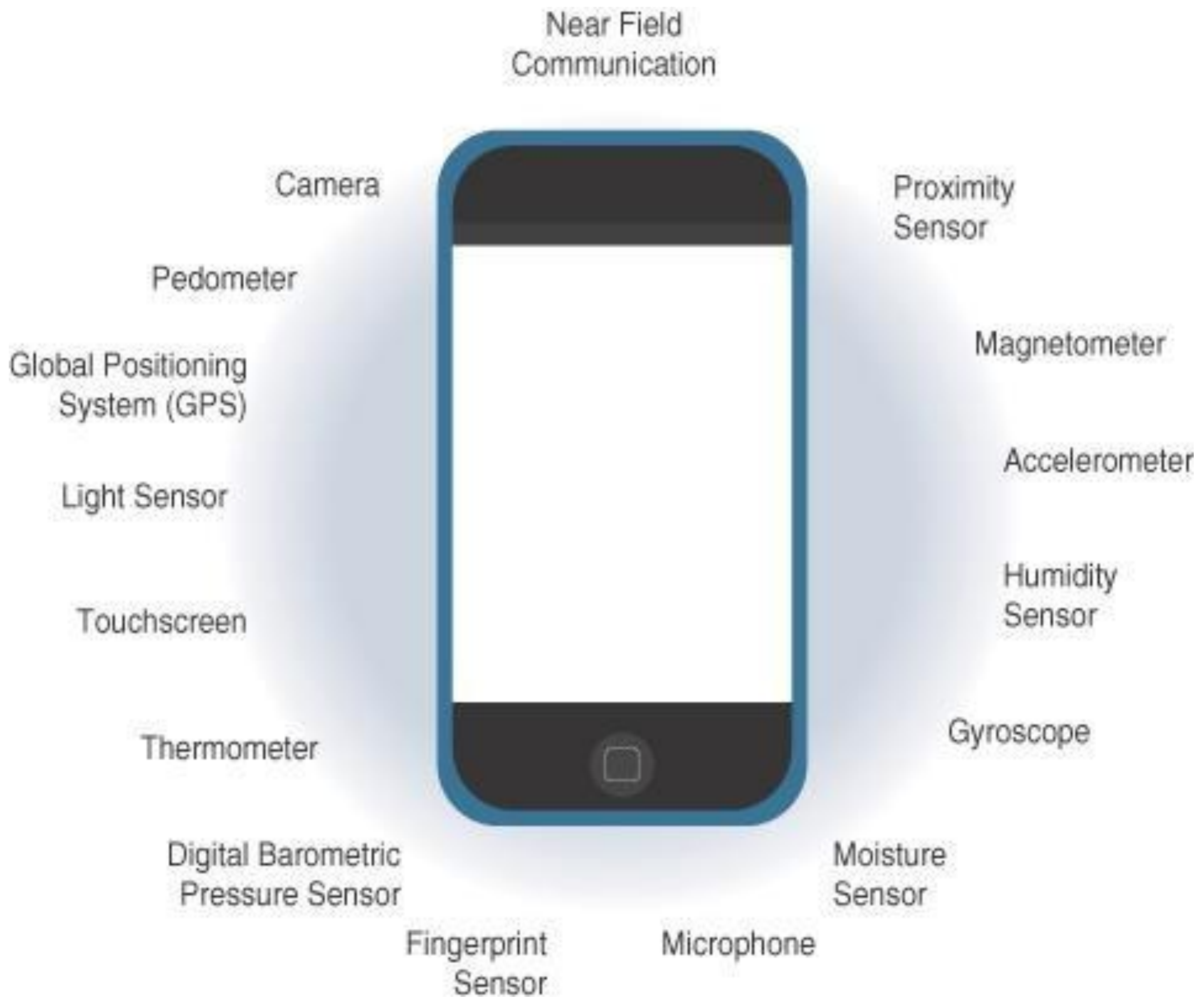
- Smart objects are **any physical objects** that contain **embedded technology to sense and/or interact with their environment in a meaningful way by being interconnected and enabling communication among themselves or an external agent.**

SENSORS, ACTUATORS, AND SMART OBJECTS

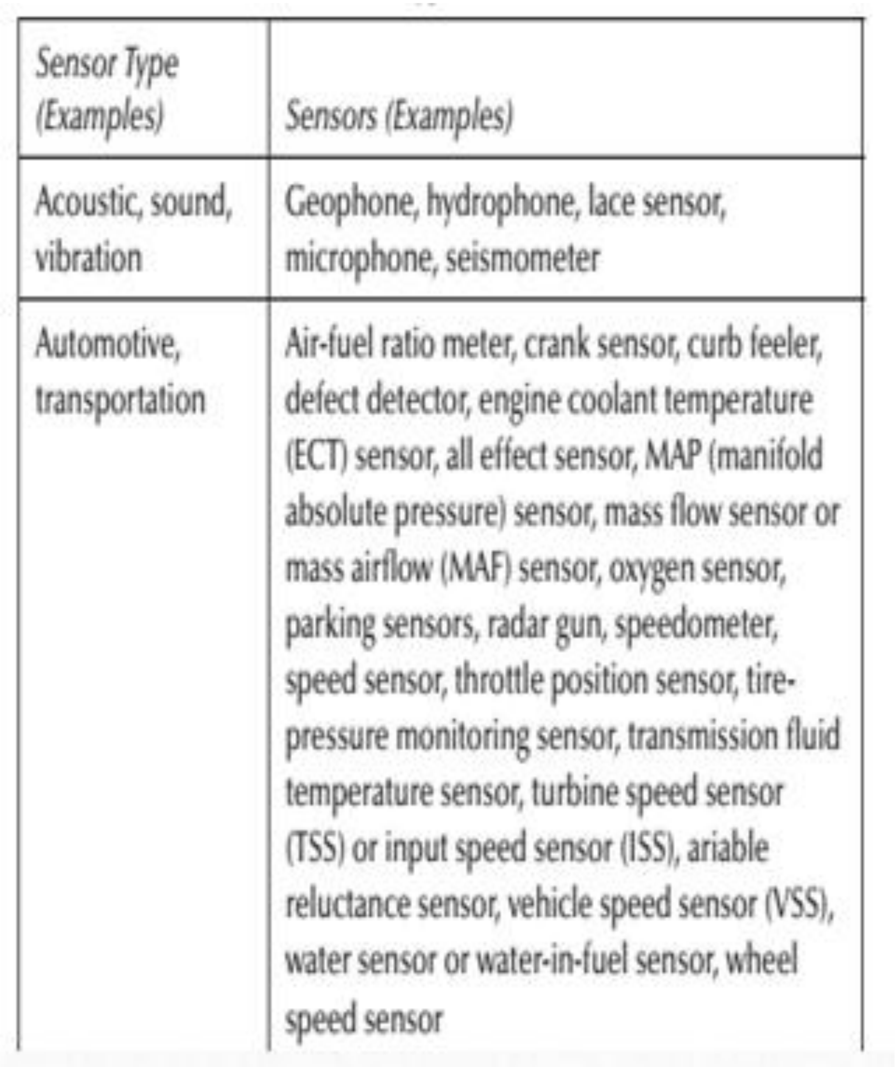
□ **A sensor**: It senses

- More specifically, ***a sensor measures some physical quantity and converts that measurement reading into a digital representation.***
- ***That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans***
- Sensors are not limited to human-like sensory data.
- They are able to provide an extremely wide spectrum of rich and diverse measurement data with far greater precision than human senses

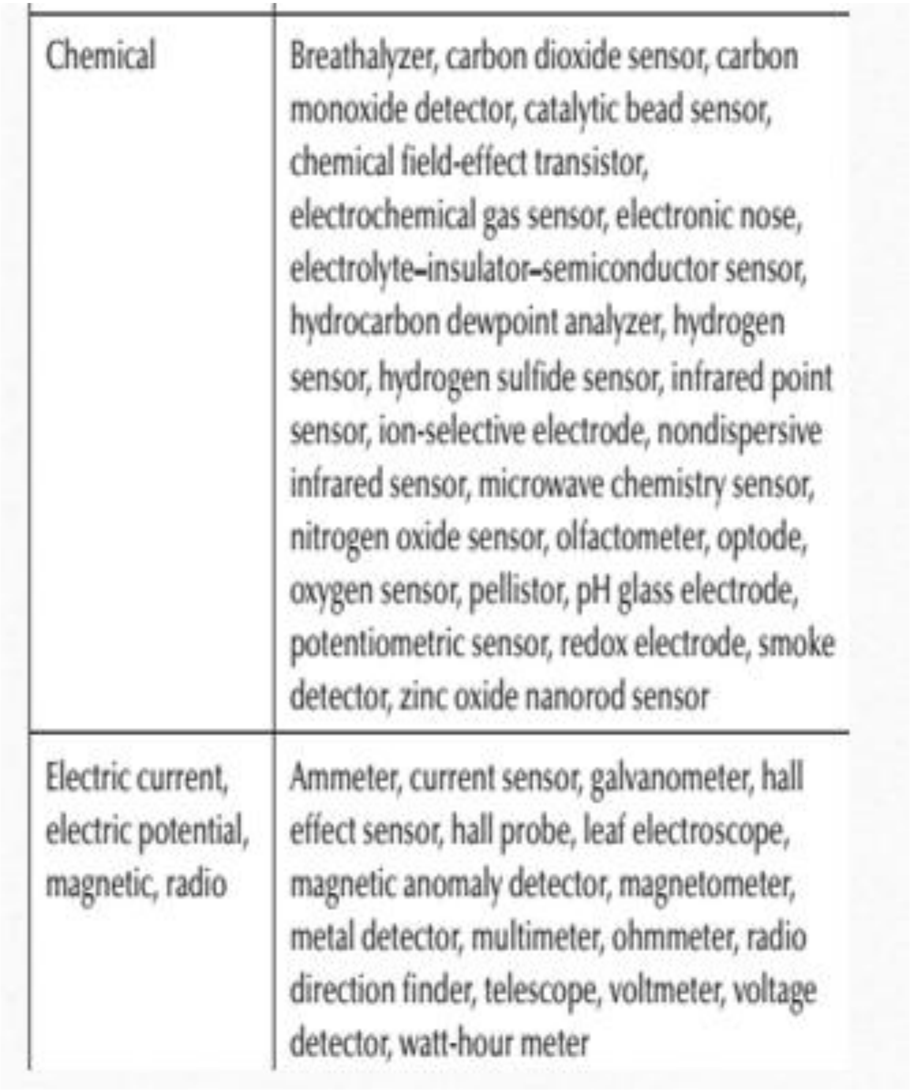
Sensors in a Smart Phone



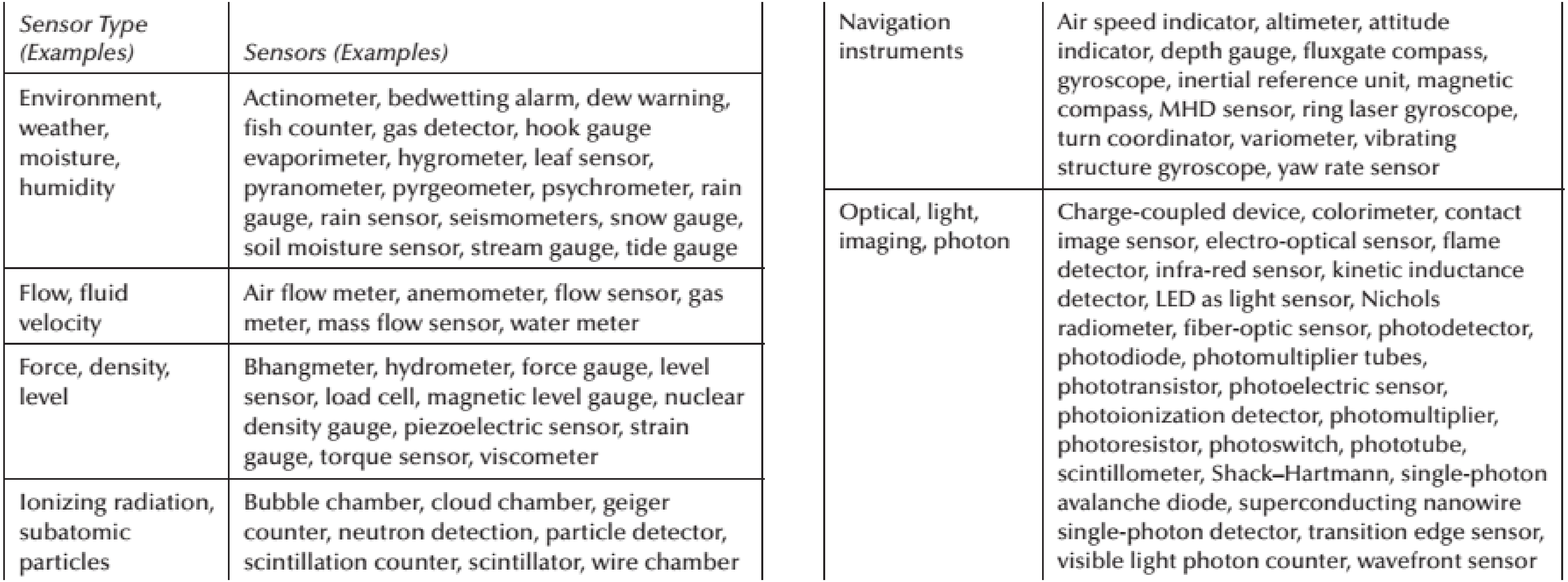
List of Sensor Types



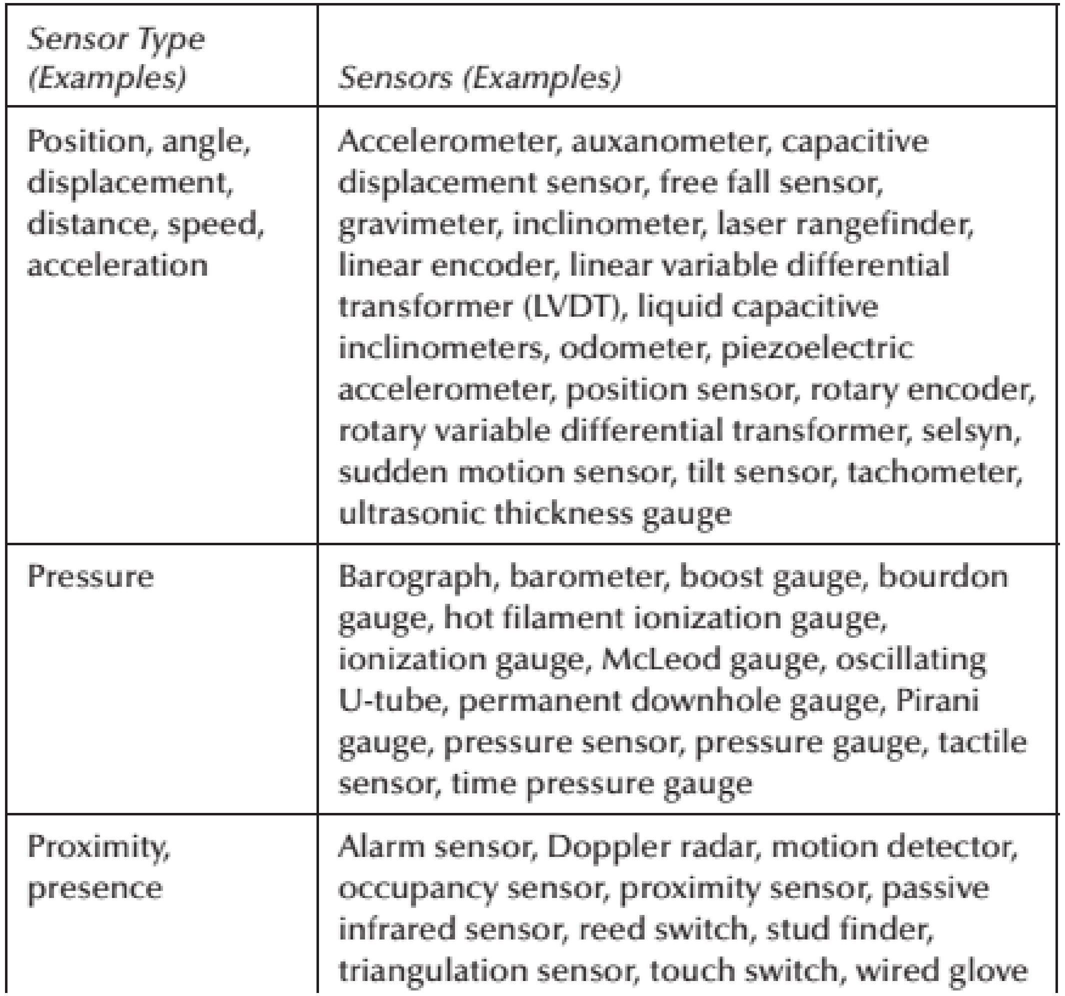
Sensor Type (Examples)	*Sensors (Examples)*
Acoustic, sound, vibration	Geophone, hydrophone, lace sensor, microphone, seismometer
Automotive, transportation	Air-fuel ratio meter, crank sensor, curb feeler, defect detector, engine coolant temperature (ECT) sensor, all effect sensor, MAP (manifold absolute pressure) sensor, mass flow sensor or mass airflow (MAF) sensor, oxygen sensor, parking sensors, radar gun, speedometer, speed sensor, throttle position sensor, tire-pressure monitoring sensor, transmission fluid temperature sensor, turbine speed sensor (TSS) or input speed sensor (ISS), ariable reluctance sensor, vehicle speed sensor (VSS), water sensor or water-in-fuel sensor, wheel speed sensor



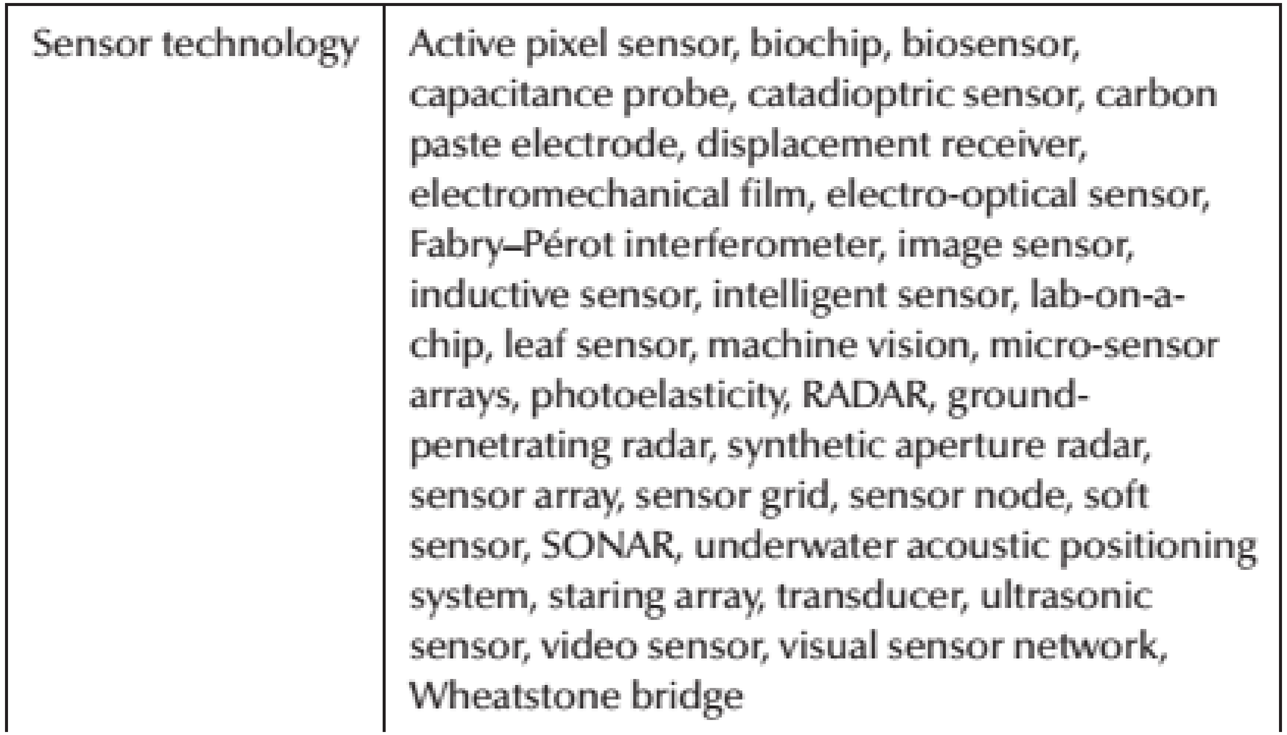
Chemical	Breathalyzer, carbon dioxide sensor, carbon monoxide detector, catalytic bead sensor, chemical field-effect transistor, electrochemical gas sensor, electronic nose, electrolyte–insulator–semiconductor sensor, hydrocarbon dewpoint analyzer, hydrogen sensor, hydrogen sulfide sensor, infrared point sensor, ion-selective electrode, nondispersive infrared sensor, microwave chemistry sensor, nitrogen oxide sensor, olfactometer, optode, oxygen sensor, pellistor, pH glass electrode, potentiometric sensor, redox electrode, smoke detector, zinc oxide nanorod sensor
Electric current, electric potential, magnetic, radio	Ammeter, current sensor, galvanometer, hall effect sensor, hall probe, leaf electroscope, magnetic anomaly detector, magnetometer, metal detector, multimeter, ohmmeter, radio direction finder, telescope, voltmeter, voltage detector, watt-hour meter



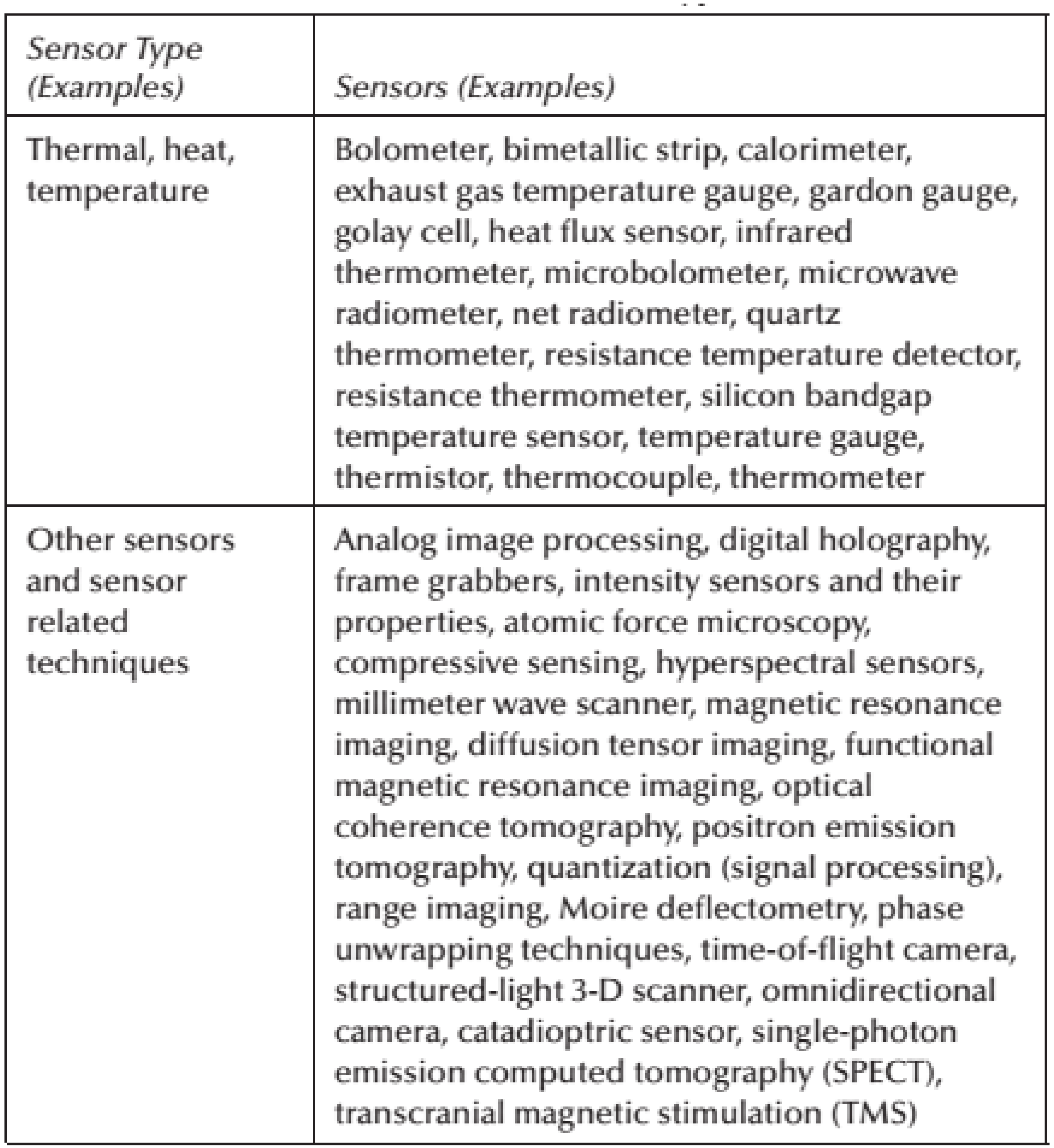
Sensor Type (Examples)	*Sensors (Examples)*
Environment, weather, moisture, humidity	Actinometer, bedwetting alarm, dew warning, fish counter, gas detector, hook gauge evaporimeter, hygrometer, leaf sensor, pyranometer, pyrgeometer, psychrometer, rain gauge, rain sensor, seismometers, snow gauge, soil moisture sensor, stream gauge, tide gauge
Flow, fluid velocity	Air flow meter, anemometer, flow sensor, gas meter, mass flow sensor, water meter
Force, density, level	Bhangmeter, hydrometer, force gauge, level sensor, load cell, magnetic level gauge, nuclear density gauge, piezoelectric sensor, strain gauge, torque sensor, viscometer
Ionizing radiation, subatomic particles	Bubble chamber, cloud chamber, geiger counter, neutron detection, particle detector, scintillation counter, scintillator, wire chamber
Navigation instruments	Air speed indicator, altimeter, attitude indicator, depth gauge, fluxgate compass, gyroscope, inertial reference unit, magnetic compass, MHD sensor, ring laser gyroscope, turn coordinator, variometer, vibrating structure gyroscope, yaw rate sensor
Optical, light, imaging, photon	Charge-coupled device, colorimeter, contact image sensor, electro-optical sensor, flame detector, infra-red sensor, kinetic inductance detector, LED as light sensor, Nichols radiometer, fiber-optic sensor, photodetector, photodiode, photomultiplier tubes, phototransistor, photoelectric sensor, photoionization detector, photomultiplier, photoresistor, photoswitch, phototube, scintillometer, Shack–Hartmann, single-photon avalanche diode, superconducting nanowire single-photon detector, transition edge sensor, visible light photon counter, wavefront sensor



Sensor Type (Examples)	*Sensors (Examples)*
Position, angle, displacement, distance, speed, acceleration	Accelerometer, auxanometer, capacitive displacement sensor, free fall sensor, gravimeter, inclinometer, laser rangefinder, linear encoder, linear variable differential transformer (LVDT), liquid capacitive inclinometers, odometer, piezoelectric accelerometer, position sensor, rotary encoder, rotary variable differential transformer, selsyn, sudden motion sensor, tilt sensor, tachometer, ultrasonic thickness gauge
Pressure	Barograph, barometer, boost gauge, bourdon gauge, hot filament ionization gauge, ionization gauge, McLeod gauge, oscillating U-tube, permanent downhole gauge, Pirani gauge, pressure sensor, pressure gauge, tactile sensor, time pressure gauge
Proximity, presence	Alarm sensor, Doppler radar, motion detector, occupancy sensor, proximity sensor, passive infrared sensor, reed switch, stud finder, triangulation sensor, touch switch, wired glove



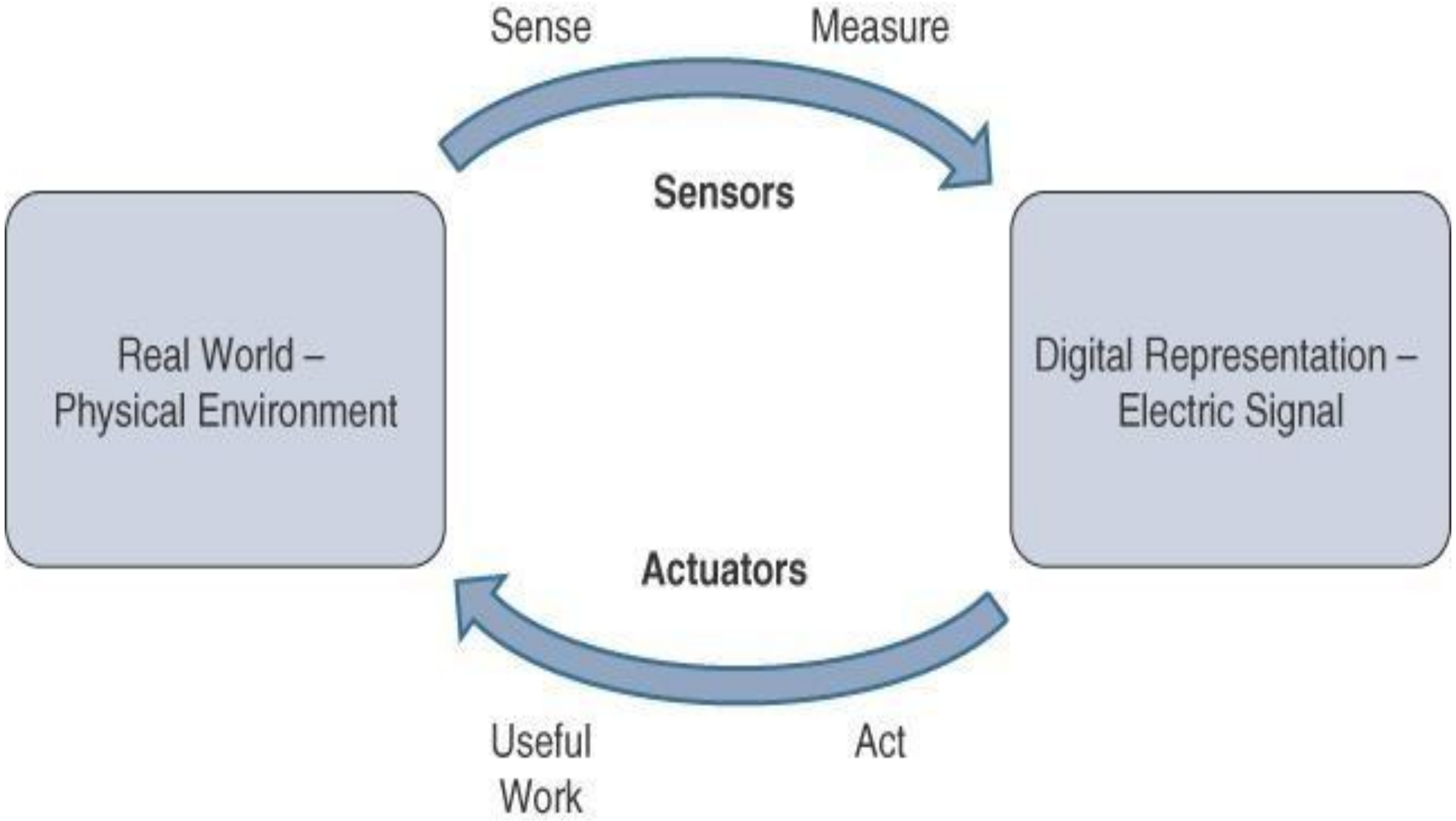
Sensor technology	Active pixel sensor, biochip, biosensor, capacitance probe, catadioptric sensor, carbon paste electrode, displacement receiver, electromechanical film, electro-optical sensor, Fabry–Pérot interferometer, image sensor, inductive sensor, intelligent sensor, lab-on-a-chip, leaf sensor, machine vision, micro-sensor arrays, photoelasticity, RADAR, ground-penetrating radar, synthetic aperture radar, sensor array, sensor grid, sensor node, soft sensor, SONAR, underwater acoustic positioning system, staring array, transducer, ultrasonic sensor, video sensor, visual sensor network, Wheatstone bridge

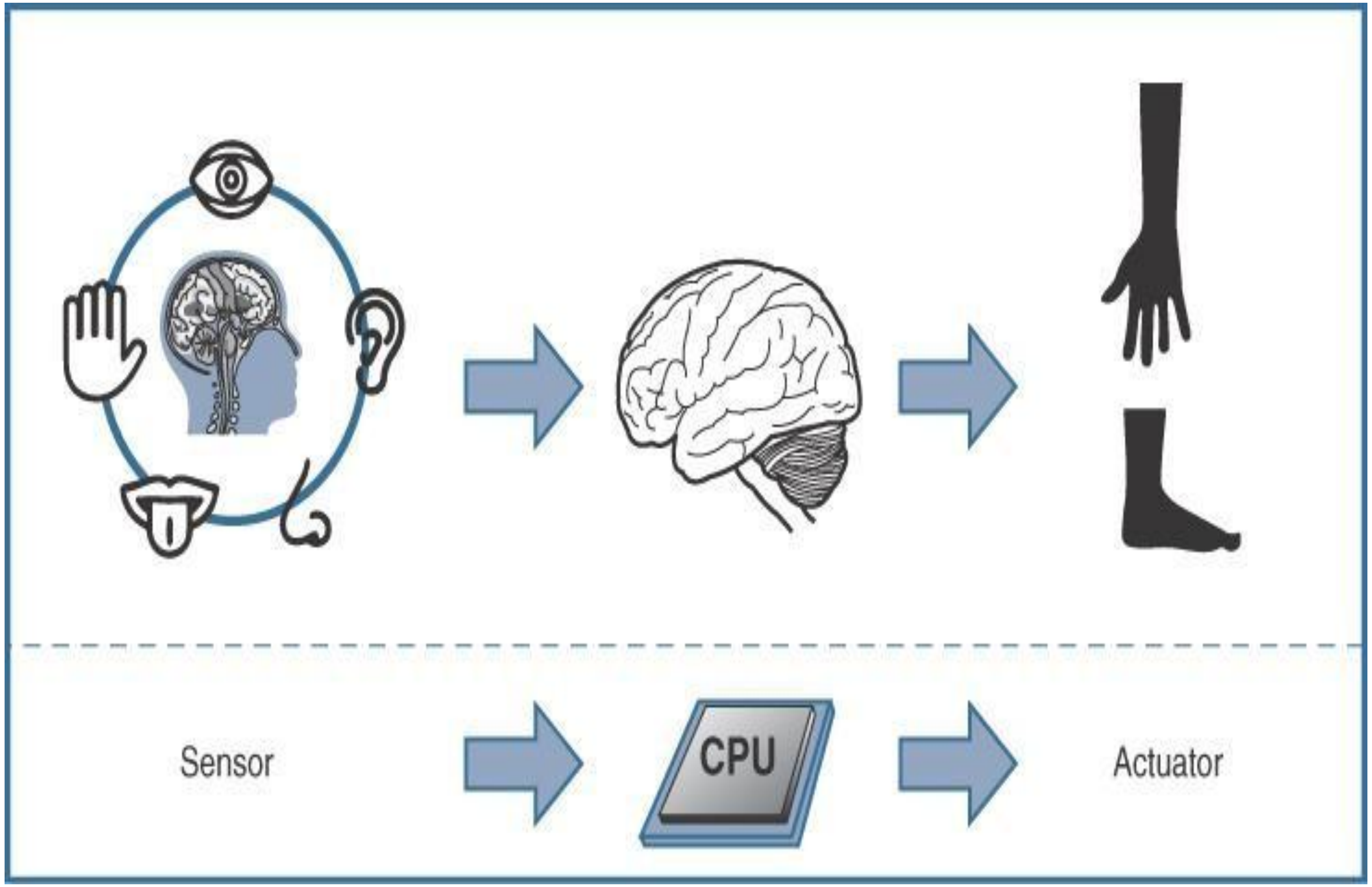


Sensor Type (Examples)	*Sensors (Examples)*
Thermal, heat, temperature	Bolometer, bimetallic strip, calorimeter, exhaust gas temperature gauge, gardon gauge, golay cell, heat flux sensor, infrared thermometer, microbolometer, microwave radiometer, net radiometer, quartz thermometer, resistance temperature detector, resistance thermometer, silicon bandgap temperature sensor, temperature gauge, thermistor, thermocouple, thermometer
Other sensors and sensor related techniques	Analog image processing, digital holography, frame grabbers, intensity sensors and their properties, atomic force microscopy, compressive sensing, hyperspectral sensors, millimeter wave scanner, magnetic resonance imaging, diffusion tensor imaging, functional magnetic resonance imaging, optical coherence tomography, positron emission tomography, quantization (signal processing), range imaging, Moire deflectometry, phase unwrapping techniques, time-of-flight camera, structured-light 3-D scanner, omnidirectional camera, catadioptric sensor, single-photon emission computed tomography (SPECT), transcranial magnetic stimulation (TMS)

Actuators

- Actuators are natural complements to sensors
- Sensors are designed to sense and measure practically any measurable variable in the physical world.
- They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).
- **Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.**
- ***Sensors provide the information, actuators provide the action***


Sense
Measure
Sensors
Real World –
Physical Environment
Digital Representation –
Electric Signal
Actuators
Useful
Work
Act



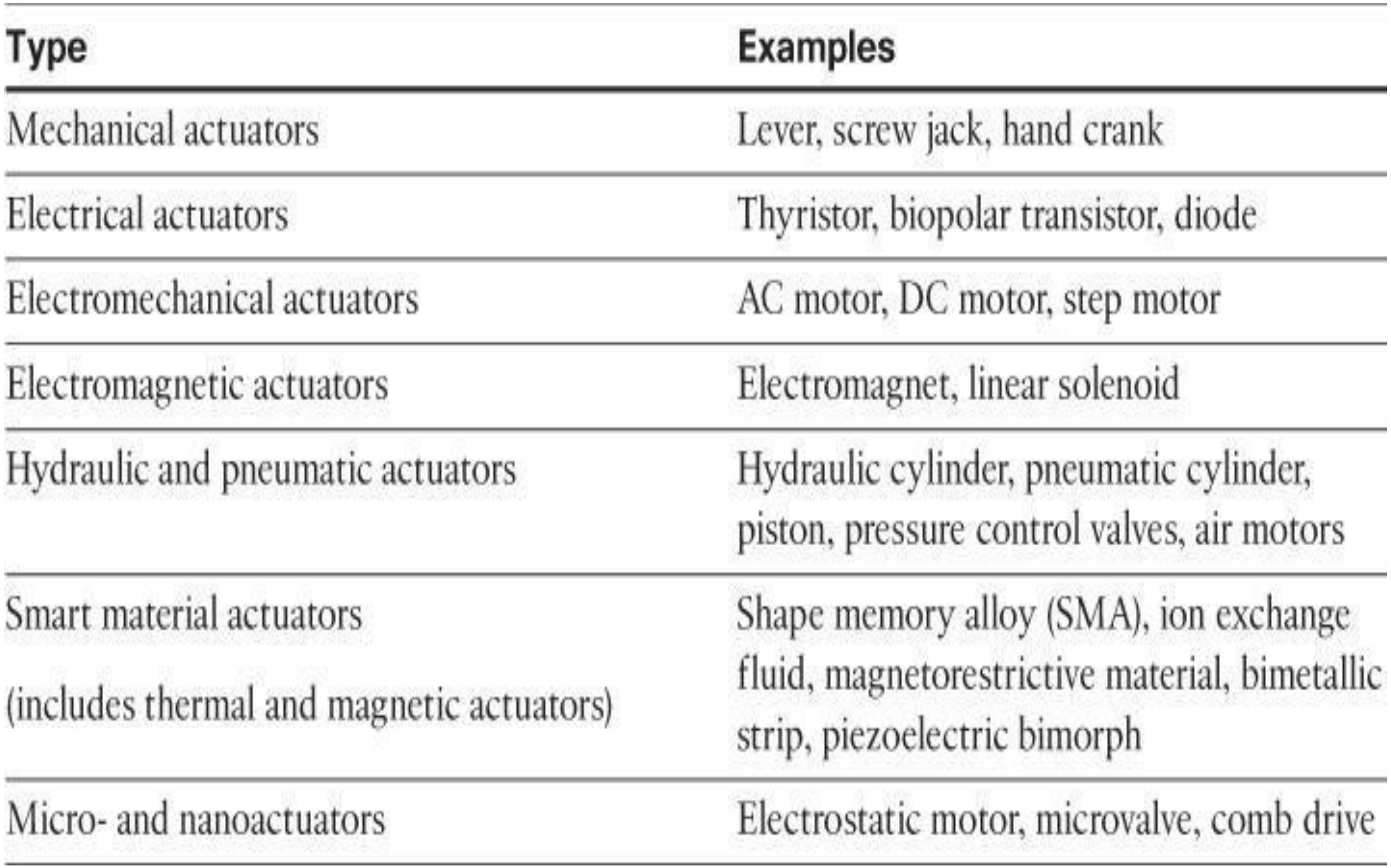
Sensor

CPU

Actuator

- Actuators also vary greatly in function, size, design, and so on.
- Some common ways that they can be classified include the following:
- **Type of motion:** Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three- axes).
- **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power)
- **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.
- **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.
- **Type of energy:** Actuators can be classified based on their energy type.

Classification based on energy type



Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

Connect: Via Pervasive Networks

- Wired vs Wireless
- Short Range Vs Long Range
- Broadband Vs Narrow band
- Packet or Circuit Switched
- Internet Protocol IPv6- expand the internet

Wired Networks Types

1. Short- range field bus–based access networks, mostly for SCADA applications

- Field bus is the name of a family of industrial computer network protocols used for real- time distributed control, now standardized as IEC 61158.
- The IEC 61158 standard includes eight different protocol sets called types:
- Field bus standards are available depending on the type of application
  - Type 1 Foundation field bus H1
  - Type 2 ControlNet
  - Type 3 PROFIBUS
  - Type 4 P- Net
  - Type 5 FOUNDATION field bus HSE (high- speed Ethernet)
  - Type 6 SwiftNet (a protocol developed for Boeing, since withdrawn)
  - Type 7 WorldFIP
  - Type 8 Interbus

2. IP- based networks, for M2M and SCADA applications.

Wireless Networks

1. Short- range (including near field communication [NFC], usually narrowband, and wireless PAN, LAN, and MAN) mesh networks, RFID, WiFi, WiMax … - RFID and WSN.
2. Long- range (via cellular networks, wireless WAN, pseudo long-range) GSM, CDMA, WCDMA, and other networks, as well as satellite communication.- M2M communication
3. Satelite IoT
   - GEO: Geostationary Earth Orbit- Immarsat
   - MEO: Medium Earth Orbit - GPS
   - LEO: Low (polar and nonpolar) Earth Orbit- Iridium

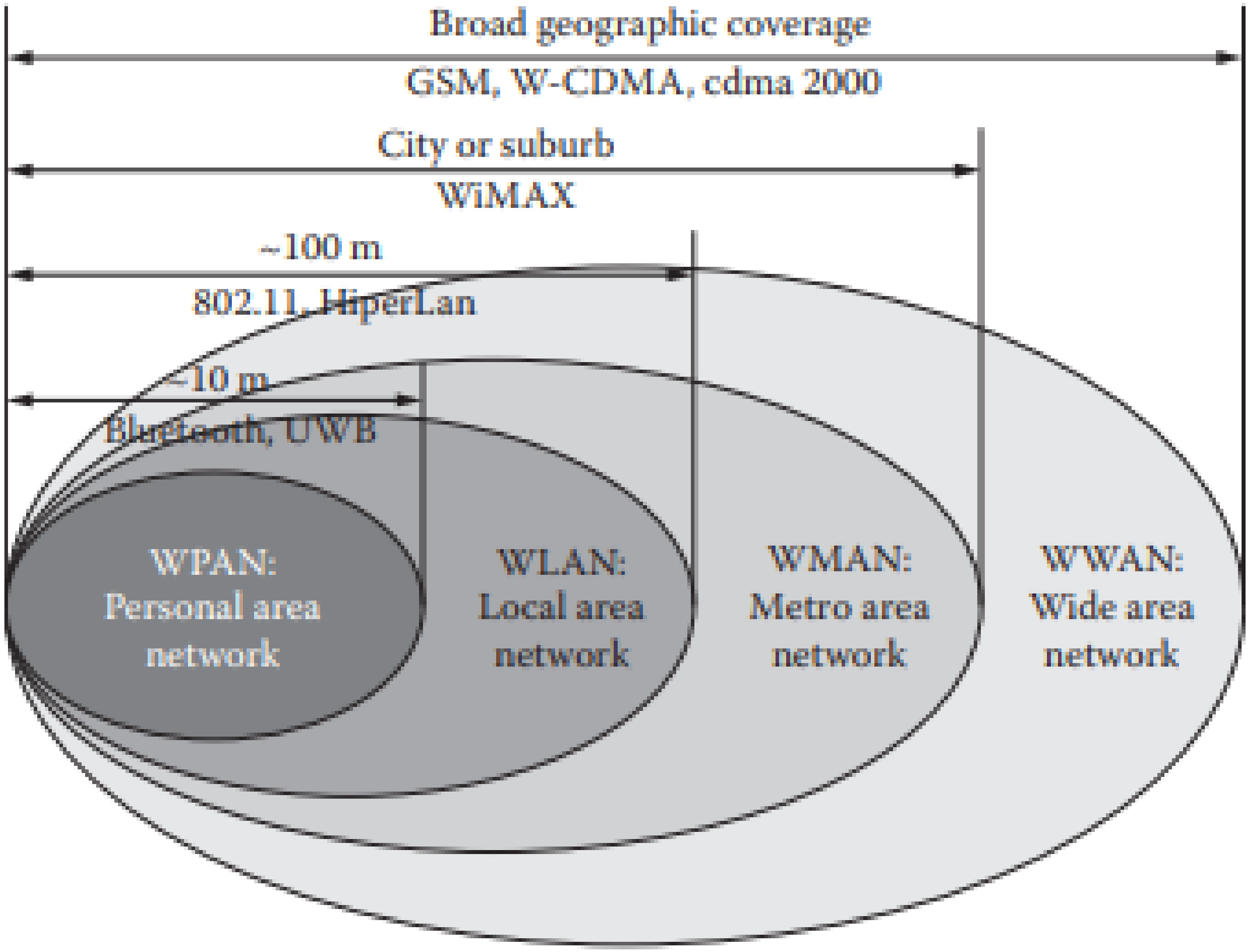
   Issues Speed and Cost- not suitable for two way communication

   LTE – Long Term Evolution -standard for wireless communication of high-speed data. It is based upon GSM/EDGE and UMTS/ HSPA network technologies.

   -an all-IP flat network architecture including end-to-end QoS, provisions for low-latency communications.

   - supports triple (Internet, telephony, and cable TV) networks

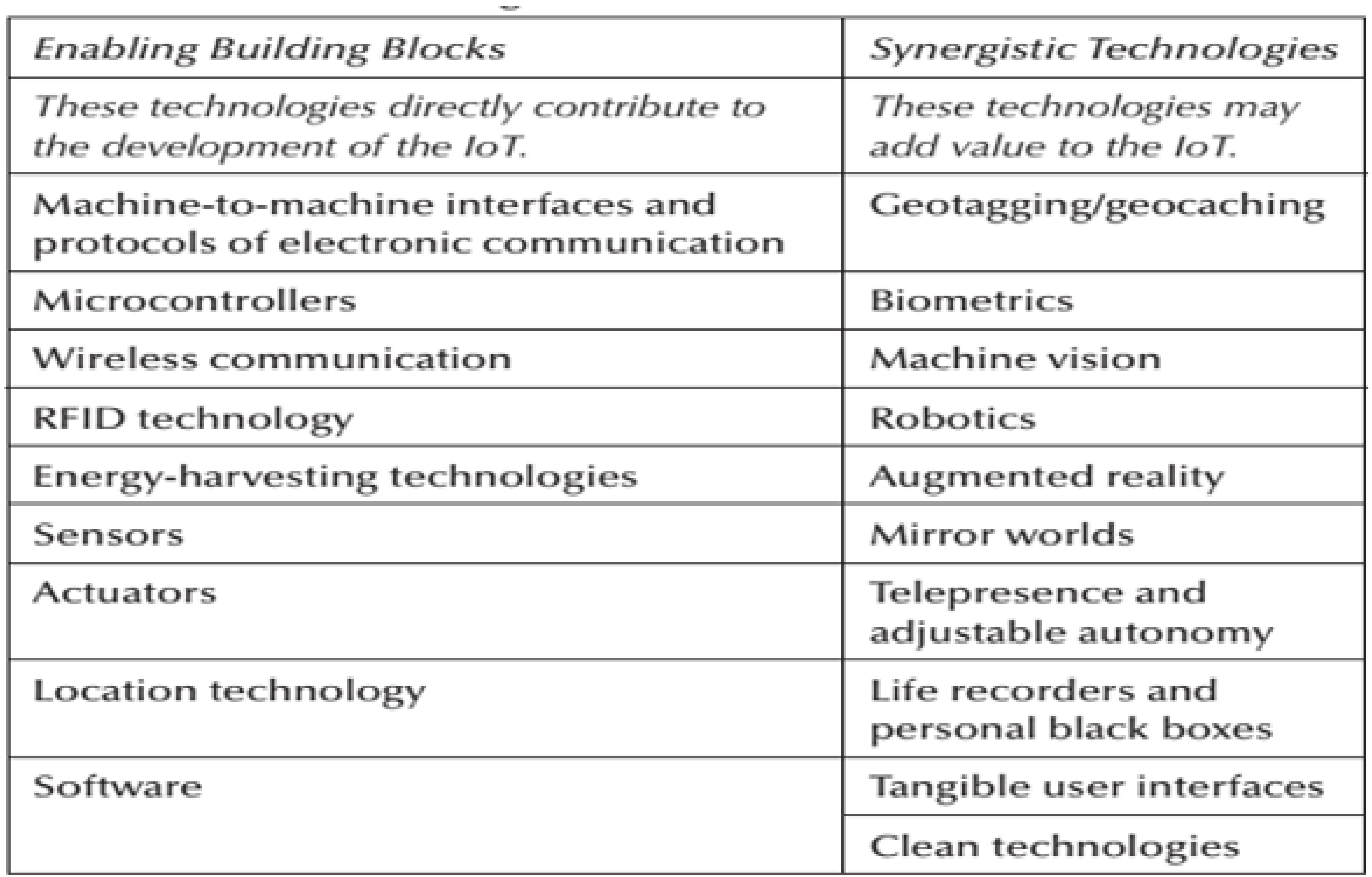
Short- and long-range wireless networks



Manage: To Create New Business Value

- In the current customer-driven, technology-based environment, it is no longer enough to offer a service or product and expect it to satisfy the customers.
- Even with the best customer service in the industry, it has to extend out offerings to meet current demand to keep the customers satisfied.
- The Internet of Things brings enormous possibilities and potentials for creating new business value and generating new revenue ecosystems with data processing and managing rules that combine intelligence from remote assets unreachable before with the intelligent enterprise systems.

IoT Technologies



Enabling Building Blocks	*Synergistic Technologies*
These technologies directly contribute to the development of the IoT.	*These technologies may add value to the IoT.*
Machine-to-machine interfaces and protocols of electronic communication	Geotagging/geocaching
Microcontrollers	Biometrics
Wireless communication	Machine vision
RFID technology	Robotics
Energy-harvesting technologies	Augmented reality
Sensors	Mirror worlds
Actuators	Telepresence and adjustable autonomy
Location technology	Life recorders and personal black boxes
Software	Tangible user interfaces
	Clean technologies

The participating entities of the IoT/M2M value chain are,

1. The business or consumer is involved in the consumption of the service. One possible way of their influencing the IoT is in terms of the demand. Changes in demand would lead to different configurations among the players in the business, in order to generate economically viable business models.
2. The system or service operator provides the basic M2M service to the end-user. The system operator works in tandem with the network operator to provide M2M services. The service operator has a direct relationship with the end-user.
3. The network operator provides the basic communications transport network service to the service operator.
4. The application provider or developer develops M2M value-added services for a service operator to be consumed by the end-user.
5. The end-user equipment vendor provides M2M-enabled equipment. A player in this role would typically work with the systems integrator.

6. The mobile equipment vendor provides the necessary mobile infrastructure such as GSM/GPRS/3G routers for M2M communications. A player in this role would work with the network operator.
7. The system integrator plays a major role in providing an end-to-end M2M solution. A player in this role can be an application developer and would work with network operators, end-user, and equipment vendors.

System integrators and service operators as well as application developers are in the “M” domain.

Network operators and equipment vendors are in the “C” domain, and

End-user equipment vendors are in the “D” domain.

Middleware for IoT

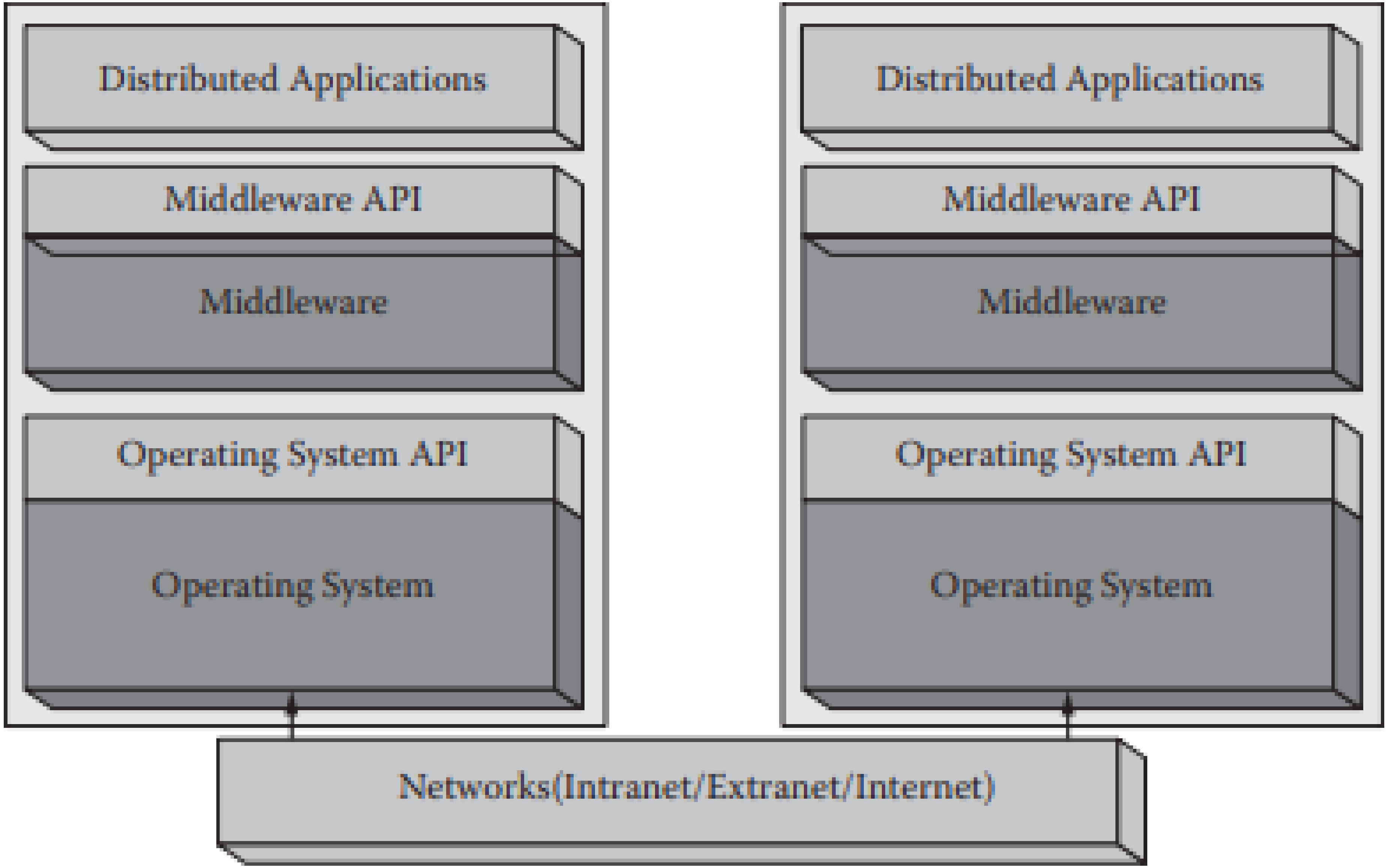
Overview

- Middleware refers to a set of enabling services such as standardized APIs, RMI, PRC, protocols, and infrastructure services for supporting the rapid and convenient development of distributed services and applications based on the client/ server and later multi-tiered paradigm, which was essential for migrating single-tiered mainframe/ terminal applications to multi-tiered architecture.
- Middleware is a layer that is arranged on top of operating systems and communications stacks and thus hides heterogeneity from the applications through a set of common, well-defined interfaces
- APIS allow different systems, applications and devices to share information with each other

Middleware Services

  - Authentication
  - Authorization
  - Soft- switching
  - Certification and
  - Security
- Accessing real-time information among the different systems
- It helps to increase the growth of organizational efficiency and also streamlines business processes
- Middleware maintains data integrity among the different systems
- Middleware increases the functionality of applications.

Omnipresent middleware



Need for Middleware

- Enables applications running across multiple platforms to communicate with each other
- Shields the developer from dependencies on network protocols, operating systems, and hardware platforms
- Is a software layer that lies between the operating system and the applications on each site of the system
- Hides heterogeneity and location independence
- Increases software portability
- Provides common functionality needed by many applications
- Aids application interoperability
- Aids scalability
- Helps integrate legacy facilities

Middleware Types

- Message- Oriented Middleware (MOM/ MQ/ JMS)
- CEP (complex event processing) Middleware (Tibco, Sybase)
- Adaptive and Reflective Middleware (TAO/ DynamicTAO/OpenORB)
- Transaction Middleware (TPM/ Tuxedo)
- Peer- to- Peer Middleware (JXTA)
- Grid Middleware (PVM/ MPI/ Schedulers)
- Model- Driven Middleware (CoSMIC)
- Games Middleware (Autodesk)
- Mobile Computing Middleware (OSA/ Parlay/ JAIN/ OMA)
- Radio- frequency Identification (RFID) (Smart Cards) Middleware (Edgeware)
- Three- tiered Application Server Middleware (Weblogic, Websphere)
- Real- time CORBA Middleware (Real- time CORBA)
- High- Availability (Fault Tolerance) Middleware (FaultTolerant CORBA)
- Security Middleware (Siteminder)
- CATV/ IPTV Middleware (MHP/ GEM/ OCAP)
- RFID Edge Middleware (OATSystems, Sybase, Oracle, IBM, SAP)
- Process- Oriented Middleware (WebMethods, SeeBeyond, Tibco, IBM, SAP, Oracle)
- Business- to- Business (B2B)-Oriented Middleware (SeeBeyond/ Oracle, Tibco, webMethods)
- Middleware for Location- Based Services
- Surveillance Middleware

M2M Middleware

- **Data management middleware**: helps programs read from and write to remote databases or files.eg: Google File System, IBM GPFS, Network File System, and Windows ; **remote database access middleware**, such as Open Database Connectivity or Java Database Connectivity libraries
- **Communication middleware**: software that support protocols for transmitting messages or data between two points as well as a system programming interface (SPI) to invoke the communication service. REST (Representational State Transfer), SOAP (simple object access protocol), MSMQ (MicroSoft Message Queuing), MQ, JMS.
- **Platform middleware:** provides the runtime hosting environment (a container) for application components; J2EE, .net framework

Communication Middleware for IoT

Three-layer DCM model can be further extended into more layers depending upon the geographical scope of the area network (AN) from BAN to interplanetary Internet as below:

- Body (BAN)
- Personal (PAN)
- Near-me (NAN)
- Machine-to-machine, or M2M (MAN)
- Local (LAN)
  - Home (HAN)
  - Storage (SAN)
- Campus (CAN)
- Backbone
- Metropolitan (MAN)
- Wide (WAN)
- Internet
- Interplanetary Internet

MTC/M2M Middleware

- Efforts are underway to build a unified communication network middleware for IoT applications.
- The connect layer of DCM can be further divided into three layers for GSM/WCDMA family cellular wireless M2M standardization:
- M2M area network layer
- access/core network layer
- external/Internet network layer

- M2M area network—provide wired or wireless connectivity between M2M devices and M2M gateways, such as personal area network
- M2M access/core network—ensure M2M devices interconnection from the gateways to the access/core communication network, such as GPRS/GSM (GGSN [Gateway GPRS Support Node], SGSN [Serving GPRS Support Node], etc.; WCDMA, and others
- External/Internet networks (long distance)—communicate between the 3GPP access/core network and the M2M middleware platform for applications, such as Internet, corporate WANs, and others

- MTC (machine-type communication) is the term 3GPP used for cellular M2M communication. It refers to communication without (or with limited) human intervention; data are input or generated by machines instead of humans, which can be significantly faster.
- Most future big data growth will be in the area of M2M machine-generated data, examples of which include
    - Satellite-based telemetry application-generated data
    - Location data such as RFID chip readings, global positioning system (GPS) output
    - Temperature and other environmental sensor readings
    - Sensor readings from factories and pipelines
    - Output from many kinds of medical devices, in hospitals and homes alike

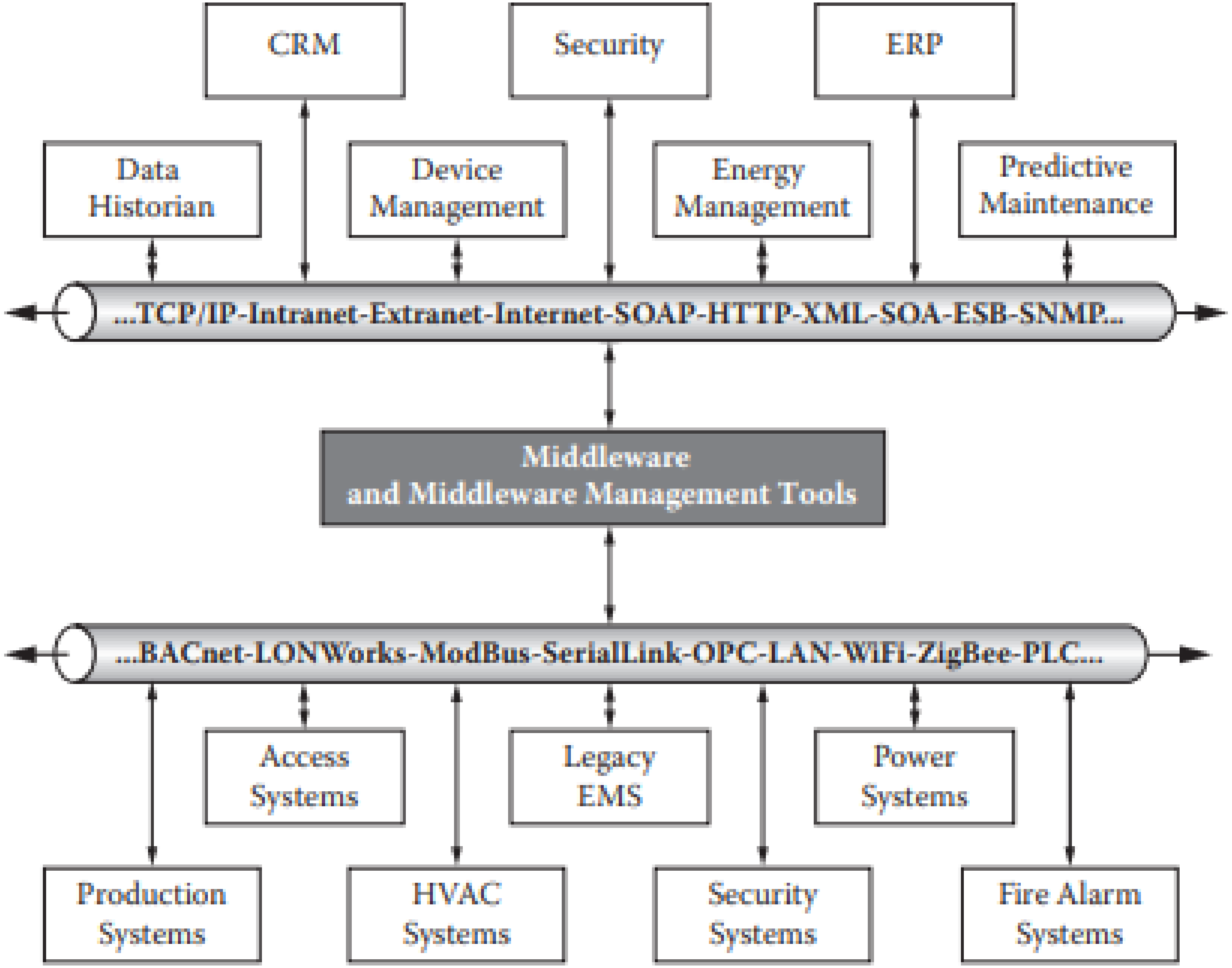
- The major issue is lacks of specifying a unified middleware framework for all MTC networks.
- A new middleware architecture with innovative aspects in terms of: full support along the whole path rather than at the front and backend nodes, highly service aware networks, network aware services, and intelligent coordination and cooperation capabilities is required in next generation networks
- In addition to the MTC optimization of the cellular wireless network, other optimizations or service enablement middleware.
- Service enablement can be built as middleware that provides reliable and efficient connectivity for adjacent industry applications and to enable operators to
  - Act as horizontal service providers across applications and industries
  - Expand their role as managed service providers
  - Capture maximum value as smart service providers

- Nokia is one of the earliest vendors that offered M2M middleware.
- The Nokia M2M platform is based on open, widely accepted middleware (built on CORBA) and communications architecture, and it supports standard GSM technology with a choice of wireless bearers.
- CORBA was popular in 1990’s and now replaced by RMI - Both of them allow Java objects to invoke methods on remote objects across a network, but they have different features, advantages, and disadvantages.
- Open interfaces facilitate easy development, operation, and maintenance of various M2M applications and services, and provide an easy upgrade path for future technologies.

SCADA Middleware

- Not all IoT applications will use a cellular network.
- Most of the traditional SCADA applications have been using local wireline networks for communications.
- The remote terminal units (RTUs), programmable logic controllers (PLCs), or even process control systems (PCSs) communicate to the SCADA middleware server via gateways (similar to MAN but all wired) that aggregate data from different wired field buses.
- The SCADA system is accessed in a LAN environment (sometimes xDSL, cable, WiFi, or WiMax can be used) before it is integrated into the corporate back office system

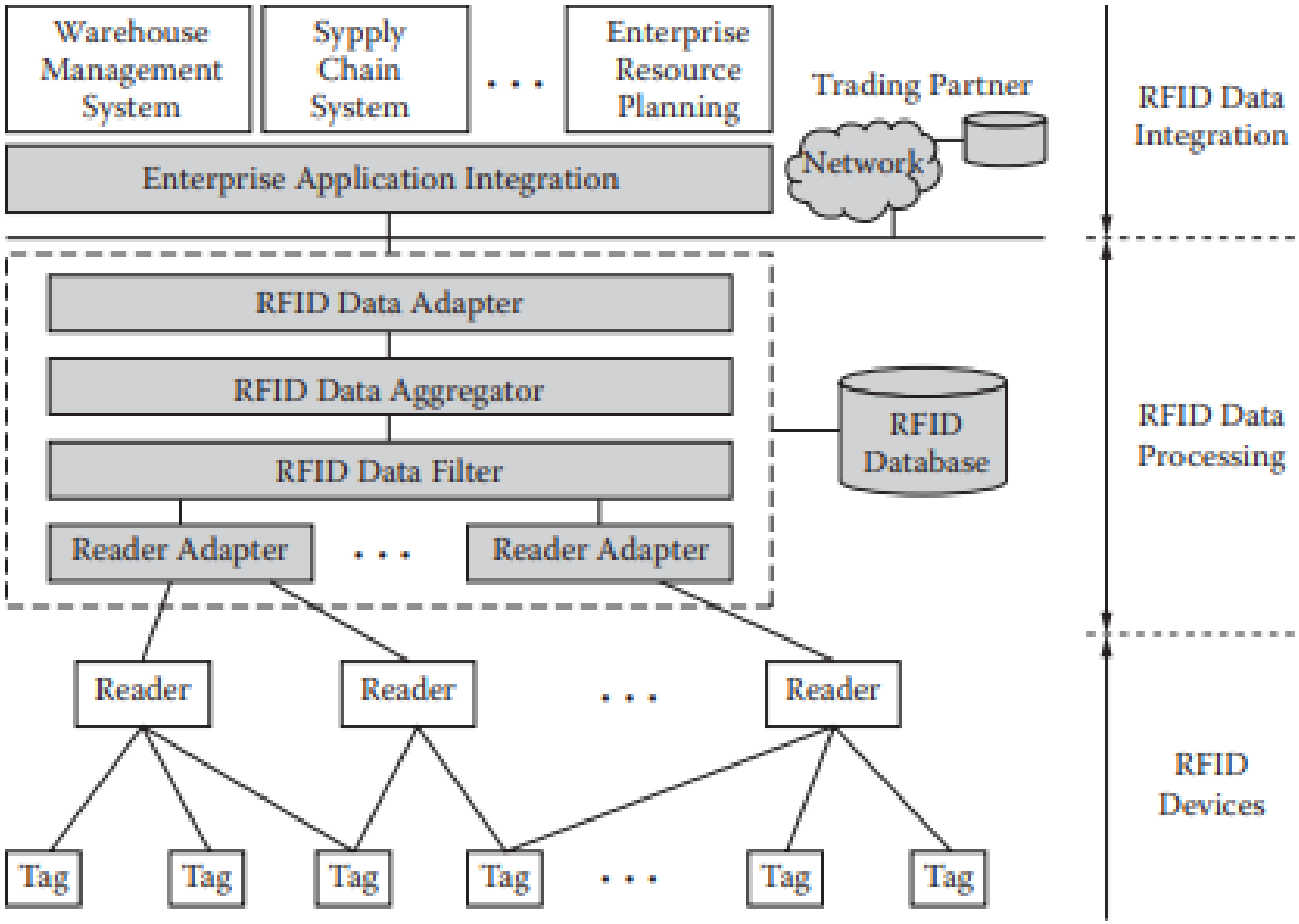
SCADA middleware architecture



RFID Middleware

- RFID middleware (including the edge middleware or edge ware) is currently the most well-defined, comprehensive and standardized middleware compared with the other three pillar segments of IoT.
- RFID middleware based system may include,
    - A format for the data called physical markup language (PML), based on XML
    - An interface to the servers containing PML records
    - A directory service called ONS (object naming service), analogous to the DNS. Given a tag's EPC (Electronic Product code), the ONS will provide pointers to the PML servers containing records related to that tag.

RFID Architecture

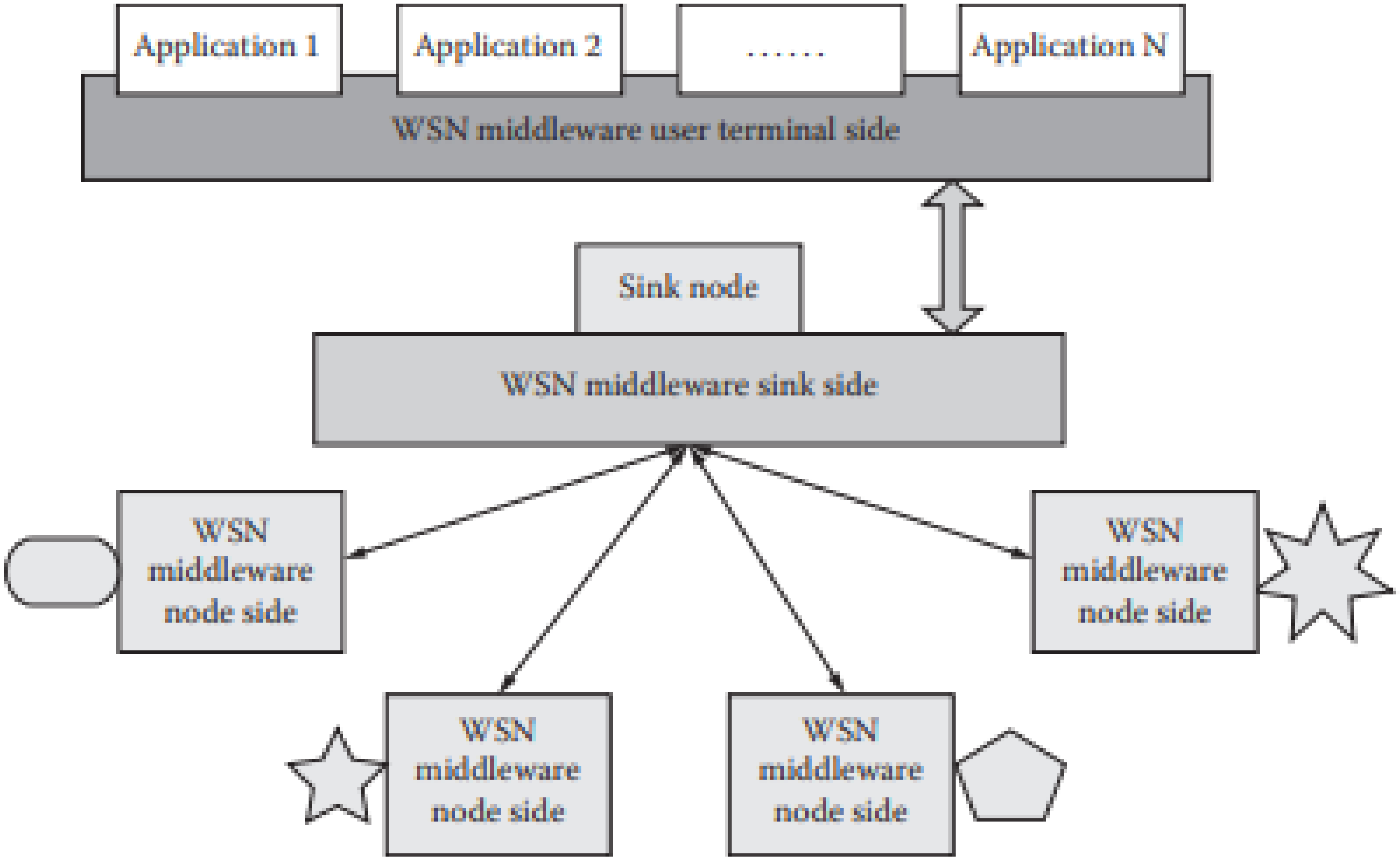


WSN Middleware

- Middleware also refer to software and tools that can help hide the complexity and heterogeneity of the underlying hardware and network platforms, ease the management of system resources, and increase the stableness of application executions.
- WSN middleware is a kind of middleware providing the desired services for sensor-based pervasive computing applications that make use of a WSN and the related embedded operating system or firmware of the sensor nodes.
- WSN middleware is implemented as embedded middleware on the node
- Embedded operating systems - Embedded Linux, Android, iOS, QNX, VxWorks, etc.

- A complete WSN middleware solution should include four major components: programming abstractions, system services, runtime support, and Quality of Service (QoS) mechanisms.
- Programming abstractions define the interface of the middleware to the application programmer.
- System services provide implementations to achieve the abstractions.
- Runtime support serves as an extension of the embedded operating system to support the middleware services.
- QoS mechanisms define the QoS constraints of the system

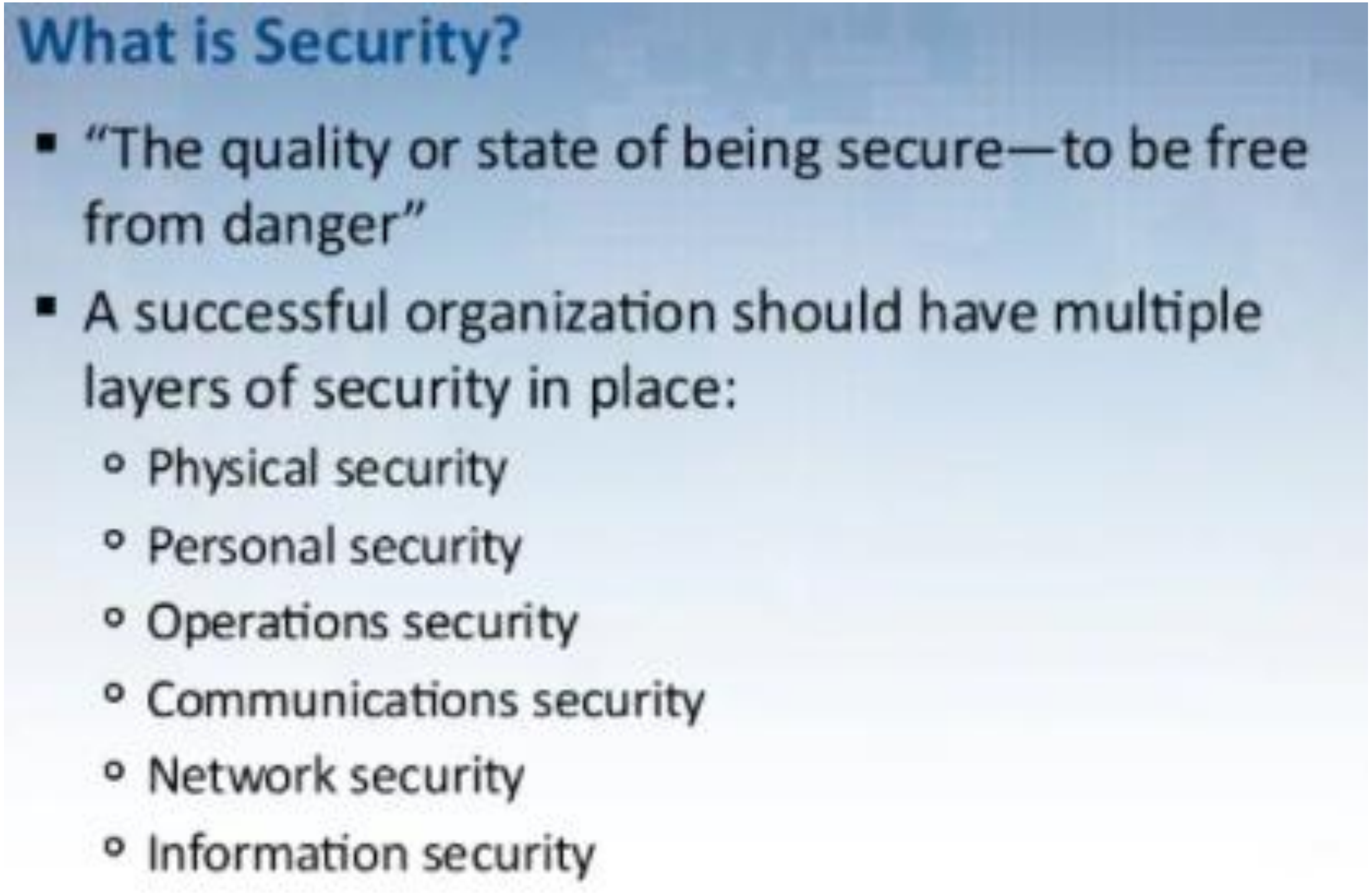
WSN Middleware Architecture



- Middleware for WSN should also facilitate development, maintenance, deployment, and execution of sensing-based applications

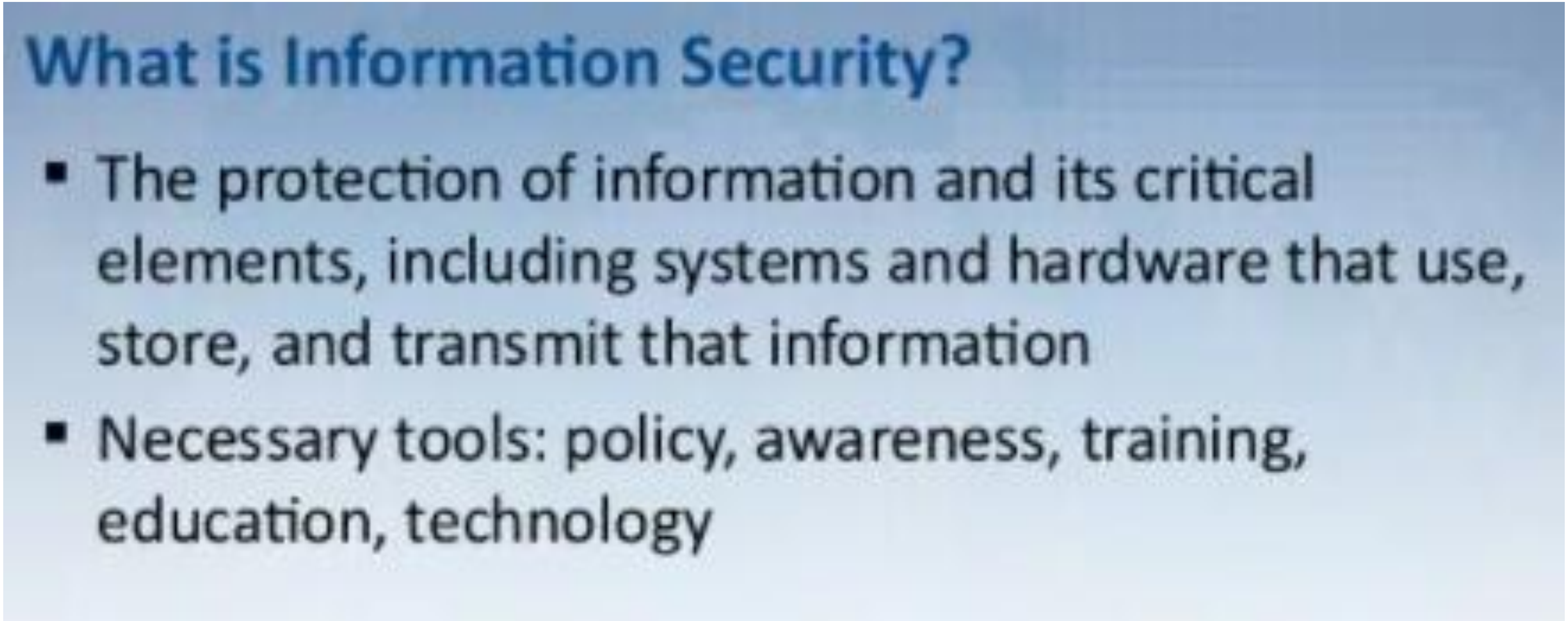
- Many challenges arise in designing middleware for WSN due to :
  - ■ Limited power and resources, e.g., battery issues
  - ■ Mobile and dynamic network topology
  - ■ Heterogeneity- various kinds of hardware and network protocols

IoT Information Security



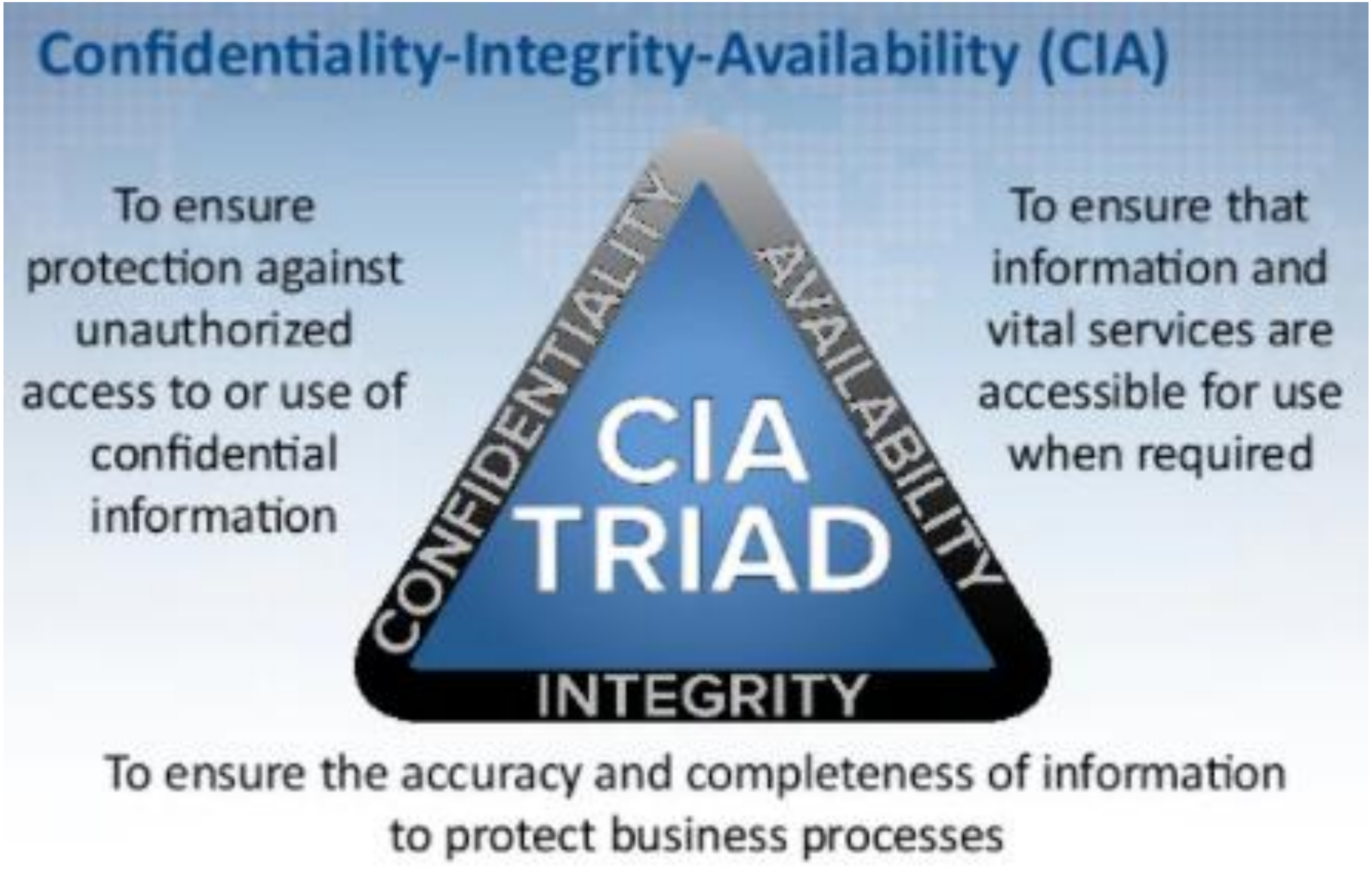
What is Security?

- "The quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security



What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology

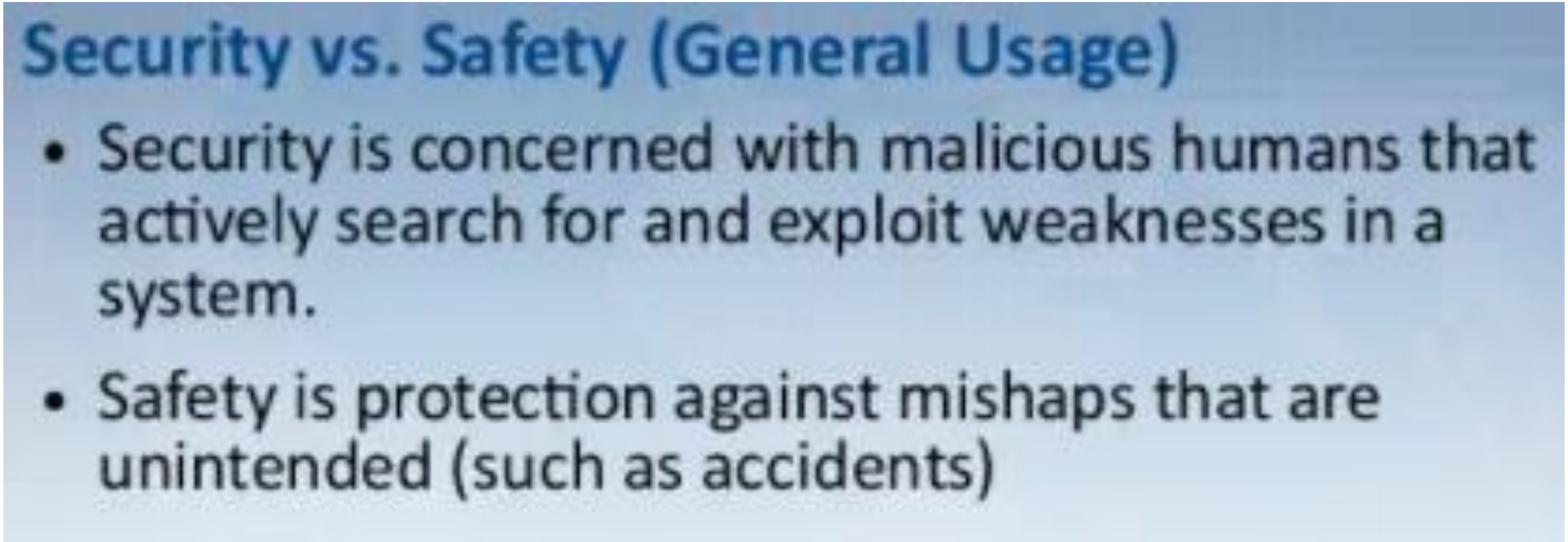


Confidentiality-Integrity-Availability (CIA)

To ensure protection against unauthorized access to or use of confidential information

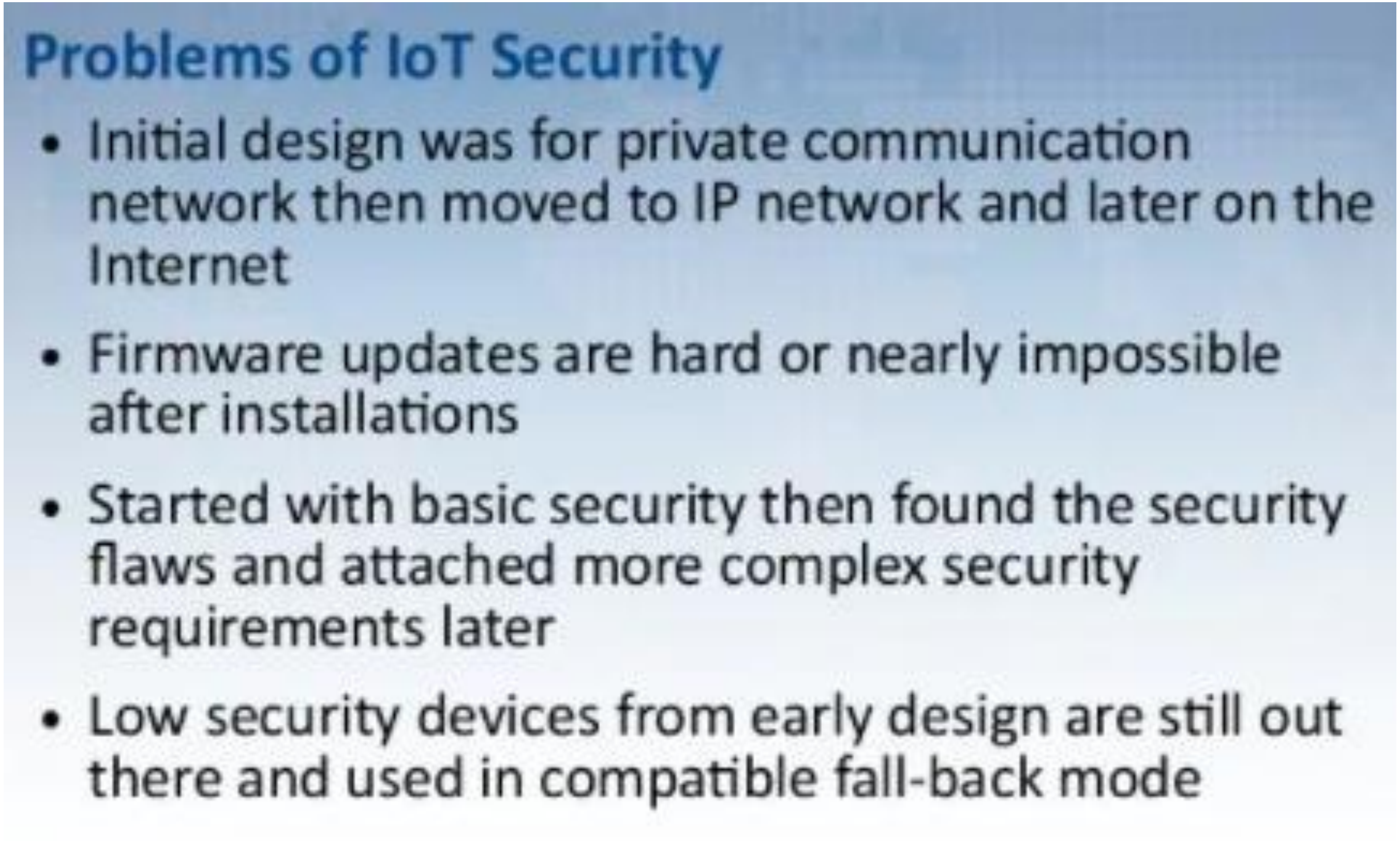
To ensure that information and vital services are accessible for use when required

To ensure the accuracy and completeness of information to protect business processes



Security vs. Safety (General Usage)

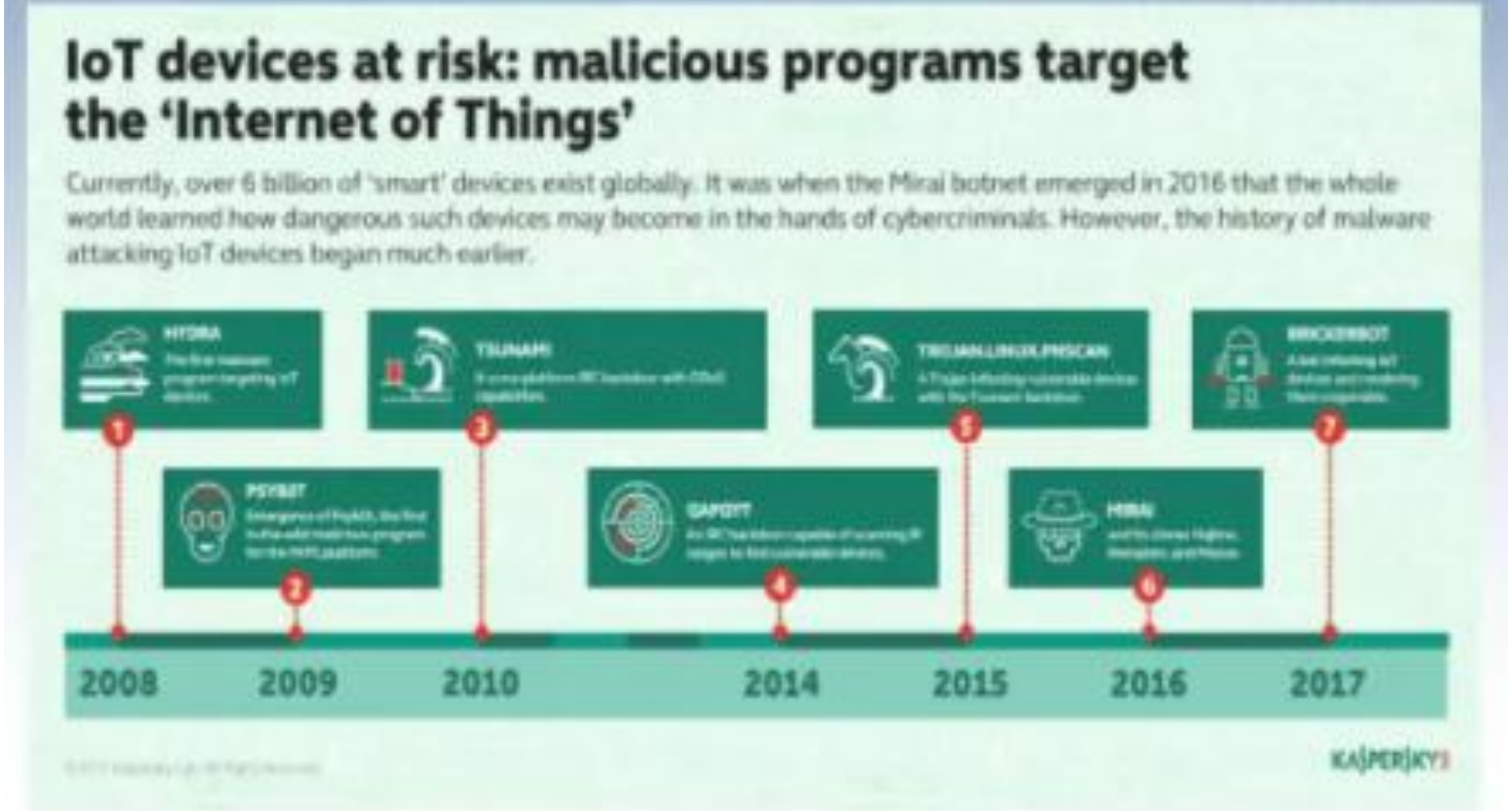
- Security is concerned with malicious humans that actively search for and exploit weaknesses in a system.
- Safety is protection against mishaps that are unintended (such as accidents)



Problems of IoT Security

- Initial design was for private communication network then moved to IP network and later on the Internet
- Firmware updates are hard or nearly impossible after installations
- Started with basic security then found the security flaws and attached more complex security requirements later
- Low security devices from early design are still out there and used in compatible fall-back mode

Rises of Threats Target IoT Devices



IoT devices at risk: malicious programs target the ‘Internet of Things’

Currently, over 6 billion of ‘smart’ devices exist globally. It was when the Mirai botnet emerged in 2016 that the whole world learned how dangerous such devices may become in the hands of cybercriminals. However, the history of malware attacking IoT devices began much earlier.

1 HYDRA
The first malware program targeting IoT devices.

2 PSYBOT
Emergence of Psybot, the first in-the-wild malicious program for the MIPS platform.

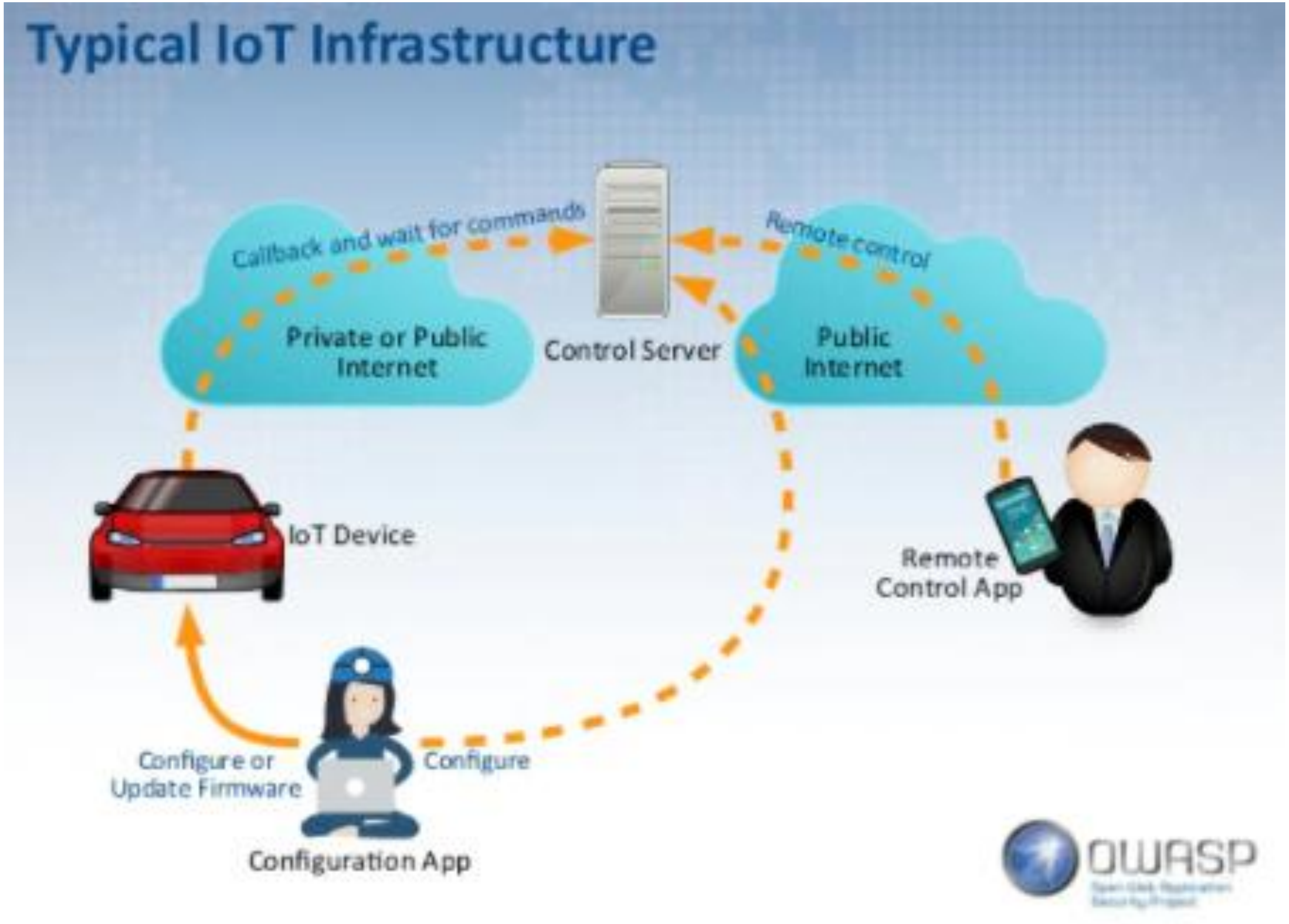
3 TSUNAMI
A cross-platform IRC backdoor with DDoS capabilities.

4 GAFGYT
An IRC backdoor capable of scanning IP ranges to find vulnerable devices.

5 TROJAN.LINUX.PNSCAN
A Trojan infecting vulnerable devices with the Tsunami backdoor.

6 MIRAI
and its clones Hajime, Amnesia, and Persirai

7 BRICKERBOT
A bot infecting IoT devices and rendering them inoperable.



Typical IoT Infrastructure

Callback and wait for commands

Remote control

Private or Public Internet

Control Server

Public Internet

IoT Device

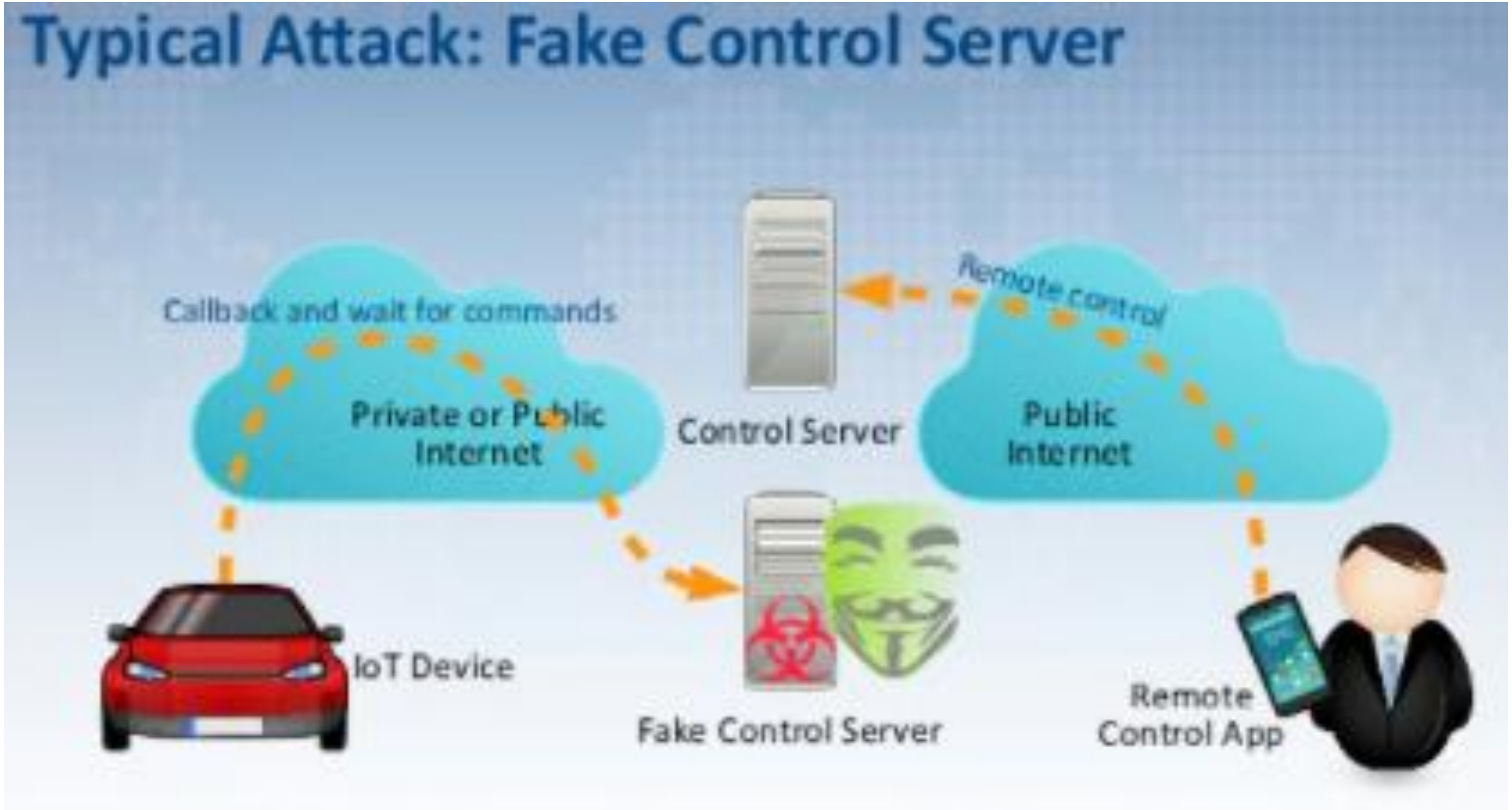
Remote Control App

Configure or Update Firmware

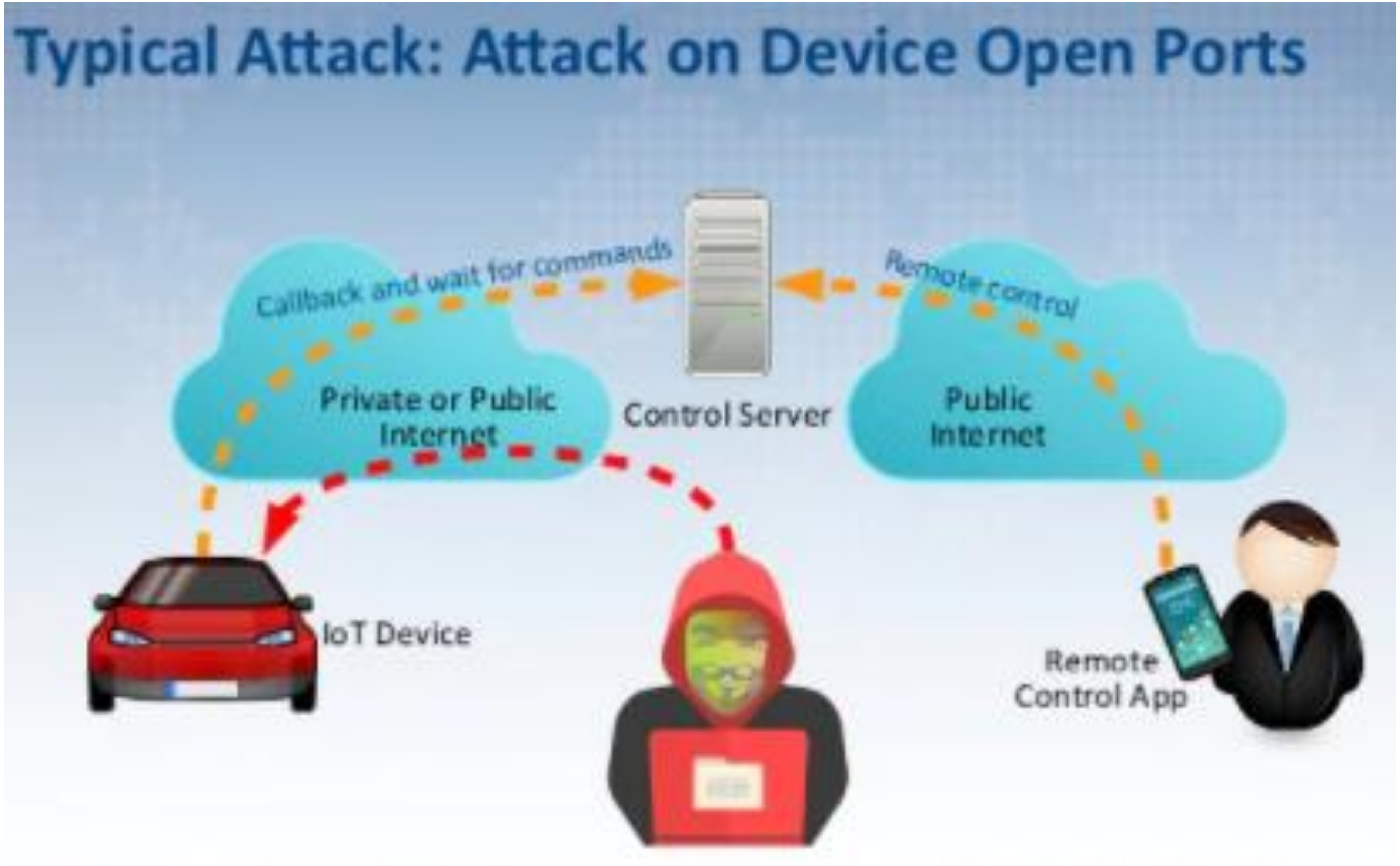
Configure

Configuration App

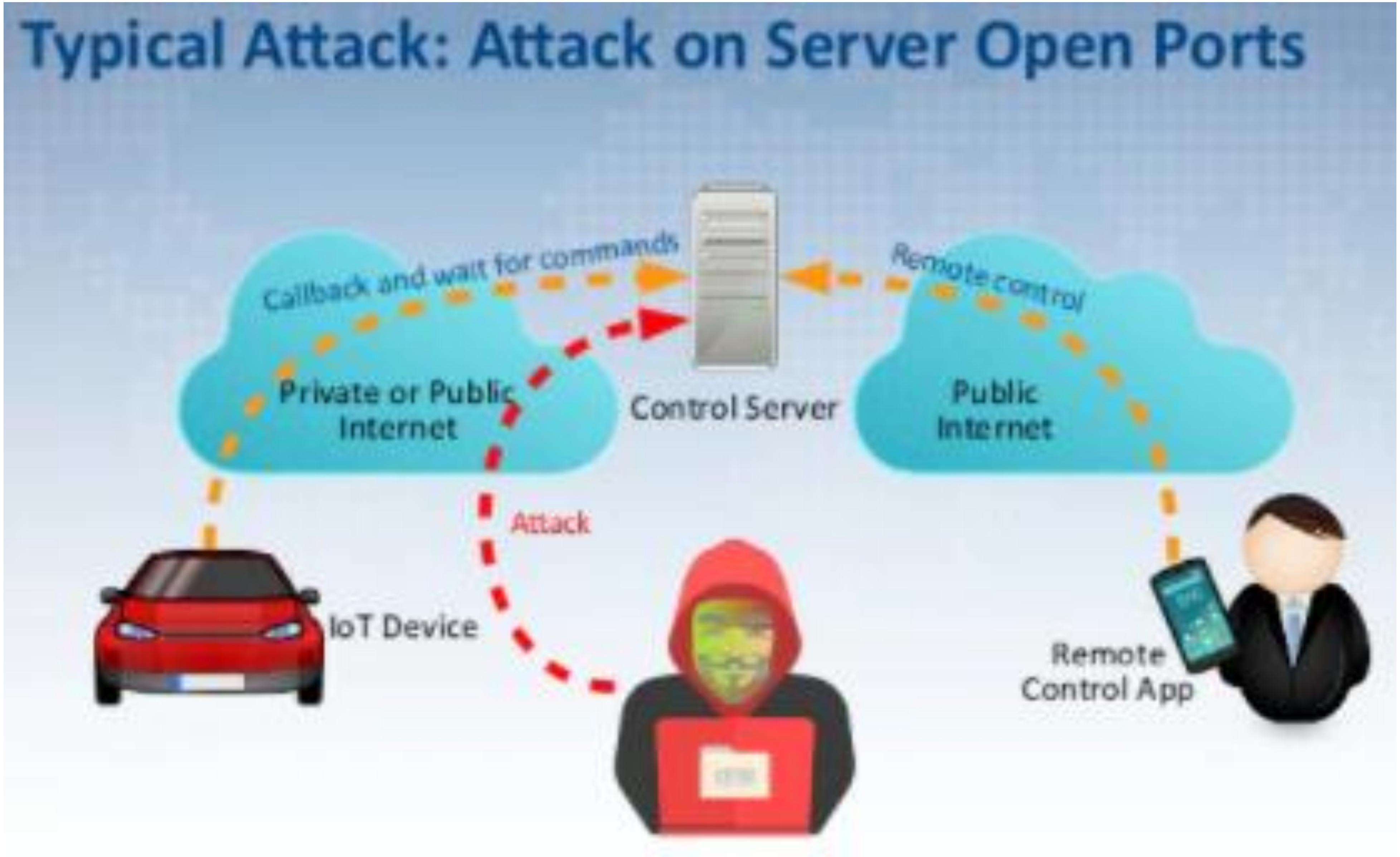
OWASP



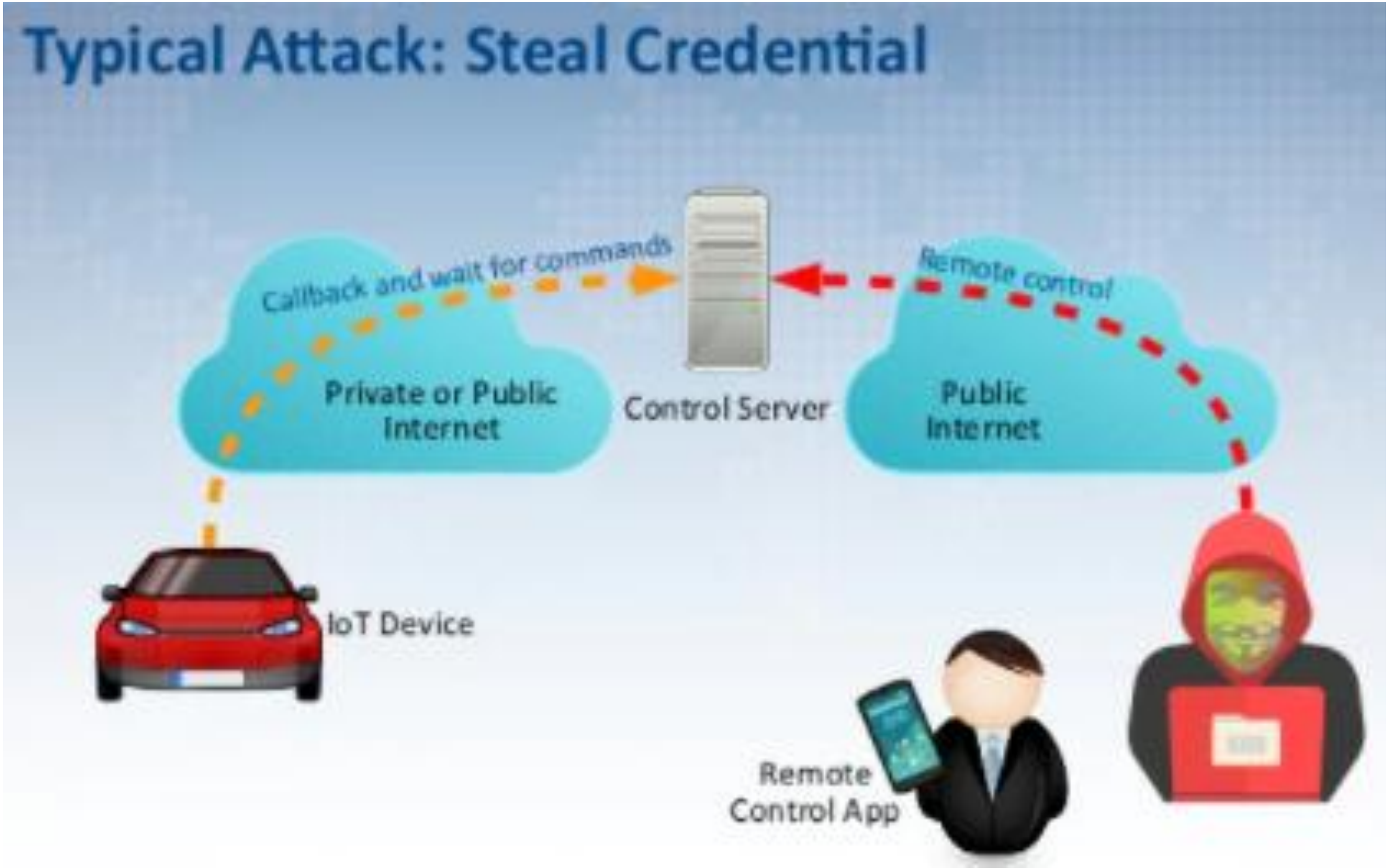
Typical Attack: Fake Control Server



Typical Attack: Attack on Device Open Ports



Typical Attack: Attack on Server Open Ports



Typical Attack: Steal Credential

Callback and wait for commands

Remote control

Private or Public Internet

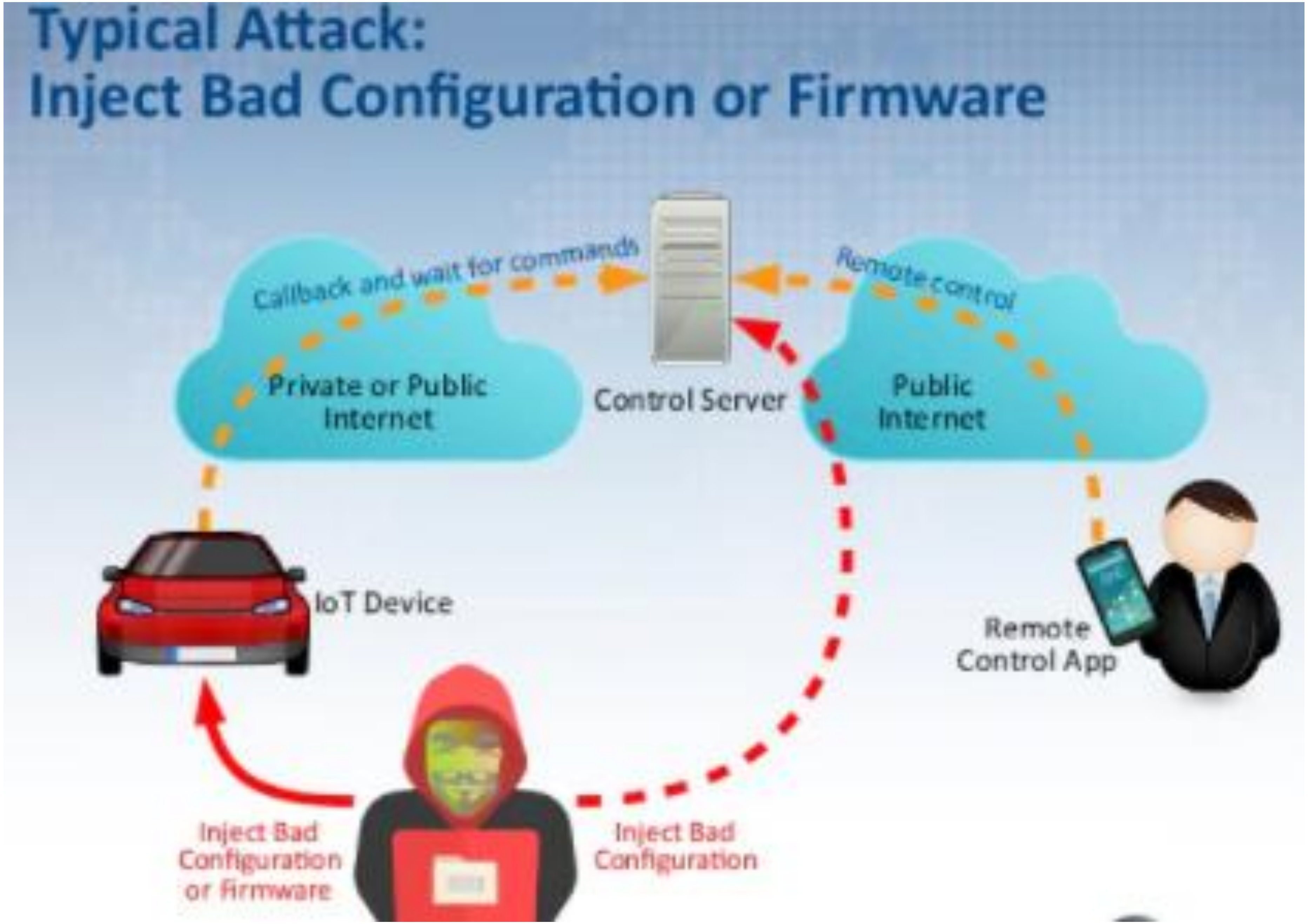
Control Server

Public Internet

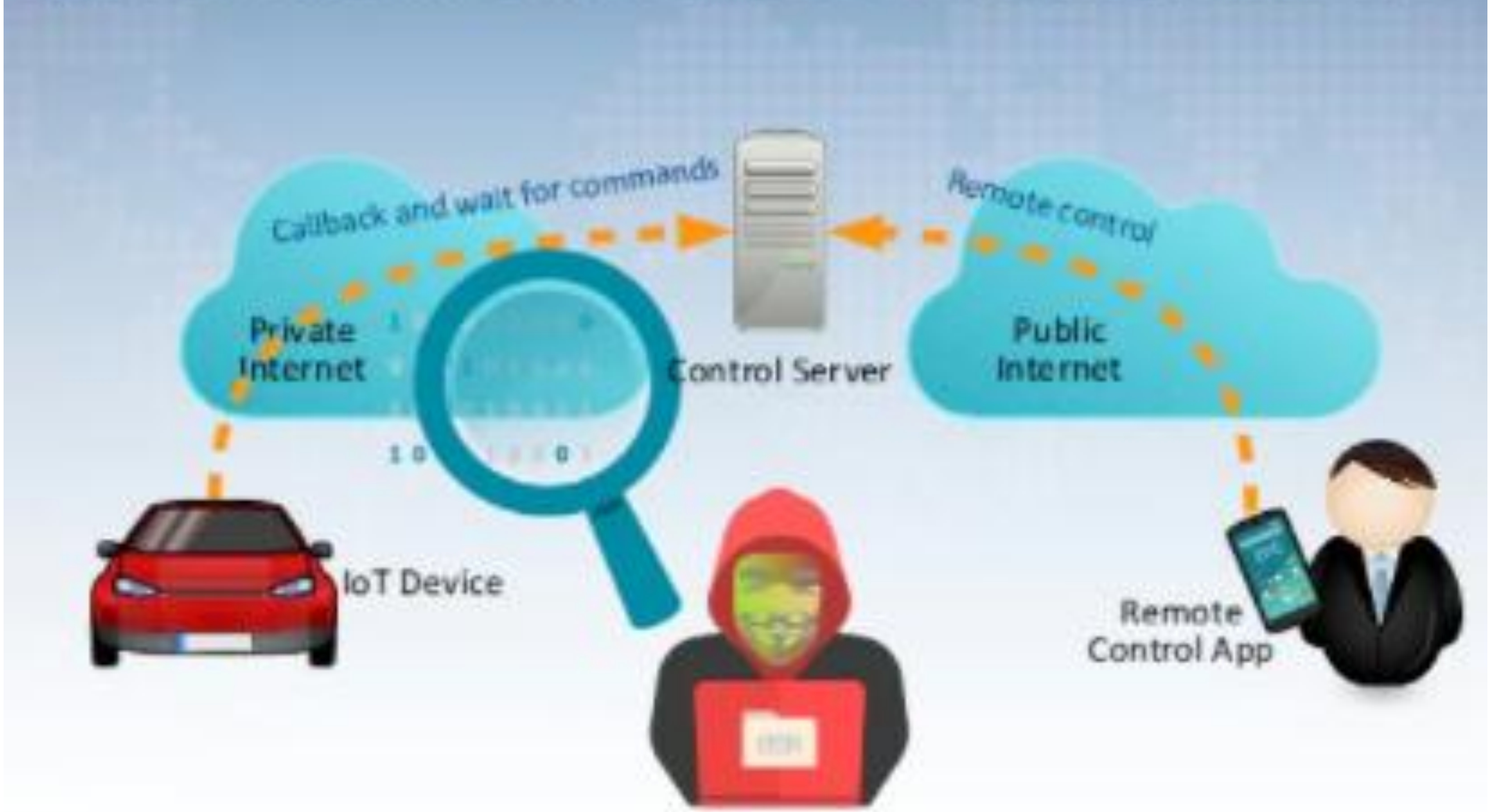
IoT Device

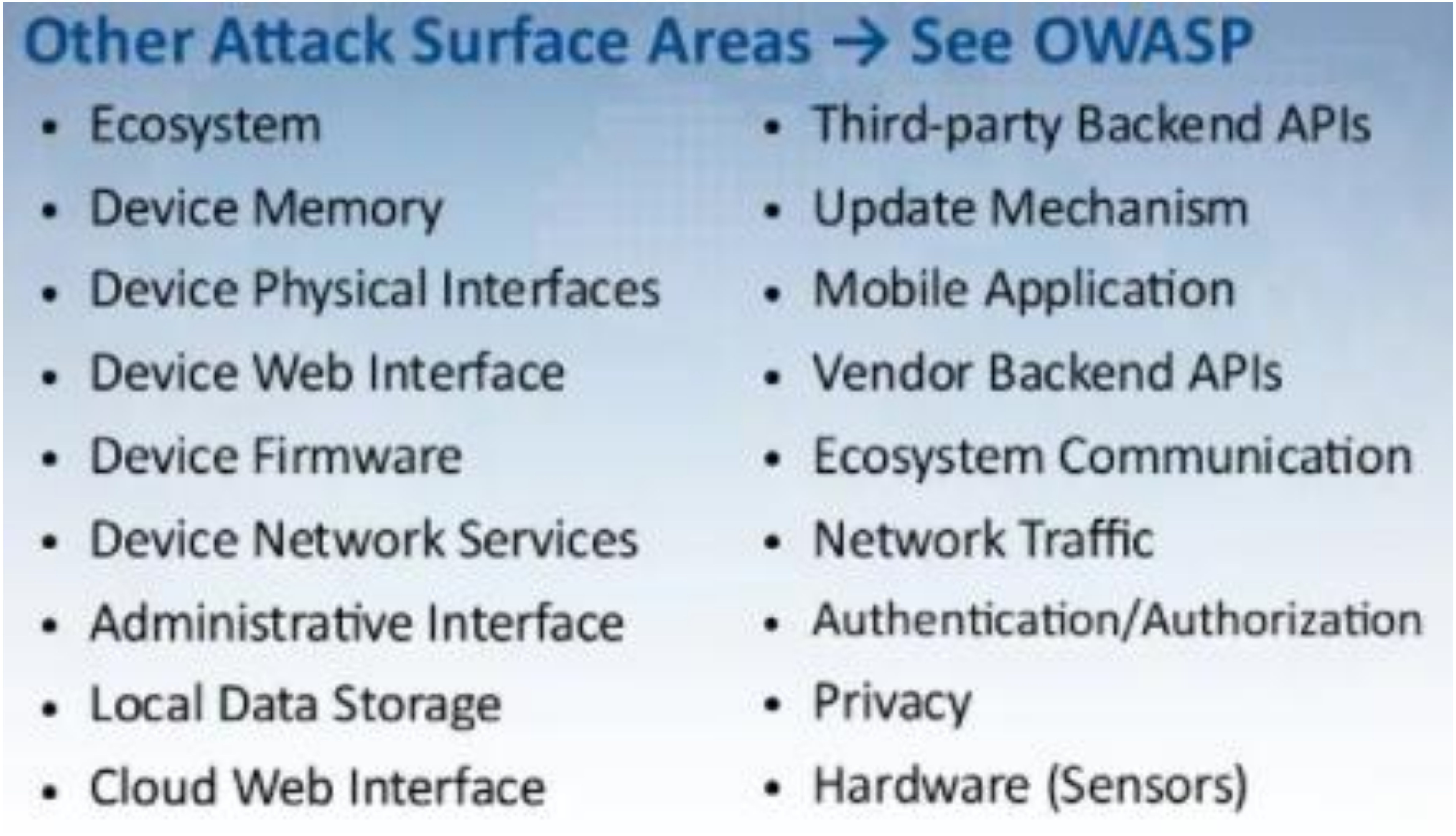
Remote Control App

Typical Attack:
Inject Bad Configuration or Firmware



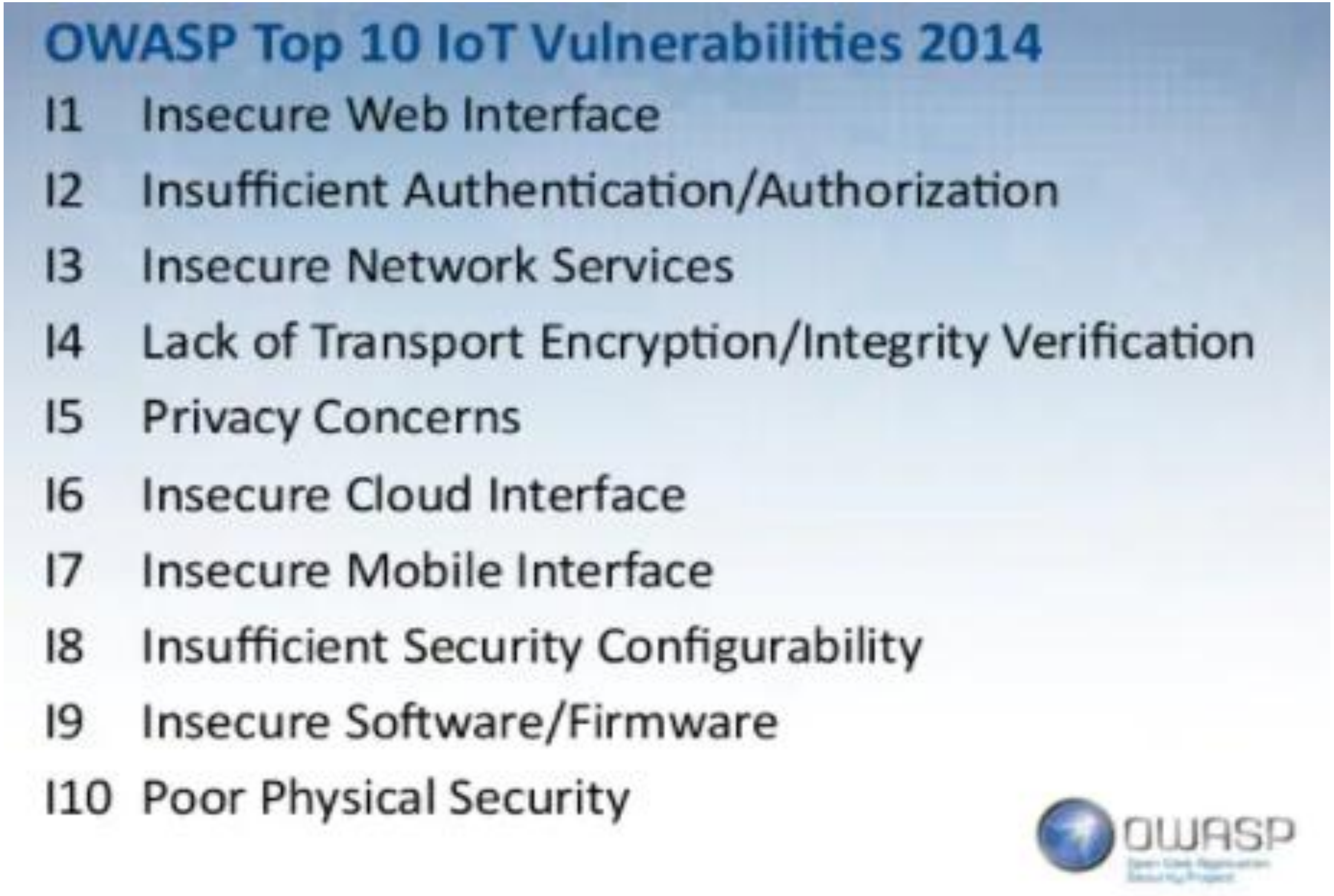
Typical Attack: Sniff Data on Private Network





Other Attack Surface Areas → See OWASP

- Ecosystem
- Device Memory
- Device Physical Interfaces
- Device Web Interface
- Device Firmware
- Device Network Services
- Administrative Interface
- Local Data Storage
- Cloud Web Interface
- Third-party Backend APIs
- Update Mechanism
- Mobile Application
- Vendor Backend APIs
- Ecosystem Communication
- Network Traffic
- Authentication/Authorization
- Privacy
- Hardware (Sensors)



OWASP Top 10 IoT Vulnerabilities 2014

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption/Integrity Verification

I5 Privacy Concerns

I6 Insecure Cloud Interface

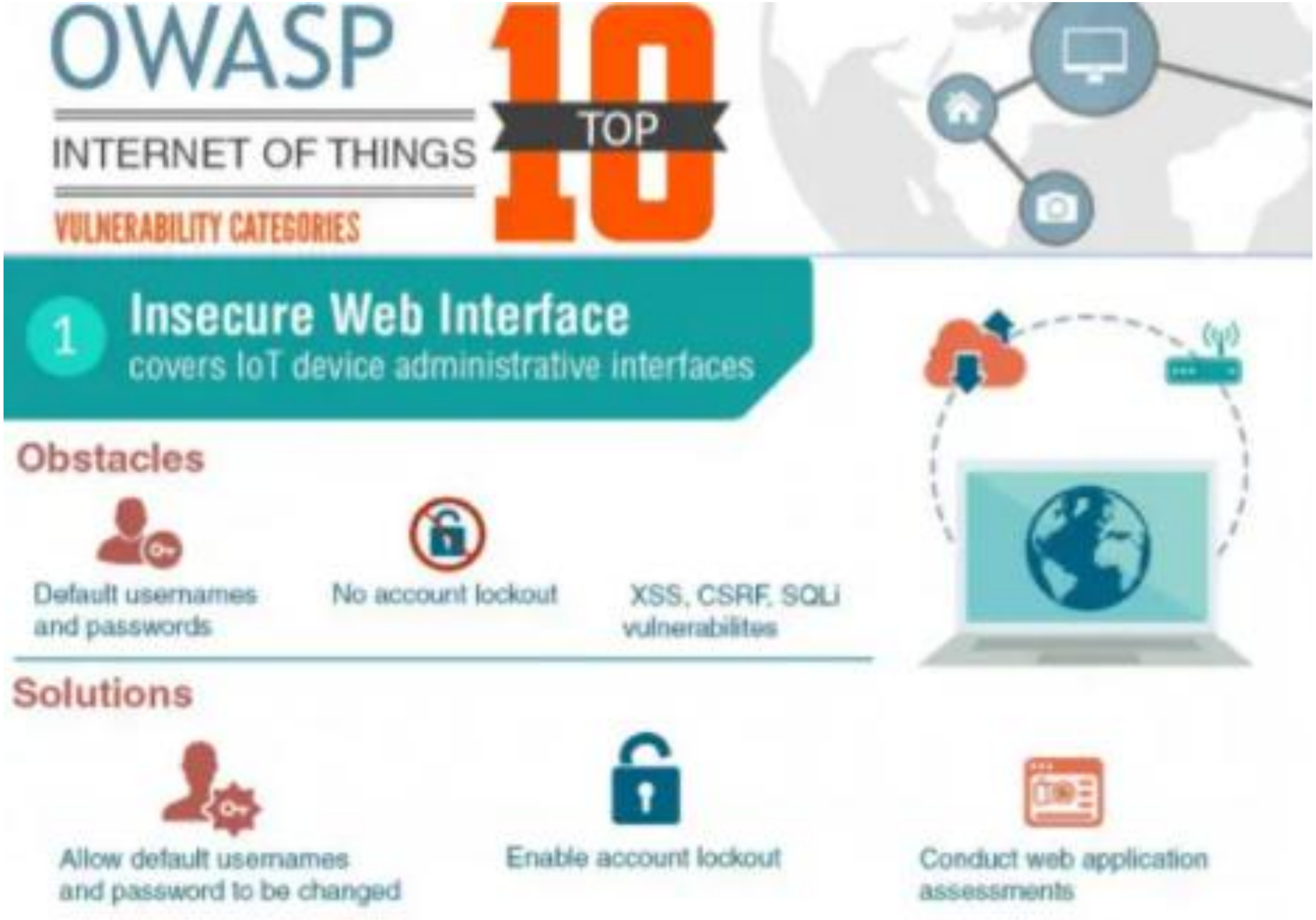
I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

I9 Insecure Software/Firmware

I10 Poor Physical Security

OWASP



OWASP

INTERNET OF THINGS

TOP 10

VULNERABILITY CATEGORIES

1 Insecure Web Interface

covers IoT device administrative interfaces

Obstacles

Default usernames and passwords

No account lockout

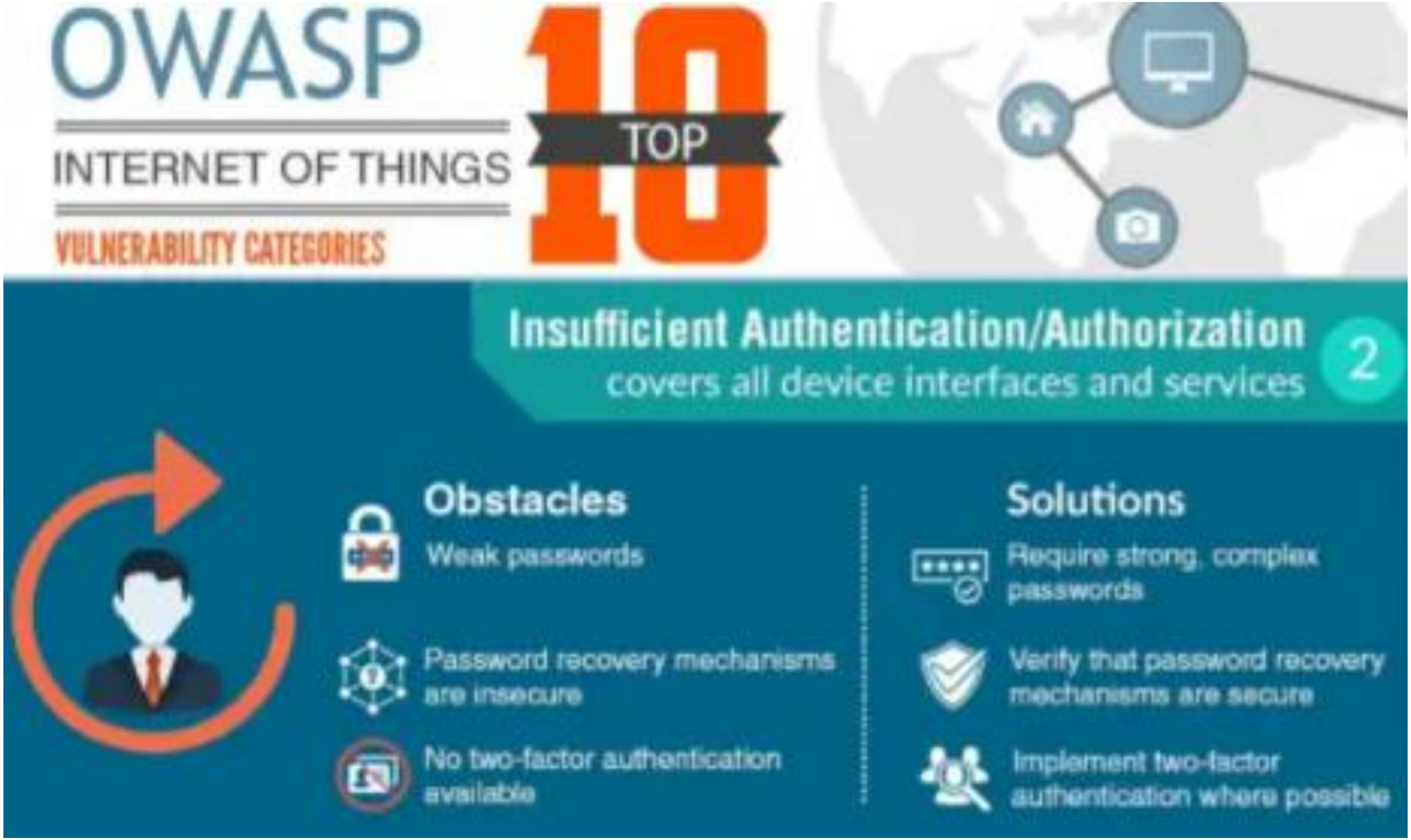
XSS, CSRF, SQLi vulnerabilites

Solutions

Allow default usernames and password to be changed

Enable account lockout

Conduct web application assessments



OWASP INTERNET OF THINGS TOP 10

VULNERABILITY CATEGORIES

Insufficient Authentication/Authorization 2

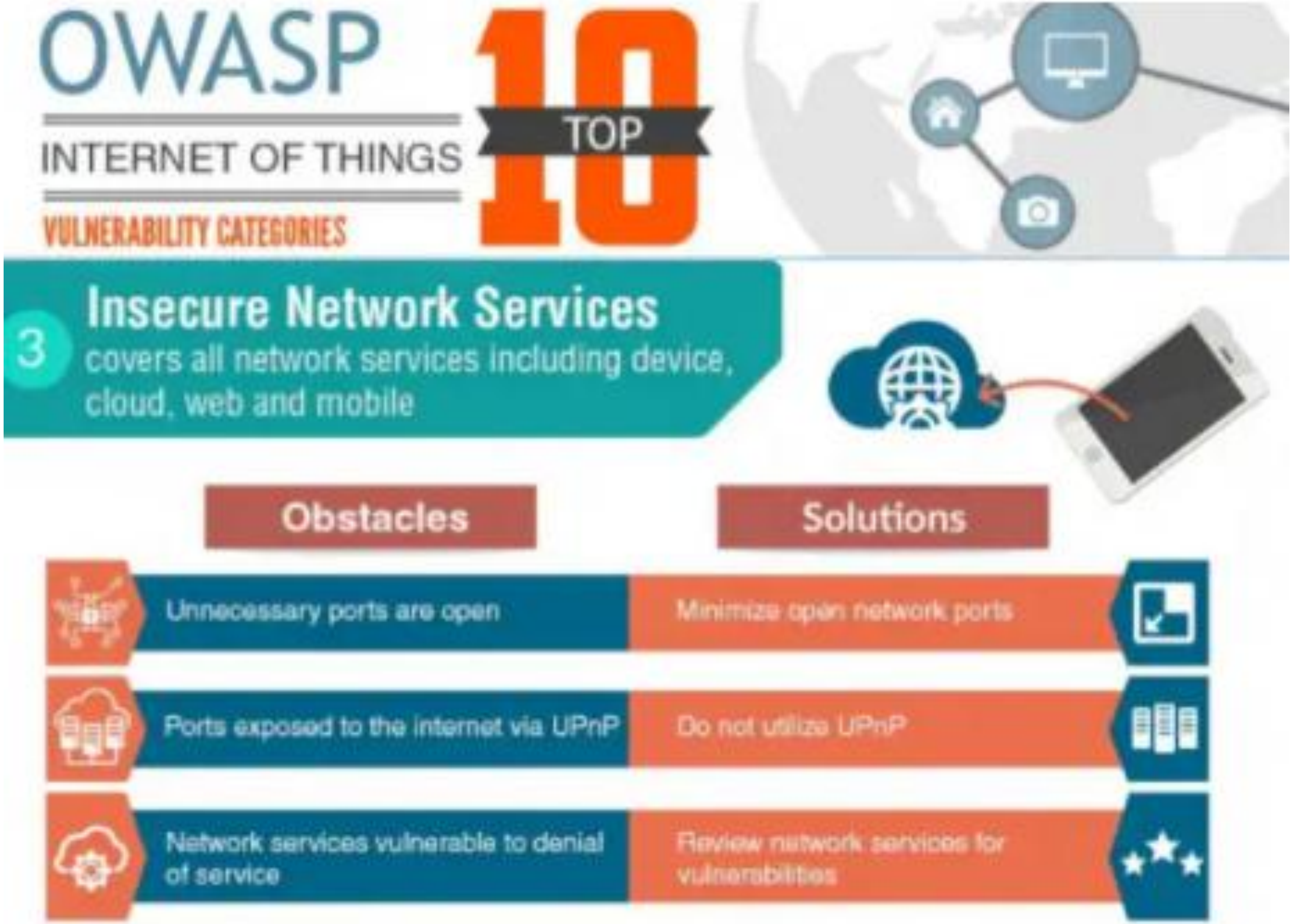
covers all device interfaces and services

Obstacles

- Weak passwords
- Password recovery mechanisms are insecure
- No two-factor authentication available

Solutions

- Require strong, complex passwords
- Verify that password recovery mechanisms are secure
- Implement two-factor authentication where possible



OWASP

INTERNET OF THINGS

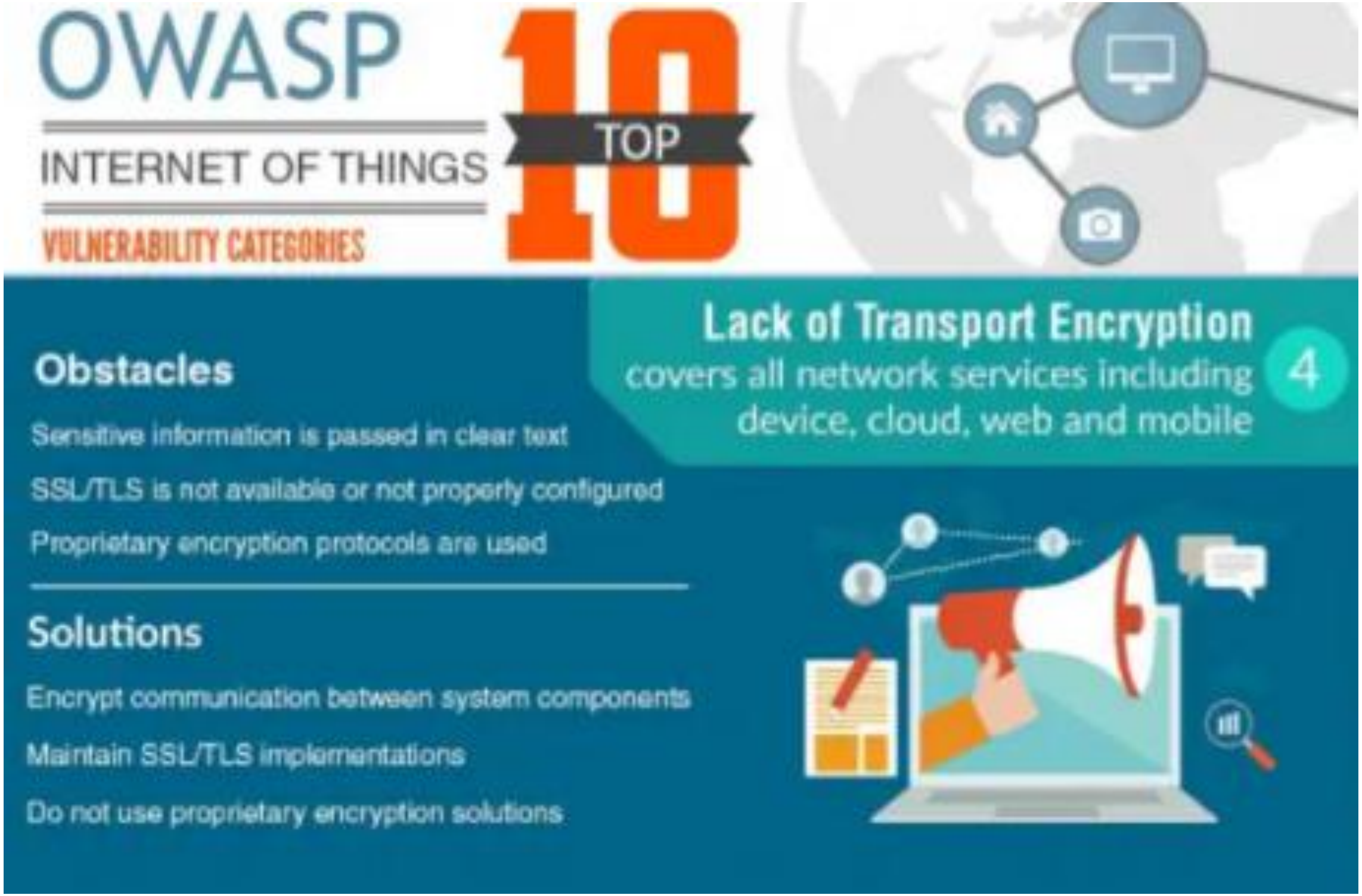
TOP 10

VULNERABILITY CATEGORIES

3 Insecure Network Services

covers all network services including device, cloud, web and mobile

Obstacles	Solutions
Unnecessary ports are open	Minimize open network ports
Ports exposed to the internet via UPnP	Do not utilize UPnP
Network services vulnerable to denial of service	Review network services for vulnerabilities



OWASP INTERNET OF THINGS TOP 10

VULNERABILITY CATEGORIES

Lack of Transport Encryption

4

covers all network services including device, cloud, web and mobile

Obstacles

Sensitive information is passed in clear text

SSL/TLS is not available or not properly configured

Proprietary encryption protocols are used

Solutions

Encrypt communication between system components

Maintain SSL/TLS implementations

Do not use proprietary encryption solutions

OWASP

INTERNET OF THINGS

TOP 10

VULNERABILITY CATEGORIES

5 **Privacy Concerns**

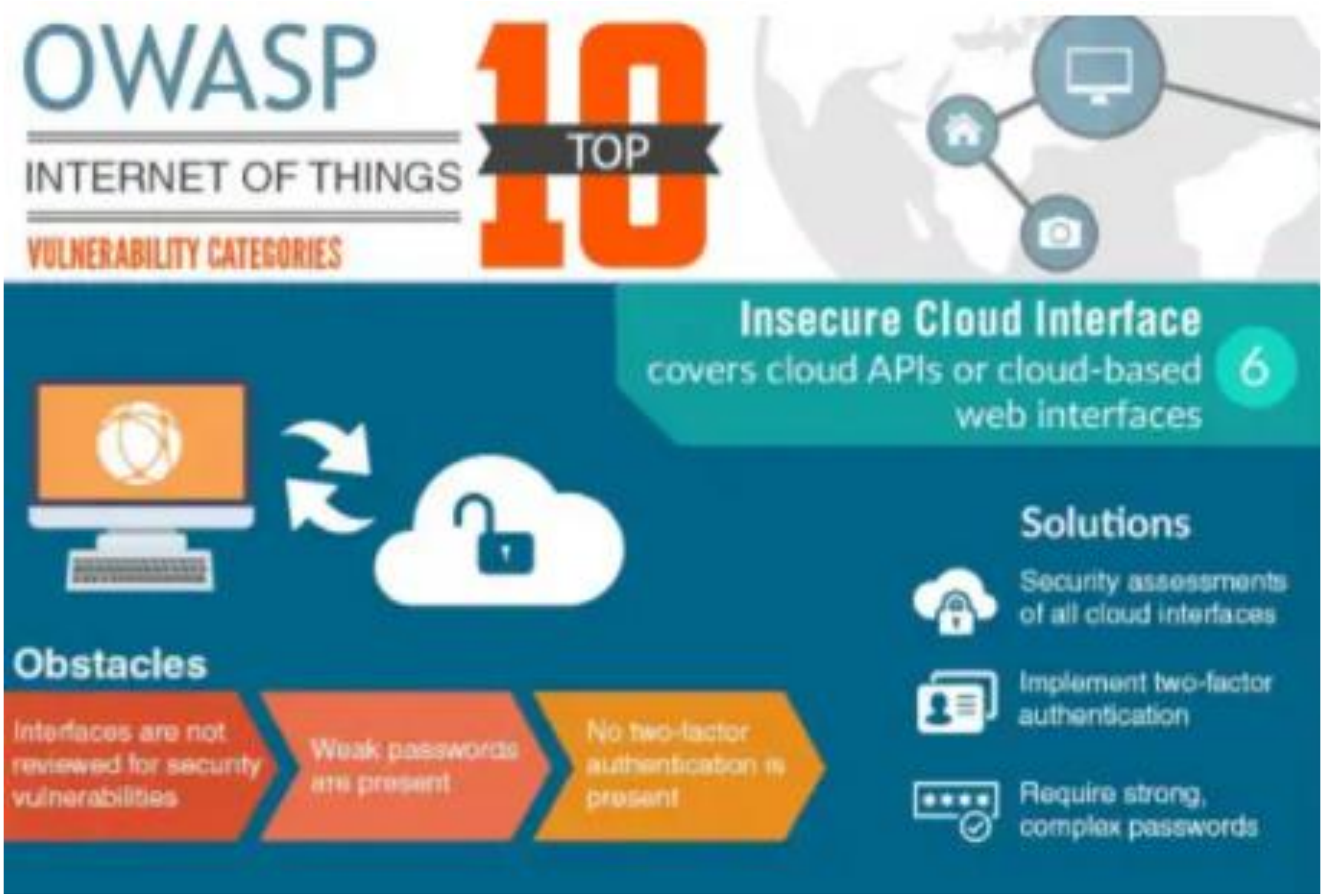
covers all components of IoT solution

Obstacles

- Too much personal information is collected
- Collected information is not properly protected
- End user is not given a choice to allow collection of certain types of data

Solutions

- Minimize data collection
- Anonymize collected data
- Give end users the ability to decide what data is collected



OWASP

INTERNET OF THINGS

VULNERABILITY CATEGORIES

10 TOP

Insecure Cloud Interface

covers cloud APIs or cloud-based web interfaces

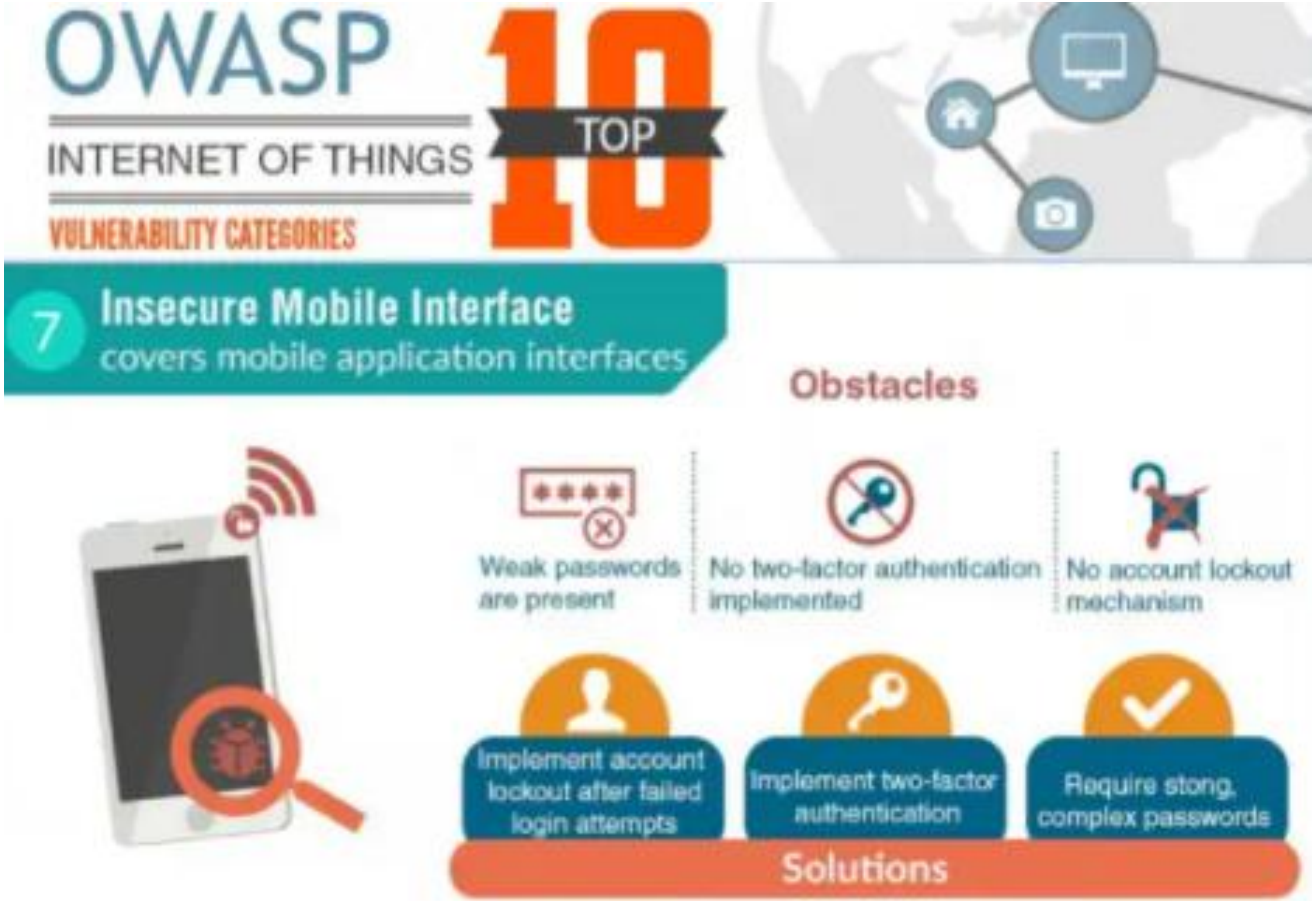
6

Obstacles

- Interfaces are not reviewed for security vulnerabilities
- Weak passwords are present
- No two-factor authentication is present

Solutions

- Security assessments of all cloud interfaces
- Implement two-factor authentication
- Require strong, complex passwords



OWASP

TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

7 **Insecure Mobile Interface**

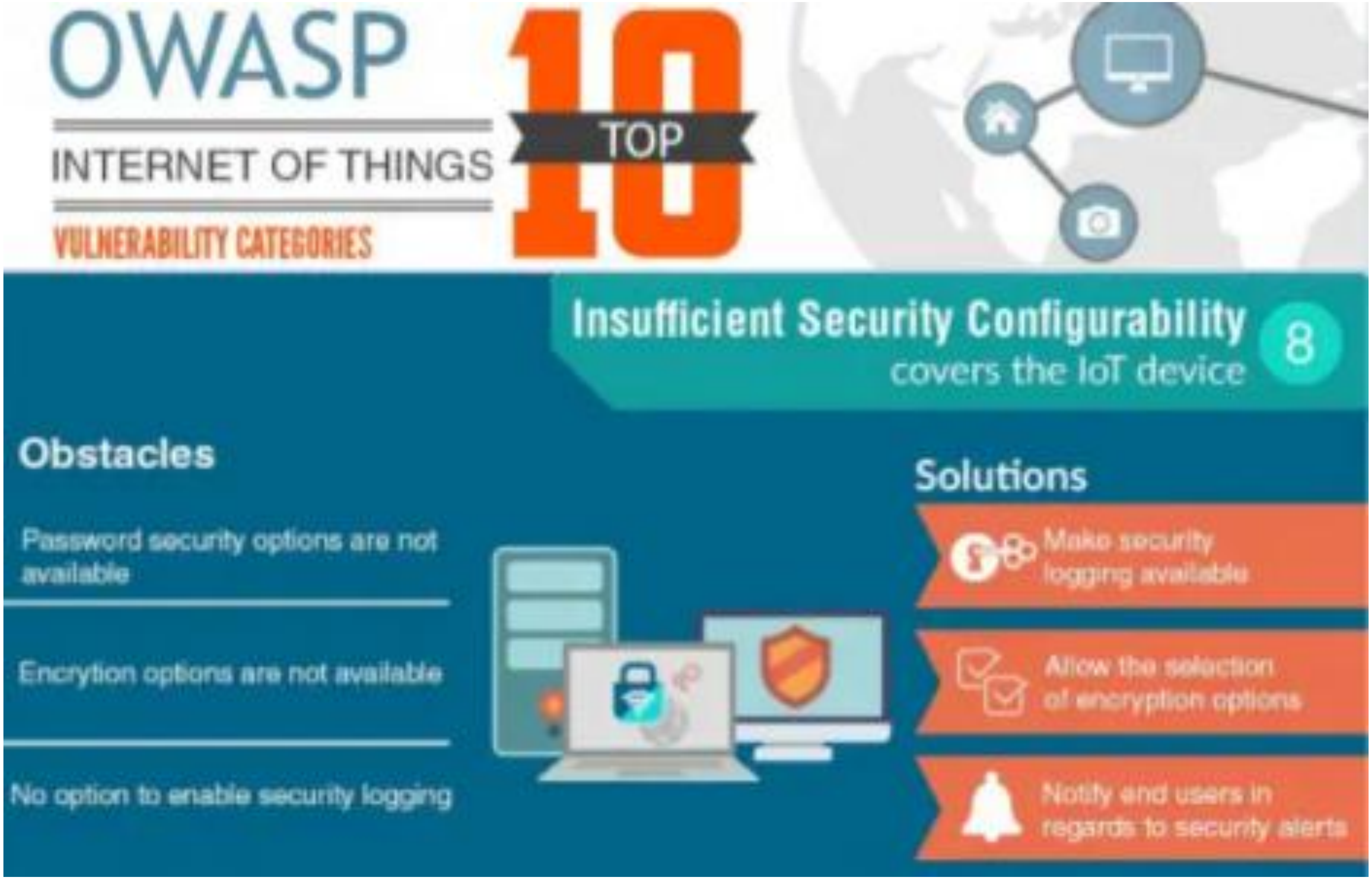
covers mobile application interfaces

Obstacles

- Weak passwords are present
- No two-factor authentication implemented
- No account lockout mechanism

- Implement account lockout after failed login attempts
- Implement two-factor authentication
- Require stong, complex passwords

Solutions



OWASP

INTERNET OF THINGS

TOP 10

VULNERABILITY CATEGORIES

Insufficient Security Configurability 8

covers the IoT device

Obstacles

Password security options are not available

Encrytion options are not available

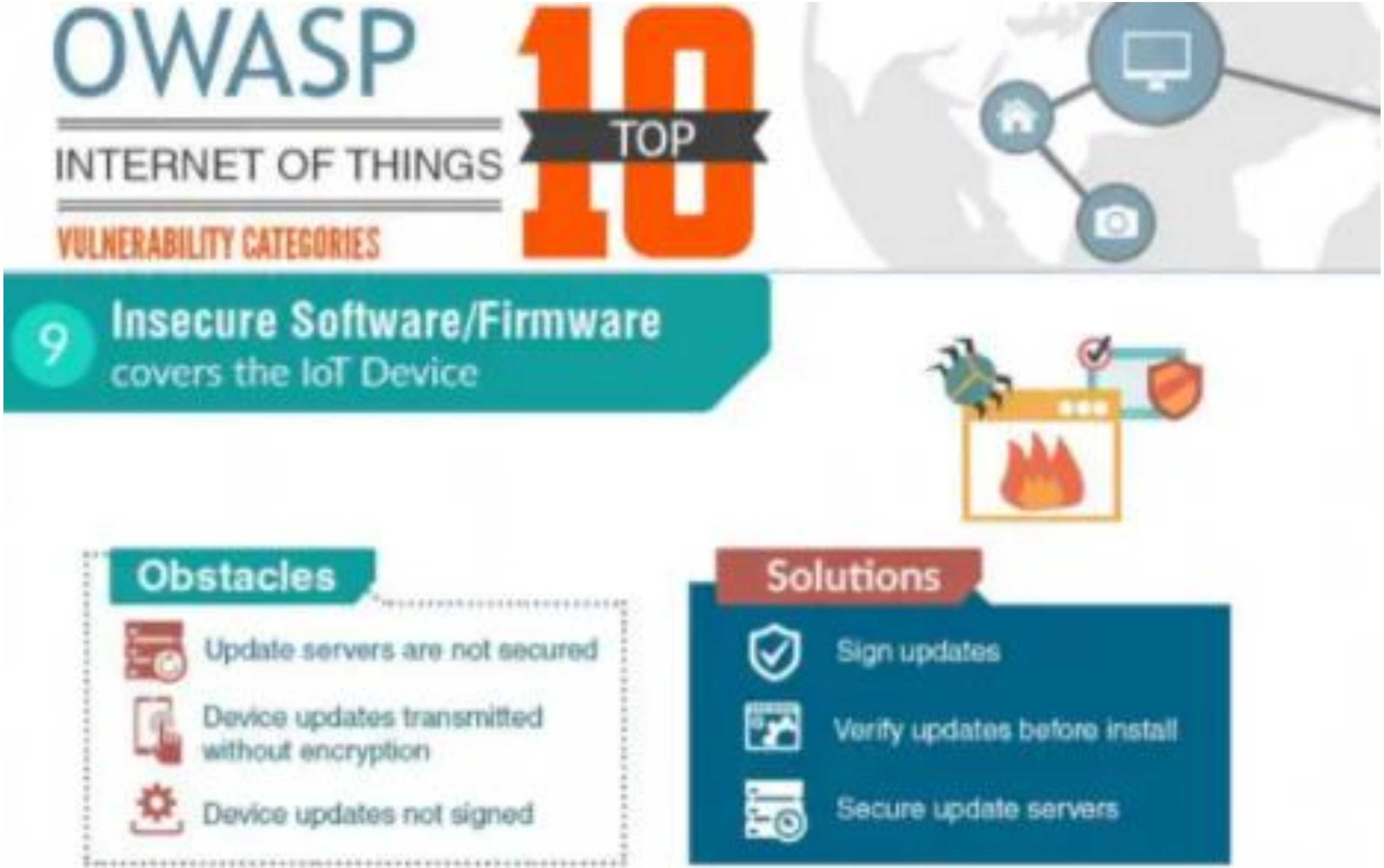
No option to enable security logging

Solutions

Make security logging available

Allow the selection of encryption options

Notify end users in regards to security alerts



OWASP INTERNET OF THINGS TOP 10

VULNERABILITY CATEGORIES

9 Insecure Software/Firmware

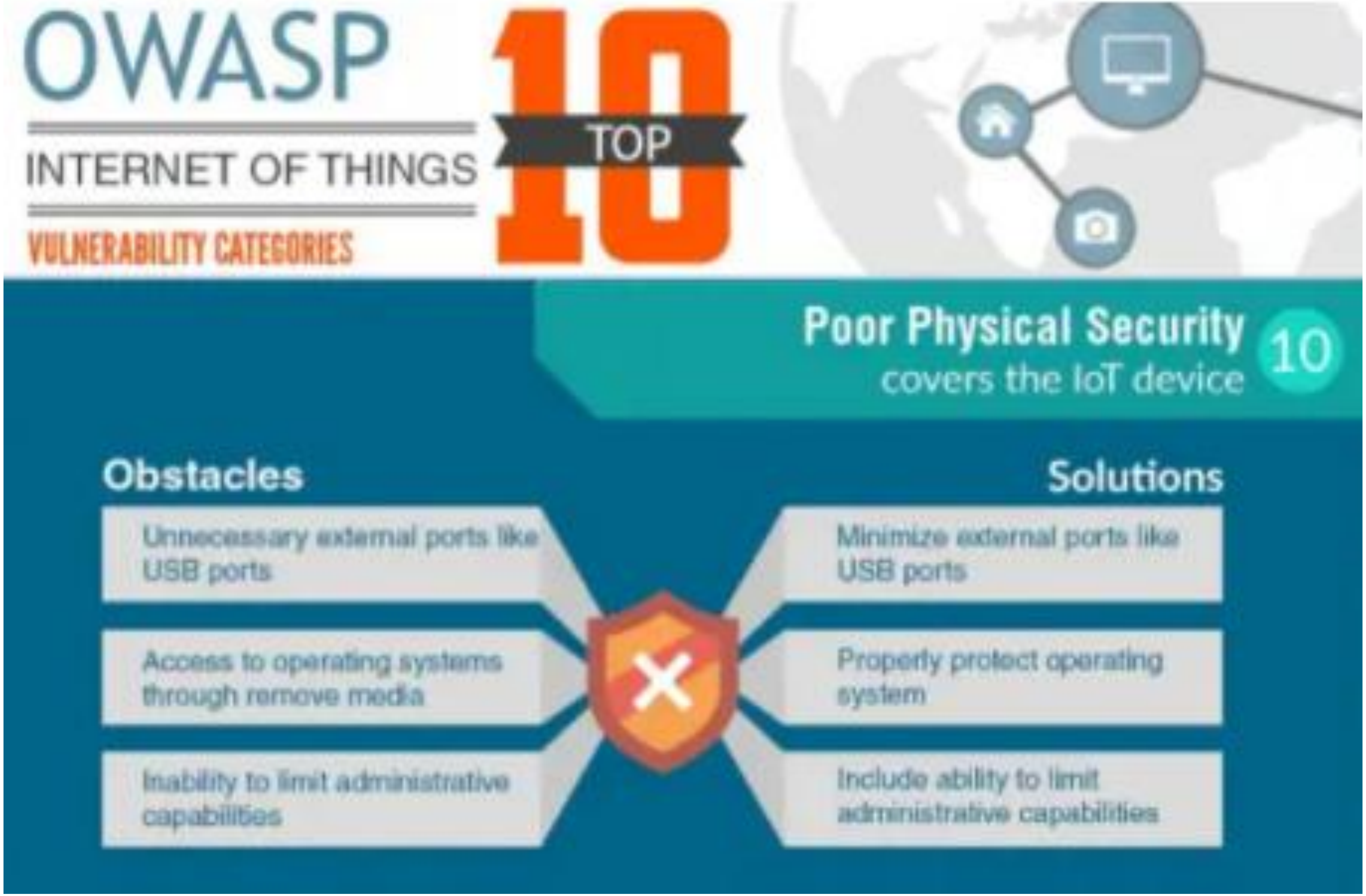
covers the IoT Device

Obstacles

- Update servers are not secured
- Device updates transmitted without encryption
- Device updates not signed

Solutions

- Sign updates
- Verify updates before install
- Secure update servers



OWASP

INTERNET OF THINGS

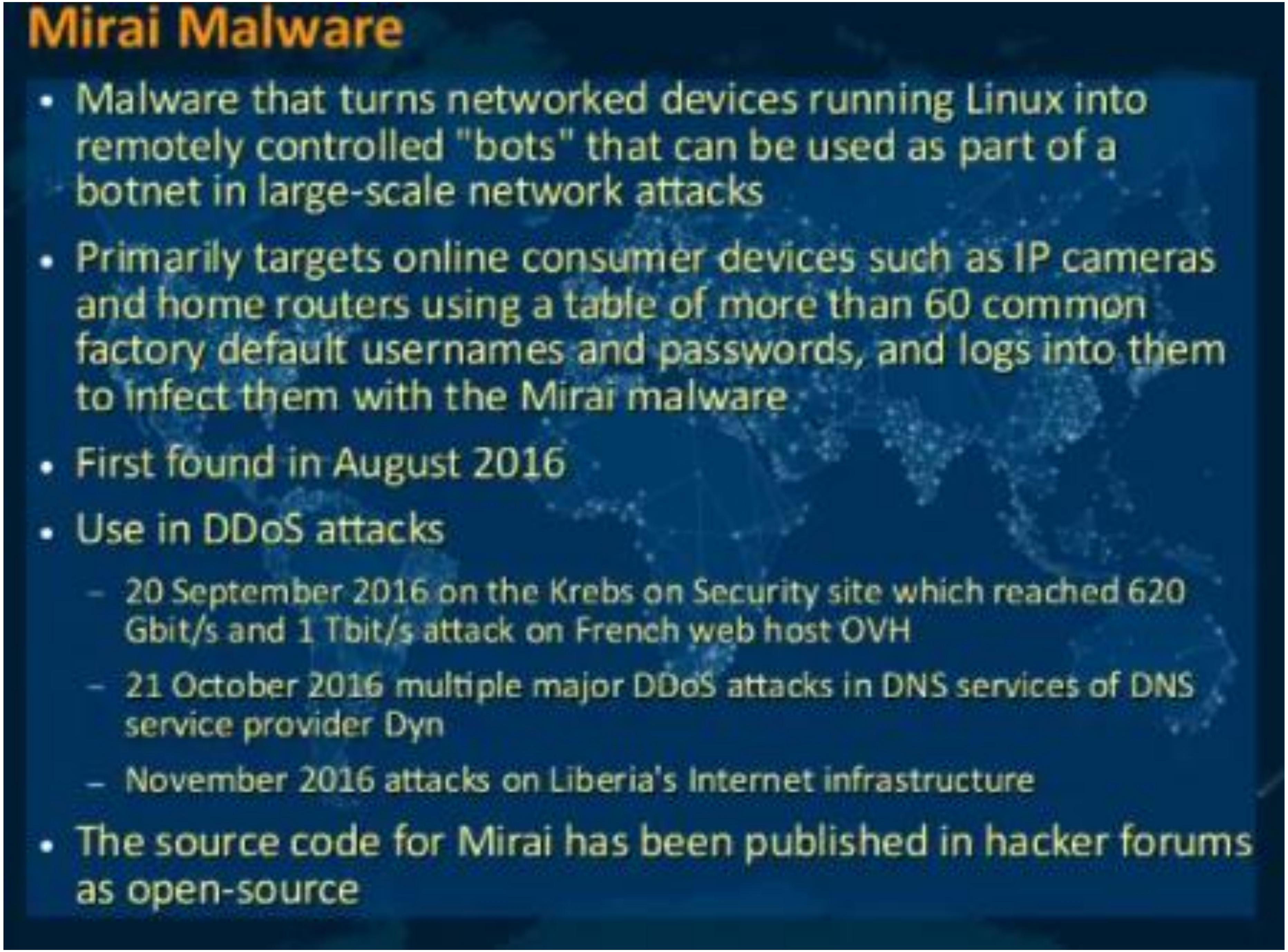
TOP 10

VULNERABILITY CATEGORIES

Poor Physical Security 10

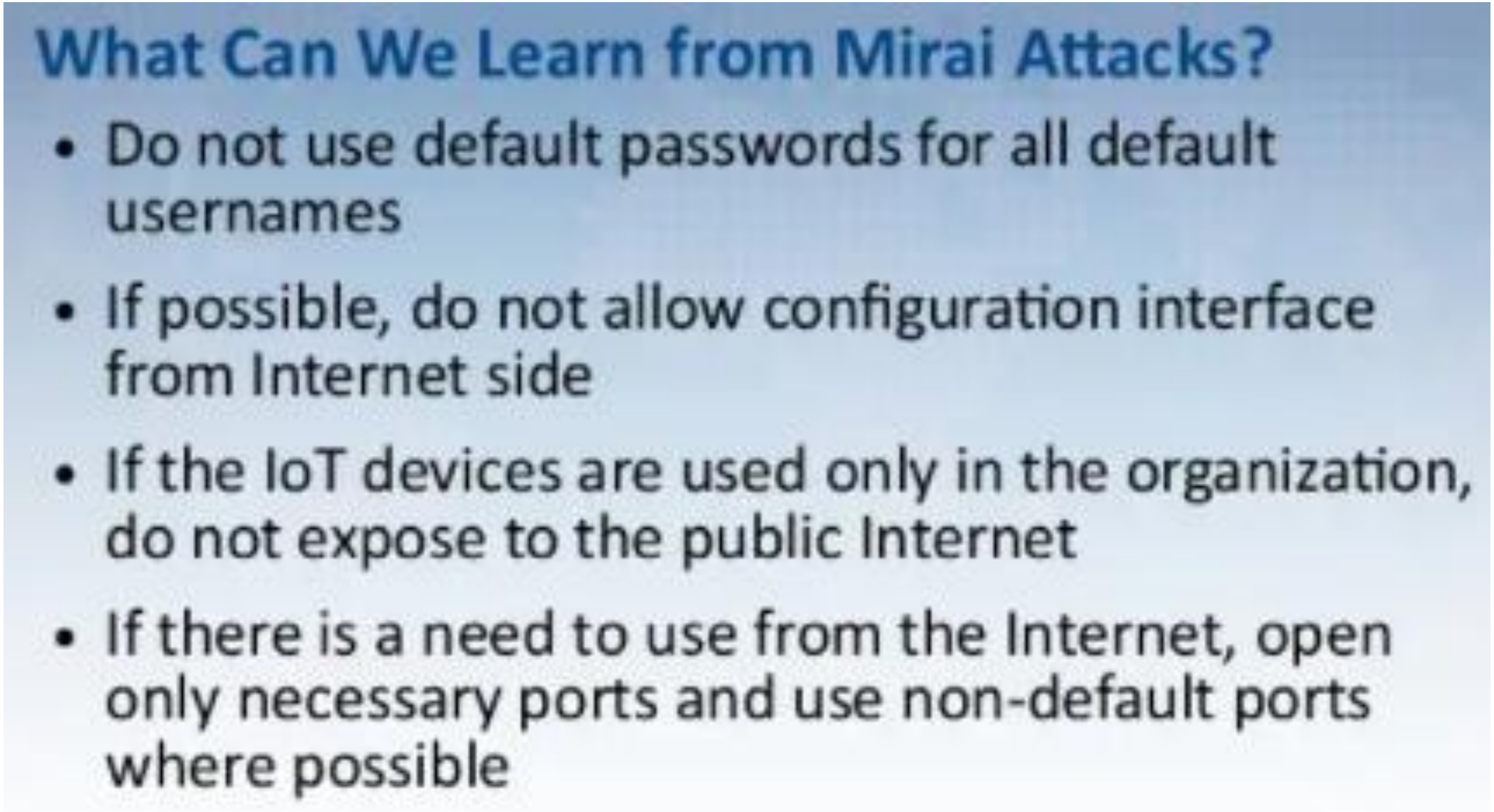
covers the IoT device

Obstacles	Solutions
Unnecessary external ports like USB ports	Minimize external ports like USB ports
Access to operating systems through remove media	Properly protect operating system
Inability to limit administrative capabilities	Include ability to limit administrative capabilities



Mirai Malware

- Malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks
- Primarily targets online consumer devices such as IP cameras and home routers using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware
- First found in August 2016
- Use in DDoS attacks
  - 20 September 2016 on the Krebs on Security site which reached 620 Gbit/s and 1 Tbit/s attack on French web host OVH
  - 21 October 2016 multiple major DDoS attacks in DNS services of DNS service provider Dyn
  - November 2016 attacks on Liberia's Internet infrastructure
- The source code for Mirai has been published in hacker forums as open-source



What Can We Learn from Mirai Attacks?

- Do not use default passwords for all default usernames
- If possible, do not allow configuration interface from Internet side
- If the IoT devices are used only in the organization, do not expose to the public Internet
- If there is a need to use from the Internet, open only necessary ports and use non-default ports where possible