SECURITY AND PRIVACY IN THE INTERNET OF THINGS

Prepared By,

SHELLY SHIJU GEORGE

Assistant Professor

CONCEPTS

- The Internet of Things leads to a new computing paradigm. It is the result of shifting computing to our real-time environment.
- The IoT devices, besides connecting to the Internet, also need to talk to each other based on the deployment context.
- More precisely, IoT is not only about bringing smart objects to the Internet, but also enabling them to talk to each other.
- This will have direct implications to our life, and change the way we live, learn, and work.
- Thus, it provides a huge opportunity for hackers to compromise security and privacy.
- Note that we should not only secure IoT systems from dangers that might attack it over the public Internet, but also protect a coopting device or well-behaved node from a bad node in the same network.

CONCEPTS (CONTINUED)

- Today, we have reasonably secure and safe online financial transactions, e-commerce, and other services over the Internet.
- Core to these systems is the use of advanced cryptographic algorithms that require substantial computing power.
- Smart objects have limited capabilities in terms of computational power and memory, and might be battery-powered devices, thus raising the need to adopt energy efficient technologies.
- Among the notable challenges that building interconnected smart objects introduces are security, privacy, and trust.

CONCEPTS (CONTINUED)

- The use of Internet Protocol (IP) has been foreseen as the standard for interoperability for smart objects.
- As billions of smart objects are expected to come to life and IPv4 addresses have eventually reached depletion, the IPv6 protocol has been identified as a candidate for smart-object communication.
- The challenges that must be overcome to resolve IoT security and privacy issues are immense.
- This is primarily because of the many constraints attached to the provision of security and privacy in IoT systems.

CONCEPTS (CONTINUED)

The deployment of the IoT raises many security issues arising as a result of the following aspects:

- the very nature of smart objects, for example, the adoption of lightweight cryptographic algorithms, in terms of processing and memory requirements
- the use of standard protocols, for example, the need to minimize the amount of data exchanged between nodes
- the bidirectional flow of information, for example, the need to build an end-to-end security architecture.

IOT REFERENCE MODEL

Table 10.1 IoT World Forum Reference Model

IoT Reference Model	
Levels	**Characteristics**
Physical devices and controllers	End point devices, exponential growth, diverse
Connectivity	Reliable, timely transmission, switching, and routing
Edge computing	Transform data into information, actionable data
Data accumulation	Data storage, persistent and transient data
Data abstraction	Semantics of data, data integrity to application, data standardization
Application	Meaningful interpretations and actions of data
Collaboration and processes	People, process, empowerment, and collaboration

IOT REFERENCE MODEL (CONTINUED)

- Today, there is no standardized conceptual model that characterizes and standardizes the various functions of an IoT system.
- Cisco Systems Inc. has proposed an IoT reference model that comprises seven levels.
- The IoT reference model allows the processing occurring at each level to range from trivial to complex, depending on the situation.
- The model also describes how tasks at each level should be handled to maintain simplicity, allow high scalability, and ensure supportability.
- Finally, the model defines the functions required for an IoT system to be complete.

IOT REFERENCE MODEL (CONTINUED)

- The fundamental idea is to present a level of abstraction and appropriate functional interfaces to provide a complete system of IoT.
- It is the coherence of an end-to-end IoT architecture that allows one to process volume of context specific data points, make meaningful information, manage intrinsic feature of large scale, and ultimately design insightful responses.
- The important design factor is that IoT should leverage existing Internet communication infrastructure and protocols.

IOT REFERENCE MODEL (CONTINUED)

- Level 3 is famously referred to as Edge Computing or Fog Computing.
- The primary function is to transform data into information, and perform limited data-level analytics.
- Context specific information processing is done at this level so that we obtain actionable data.
- An important feature of fog computing is its capability of real time processing and computing.
- More precisely, levels 1, 2, and 3 are concerned with data in motion, and the higher levels are concerned with information derived from the data items.

IOT REFERENCE MODEL (CONTINUED)

- It leads to an unprecedented value zone wherein people and the processes are empowered to take meaningful action from the underneath world of IoT.
- The core objective is to automate most of the manual processes, and empower people to do their work better and smarter.

IOT REFERENCE MODEL (CONTINUED)

- At each level of the reference model, the increasing number of entities, heterogeneity, interoperability, complexity, mobility, and distribution of entities represent an expanding attack surface, measurable by additional channels, methods, actors, and data items.
- Further, this expansion will necessarily increase the field of security stakeholders and introduce new manageability challenges that are unique to the IoT.

IOT SECURITY THREATS

- There are three broad categories of threats: Capture, Disrupt, and Manipulate.
- **Capture threats** are related to capturing the system or information.
- **Disrupt threats** are related to denying, destroying, and disrupting the system.
- **Manipulate threats** are related to manipulating the data, identity, time-series data, etc.
- The simplest type of **passive threats** in the IoT is that of eavesdropping or monitoring of transmissions with a goal to obtain information that is being transmitted.
- It is also referred to as capture attacks.
- **Capture attacks** are designed to gain control of physical or logical systems or to gain access to information or data items from these systems.

IOT SECURITY THREATS (CONTINUED)

- The ubiquity and physical distribution of the IoT objects and systems provide attackers with great opportunity to gain control of these systems.
- The distribution of smart objects, sensors, and systems results in self-advertisements, beacons, and mesh communications, providing attackers greater opportunity to intercept or intercede in information transmission within the environment.
- Moreover, the frequency of the data transmissions, data models, and formats help attackers in cryptanalysis.

IOT SECURITY THREATS (CONTINUED)

Some of the well-known active threats are as follows:

- **Masquerading**: an entity pretends to be a different entity. This includes masquerading other objects, sensors, and users.
- **Man-in-the-middle**: when the attacker secretly relays and possibly alters the communication between two entities that believe that they are directly communicating with each other.
- **Replay attacks**: when an intruder sends some old (authentic) messages to the receiver. In the case of a broadcast link or beacon, access to previous transmitted data is easy.
- **Denial-of-Service (DoS) attacks**: when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions.

IOT SECURITY THREATS (CONTINUED)

- Active threats such as masquerading, replay attacks, DoS attacks are, in general, comparatively easy in an IoT environment.
- One example is the implementation of cloned beacons from an untrusted source.
- **Beacons** are small wireless devices that continuously transmit a simple radio signal saying, “I am here, this is my ID.”
- In most cases, the signal is picked up by nearby smartphones using Bluetooth Low Energy (BLE) technology.

IOT SECURITY THREATS (CONTINUED)

- When the mobile device detects the beacon signal, it reads the beacon's identification number (ID), calculates the distance to the beacon and, based on these data, triggers an action in a beacon compatible mobile app.
- The IoT threats are enumerated as cloning of smart objects by untrusted manufacturers, counterfeiting/substitution of the IoT devices by the third parties, malicious firmware replacement, and attacks on relatively unprotected devices by eavesdropping or extraction of credentials or security properties, in addition to the standard threat vectors such Man-in-the-middle and DoS attacks.
- The security and privacy requirements are determined by the nature of attacks in an IoT environment.

IOT SECURITY REQUIREMENTS

The basic security properties that need to be implemented in IoT are listed :

- **Confidentiality**: transmitted data can be read only by the communication endpoints;
- **availability**: the communication endpoints can always be reached and cannot be made inaccessible;
- **integrity**: received data are not tampered with during transmission, and assured of the accuracy and completeness over its entire lifecycle;
- **authenticity**: data sender can always be verified and data receivers cannot be spoofed and
- **authorization**: data can be accessed only by those allowed to do so and should be made unavailable to others.

IOT SECURITY REQUIREMENTS (CONTINUED)

- The requirements for securing the IoT are complex, involving a blend of approaches from mobile and cloud architectures, combined with industrial control, automation, and physical security.
- Many of the security requirements for the IoT are similar to the requirements for the IP protocol-based Internet.
- The technologies and services that have been used to secure the Internet are applicable in most cases with suitable adaptation required at each level of the IoT reference model.
- Besides the standard security requirements, and from the threats discussed, the following security requirements can be derived.

SCALE

- The important requirement is the scale in which an IoT environment is expected to grow.
- The population of entities is expected to grow exponentially as users embrace more smart and connected objects and devices, more sensors are deployed, and more objects are embedded with intelligence and information.
- Each entity, depending on its nature, characteristics, carries with it an associated set of protocols, channels, methods, data models, and data items, each of which is subject to potential threat.

SCALE (CONTINUED)

- This increased scale has the effect of expanding the target surface.
- As noted earlier, the scale and complexity at each level of the IoT model determine the amount of compute and storage requirements, and hence the cost and power budget.
- The trade-off between cost and resources determines the availability of resources for system security, cryptographic algorithms, key size, and methods.

IP PROTOCOL-BASED IOT

- The use of IP technologies in IoT brings a number of basic advantages such as a seamless and homogeneous protocol suite, and proven security architecture.
- It also simplifies the mechanisms to develop and deploy innovative services by extending the tested IP-based frameworks.
- It leads to a phenomenon called “expansion of attack surface.”
- It implies that when we connect the previously unconnected—by introducing new devices that stream context sensitive data, by placing data in mobile cloud, or by pushing computing to edge devices—new points of ingress for security threats inevitably materialize.

IP PROTOCOL-BASED IOT (CONTINUED)

As the networks of smart objects and IP merge, there is a high probability of security vulnerabilities due to protocol translations, incompatible security infrastructures, etc. The enterprise security model has been marked by two chief tenets:

- Security has been focused on best-of-breed applications and appliances: solutions for firewall, for network security, for data security, for content security, and so forth.
- Security has been perimeter-based, meaning organizations secured the end device and the server, and reacted to recognized intrusions or threats such as viruses or DoS attacks.

IP PROTOCOL-BASED IOT (CONTINUED)

- In the context of IoT, perimeter-based security mechanisms have little relevance.
- The attack surface is much broader, often borderless, and involves heterogeneous systems.

HETEROGENEOUS IOT

- Another important design consideration in the IoT is how the connected things can work together to create value and deliver innovative solutions and services.
- IoT can be a double-edged sword.
- Although it provides a potential solution to the innovation imperative, it can also significantly boost operational complexity if not properly integrated with key organizational processes.
- Security processes should also be properly designed to align with the organization processes.
- The complex operational technologies make it difficult for designing a robust security architecture in IoT.

HETEROGENEOUS IOT (CONTINUED)

- It is a common opinion that in the near future IP will be the base common network protocol for IoT.
- This does not imply that all objects will be able to run IP.
- In contrast, there will always be tiny devices, such as tiny sensors or Radio-Frequency Identification (RFID) tags, that will be organized in closed networks implementing very simple and application-specific communication protocols and that eventually will be connected to an external network through a proper gateway.
- In short, the heterogeneous characteristics of the networks make it harder to implement certain IP-based security systems such as symmetric cryptosystems.

LIGHTWEIGHT SECURITY

- The unprecedented value of IoT is realized only when smart objects of different characteristics interact with each other and also with back-end or cloud services.
- IPv6 and web services become the fundamental building blocks of IoT systems and applications.
- In constrained networked scenarios, smart objects may require additional protocols and some protocol adaptations in order to optimize Internet communications and lower memory, computational, and power requirements.
- The use of IP technologies in IoT brings a number of basic advantages such as a seamless and homogeneous protocol suite, and proven security architecture.

LIGHTWEIGHT SECURITY (CONTINUED)

- It also simplifies the mechanisms to develop and deploy innovative services by extending the tested IP-based frameworks.
- However, it also introduces new challenges in adopting certain frameworks as is.
- The IoT provides interconnectedness of people and things on a vast scale with billions of devices.
- It is at once a huge opportunity for better efficiency and better services, as well as a huge opportunity for hackers to compromise security and privacy.

LIGHTWEIGHT SECURITY (CONTINUED)

- It may be noted that one of the key elements of the state-of-the-art security in the Internet is the use of advanced cryptographic algorithms needing substantial processing power.
- Many, if not most, IoT devices are based on low-end processors or microcontrollers that have low processing power and memory, and are not designed with security as a priority design goal.
- Privacy enforced through encryption, authentication to conform identity, and Information authentication by using digitally signed certificates are the key security mechanisms in the Internet today.

LIGHTWEIGHT SECURITY (CONTINUED)

These mechanisms rely on the following:

- Cryptographic ciphers such as Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA2), and the public-key ciphers RSA and elliptic-curve cryptography (ECC).
- Transport Layer Security (TLS) protocol, and predecessor Secure Sockets Layer (SSL) protocol, which provide authentication and information encryption using the ciphers mentioned.
- Public-Key Infrastructure (PKI) provides the building blocks for authentication and trust through a digital certificate standard and Certificate Authorities (CA).

LIGHTWEIGHT SECURITY (CONTINUED)

- Current IoT implementations have gaps in terms of implementing the above security mechanisms, even though these mechanisms have widespread adoption in the IP networks.
- For example, there are multiple commercial and open-source TLS implementations that can be adopted in an IoT device.
- These libraries typically consume more than 100 KB of code and data memory, which is not a lot for a conventional computing device, but is impractical for an IoT device such as a medical sensor.
- The cryptographic ciphers used by the TLS protocol are a source of significant computational load on the low end CPU of the typical IoT device.

LIGHTWEIGHT SECURITY (CONTINUED)

- This computational load results in higher power consumption as well.
- For example, the data rate supported by a 32 bit MCU implementing AES-128 may fall from 3 Mbps to 900 Kbps if the MCU is substituted with a 16 bit processor.
- Note that this in turn leads to indirect effects like longer active time, more power drain, and a shorter battery life.
- Essentially the challenge is to make the resource constrained IoT networks interoperate with the resourceful IP networks.

LIGHTWEIGHT SECURITY (CONTINUED)

- The current principles of IT security need to be deconstructed by reevaluating and redesigning protocols, algorithms, and processes in light of the evolving IoT architecture.
- More precisely, network scale, heterogeneous, power constraints, and mobility alter the attack surface on a much larger scale and in greater breadth.
- It necessitates reinvention and adaption of IP-based protocols and introduction of IoT specific protocols.

IOT SECURITY OVERVIEW

Table 10.2 Security Mechanisms to Mitigate the Threats in the IoT Networks

Threats/Security Mechanism	Data Privacy	Data Freshness	Source Authentication	Data Integrity	Intrusion Detection	Identity Protection
Capture						
Physical systems						X
Information	X			X		X
Disrupt						
DoS Attack		X	X		X	
Routing attack					X	
Manipulate						
Masquerading	X		X	X		X
Replay attack		X	X	X	X	
Man-in-the-middle			X	X	X	

IOT PROTOCOLS

- There are currently IETF (Internet Engineering Task Force) working groups focusing on extending existing protocols for resource-constrained networked environments.
- These are: CoRE, 6LoWPAN, Routing Over Low power and Lossy networks (ROLL), and the Light-Weight Implementation Guidance (LWIG) working groups.
- Significant reasons for proper protocol optimizations and adaptations for resource-constrained objects are targeted toward protocol compression to fit into smaller Maximum Transmission Units (MTU), thereby reducing power consumption with smaller packets, elimination of fragmentation, and reducing the handshake messages.

IOT PROTOCOLS (CONTINUED)

Table 10.3 Bluetooth Smart Device Protocol Stack

Application layer	CoAP MQTT
Transport layer	UDP TCP
Network layer	IPv6 ICMPv6 RPL
Adaptation layer	Bluetooth Smart 6LoWPAN
Physical and link layer	IPSP

IOT PROTOCOLS (CONTINUED)

- IPv6 significantly expands the number of available IP addresses for use by providing 2128 addresses.
- This means that, if necessary, every device can have its own unique IPv6 address.
- Standards such as 6LoWPAN have made it possible to integrate sensors in a transport agnostic manner.
- 6LoWPAN enables sensors to talk to IP Protocols natively.
- Furthermore, new application layer protocols such as CoAP and Message Queue Telemetry Transport (MQTT) ensure optimal use of bandwidth and resources of constrained IoT devices.
- Bluetooth Smart is an open standard that is specifically designed for the needs of battery powered sensors and wearables.

IOT PROTOCOLS (CONTINUED)

- Now powered with the 6LoWPAN IETF draft, Bluetooth Smart is well placed to address evolving needs of sensors connecting to the cloud without the need for intelligent gateways.
- The Internet Protocol Service Profile (IPSP) defines establishing and managing the Bluetooth logical link control and adaptation protocol (L2CAP) connection oriented channel.
- IPSP and Bluetooth Smart 6LoWPAN standard ensures optimal IP stack performance over Bluetooth Smart as a physical layer.
- 6LoWPAN defines the creation of an IPv6 address of a device from its Bluetooth Smart device address.
- It also compresses the IP header where possible to ensure optimal use of RF bandwidth for power saving purposes.

IOT PROTOCOLS (CONTINUED)

- A static profile of an IoT object represents the knowledge by an endpoint of its own resources (such as identity, battery, computing power, memory size, etc.) and the security settings it intends to use or needs from the network.
- The static profile can be read-only (preset by vendor), write-once (set by manufacturer), or rewritable (user enabled).
- Note that certain security primitives may be computationally prohibitive for IoT objects; a negotiation is thus required before the establishment of a secure channel so that the concerned endpoints can agree upon a cryptographic suite.

NETWORK AND TRANSPORT LAYER CHALLENGES

- The IPSec uses the concept of a Security Association (SA), defined as the set of algorithms and parameters (such as keys) used to encrypt and authenticate a particular flow in one direction.
- To establish a SA, IPSec can be preconfigured (specifying a preshared key, hash function, and encryption algorithm) or can be dynamically negotiated by the IPSec Internet Key Exchange (IKE) protocol.
- The IKE protocol uses asymmetric cryptography, which is computationally heavy for resource-constrained devices.

NETWORK AND TRANSPORT LAYER CHALLENGES (CONTINUED)

- To address this issue, IKE extensions using lighter algorithms should be used.
- Data overhead is another problem for IPSec implementations in IoT environments.
- This is introduced by the extra header encapsulation of IPSec AH and/or Encapsulating Security Payload (ESP), and can be mitigated by using header compression.
- CoAP proposes to use the DTLS protocol to provide end-to-end security in IoT systems.
- The DTLS protocol provides a security service similar to TLS, but on top of UDP.
- This is highly suitable for IoT environments due to its usage of UDP as transport protocol.

NETWORK AND TRANSPORT LAYER CHALLENGES (CONTINUED)

- This results in avoidance of problems from the use of TCP in network-constrained scenarios that are caused due to the extremely variable transmission delay and loss links.
- DTLS is a heavyweight protocol and its headers are too long to fit in a single IEEE 802.15.4 MTU.
- 6LoWPAN provides header compression mechanisms to reduce the size of upper layer headers.
- 6LoWPAN header compression mechanisms can be used to compress the security headers as well.

NETWORK AND TRANSPORT LAYER CHALLENGES (CONTINUED)

- A new 6LoWPAN header compression algorithm for DTLS is proposed.
- It links the compressed DTLS with the 6LoWPAN standard using standardized mechanisms.
- It is shown that the proposed DTLS compression significantly reduces the number of additional security bits.
- A two-way authentication security scheme for the IoT based on DTLS.
- The proposed security scheme is based on the widely used public-key based RSA cryptography protocol and works on top of standard low power communication stacks.

IOT GATEWAYS AND SECURITY

- Connectivity is one of the important challenges in designing the IoT network.
- The diversity of end points makes it very difficult to provide IP connectivity.
- It is important that non-IP devices too have a mechanism to connect with IoT.
- The IoT gateways can simplify IoT device design by supporting the different ways nodes natively connect, whether this is a varying voltage from a raw sensor, a stream of data over an inner integrated circuit (I2C) from an encoder, or periodic updates from an appliance via Bluetooth.

IOT GATEWAYS AND SECURITY (CONTINUED)

- Gateways effectively mitigate the great variety and diversity of devices by consolidating data from disparate sources and interfaces and bridging them to the Internet.
- The result is that individual nodes do not need to bear the complexity or cost of a high-speed Internet interface in order to be connected.
- There are several ways that an IoT gateway can extend connectivity to nodes as described.

IOT GATEWAYS AND SECURITY (CONTINUED)

- The network nodes connect to the IoT via a gateway. The nodes themselves are not IP-based and thus cannot directly connect to the Internet/WAN.
- Rather, they use either wired or wireless PAN technology to connect to the gateway with a less expensive and less complex mode of connectivity.
- The gateway maintains an IoT agent for each node that manages all data to and from nodes.
- In this case, application intelligence can also be located in the gateway.

IOT GATEWAYS AND SECURITY (CONTINUED)

- The nodes can also connect directly to the Internet using a WAN connection such as Wi-Fi or Ethernet. The gateway serves primarily as a router; in fact, it can be simply a router when nodes have their own IoT agent and autonomously manage themselves.
- Alternatively, the nodes can connect directly to the Internet using a PAN connection such as 6LoWPAN.
- In this case, the gateway serves as a translation point between the PAN and WAN.

IOT GATEWAYS AND SECURITY (CONTINUED)

- Many IoT applications handle potentially sensitive data.
- Data collected from location services, for example, need to be protected from hacking.
- Similarly, medical devices need to maintain the privacy of individuals.
- In the context of the IoT gateway architecture, the security processing and mechanisms can be offloaded from nodes to the gateway to ensure proper authentication, protecting exchanges of data, and safeguarding intellectual property.
- This enables IoT nodes to implement greater security than could be economically implemented in individual end points.

IOT ROUTING ATTACKS

- Threats arising due to the physical nature of IoT devices can be mitigated by appropriate physical security safeguards, whereas secure communication protocols and cryptographic algorithms are the only way of coping with the fact that they arise due to IoT devices communicating with each other and the external world.
- For the later, IoT devices can either run the standard TCP/IP protocol stack, if their computational and power resources allow, or can run adaptions which are optimized for lower computational and power consumption.

IOT ROUTING ATTACKS (CONTINUED)

- There are some well-known routing attacks that can be exploited by attackers.
- The 6LoWPAN networks or an IP-connected sensor networks are connected to the conventional Internet using 6LoWPAN Border Routers (6LBR).
- The Routing Protocol for Low-Power and Lossy Networks (RPL) is a novel routing protocol standardized for 6LoWPAN networks.
- RPL creates a destination-oriented directed acyclic graph (DODAG) between the nodes in a 6LoWPAN.
- It supports unidirectional traffic toward DODAG root and bidirectional traffic between 6LoWPAN devices and between devices and the DODAG root (typically the 6LBR).

IOT ROUTING ATTACKS (CONTINUED)

- RPL enables each node in the network to determine whether packets are to be forwarded upwards to their parents or downwards to their children.

Attacks on sensor networks that are applicable to IoT are discussed. Some well known routing attacks on IoT are as follows:

- Selective-forwarding attacks
- Sinkhole attacks
- Hello flood attacks
- Wormhole attacks
- Clone Id and Sybil attacks

IOT ROUTING ATTACKS (CONTINUED)

- With **selective-forwarding attacks**, it is possible to launch DoS attacks where malicious nodes selectively forward packets.
- This attack is primarily targeted to disrupt routing paths.
- For example, an attacker could forward all RPL control messages and drop the rest of the traffic.
- This attack has severer consequences when coupled with other attacks such as sinkhole attacks.
- One of the solutions to guard against selective forwarding attacks is to create disjoint paths between the source and the destination nodes.
- Another effective countermeasure against selective-forwarding attacks is to make sure the attacker cannot distinguish between different types of traffic, thus forcing the attacker to either forward all traffic or none.

IOT ROUTING ATTACKS (CONTINUED)

- In **sinkhole attacks**, a malicious node advertises a fraudulent routing path with a seemingly favorable route metric and attracts many nearby nodes to route traffic through it.
- An intrusion detection system could be hosted in the 6LBR and can utilize information from multiple DODAGs to detect sinkhole attacks.
- In the **hello-flood attack**, The HELLO message refers to the initial message a node sends when joining a network.
- By broadcasting a HELLO message with strong signal power and a favorable routing metric, an attacker can introduce himself as a neighbor to many nodes, possibly the entire network.
- A simple solution to this attack is for each HELLO message the link is checked to be bidirectional.

IOT ROUTING ATTACKS (CONTINUED)

- A **wormhole** is an out-of-band connection between two nodes using wired or wireless links.
- Wormholes can be used to forward packets faster than via normal paths.
- A wormhole created by an attacker and combined with another attacks, such as sinkhole, is a serious security threat.
- One approach is to use separate link-layer keys for different segments of the network.
- This can counteract the wormhole attack, as no communication will be possible between nodes in two separate segments.
- Also, by binding geographic information to the neighborhoods it is possible to overcome a wormhole.

IOT ROUTING ATTACKS (CONTINUED)

- In a **clone-ID attack**, an attacker copies the identities of a valid node onto another physical node.
- This can, for example, be used in order to gain access to a larger part of the network or in order to overcome voting schemes.
- In a **Sybil attack**, which is similar to a clone ID attack, an attacker uses several logical entities on the same physical node.
- Sybil attacks can be used to take control over large parts of a network without deploying physical nodes.
- By keeping track of the number of instances of each identity it is possible to detect cloned identities.
- It would also be possible to detect cloned identities by knowing the geographical location of the nodes, as no identity should be able to be at several places at the same time.

BOOTSTRAPPING AND AUTHENTICATION

- Bootstrapping and authentication controls the network entry of nodes.
- Authentication is highly relevant to IoT and is likely to be the first operation carried out by a node when it joins a new network, for instance, after mobility.
- It is performed with a (generally remote) authentication server using a network access protocol such as the PANA.
- For greater interoperability, the use of the EAP is envisioned.

BOOTSTRAPPING AND AUTHENTICATION (CONTINUED)

- Upon successful authentication, higher layer security associations could also be established (such as IKE followed by IPSec) and launched between the newly authenticated endpoint and the access control agent in the associated network.
- The Internet Key Exchange (IKEv2)/IPSec and the HIP reside at or above the network layer.
- Both protocols are able to perform an authenticated key exchange and set up the IPSec transforms for secure payload delivery.
- Currently, there are also ongoing efforts to create a HIP variant called Diet HIP that takes loss low-power networks into account at the authentication and key exchange level.

AUTHORIZATION MECHANISMS

- The present day services that run over the Internet, such as popular social media applications, have faced and handled privacy-related problems when dealing with personal and protected data that might be made accessible to third parties.
- In the future, the IoT applications will face similar issues, and others that may be unique to the domain.
- The OAuth (Open Authorization) protocol has been defined to solve the problem of allowing authorized third parties to access personal user data.
- OAuth2.0 is an authorization framework that allows a third party to access a resource owned by a resource owner without giving unencrypted credentials to the third party.

AUTHORIZATION MECHANISMS (CONTINUED)

- For example, assume that a healthcare sensor or mobile app wants to access a Facebook profile to post status updates.
- There is no need to provide the Facebook credentials to the app; instead, the user logs into Facebook, and as a result the app is authorized to use Facebook on the user's behalf.
- The user can also revoke this authorization any time by deleting the privilege in the Facebook settings.
- The OAuth 2.0 protocol defines the following four roles.

AUTHORIZATION MECHANISMS (CONTINUED)

1. Resource Owner

- It is an entity capable of granting access to a protected resource.
- When the resource owner is a person, it is referred to as an end user.
- In the above example, this could be the end user of the healthcare device.

AUTHORIZATION MECHANISMS (CONTINUED)

2. Resource Server (Service Provider, SP)

- It is the server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
- In the example, this is the Facebook server.

AUTHORIZATION MECHANISMS (CONTINUED)

3. Client (Service Consumer, SC)

- It is the application making protected resource requests on behalf of the resource owner and with its authorization.
- The term client does not imply any particular implementation characteristics (eg, whether the application executes on a server, a desktop, or other devices).
- In this case, it is the healthcare sensor or mobile application.

AUTHORIZATION MECHANISMS (CONTINUED)

4. Authorization Server

- It is the server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.
- In this example, it would be the Facebook authorization server.

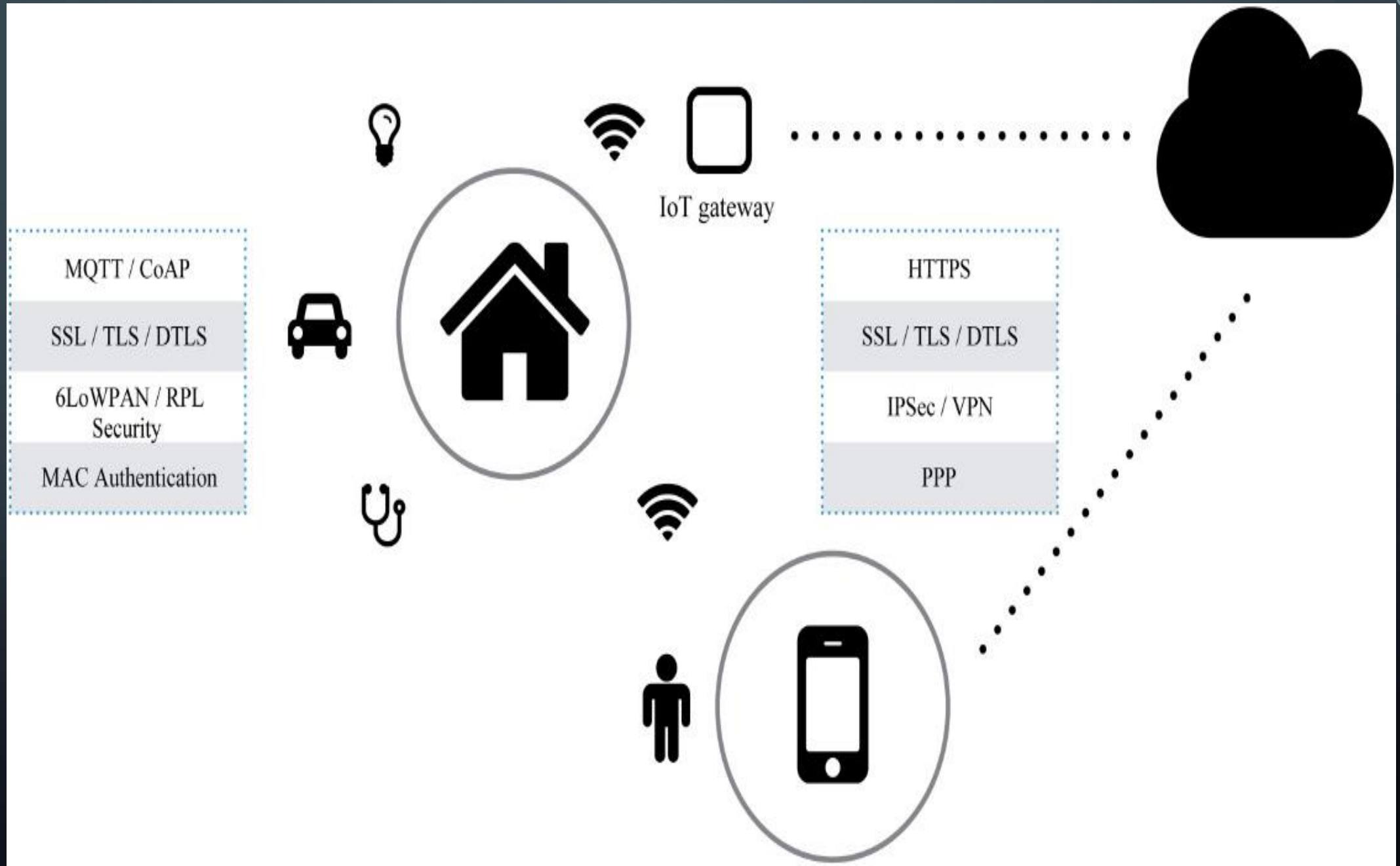
IOT OAS

- Note that the IoT devices may have challenges in implementation of OAuth due to the CPU intensive nature of cryptographic computations.
- A modified architecture called IoTOAS is proposed.
- In this approach, authorization-related functions are delegated to an external IoT-OAS authorization service, in order to minimize the memory and CPU requirements on the IoT device itself.
- An incoming OAuth secured request is forwarded to an IoT-OAS service for verification of the access token contained in the request.

IOT OAS (CONTINUED)

- The IoT-OAS service computes the digital signature of the incoming request using the appropriate scheme (PLAINTEXT/HMAC/RSA) and matches it with its internal store to verify the user and client credentials and permissions for resource access.
- It then provides an appropriate response back allowing or denying the requested access from the client.
- This approach enables the IoT device to focus on its own service logic and frees up computational resources from being overwhelmed by security and cryptographic implementations.
- The security protocols at each layer between different networks are shown in following diagram.

AN OVERVIEW OF IOT AND IP SECURITY PROTOCOLS



SECURITY FRAMEWORKS FOR IOT

- The low capabilities of IoT devices in terms of their energy and computing capabilities, wireless nature, and physical vulnerability are discussed to be the contributing factors to some unique security vulnerabilities.
- In particular, we cover the tight resource constraints, protocol translation such as HTTP ↔ CoAP, and end-to-end Security.
- Other important topics include the architecture framework aspects: Distributed vs Centralized approach, bootstrapping identity and key interchange, privacy aware identification, mobility, and IP network dynamics.

SECURITY FRAMEWORKS FOR IOT (CONTINUED)

- In the era of pervasive computing with large networks of resource constrained IoT devices, Moore's law can be interpreted differently: rather than a doubling of performance, we see a halving of the price for constant computing power every 18 months.
- Since many foreseen applications have extremely tight cost constraints over time, such as RFID in tetra packs, Moore's law will increasingly enable such applications.
- Many applications will process sensitive health monitoring or biometric data, so he demand for cryptographic components that can be efficiently implemented is strong and growing.

LIGHT WEIGHT CRYPTOGRAPHY

- The term lightweight cryptography refers to a family of cryptographic algorithms with smaller footprint, low energy consumption, and low computational power needs.
- Every designer of lightweight cryptography must cope with the trade-offs between security, cost, and performance.
- It is generally easy to optimize any two of the three design goals: security and cost, security and performance, or cost and performance; however, it is very difficult to optimize all three design goals at once.

LIGHT WEIGHT CRYPTOGRAPHY (CONTINUED)

- When we compare lightweight cryptographic implementations, we can make a distinction between symmetric and asymmetric ciphers.
- Symmetric ciphers serve mainly for message integrity checks, entity authentication, and encryption, whereas asymmetric ciphers additionally provide key-management advantages and nonrepudiation.
- Asymmetric ciphers are computationally far more demanding, in both hardware and software.
- The performance gap on constrained devices such as 8-bit microcontrollers is huge.

LIGHT WEIGHT CRYPTOGRAPHY (CONTINUED)

- For example, an optimized asymmetric algorithm such as ECC performs 100–1000 times more slowly than a standard symmetric cipher such as the AES algorithm, which correlates with a two to three orders of-magnitude higher power consumption.
- Symmetric-key cryptographic algorithms use the same key for encryption of a plain text and decryption of a message.
- The encryption key represents a shared secret between the parties that are involved in the secure communication.

SYMMETRIC-KEY LWC ALGORITHMS

- The Tiny Encryption Algorithm (TEA) is a block cipher renowned for its simplicity of description and implementation, typically a few lines of code.
- TEA operates on two 32-bit unsigned integers (could be derived from a 64-bit data block) and uses a 128-bit key.
- TEA relies only on arithmetic operations on 32-bit words and uses only addition, XORing, and shifts.
- For IoT devices with small memory footprints, TEA is very suitable since its algorithm uses a large number of iterations, rather than a complicated program, in order to avoid preset tables and long setup times.
- TEA defines a simple and short cipher that does not rely on preset tables or precomputations, thus saving on memory resources.

SYMMETRIC-KEY LWC ALGORITHMS (CONTINUED)

- The Scalable Encryption Algorithm (SEA) is targeted for small embedded applications.
- The design explicitly accounts for an environment with very limited processing resources and throughput requirements.
- A design principle of SEA is flexibility: the plaintext size n, key size n, and processor (or word) size b are design parameters, with the only constraint that n is a multiple of 6b; for this reason, the algorithm is denoted as SEAn;b.
- The main disadvantage is that SEAn;b trades space for time and this may not be trivial on devices with limited computational power.

SYMMETRIC-KEY LWC ALGORITHMS (CONTINUED)

- PRESENT is an ultra-lightweight block cipher algorithm based on a Substitution-Permutation Network (SPN).
- PRESENT has been designed to be extremely compact and efficient in hardware.
- It operates on 64-bit blocks and with keys of either 80 or 128 bits.
- It is for use in situations where low-power consumption and high chip efficiency are desired, thus making it of particular interest for constrained environments.

SYMMETRIC-KEY LWC ALGORITHMS (CONTINUED)

- The HIGh security and lightweigHT (HIGHT) encryption algorithm is a generalized Feistel network with a block size of 64 bits, 128-bit keys, and 32 rounds.
- HIGHT was designed with an eye on low-resource hardware performance.
- HIGHT uses very simple operations, such as XORing, addition mod 28, and bitwise rotation.

ASYMMETRIC LWC ALGORITHMS

- Public-key (asymmetric) cryptography requires the use of a public-key and a private key.
- Public keys can be associated with the identity of a node by including them into a public certificate, signed by a Certification Authority (CA) that can be requested to verify the certificate.
- Public-key cryptography requires the significant effort of deploying a PKI.
- Moreover, asymmetric cryptography requires higher processing and long keys (at least 1024 bits for RSA) to be used.
- Alternative public-key cryptographic schemes, such as ECC, might require shorter keys to be used in order to achieve the same security than RSA keys.

ASYMMETRIC LWC ALGORITHMS (CONTINUED)

- However, because of these reasons, symmetric cryptography is preferred in terms of processing speed, computational effort, and size of transmitted messages.
- Public key can be used to setup symmetric keys to be used in subsequent communications.
- Lightweight cryptography algorithms are suitable for environments that do not have stringent security requirements and where the constraints on available hardware and power budget cannot be relaxed.

KEY AGREEMENT, DISTRIBUTION, AND BOOTSTRAPPING

- A mechanism for key distribution and management has to be in place when security mechanisms have to be adopted.
- Asymmetric (public-key) cryptographic algorithms are usually used in key agreement protocols.
- However, other mechanisms that do not involve the adoption of asymmetric cryptography have been proposed, to address the challenges of resource-constrained devices.
- A polynomial-based key predistribution protocol has been defined and applied to Wireless Sensor Networks.
- A possible alternative key agreement protocol is SPINS, which is a security architecture specifically designed for sensor networks.

KEY AGREEMENT, DISTRIBUTION, AND BOOTSTRAPPING (CONTINUED)

- In SPINS, each sensor node shares a secret key with a base station, which is used as a trusted third party to set up a new key, with no need of public-key cryptography.
- Three efficient random key predistribution schemes for solving the security-bootstrapping problem in resource-constrained sensor networks, each of which represents a different tradeoff in the design space of random key protocols.

SECURITY BOOTSTRAPPING

- The key agreement protocols require that some type of credentials such as symmetric keys, certificates, and public–private key pairs are preconfigured on the nodes, so that the key agreement procedure can occur.
- Bootstrapping refers to the sequence of tasks that need to be executed before the network can interwork, requiring the correct configuration at all layers of the OSI model from link layer to application layer.
- It can be viewed as a process of creating a security domain from a set of previously unassociated IoT devices.
- Current IoT architectures are fully centralized in most cases, so that a central party handles all the security relationships in an administrative domain.

SECURITY BOOTSTRAPPING (CONTINUED)

- In the ZigBee standard, this entity is the trust center. Current proposals for 6LoWPAN/Core identify the 6LoWPAN Border Router (6LBR) as such an entity.
- A centralized architecture allows for central management of devices and key associations.
- The limitation is that there is a single point of failure; a decentralized approach will allow creating ad-hoc security domains that might not require a centralized online management entity and will allow subsets of nodes to work in a stand-alone manner.
- The ad-hoc security domains can be synced to centralized entity later, allowing for both centralized and distributed management.

PRIVACY IN IOT NETWORKS

- The smart, connected objects will interact with both humans and other smart objects by providing, processing, and delivering all sorts of information and signals.
- All of these objects and their communications with the environment carry with them a risk to privacy and information leakage.
- Healthcare applications represent the most outstanding application of IoT.
- The lack of confidence regarding privacy results in decreased adoption among users and is therefore one of the driving factors in the success of IoT.

PRIVACY IN IOT NETWORKS (CONTINUED)

- The ubiquitous adoption of the wireless medium for exchanging data may pose new issue in terms of privacy violation.
- In fact, wireless channel increases the risk of violation due to the remote access capabilities, which potentially expose the system to eavesdropping and masking attacks.
- IoT devices and applications add a layer of complexity over the generic issue of privacy over the Internet, for example due to generation of traceable characteristics and attributes of individuals.
- IoT devices in healthcare present a major concern, since these devices and applications typically generate large volumes of data on individual patients through continuous monitoring of vital parameters.

PRIVACY IN IOT NETWORKS (CONTINUED)

- In this case, it is crucial to delink the identities of the device from that of the individual, through mechanisms such as data anonymization.
- Data anonymization is the process of either encrypting or removing personally identifiable information from data sets, so that the originator of the data remains anonymous.
- Similar to the preceding discussion of the OAuth protocol, digital shadows enable the individual's objects to act on their behalf, storing just a virtual identity that contains information about their parameters.
- Identity management in IoT may offer new opportunities to increase security by combining diverse authentication methods for humans and machines.
- For example, bio-identification combined with an object within the personal network could be used to open a door.

SECURE DATA AGGREGATION

- Homomorphic encryption is a form of encryption that allows specific types of computations to be executed on cipher texts and obtain an encrypted result that is the cipher text of the result of operations performed on the plain text.
- Applying the standard encryption methods presents a dilemma: If the data is stored unencrypted, it can reveal sensitive information to the storage/database service provider.
- On the other hand, if it is encrypted, it is impossible for the provider to operate on it.
- If data are encrypted, then answering even a simple counting query (for example, the number of records or files that contain a certain keyword) would typically require downloading and decrypting the entire database content.

SECURE DATA AGGREGATION (CONTINUED)

- A homomorphic encryption allows a user to manipulate without needing to decrypt it first.
- An example of homomorphic encryption is the RSA algorithm.
- Other examples of homomorphic encryption schemes are the ECC encryption, the ElGamal cryptosystem, and the Pailler cryptosystem.
- Homomorphic encryption has a lot of relevance to IoT networks, since privacy can be preserved at all stages of the communication, especially without the need for intermediate nodes to decrypt the information.
- For example, a lot of processing and storage can be eliminated at intermediate nodes by data aggregation with operations such as sums and averages.

SECURE DATA AGGREGATION (CONTINUED)

- This in turn results in lower power consumption, which is relevant for constrained environments.
- However, note that this type of homomorphic cryptosystems is more compute-intensive and needs longer keys to achieve a comparable security level than typical symmetric-key algorithms.

SECURE DATA AGGREGATION (CONTINUED)

Typically, secure data aggregation mechanisms require nodes to perform the following operations:

- at the transmitting node, prior to transmission, data are encrypted with some cryptographic function E
- at the receiving node, all received data packets are decrypted with the inverse cryptographic function $D = E^{-1}$ to retrieve the original data;
- data are aggregated with an aggregation function;
- prior to retransmission, aggregated data are encrypted through E and relayed to the next hop.

ENIGMA

- MIT Researchers, Guy Zyskind and Oz Nathan, have recently announced a project dubbed Enigma that makes a major conceptual step toward this Holy Grail of a fully homomorphic encryption protocol.
- A peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping the data completely private is proposed.
- Enigma's computational model is based on a highly optimized version of secure multiparty computation, guaranteed by a verifiable secret-sharing scheme.
- For storage, it uses a modified distributed hash table for holding secret-shared data.

ENIGMA (CONTINUED)

- An external block chain is utilized as the controller of the network, manages access control, identities, and serves as a tamper-proof log of events.
- Security deposits and fees incentivize operation, correctness, and fairness of the system.
- Similar to Bitcoin, Enigma removes the need for a trusted third party, enabling autonomous control of personal data.
- For the first time, users are able to share their data with cryptographic guarantees regarding their privacy.

ENIGMA (CONTINUED)

- The typical use case of Enigma would be for interactions between hospitals and health-care providers who store encrypted patient data as per HIPAA regulations.
- Research organizations and pharmaceutical companies would benefit from access to these data for clinical analysis.
- For example, a hospital can encrypt its data and store it in the cloud, where potentially other universities, pharma companies, and insurance companies could access it with permission from the originating hospital.
- With the usage of Enigma, note that there is no need for the originating hospital to first decrypt and anonymize the data, it only needs to authorize the third party for access.

ZERO KNOWLEDGE PROTOCOLS

- Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation and with smaller computational requirements than using comparable public-key protocols.
- Thus Zero-knowledge protocols seem very attractive especially in the context of IoT networks, especially for some applications like smart cards.
- Zero-knowledge protocols have been claimed to have lighter computational requirements than, for example, public-key protocols.

ZERO KNOWLEDGE PROTOCOLS (CONTINUED)

- The usual claim is that zero-knowledge protocols can achieve the same results than public-key protocols with one to two orders of magnitude less (1/10, 1/100) computing power.
- A typical implementation might require 20–30 modular multiplications (with full-length bit strings) that can be optimized to 10–20 with precalculation.
- This is much faster than RSA.
- The memory requirements seem to be about equal: to have very high security with zero-knowledge protocols, we need very long keys and numbers, so in memory terms, the requirements may not be very different.

PRIVACY IN BEACONS

- Beacon in wireless technology is the concept of broadcasting small pieces of information.
- The information may be anything, ranging from ambient data to vital signs such as body temperature, blood pressure, pulse, and breathing rate or microlocation data such as asset tracking.
- Based on the context, the transmitted data maybe static or dynamic and change over time.
- The Bluetooth beacon opens a new world of possibilities for location awareness, and countless opportunities for smart applications.
- Beacons are becoming one of the key enablers of the IoT.

PRIVACY IN BEACONS (CONTINUED)

- One kind of beacon is a low energy Bluetooth transmitter or receiver.
- The power efficiency of Bluetooth Smart makes it perfect for devices needing to run off a tiny battery for long periods.
- The advantage of Bluetooth Smart is its compatibility to work with an application on the smartphone or tablet you already own.
- An important use case of beacons is to obtain context-specific observations and repeated measurements over time.
- Most data collected from beacons are correlated in time, which might cause serious threats to data security and user privacy.

PRIVACY IN BEACONS (CONTINUED)

- Security and privacy issues specific to beacons and time series data transmitted from them are emerging areas of research interest.
- There are both advantages and disadvantages of security based on the difficulty of an underlying computation problem and information theoretic security, which is based on lack of information content.
- A more basic measure of the information-theoretic security is the inherent information available for exploitation by an adversary, independent of how the adversary exploits it or indeed any assumed computational limitations of the adversary.

PRIVACY IN BEACONS (CONTINUED)

- A new measure of information theoretic measure such as conditional entropy is shown to be suited for evaluating the privacy of perturbed real-world time-series data, compared with other existing measures.
- Much of the research and study of privacy issues in ubiquitous computing systems is applicable to the IoT.
- Establishing meaningful identity, using trusted communication paths, and protecting contextual information is all very important to ensure the protection of user privacy in this environment.
- Anonymous communication techniques and the use of pseudonyms to protect user privacy while also working on metrics to assess user anonymity.

PRIVACY IN BEACONS (CONTINUED)

- A novel approach by hiding identity from the applications that utilize it in order to better protect the user consuming those services.
- New technologies that enable the bootstrapping of trust, and subsequently, the calculation of trust metrics that are better suited to mobile, ad-hoc networks is proposed.
- The model showcases the inherent problems with establishing trust in ad-hoc networks like those in the IoT where new sensors, services, and users are constantly introduced and asked to share data.

PRIVACY IN BEACONS (CONTINUED)

- Finally, applications in the IoT, which will be enabled by a ubiquitous computing and communications infrastructure, will provide unobtrusive access to important contextual information as it pertains to users and their environment.
- Clearly, the successful deployment of such applications will depend on our ability to secure them and the contextual data that they share.

PRIVACY IN BEACONS (CONTINUED)

- One example of sensitive contextual information is location.
- When location-aware systems track users automatically, an enormous amount of potentially sensitive information is generated and made available.
- Privacy of location information is about both controlling access to the information and providing the appropriate level of granularity to individual requestors.
- The Location Services Handbook explores a variety of location-sensing technologies for cellular networks and the coverage quality and privacy protections that come with each.