IoT Security
(Security & Privacy risks of IoT, IoT Security Concerns and ways to resolve them)

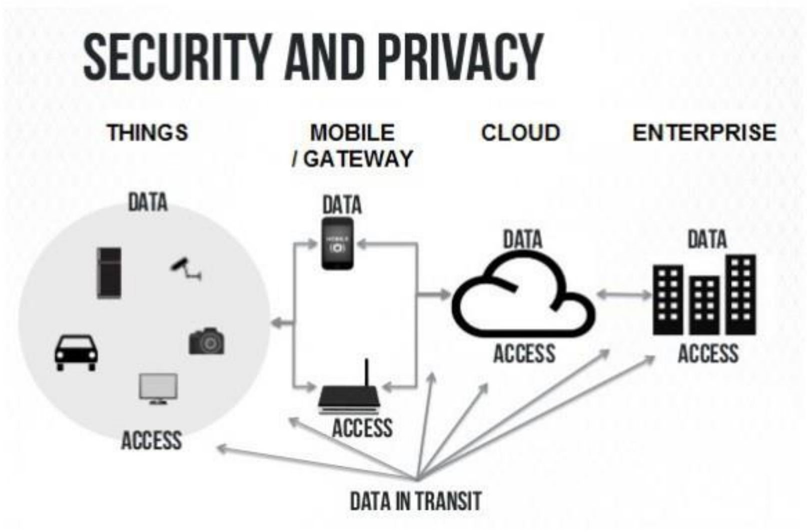
By

Dr Shola Usharani

3rd Module

- Security and privacy risks, analyze security risks, Technologies and methods that mitigate security, Privacy standards and regulations, Social and privacy impacts

SECURITY, PRIVACY RISKS



Issues to IoT security

- Preservation of privacy or secrecy of the data
- Integrity of the data for safety
  - safeguarding of data's completeness and precision during storage and retrieval.
- Staleness or latency permissible in the data share
- Level of restriction of access to or control of the device
- Updating of the software on the device
- Ownership of the device whether to be managed or transferred in a secure manner
- Necessity for the data to be audited

Possibility of Security & Privacy Risks in IoT

- Security Risks:
  - IoT devices are connected to your desktop or laptop.
    - Lack of security increases the risk of your personal information leaking while the data is collected and transmitted to the IoT device.
  - IoT devices are connected with a consumer network.
    - This network is also connected with other systems. So if the IoT device contains any security vulnerabilities, it can be harmful to the consumer's network. This vulnerability can attack other systems and damage them.
  - Sometimes unauthorized people might exploit the security vulnerabilities to create risks to physical safety.
- Privacy Risks
  - in IoT, devices are interconnected with various hardware and software,
    - chances of sensitive information leaking through unauthorized manipulation.
  - All the devices are transmitting the user's personal information
    - name, address, date of birth, health card information, credit card detail and much more without encryption.
- IoT can – intentionally or unintentionally – lead to the direct collection of sensitive personal information
    - as geolocation, financial account numbers, and health information

SECURITY ISSUES

Need of IoT security

- **Malicious nodes**
  - Manipulating the data that is transmitted between network devices.
  - Tampering the devices leads to
    - Theft of sensitive data
    - loss of the consumer privacy
    - Interruption to business operations
- **Denial of service attacks**
  - Slowdown of internet functionality
  - Disruption to critical infrastructure
- Need to **build the IoT ecosystem in high secure and trustworthy** environment.

Need of attending Security

- **Public perception** about smartly connected data
  - 44% of smartly connected information is getting stolen.
  - 27% people worried and hesitated to purchase the connected devices.
- Vulnerability to Hacking
  - The efforts to hack the real time market devices is getting increased
    - Eg: A group of researchers XYZ organization pushed multiple holes in the security of Samsung's SmartThings smart home platform
    - Schlage smart lock
      - hackers could use these vulnerabilities to **seize control of devices** such as smart locks and **smoke detectors** connected to the SmartThings system.
      - The attack began with a spear **phishing email** that would fool users into clicking a link that would take them to the real login page for the SmartThings site. The victim of the hack would then log in, but a flaw in the SmartThings web server would let the attackers steal his or her credentials.
      - then create **a four-digit PIN to unlock** it whenever they wanted
    - fooling users into **downloading malicious apps** from SmartThings' dedicated app store.
- Secure the devices against hackers
    - Is the companies are ready to deliver secure IoT devices .
- True Security
  - Security need to be build both in device level and software level

How Hacking will happen in IoT

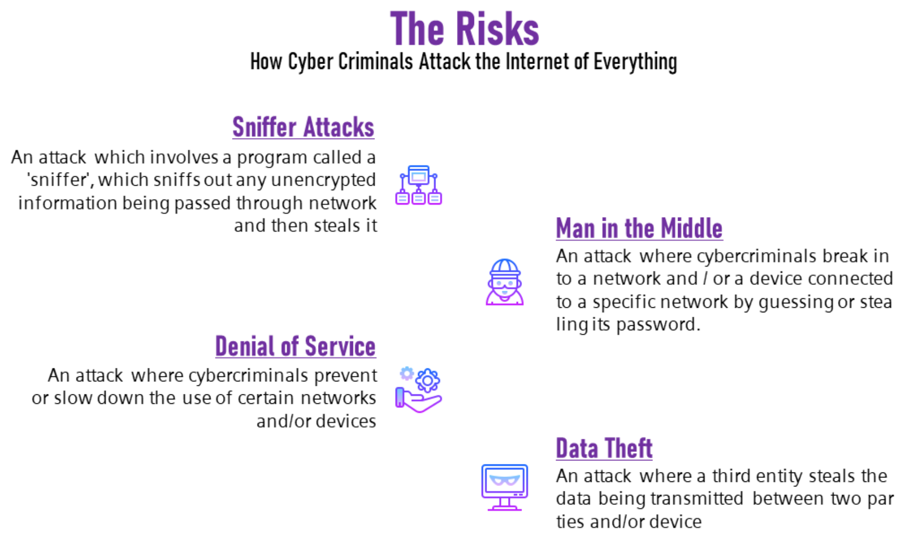
- Man in the middle
  - Connected cars in smart city applications
    - New developments would allow connected cars to link up with smart city infrastructure to create an entirely different ecosystem for the driver, who is simply used to the traditional way of getting from Point A to Point B.
- Denial of Service
  - Connected Health
    - connected healthcare devices give people a deeper and fuller look at their own health services effected
  - Hackers at power grid region
    - ways to strike critical infrastructure, such as power grids, hydroelectric dams, chemical plants, and more.
- Unencrypted data
  - All these connected devices benefits comes with risk, as the increase in connected devices gives hackers and cyber criminals more entry points.
  - Sending the data among those with out security mechanisms

IoT Privacy Issues

- Too Much data
  - data that IoT devices can generate is getting **staggered and huge**.
  - "Internet of Things: Privacy & Security in a Connected World" found that fewer than 10,000 households can generate 150 million discrete data points *every day*. This creates more entry points for hackers and leaves sensitive information vulnerable.
- Collection of Public data
  - Agreeing the terms during the service point with out reading.
  - Many companies collects the consumer data for their company decision usages.
    - Example : an insurance company might gather information from you about your driving habits through a connected car when calculating your insurance rate and for health care insurances too.
- Eavesdropping
  - **Intercepting the unencrypted data**.
  - Hackers connected to consumer connected home device.
    - A smart meter device is used to determine what information is watching in the TV by that moment.
- Confidence of consumer data
  - check for consumer to proceed to purchase the products

Risks in the internet

- Sniffer Attacks
  - An attack which involves a program called a ‘sniffer’ which sniffs(obtains) out any unencrypted information being passed through a network and then steals it.
- Man in the middle
  - A device connected to the network by guessing or stealing its password.
  - Stealing data between two parties or device.
- Denial of service
  - An attack where cyber criminals prevent or slow down the use of certain networks and/or devices.
- Device Security
  - Edge devices, Gateways, Access points



The Risks

How Cyber Criminals Attack the Internet of Everything

Sniffer Attacks

An attack which involves a program called a 'sniffer', which sniffs out any unencrypted information being passed through network and then steals it

Man in the Middle

An attack where cybercriminals break in to a network and / or a device connected to a specific network by guessing or stealing its password.

Denial of Service

An attack where cybercriminals prevent or slow down the use of certain networks and/or devices

Data Theft

An attack where a third entity steals the data being transmitted between two parties and/or device

Addressing IoT Security

- Access level
- Encryption of data
- Enabling the security practices
  - through unique procedure of username and password.
    - Automatic closure of the access beyond specific time of inactivity.
  - Use hardware that incorporates security features to strengthen the protection and integrity of the device.
    - For example, computer chips with integrate security at the module/component level, embedded in the processor and provide encryption and anonymity. This is to enable encrypted transaction.

What is IoT device security

- It is
  - To **stop hackers from gaining access to each device** and its data is the main challenge.
  - Properly and consistently **monitoring devices** and planning regular updates to firmware and security protocols
  - There are many IoT devices out there with different hardware configuration and operating systems. These variations make it impossible to **deploy a one-size-fits-all** solution.
  - Security platform for IoT devices is different from security practices for a web application or software platform .

Security Ways for IoT Devices

- Device communication
- Install security
- Password/passcode communication
- IP white listing filters
- SMS text messaging

Device communication

- Exchanging the messages with IoT platforms or other devices/hubs.
  - Supports public/private key encryption.
    - Uses TLS/SSL encryption
    - Can use generate X.509 certificates to use for TLS/SSL communication. These certificates are easier to manage and do not expire
  - Use of private key encryption at the device level.
    - Use separate private keys for each device to stop the compromised node instead of the entire operation.
  - A digital certificate is used to ensure authenticity.
    - Digital certificates issued by a trusted Certification Authority (CA) expire after a certain period
      - easy way to remotely update the digital certificate for device firmware.

Install security

- Drawbacks of previous approach
  - requires a lot of resources, such as memory and processing power.
  - Not supported by many IoT devices
- Installs the security patch.
  - Uses the required unique piece of information as part of the communication.

Password/passcode communication

- IoT devices send a password/passcode along with every command .
- During deployment of the device uses default password.
- The IoT software responsible for communicating with these devices should change the default password at the time of activation.
- The passwords for the devices should be kept securely (encrypted) in the IoT software layer.

IP white listing filters

- It is a filter for untrusted messages at device level.
- It is implement by using static IP address or range of IPs.
- With a static IP address, the known static IP list filters the messages coming into the IoT software layer from devices.
- The communication happens between devices does not happen directly but it is through a broker.

SMS text messaging

- IP-enabled, IoT devices keep a port open for the incoming traffic.
  - Keeping this port open, in listening mode, drains the battery. Some applications prefer to be in sleep mode to save battery.
  - It is even for unsecure connections.
- SMS text messaging can send an instruction to wake a device when no open communication port is available.
- SMS text messages will be sent through SMPP gateways is a common commercial solution.
- Sending SMS text messages requires the use of a phone number, or a set of phone numbers.
- IoT devices can keep a list of trusted numbers to quickly discard messages from unknown sources.

Recommendations for IoT ecosystem security

- Enable all security features on small devices
- Always keep the firmware of smart devices updated.
- Close any unused ports on all devices and routers
- Use secure passwords
- Patch the vulnerabilities as soon as they are announced.
- Utilize encryption for network and smart devices

Issues to Address Security Point of View

- Preservation of **privacy or secrecy** of the data.
- **Integrity** of the data for safety.
- **Staleness** in the data share.
- **Level of restriction of access** to or control of the device.
- **Updating of the software** on the device.
- **Ownership of the device** whether to be managed or transferred in a secure manner.
- **Necessity for the data** to be audited.

References

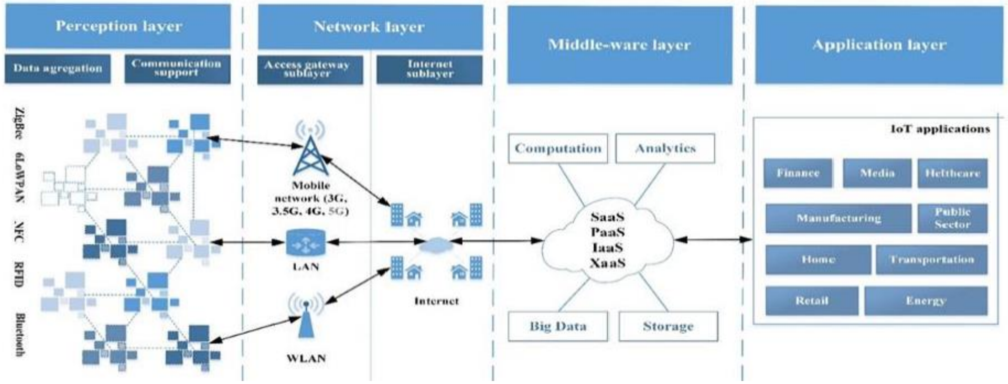
- https://www.businessinsider.com/iot-security-privacy?IR=T
- https://medium.com/@arindey/internet-of-things-iot-security-privacy-applications-trends-3708953c6200
- https://datasilk.com/iot-cybersecurity/
- IotT nasscom text book
- IoT ebook

Analysis of Security risks

Introduction

- IoT layered architecture
- Security risks based on the layer of each layer in architecture
- Vulnerable layers risks, protection implementation methods based on the application.
- Risk classification in each layer

Architecture of IoT Concept



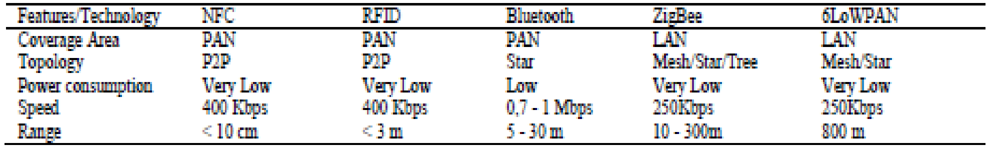
- Perception layer
  - Data collection and collaboration among the elements of the same layer.
- Network layer
  - Two sub layers
    - Access sublayer
      - collecting the data from perception layer and sending it to the Internet sublayer
    - Internet sublayer
      - the backbone of IoT environment and its main task is the transfer of data to the next layer, middleware
- Middle layer
  - Responsible for data collecting, its filtering, transformation and the intelligent processing most commonly with the use of cloud computing concept.
- Application layer
  - After processing, the data is passed to the application layer, which uses the given data in order to provide and present various services to the end user

Security aspects of IoT architecture layers

- *Security aspect of* the perception layers.
- *Security aspect of the network layer*
- *Security aspect of the middleware layer*
- *Security aspect of the application layer*

Security aspect of the perception layers

- The devices of perception layer have limited process and data storage resources
- Applied technologies for limited data transmission range and rate
  - – RFID/NFC, Bluetooth, ZigBee and 6loWPAN
- Basic features of each transmission technology



Features/Technology	NFC	RFID	Bluetooth	ZigBee	6LoWPAN
Coverage Area	PAN	PAN	PAN	LAN	LAN
Topology	P2P	P2P	Star	Mesh/Star/Tree	Mesh/Star
Power consumption	Very Low	Very Low	Low	Very Low	Very Low
Speed	400 Kbps	400 Kbps	0,7 - 1 Mbps	250Kbps	250Kbps
Range	< 10 cm	< 3 m	5 - 30 m	10 - 300m	800 m

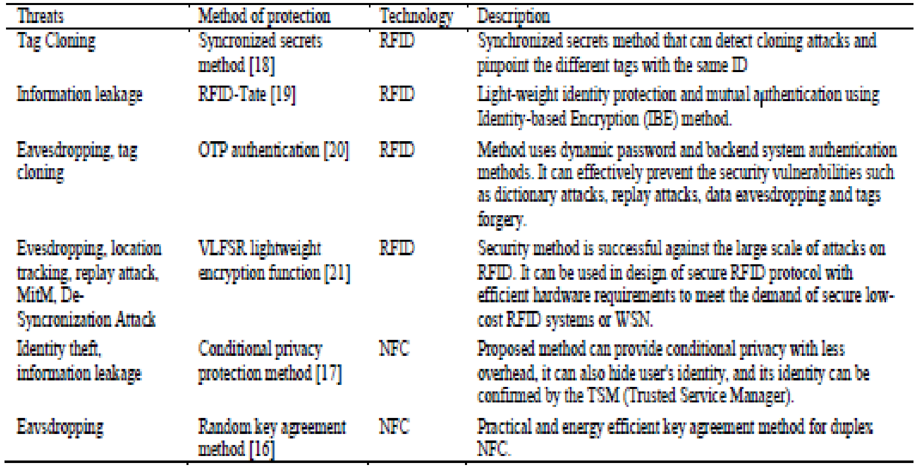
Security aspects of RFID

- Used mostly for the automated information exchange.
- Security disadvantages of this technology.
- Unauthorized access of the content
  - – Lack of adequate authentication mechanisms in a number of RFID tags.
  - – the content of the tag is not easy to read, the unauthorized alteration of its content or its deletion is very possible.
- The attack on the availability of RFID tags can be carried out through a **DoS attacks.**
  - – the **failure of transmission of identification** information stored in the tags.
  - – Threats against the confidentiality of the data include attacks such **as tag monitoring** with the use of an unauthorized reader which can result in the interception of **sensitive information** such as street addresses, phone numbers, and identification tags (Ration card based website application).
  - – Attacks on the data integrity are related to unauthorized **tag cloning** with the use of unauthorized readers which allow cloning in order to bypass implemented protection methods.
- RFID technology are also vulnerable on **eavesdropping, MitM attacks, spoofing**, and others.

Security aspects of NFC

- The technology is based on the principles and the relations between magnetism and the electricity, or on the principles of the inductive loop.
- NFC technology is vulnerable to many threats such as eavesdropping, unauthorized manipulation of data and MitM attacks

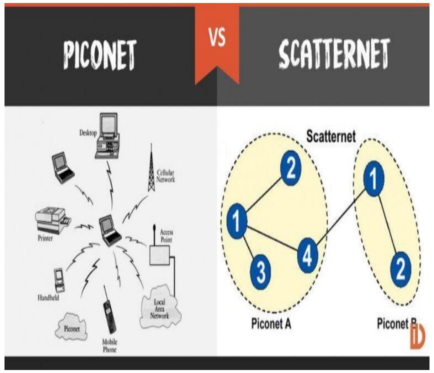
Threats and the protection methods for the RFID and NFC technology



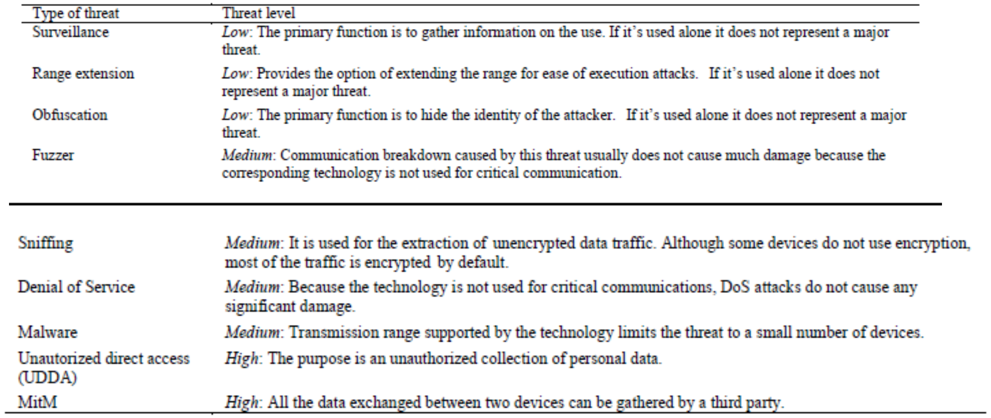
Threats	Method of protection	Technology	Description
Tag Cloning	Syncronized secrets method [18]	RFID	Synchronized secrets method that can detect cloning attacks and pinpoint the different tags with the same ID
Information leakage	RFID-Tate [19]	RFID	Light-weight identity protection and mutual apthentication using Identity-based Encryption (IBE) method.
Eavesdropping, tag cloning	OTP authentication [20]	RFID	Method uses dynamic password and backend system authentication methods. It can effectively prevent the security vulnerabilities such as dictionary attacks, replay attacks, data eavesdropping and tags forgery.
Evesdropping, location tracking, replay attack, MitM, De-Syncronization Attack	VLFSR lightweight encryption function [21]	RFID	Security method is successful against the large scale of attacks on RFID. It can be used in design of secure RFID protocol with efficient hardware requirements to meet the demand of secure low-cost RFID systems or WSN.
Identity theft, information leakage	Conditional privacy protection method [17]	NFC	Proposed method can provide conditional privacy with less overhead, it can also hide user's identity, and its identity can be confirmed by the TSM (Trusted Service Manager).
Eavsdropping	Random key agreement method [16]	NFC	Practical and energy efficient key agreement method for duplex NFC.

Security aspect of the Bluetooth technology

- Bluetooth is a wireless communication technology for short-range communication. The technology enables the creation of Adhoc-piconet network between two or more devices.



The threats intended for the Bluetooth technology



Type of threat	Threat level
Surveillance	*Low*: The primary function is to gather information on the use. If it's used alone it does not represent a major threat.
Range extension	*Low*: Provides the option of extending the range for ease of execution attacks. If it's used alone it does not represent a major threat.
Obfuscation	*Low*: The primary function is to hide the identity of the attacker. If it's used alone it does not represent a major threat.
Fuzzer	*Medium*: Communication breakdown caused by this threat usually does not cause much damage because the corresponding technology is not used for critical communication.
Sniffing	*Medium*: It is used for the extraction of unencrypted data traffic. Although some devices do not use encryption, most of the traffic is encrypted by default.
Denial of Service	*Medium*: Because the technology is not used for critical communications, DoS attacks do not cause any significant damage.
Malware	*Medium*: Transmission range supported by the technology limits the threat to a small number of devices.
Unautorized direct access (UDDA)	*High*: The purpose is an unauthorized collection of personal data.
MitM	*High*: All the data exchanged between two devices can be gathered by a third party.

Security methods for Bluetooth

- protection methods that are based on authentication and encryption.
- four modes of protection
  - Security mode 1:
    - does **not require authentication** and encryption
  - Security mode 2:
    - applies authentication and encryption exclusively for individual services such **as data transfer**
  - Security mode 3 :
    - forces authentication, and encryption before the connection with the **device is established**
  - Security mode 4:
    - uses a simple method of pairing with the aim of establishing security on the **service level**

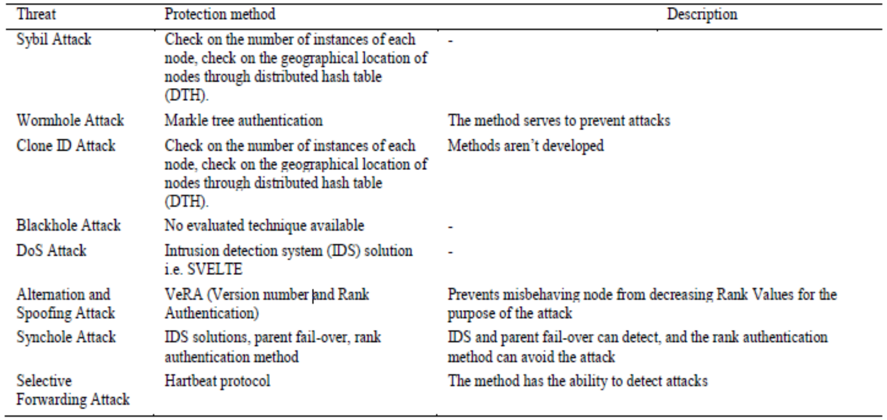
The security aspect of the ZigBee technology

- The ZigBee technology plays an important role in the formation of WSN because of **low cost, high reliability, low complexity** and variety of application in the IoT environment.
- The advantages of this technology are the autonomy, flexibility, scalability and low cost of the devices.
- security threats of the ZigBee technology are
  - **the unauthorized traffic gathering, packet decoding and data manipulation.**
    - For example, unauthorized access to a sensor node within a ZigBee network gives access to the shared secret key of the network and thus the traffic within the network.
  - the **sabotage (damage) of terminal devices** in the ZigBee network with the purpose of the exhaustion (by gaining the access of the unfairly)of the battery capacity and the exploitation of the key exchange process

The security aspect of the 6LoWPAN technology

- IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is a communication technology that enables connectivity of the **hardware limited devices (sensors, actuators, etc.) onto IPv6 network.**
- It has an increasing role in the IoT environment due to the high presence of devices with **limited processing, memory**, and the other features.

Threats and protection methods of the 6LoWPAN technology



Threat	Protection method	Description
Sybil Attack	Check on the number of instances of each node, check on the geographical location of nodes through distributed hash table (DTH).	-
Wormhole Attack	Markle tree authentication	The method serves to prevent attacks
Clone ID Attack	Check on the number of instances of each node, check on the geographical location of nodes through distributed hash table (DTH).	Methods aren't developed
Blackhole Attack	No evaluated technique available	-
DoS Attack	Intrusion detection system (IDS) solution i.e. SVELTE	-
Alternation and Spoofing Attack	VeRA (Version number and Rank Authentication)	Prevents misbehaving node from decreasing Rank Values for the purpose of the attack
Synchole Attack	IDS solutions, parent fail-over, rank authentication method	IDS and parent fail-over can detect, and the rank authentication method can avoid the attack
Selective Forwarding Attack	Hartbeat protocol	The method has the ability to detect attacks

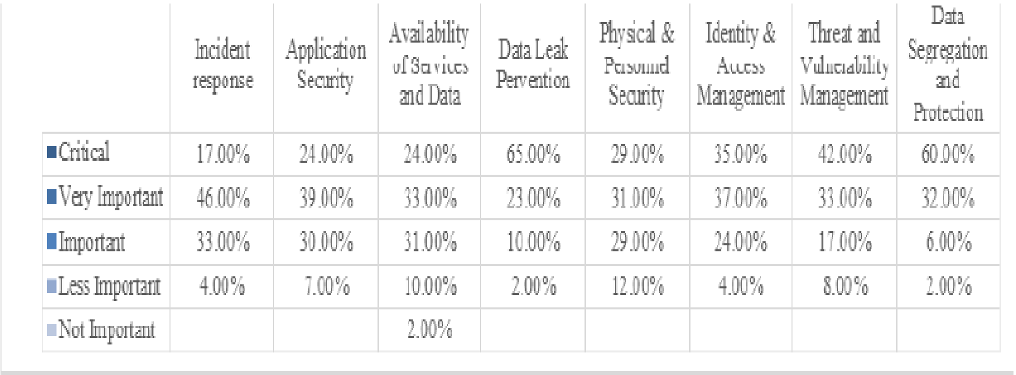
Security aspect of the network layer

- The network layer is the backbone of every information and communication environment.
- The network layer of IoT concept consists of the access sublayer and the Internet sublayer.
  - The access sublayer is used for the perception layer data acquisition, and for transferring the data to the core network by Internet sublayer, which forwards received data to the middleware layer.
- Typical **security problems of this layer are traditional security problems**, or communication networks security problems that affect
  - confidentiality, availability and integrity of data.
  - The most common security challenges are unauthorized network access, **eavesdropping, confidentiality breaches, integrity violation, DoS attacks, MitM attacks**, etc.
- There are security concerns at this layer, protection methods are numerous and are well defined regarding other layers of the IoT concept.

Security aspect of the middleware layer

- It is based on cloud computing because of its benefits, such as delivery of **computing resources as a service to end** users, flexibility, scalability, etc.
- This makes it suitable for **processing large amount of data** collected on the perception layer and the presentation of processed data to end users through a variety of applications.
- Due to the **rapid evolution and a high acceptance** degree, this concept has a **large number of threats and vulnerabilities** that inherit the middleware layer of the IoT concept based on cloud computing.
- The **public or hybrid cloud computing model**, where a single physical server can contain multiple virtual machines from different IoT service providers or even the **presence of malicious users** with the possibility to gain **unauthorized access to other virtual machines** and to manipulate stored data.

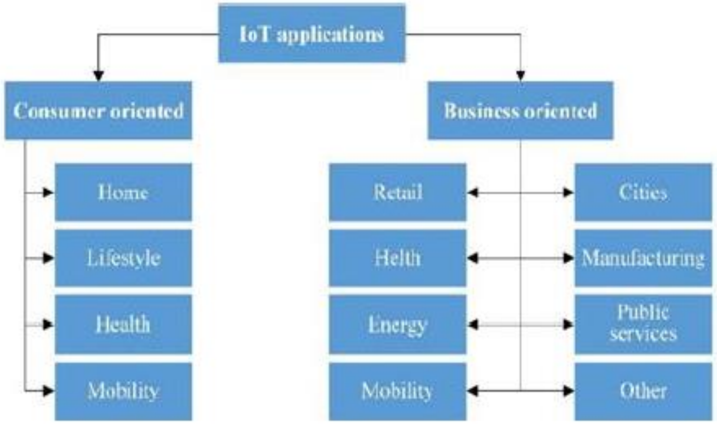
The presentation of the threats in Cloud Computing



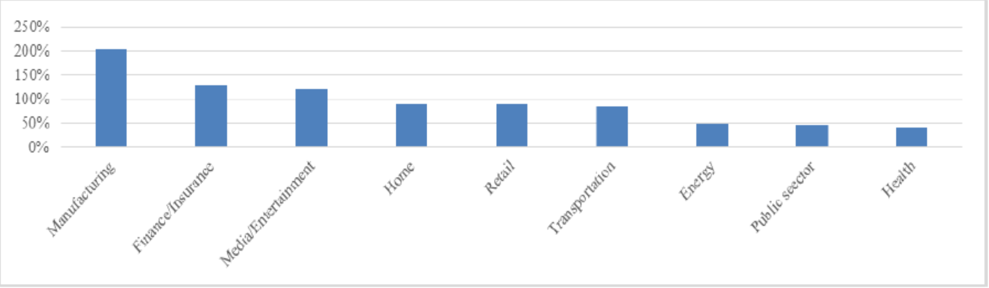
	Incident response	Application Security	Availability of Services and Data	Data Leak Pervention	Physical & Personnel Security	Identity & Access Management	Threat and Vulnerability Management	Data Segregation and Protection
■Critical	17.00%	24.00%	24.00%	65.00%	29.00%	35.00%	42.00%	60.00%
■Very Important	46.00%	39.00%	33.00%	23.00%	31.00%	37.00%	33.00%	32.00%
■Important	33.00%	30.00%	31.00%	10.00%	29.00%	24.00%	17.00%	6.00%
■Less Important	4.00%	7.00%	10.00%	2.00%	12.00%	4.00%	8.00%	2.00%
■Not Important			2.00%					

Security aspect of the application layer

- The increase in the usage results in a greater number of applications and their instances, and thus a larger number of the existing devices and the transmitted data.



Usage of IoT concepts in each sector



The largest increase in the use of the IoT concept was recorded in the manufacturing sector and amounted to 204%, followed by the financial sector with a 128%, multimedia sector with 120% and the home sector with 89%

Which risks need to address among all four layer or which layer security is still need to address?

Risk Classification of IoT layers

- Three kinds of security risks for IoT layers; High, Medium and Low.
  - Perception Layer (high security risk)
  - Network layer (Low to Medium)
  - Middle Layer (Medium)
  - Application Layer (High, Medium and Low)

Perception layer

- Perception Layer (high security risk) **very large hardware** limitations that prevent the implementation of robust protection methods of the data collected, stored and transmitted at this layer.
- The risk level is also contributed by the **heterogeneity of the devices** within the perception layer which makes the establishment of security and **the standardization** of communication protocols more difficult

Network Layer

- Access sublayer
  - Risk level from Low to Medium
  - the known wireless data transfer standards, as well as known threats in access networks.
  - research of the vulnerabilities and the continuous development of protection methods in the field of computer networks,
  - robust protection methods assured from the devices used at the network layer.
- Internet sublayer
  - Risk level is Low
  - complex extraction of data transmitted from the access layer to the middleware layer
  - Threats that can exploit the vulnerabilities in routing protocols and publicly available routers are various forms of DDoS attacks that can disrupt the availability within the IoT environment.

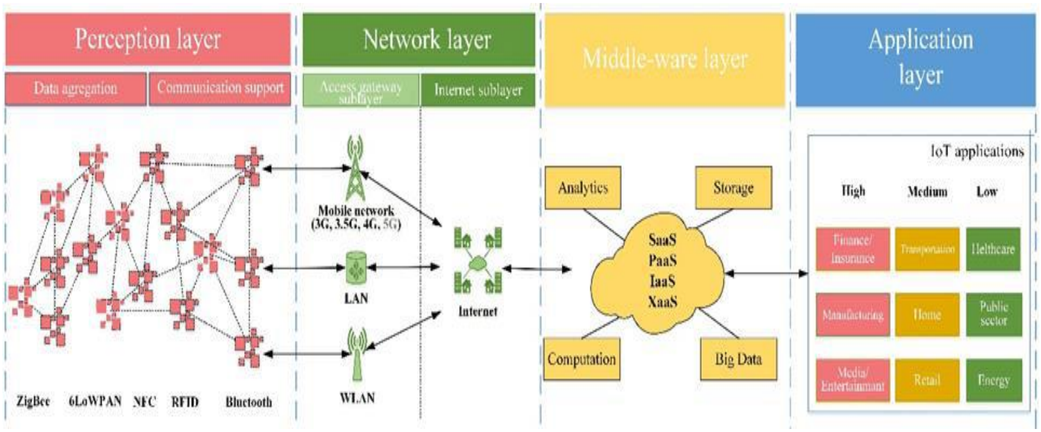
Middle Layer

- Medium security risk level
- large number of users and the data to be stored and processed within the layer.
- known vulnerabilities of virtualization whose exploitation can cause extensive simultaneous damage to a large number of users.
- Services related to threats and vulnerability is already implemented .

Application Layer

- Risk classification for the use of the IoT concept in various environments according to the increase of the use of IoT concept in a particular environment, as presented through
- According to the presented data the largest increase in the use of IoT concept relates to the manufacturing sector (204%), followed by the financial sector (128%) and the multimedia sector (120%),
  - which is the reason for manufacturing sectors of the IoT concept to be classified as High security risk level.
  - Sectors house (89%), sales (88%) and transport (83%) are classified as Medium security risks level,
  - while energy (49%), public (46%) and healthcare (40%) sectors are classified as Low security risk level.

Presentation of the risks of the IoT architecture layers



References

- Ivan Cvitić, Miroslav Vujić, Siniša Husnjak, “**CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT**”, 26TH DAAAM INTERNATIONAL SYMPOSIUM ON INTELLIGENT MANUFACTURING AND AUTOMATION, 2016.

IoT Security

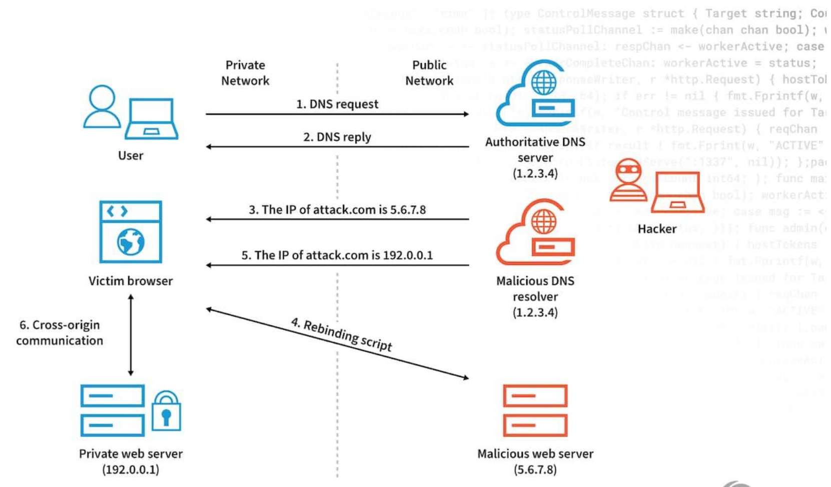
(DNS rebinding):

a type of cyberattack that leverages the Domain Name System (DNS) to run malicious JavaScript and attack devices on a user's private network

End of the session

- What is Impact of DNS Rebinding attack?
- What is DNS Rebinding attack?
- Suggest the solutions to consider?

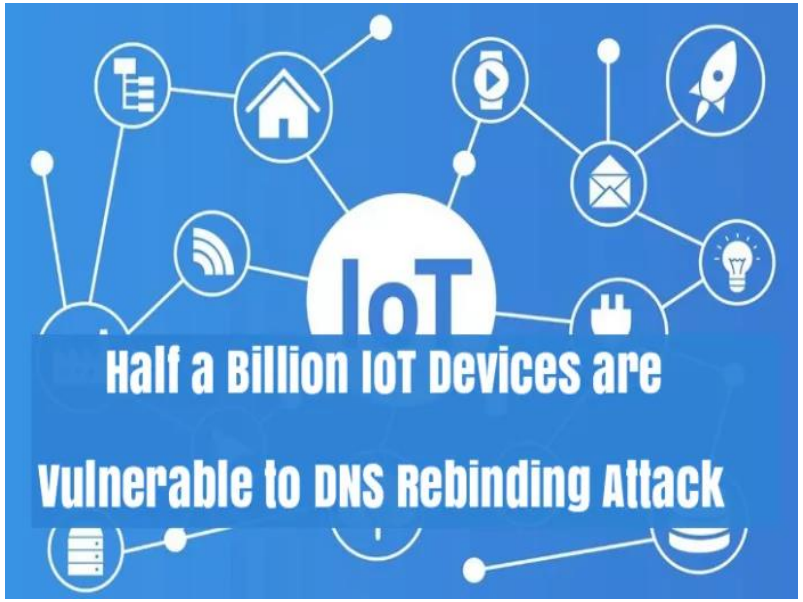
DNS Rebinding Attack



Private Network
Public Network
User
1. DNS request
2. DNS reply
Authoritative DNS server (1.2.3.4)
Hacker
Victim browser
3. The IP of attack.com is 5.6.7.8
5. The IP of attack.com is 192.0.0.1
Malicious DNS resolver (1.2.3.4)
6. Cross-origin communication
4. Rebinding script
Private web server (192.0.0.1)
Malicious web server (5.6.7.8)

What is DNS rebinding?

- The upside of IoT is that we are able to do things we never before imagined.
- But as with every good thing, there’s a downside to IoT.
- It is becoming an increasingly attractive target for cybercriminals.
- More connected devices mean more attack vectors and more possibilities for hackers to target us.

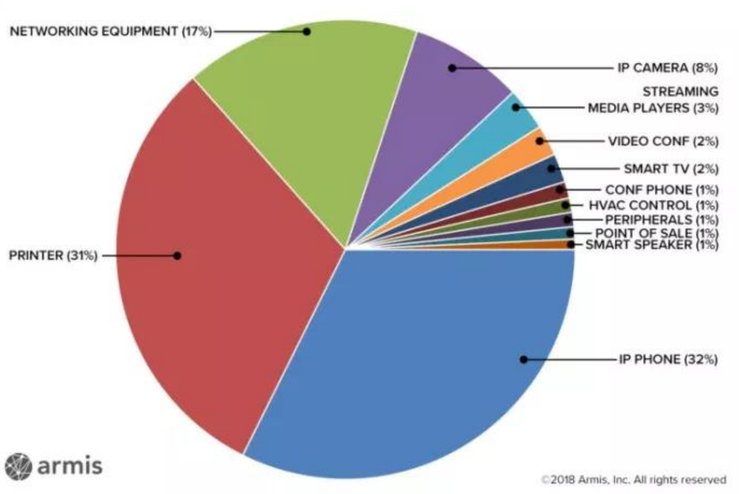

IoT
Half a Billion IoT Devices are
Vulnerable to DNS Rebinding Attack

DNS rebinding

- an attack method that has been known for more than a decade,
- allows a remote hacker to **bypass the targeted entity's network firewall** and
- Misuse the web browser to directly communicate with devices on the local network and
- **exploit any vulnerabilities they may have**.
- Getting **the target to access a malicious page or view a malicious advertisement** is often enough to conduct an attack that can **lead to theft of sensitive information and taking control** of vulnerable devices.

- A new researcher revealed that Half a Billion home and enterprise based devices – IoT Devices are vulnerable to DNS Rebinding **Attack including IP phones, printers, networking equipment and cameras**.
- DNS Rebinding Attack taking advantage of the **outdated web browsers that allow to redirect victims to the malicious domain** and
- **Compromise the network** where it uses the **network firewall web browser as a proxy to communicate with vulnerable local network devices.**

Almost All IoT Device Model's are Vulnerable



©2018 Armis, Inc. All rights reserved

- **The printer** is one of the **least managed IoT devices** in most of the enterprise typically deploy printers with **default settings which could be one the main loophole** for an attacker to compromise the target and exfiltrate information by downloading documents scanned, stored, or cached on the printer.

- Enterprise networks should use **best IDS, IPS protection system** to keep their network safe and secure from IoT based attacks.
  - IDS : Intrusion detection system
  - IPS: Intrusion prevention system

How does this DNS Rebinding Attack Works

1. Initially, this attack started via **Phishing email** that used **to compromise users and takes him or her to a malicious site** which contains malicious Javascript to run on the victims local browser.
2. It is Avoiding the firewall protection:
   - Attackers using an **obfuscation technique to avoid detection by a firewall, network security solution, or even endpoint protection.**
3. **Scan the local network** to detect the presence of a particular **type of IoT device which can accomplish by DNS rebinding** and JavaScript the malicious command will scan the local IP address and send back to the malicious website.
4. **The malicious website sends an appropriate set of commands to the end user's browser** — for example, commands to log into the HTTP web server of a security camera on the internal network.
5. Using **DNS rebinding Browser** can able to sends those commands directly to the IP address owned IoT device inside of the targeted organization.
6. Establish an **outbound connection to a C&C server**, directly from the compromised IoT/unmanaged device since the firewall typically considers outbound connections to be safe.

Mitigation

- Placing a **web-application firewall** (WAF) can filter out the malicious Backdoor shell access and isolate the **browser based attacks**.
- Implement the highly recommended **backdoor shell protection** to avoid attacker control the vulnerable device remotely.
- Protect your web applications from vulnerabilities with Worlds best **WAF solutions.**

NASA's system hacked with a $25 Raspberry Pi - 21 Jun 2019

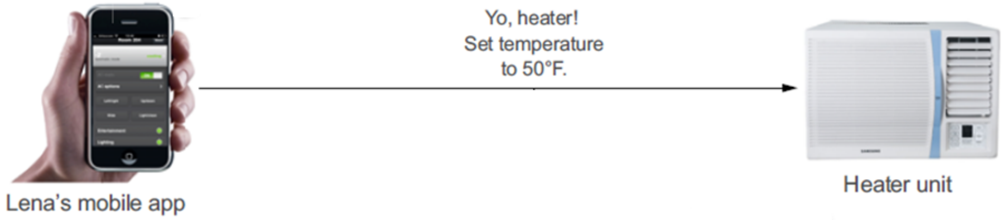
- Despite advancing significantly in space technology, NASA has persistently faced cybersecurity-related issues.
- the agency's **Jet Propulsion Laboratory** had suffered a major breach, one that compromised **critical mission-related data**.
- the attack was conducted with Raspberry Pi, a low cost, credit-card-sized computer that plugs into a computer monitor/TV.

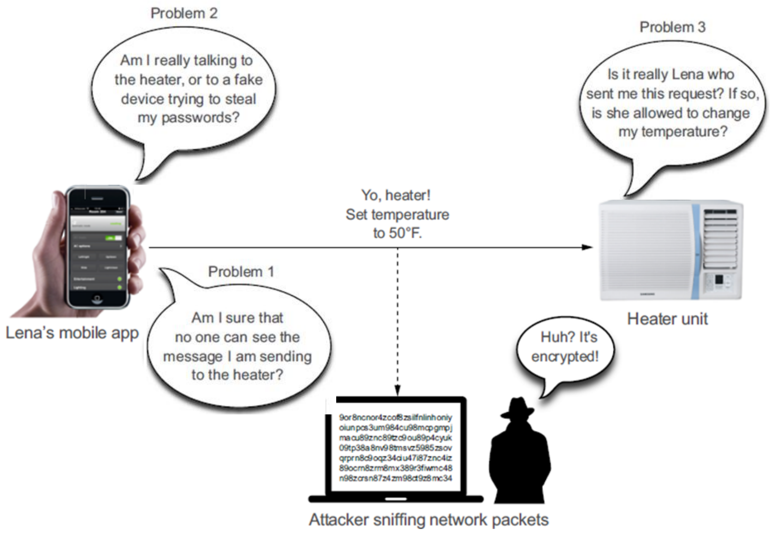
Basic, build-it-yourself Raspberry Pi used for hacking

- Raspberry Pi has long been serving as a basic, build-it-yourself computing machine, one that costs just around $25-35.
- Report from the US Office of the Inspector General has revealed that a **cyber snooper used the same computer to break into two of JPL's network and stole as much as 500 megabytes of data from 23 files on their system.**

Security for the Internet of Things:

A Survey of Existing Protocols and Open Research issues




Problem 2
Am I really talking to the heater, or to a fake device trying to steal my passwords?
Problem 3
Is it really Lena who sent me this request? If so, is she allowed to change my temperature?
Yo, heater! Set temperature to 50°F.
Lena's mobile app
Heater unit
Problem 1
Am I sure that no one can see the message I am sending to the heater?
Huh? It's encrypted!
Attacker sniffing network packets

Six IoT Security Technologies

- **IoT network security**
- **IoT authentication**
- **IoT encryption**
- **IoT PKI**
- **IoT security analytics**
- **IoT API security**

IoT network security

- **Protecting and securing the network connecting IoT devices to back-end systems on the internet.**
- IoT network security is a bit more challenging than traditional network security because
- there is a wider range of **communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity**.
- Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems.

IoT authentication

- Providing the ability for users to authenticate an IoT device,
- including managing multiple users of a single device (such as a connected car),
- ranging from simple **static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics.**
- Unlike most enterprise networks where the authentication processes involve a human being entering a credential,
- many IoT authentication scenarios (such as embedded sensors) are **machine-to-machine based without any human intervention**.

IoT Encryption

- Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers.
- The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols.
- Moreover, all IoT encryption must be accompanied by equivalent **full encryption key lifecycle management processes,** since poor key management will reduce overall security.

IoT PKI (Public Key infrastructures)

- Providing complete **X.509 digital certificate** and cryptographic key and life-cycle capabilities,
- including public/private key generation, distribution, management, and revocation.
- The **hardware specifications for some IoT devices may limit or prevent their ability to utilize PKI**.
- Digital certificates can be securely loaded onto IoT devices at the time of manufacture and
- then activated/enabled by third-party PKI software suites; the certificates could also be installed post-manufacture.

IoT security analytics

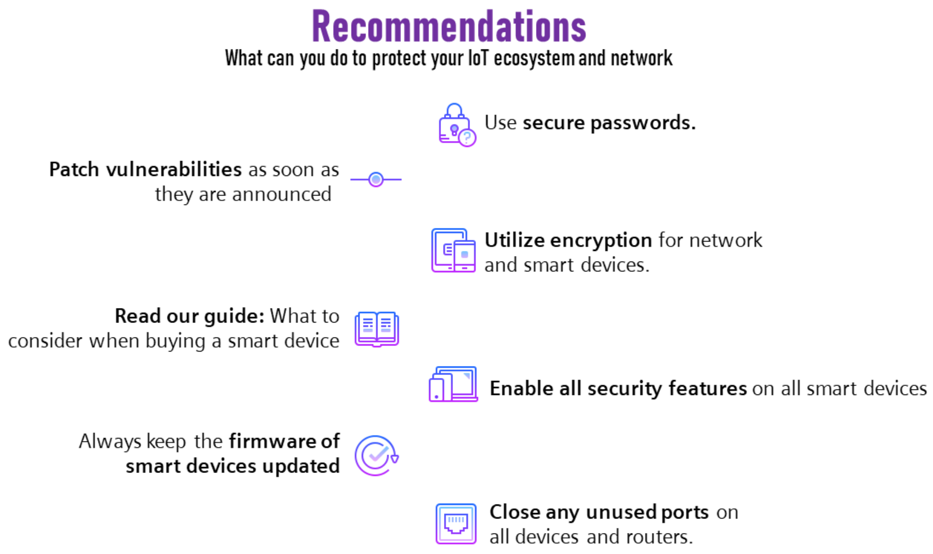
- **Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting** on specific activities or when activities fall outside established policies.
- These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging.
- IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls.

IoT API security

- Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs.
- API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs.

- **IoT network security:** Bayshore Networks, Cisco, Darktrace, and Senrio.
- **IoT authentication:** Baimos Technologies, Covisint, Device Authority, Entrust Datacard, and Gemalto.
- **IoT encryption:** Cisco, Entrust Datacard, Gemalto, HPE, Lynx Software Technologies, and Symantec.
- **IoT PKI:** DigiCert, Entrust Datacard, Gemalto, HPE, Symantec, and WISeKey.
- **IoT security analytics:** Cisco, Indegy, Kaspersky Lab, SAP, and Senrio
- **IoT API security:** Akana, Apigee/Google, Axway, CA Technologies, Mashery/TIBCO, MuleSoft, and WS02.

Privacy standards and regulations (IoT security standards & guidelines)



Recommendations

What can you do to protect your IoT ecosystem and network

Use **secure passwords.**

Patch vulnerabilities as soon as they are announced

Utilize encryption for network and smart devices.

Read our guide: What to consider when buying a smart device

Enable all security features on all smart devices

Always keep the **firmware of smart devices updated**

Close any unused ports on all devices and routers.

Best Practices or Recommendations that must be taken to enhance IoT security:

- **No universal or easily guessed pre-set passwords.**
  - **Strong password settings**
- **Data should be transmitted and stored securely using strong encryption.**
- **Data collection should be minimized to only what is necessary for a device to function.**
- **Devices should be capable of receiving security updates and patches.**
- **Device manufacturers should notify consumers if there is a security breach.**
- **Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.**

Need of IoT Security standards

- First, **governments and regulatory agencies** increasingly considering the promotion of IoT security.
- Second, the **analysis reveals that the IoT security standards** landscape is dominated by de facto standards initiated by a diverse range of industry associations across the IoT ecosystem.
- Third, **identifies a number of key challenges for IoT security standardization**, setting a baseline for IoT security across all IoT applications and domains

Reasons for IoT Security standards

- To protect assets based on certification purposes
- To achieve interoperability
- For regulatory compliance
  - Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business processes.
- To comply with public tendering requirements
- for market intelligence purposes
- Policy makers, regulatory agencies and the industry agreeing
  - IoT security is required to ensure data protection, service continuity and public safety

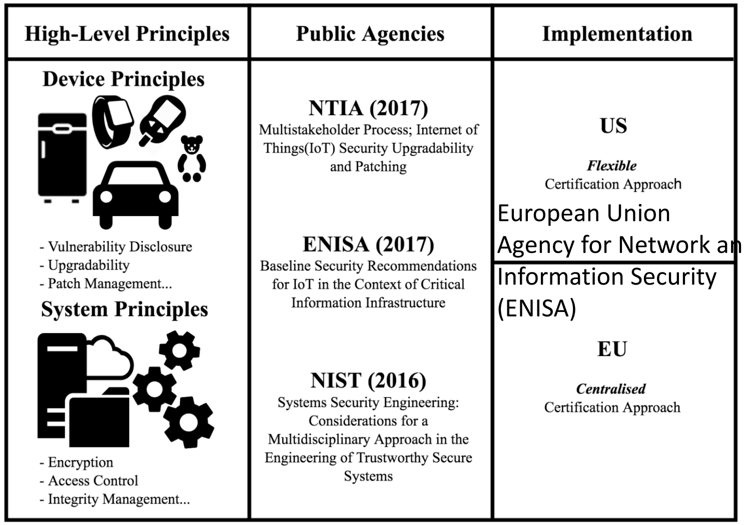
Standardisation includes

- Principles, guidelines, codes of practice and technical specifications
- These are developed by **public, private and non-for-profit entities**, including government departments and agencies, national standardization bodies, industry alliances and associations
- standards for specific domains, such as connected autonomous vehicles, medical devices and industrial applications.

What are policies, Regulatory Frameworks and High-Level Guidelines for IoT Security

- Policies are **data protection impact assessments** or **cybersecurity risk assessments** for organizations
  - It is used to provide new technologies and **essential services that result in a high risk to the rights** and freedoms of individuals or the integrity of critical infrastructure.
- security guidelines for **specific IoT applications** have been put forward such as the '**Key Principles of Cyber Security for Connected and Automated Vehicles**' developed by Some group of (example,HMG) people.
  - Department for Transport Strategic Principles for Securing the IoT',
    - proposing an integrated, end-to-end approach to securing the IoT based on security by design as well as continuous product, system and business lifecycle risk assessment.
- Regulatory frameworks are the specialized agencies from **government bodies or group of people have** also promoted as non-binding cybersecurity guidelines and recommendations for various sectors like automated vehicles and for medical devices.

Agencies covering IoT Security legislations and guidelines(EU,US)



High-Level Principles	Public Agencies	Implementation
Device Principles - Vulnerability Disclosure - Upgradability - Patch Management... System Principles - Encryption - Access Control - Integrity Management...	NTIA (2017) Multistakeholder Process; Internet of Things(IoT) Security Upgradability and Patching ENISA (2017) Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructure NIST (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	US *Flexible* Certification Approach EU *Centralised* Certification Approach

the National Telecommunications and Information Administration (NTIA)

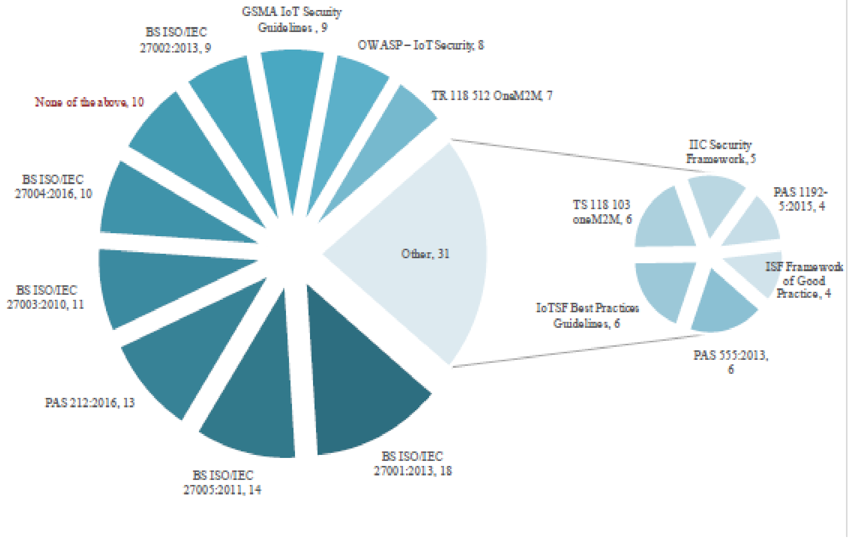
European Union Agency for Network and Information Security (ENISA)

US National Institute of Standards and Technology (NIST)

PETRAS IoT

- **The PETRAS National Centre of Excellence exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely.**
- **It does by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.**
- Types of standards are given by formal regional and international standardization organizations, and by transnational industry associations and alliances
  - ISO/IEC 27000 series
  - Formal
  - De Facto

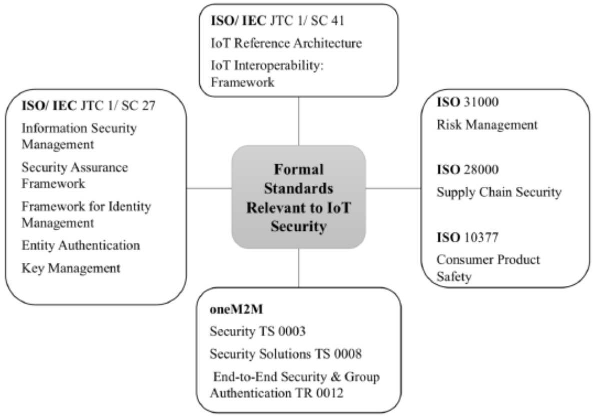
Standards related to IoT Cyber security



ISO/IEC 27000 series

- The development of formal security standards specific to the IoT which take into account both **device and end-to-end security.**
- standards **does not apply to all components of the IoT ecosystem**

Formal standards



ISO/ IEC JTC 1/ SC 41
IoT Reference Architecture
IoT Interoperability: Framework

ISO/ IEC JTC 1/ SC 27
Information Security Management
Security Assurance Framework
Framework for Identity Management
Entity Authentication
Key Management

Formal Standards Relevant to IoT Security

ISO 31000
Risk Management
ISO 28000
Supply Chain Security
ISO 10377
Consumer Product Safety

oneM2M
Security TS 0003
Security Solutions TS 0008
End-to-End Security & Group Authentication TR 0012

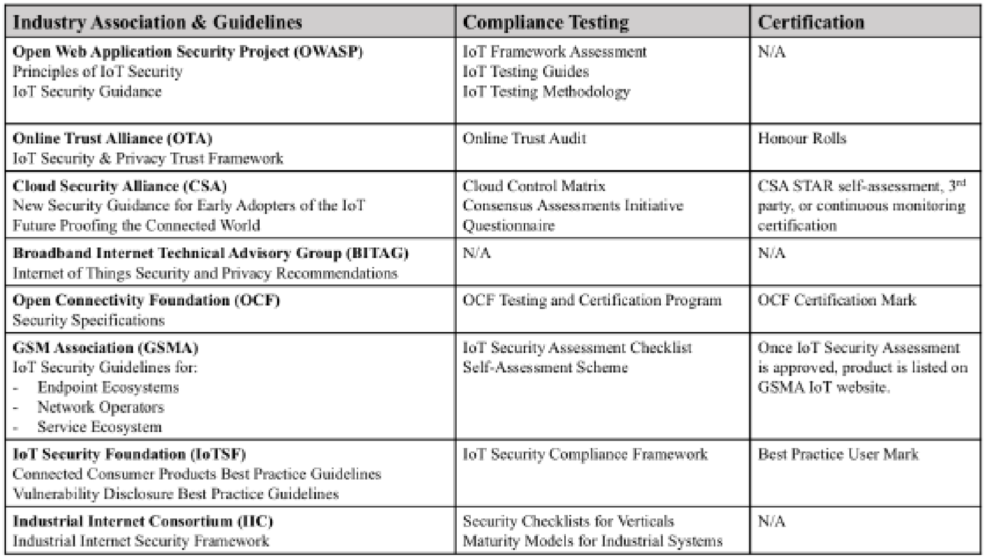
Drawbacks of formal standards

- standardization **processes are generally longer than market driven** ones, due to the highly **institutionalized (traditional) approval and review** process.
- formal standards development in **regional** and international organizations is more politicized, due to the **complex voting structure** (e.g. national weighted voting in ETSI) or the competitive **promotion of national standards** for international adoption
- Challenge with the topology of the IoT ecosystem (i.e. edge, connectivity, services) as well as its large application area (e.g. consumer goods, critical infrastructure and essential services)
- challenge the current organization of formal standards development Activities
- the formal standards landscape is complicated by standardization activities pertaining to specific IoT application
- Areas, such as the development of security standards for smart grid systems in CEN/CENELEC (EU) or NIST agency IoT security are advancing, it is difficult to say that a baseline for IoT security are not much attracted by these standards.

De facto standards

- Developed by a diverse range of industry alliances and associations across the IoT ecosystem.
- The above industry alliances and interest associations have responded to the gaps in formal standards development by proposing their own guidelines for securing the IoT
  - GSM association (GSMA): IoT security guidelines
  - Open Web Application Security project (OWASP) : IoT Security Guidance

De facto standard alliance group and its frameworks for IoT security



Industry Association & Guidelines	Compliance Testing	Certification
Open Web Application Security Project (OWASP) Principles of IoT Security IoT Security Guidance	IoT Framework Assessment IoT Testing Guides IoT Testing Methodology	N/A
Online Trust Alliance (OTA) IoT Security & Privacy Trust Framework	Online Trust Audit	Honour Rolls
Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT Future Proofing the Connected World	Cloud Control Matrix Consensus Assessments Initiative Questionnaire	CSA STAR self-assessment, 3rd party, or continuous monitoring certification
Broadband Internet Technical Advisory Group (BITAG) Internet of Things Security and Privacy Recommendations	N/A	N/A
Open Connectivity Foundation (OCF) Security Specifications	OCF Testing and Certification Program	OCF Certification Mark
GSM Association (GSMA) IoT Security Guidelines for: - Endpoint Ecosystems - Network Operators - Service Ecosystem	IoT Security Assessment Checklist Self-Assessment Scheme	Once IoT Security Assessment is approved, product is listed on GSMA IoT website.
IoT Security Foundation (IoTSF) Connected Consumer Products Best Practice Guidelines Vulnerability Disclosure Best Practice Guidelines	IoT Security Compliance Framework	Best Practice User Mark
Industrial Internet Consortium (IIC) Industrial Internet Security Framework	Security Checklists for Verticals Maturity Models for Industrial Systems	N/A

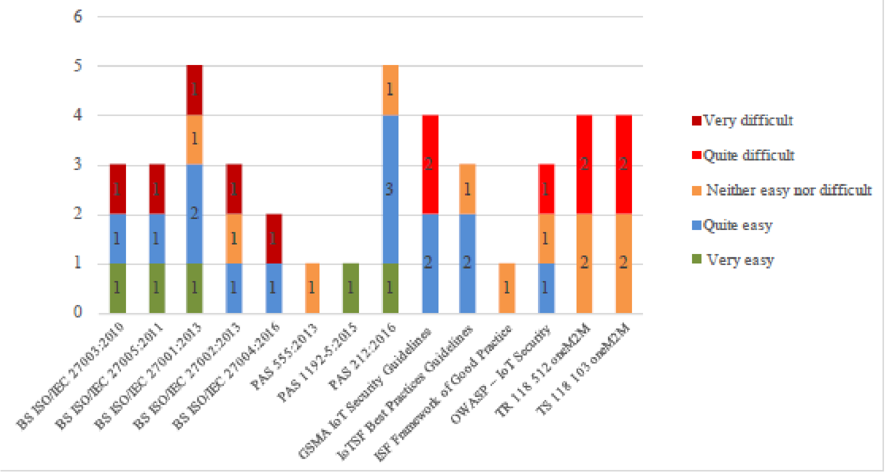
OWASP Foundation

- The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software
- It is a leading authority globally on application security. OWASP is famous for its Top 10 and Application Security Verification Standard (ASVS) guidance
- OWASP Foundation is the source for developers and technologists to secure the web.
  - Tools and Resources
  - Community and Networking
  - Education & Training
- OWASP ISVS : OWASP have tackled Internet of Things security, with the new IoT Security Verification Standard (ISVS)
- has a few different verification standards
  - the OWASP Mobile Application Security Verification Standard (MASVS)
  - have a Software Component Verification Standard (SCVS)

Compliance testing

- Detects a broad range of security bugs across a wide range of platforms and hardware architectures.
- To test and validate our developed prototype

ease of implementing and deploying current standards for IoT security



Technologies and methods that mitigate security

Challenges in IoT Security

- complexity to defining specifications that clarify the relationship between **data integrity — cyber and physical security — safety — resilience — trustworthiness**.
- the difficulties of monitoring the adoption and implementation of IoT security standards and best practices by market entities involved in the development, manufacturing and service provision of IoT.

The various security risks and vulnerabilities involved in IoT

1.Security Risks in IoT Systems

- **Data security**
- **Authentication**

2.Vulnerabilities in IoT Systems

- **Absence of Transport layer security**
- **Inadequate Security Features**
- **Poor mobile security**
- **Storing data on cloud servers**
- **Network attacks**

Security Risks in IoT Systems

- IoT system has a cloud database that is connected to all your devices.
- These devices are connected to the internet and it could be accessed by the cybercriminals and hackers.
- As the number of connected devices increases, chances for hackers to breach the security system gets increased.
- Any unauthenticated access in the IoT network system must be detected at an early stage so that degree of damage can be mitigated.

For making secure IoT systems, two important things are

1.Data security: It is the initial step to prevent any unauthenticated access to the devices in the IoT network.

- Layered architecture must be used in data security system.
- Therefore, any breach of initial security level does no expose all the data.
- Rather it must alarm the authorities about the potential threats and initial level security breach.

2.Authentication: Devices must be secured with the strong passwords for the authentication.

- Bio metrics, facial recognition, speech processing systems etc.

Some of the vulnerabilities that IoT systems are facing

1. Absence of Transport layer security:

- In most of the IoT systems data is stored on the online cloud servers, mobile phones or online databases.
- This data can be hacked easily as it is not encrypted in the transport layer before storing.
- This enhances the data security risk in IoT system.

2. Inadequate Security Features:

- With the growing competition and huge demand, technology giants want to launch their IoT software system as soon as soon as possible.
- Thus the important part of the software life cycle such as testing, quality assurance, and security vulnerabilities are not done properly.

3. Poor mobile security:

- Poor mobile security in IoT systems make it more vulnerable and risky.
- Data is stored in a very unsecure way in mobile devices.
- However, iOS devices are more secure than the Android devices.

4. Storing data on cloud servers:

- Storing data on the cloud servers is also considered as a weak link in the security of IoT systems.
- Cloud servers have less security and are open to attackers from all the dimensions.
- Developers must make sure that data stored on the cloud servers must always be in the encrypted format.

5. Network attacks:

- Another big vulnerability in the IoT systems is the wireless connection that is exposed for the attackers.
- For example, hackers can jam the functionality of a gateway in IoT systems.
- This can bring down the whole IoT system.

How to mitigate IoT security risks

- There are five steps organizations can take to prepare for the introduction of IoT-based systems to ensure the security risks

1. Encrypt data

2. Improve data authentication processes

3. Manage hardware and software

4. Isolate IoT devices

5. Invest in mobile monitoring

6. A multi-layered approach to protect connections and devices.

Top 5 encryption algorithms for IoT

1. The Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)
3. Triple Data Encryption Standard (DES).
4. RSA Encryption.
5. Twofish Encryption Algorithm

The Data Encryption Standard (DES).

- National Institute of Standards and Technology (NIST)
- DES uses the **same encryption key to encrypt and decrypt data.**
- Both the sender and the receiver must have the **same private key.**
- The latter process is known as a **symmetric key algorithm.**
- The important difference between DES and AES is that DES is less secure than AES

Advanced Encryption Standard (AES)

- AES uses a single **encryption key of varying lengths**.
- The AES algorithm concentrates on a single block of data and re-encrypts it 10 to 14 times, depending on the key length.
- When using an internet connected medical device, AES meets U.S. Government requirements for HIPAA data protection.
- AES also meets FINRA standards for protecting financial records.
- AES is an efficient and elegant algorithm whose strength resides in its key length options.
- The longer the key length, the more exponentially difficult it is to break the encryption.

Triple Data Encryption Standard (DES)

- This algorithm is a type of computerized cryptography where each block of data receives three passes.
- Additional security comes from the larger key length.
- Triple DES was replaced by NIST, which adopted the AES.
- Triple DES is now considered obsolete, but is still used by some IoT products because of its compatibility and flexibility.
- What Triple DES does well is protect against brute force attacks.
- Brute force is an exhaustive effort (as opposed to intellectual strategies) through repeated trial and effort.
- Brute force attacks use automated tools to guess various combinations until the hacker cracks the key.

RSA Encryption

- RSA encryption allows users to send encrypted information without having to previously share the code with the recipient.
- It is a **public-key encryption**, and the public key can be shared openly.
- However, the data can only be decrypted by **another private key.**
- Each RSA user has the common public key, but only designated recipients are known to the private key.

References

- https://www.pivotpointsecurity.com/blog/the-new-owasp-isvs-what-why-and-who/
- https://owasp.org/
- Irina Brass, Leonie Tanczer, Madeline Carr, Miles Elsden and Jason Blackstock, “Standardising a Moving Target: The Development and Evolution of IoT Security Standards”, June 2018.

Twofish Encryption Algorithm

- Twofish uses a **block ciphering system** based on a single key of any length up to 256 bits.
- This encryption standard is efficient on computers with lower capacity processors and IoT device smart cards.