happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

IoT Security-
Challenges & Best Practices

CONTENTS

ABSTRACT

The use of IoT devices is rapidly increasing, and IoT services have become vital. Along with success, several security risks and exploits against IoT devices have been identified, and it is growing with the technology.

High-profile, IoT-driven cyberattacks are forcing industries to identify and manage IoT's security risks to safeguard their core business operations. Markets such as healthcare, aviation are exposed to high amount of security risk that transcend previous expectations.

Some IoT attacks are so catastrophic that it can exfiltrate confidential data from an organization even through smart cameras, watches, speakers and more. And some of them could have life minatory consequences if the industry targeted belongs to health sector. Therefore, there is a real need to understand the security threats and attacks on IoT infrastructure comprehensively.

WHAT IS INTERNET OF THINGS (IOT)?

The internet of things (IoT) which is also known as IOE-Internet of Everything is apace growing technology which connects billions of physical IoT devices (Ex:- coffee maker, A.C, washing machine, ceiling fan, lights, security cameras, aviation, healthcare industry and more) to the existing internet infrastructure. All these connected devices are talking to each other by collecting and sharing data about the way they are being used and their surrounding environment. The IoT imparts the power of the internet, data processing and analytics to the real world of physical objects.

WHAT IS INTERNET OF THINGS (IOT) SECURITY?

Securing the IoT network has always been a major issue. In routine security assessment, flaws are discovered in software, even in the old codes which are well-used. Several IoT appliances/devices cannot be patched with security fixes as a result almost all device will be at risk. Moreover, IoT Sensors which collects the data from these IoT Devices are also amassing in several cases.
Extreme highly sensitive data, what you say, and what you do at your home for example, permitting devices to connect to the internet exposes them to several serious vulnerabilities if they are not appropriately secured.

Hackers are now actively aiming IoT devices such as routers and webcams because their inherent lack of security makes them vulnerable and easy to compromise.

INTERNET OF THINGS (IOT) VS OPERATIONAL TECHNOLOGY (OT)

The Internet of Things (IoT) has revolutionized the shape of the energy industry. Innovative operational technology (OT) has influenced internet of things-based (IoT) robotics, asset management, supply chain management, demand-driven offerings, and intelligent forecasting.. This represents a convergence between Supervisory Control and Data Acquisition (SCADA), Advanced Metering Infrastructure (AMI), Distribution Automation (DA) and consumer engagement systems.

INTERNET OF THINGS (IOT) IS EVERYWHERE

IOT ENDPOINT INSTALLED BASE, WORLDWIDE, 2020 AND 2023 (THOUSANDS OF UNITS) BY GARTNER

SEGMENT	2020 VOLUME	2020 MARKET SHARE (%)	2023 VOLUME	2023 MARKET SHARE (%)
Connected cars — embedded (consumer and commercial)	393	11	19,087	39
Outdoor surveillance cameras	2,482	70	15,762	32
Fleet telematics devices	135	4	5146	11
In-vehicle toll devices	50	1	1,552	3
Emergency services	61	2	1,181	2
Others	400	11	5,863	12
Total	**3,522**	**100**	**48,590**	**100**

INTERNET OF THINGS (IOT) SECURITY LANDSCAPE

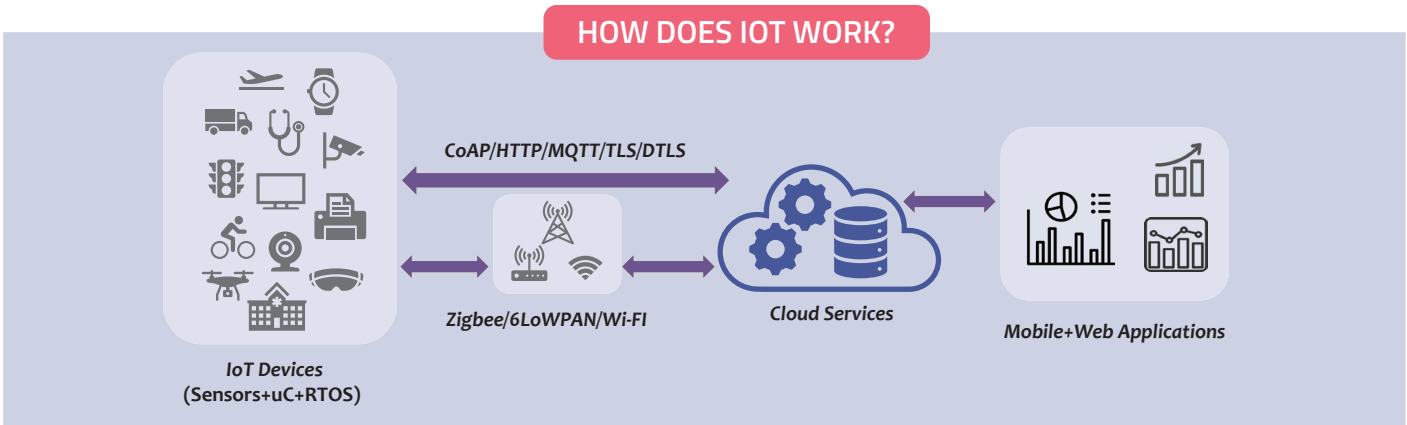
Cybersecurity concerns are turning out to be a day-to-day struggle for businesses. Recent trends and cybersecurity statistics reveal a high growth in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. (as per varonis & unit42)

98% of all IoT traffic is unencrypted, exposing personal and confidential data on the network.	57% of IoT devices are vulnerable to medium- or high severity attacks, making IoT the low-hanging fruit for attackers.	83% of medical imaging devices run on unsupport-ed operating systems—a 56% jump from 2018, as a result of Windows 7 reaching its end of life.
61% of organizations have experienced an IoT security incident. (CSO Online)	IoT devices experience an average of 5,200 attacks per month. (Symantec)	Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16% of the attacks, was the third most common IoT threat. (Symantec)
IoT security statistics state that 84% of companies that have adopted IoT have reported security breach. (Aruba HPE)		

And yet – whatever the state of its security – the IoT is growing voraciously. McKinsey estimates that there will be 43 billion IoT devices connected to the internet by 2023. If current trends continue – and 98 percent of IoT traffic is left unencrypted – it will be a feeding frenzy for cyber-criminals.

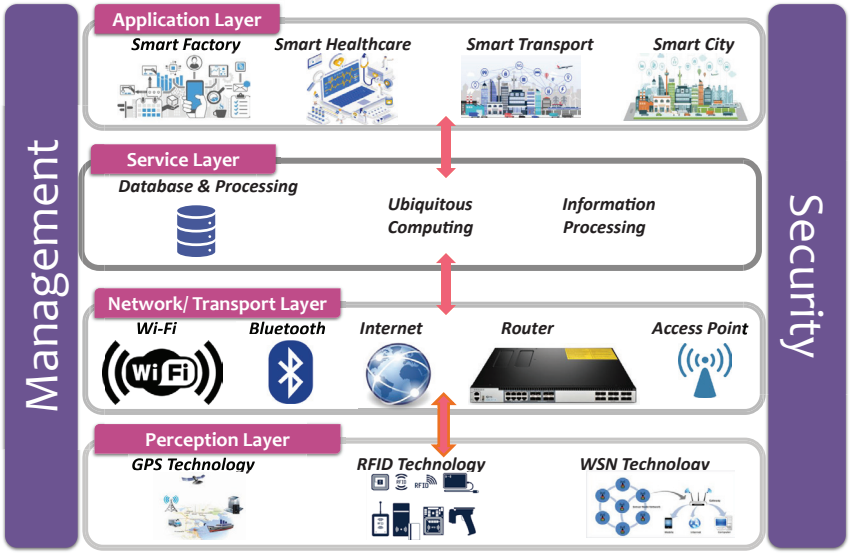
Source: https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

HOW DOES IOT WORK?



IOT ARCHITECTURE & LAYER INFORMATION

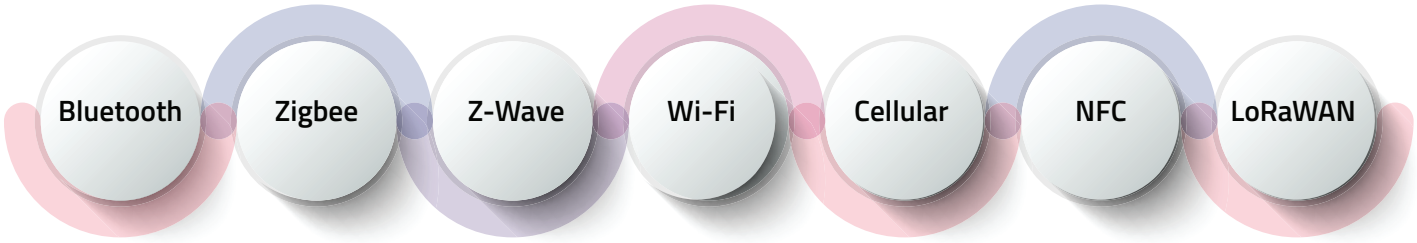
There are various IoT Layer Model but in this paper using ITU-T Y.4000 Four Layer Architecture.



Ref. to ITU-T Y.4000 Four Layer Architecture

IOT TECHNOLOGIES & PROTOCOLS

Below is the list of IoT Technologies and Protocols being used for IoT Communication

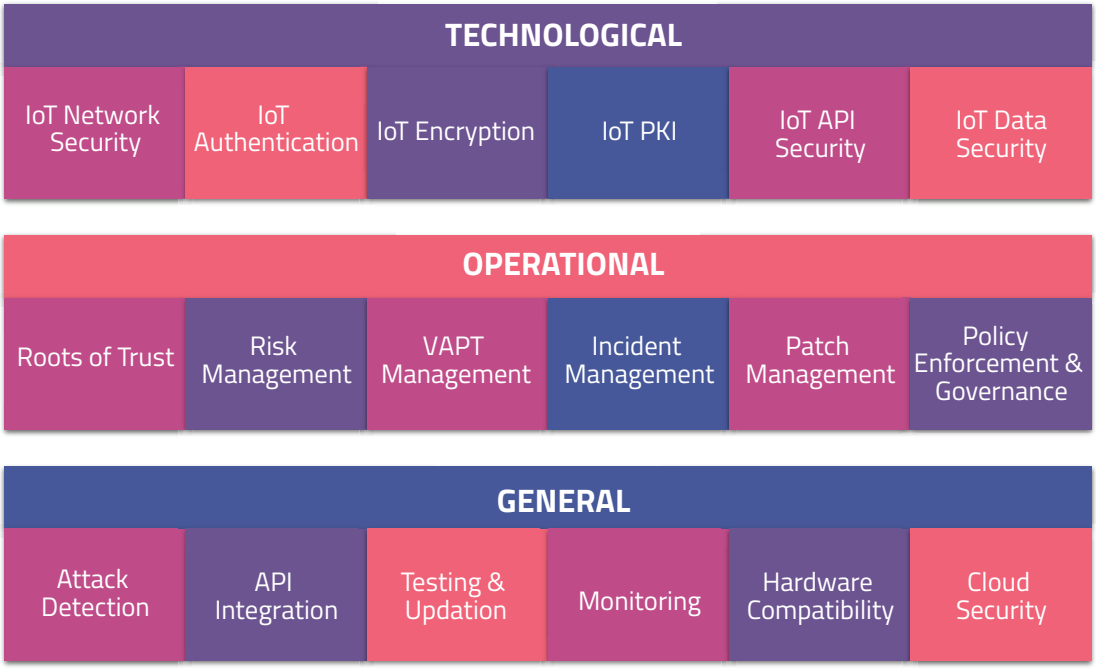


POPULAR OPERATING SYSTEM FOR IOT – YEAR 2020

IoT operating system particularly common for low power microcontrollers and other IoT devices to run effectively using Internet protocol IPv6, and IPv4. Mostly this IoT OS is very appropriate for low powered internet connectivity.

Contiki	Apache Mynewt	TinyOS	TizaenRT
Amazon FreeRTOS	Huawei LightOS	Fuchsia	Embedded Linux
Android Things	Zephyr	Windows IoT	Mbed OS
Riot	Snappy	Raspbian	Nucleus RTOS

IOT SECURITY CHALLENGES



TOP 10 IOT SECURITY FLAWS THAT ARE PUTTING YOUR BUSINESS AT RISK

Not having a security and privacy program	Lack of owner-ship/governance to drive security and privacy for IoT devices or appliances	Security not being incorporated into the product designing and ecosystems	Insufficient security understanding and training for engineers and architects
Lack of IoT/IIoT and device security and privacy resources	Insufficient monitoring of devices and systems to expose security events	Unavailability of post-market/ implementation security and privacy risk management	Lack of visibility of devices or not having a full device inventory
Detecting and treating risks of fielded and legacy products	Immature incident response practice		

IOT SECURITY INDUSTRY FRAMEWORK

There are multiple IoT Security Industry Frameworks but below listed are few popular one.

	industrial internet CONSORTIUM	GSMA	IoT Security Foundation	CISCO
Framework Name	IIoT Security Framework	IoT Security Guidelines for Network Operators	IoT Security Compliance Framework (NIST)	Securing the Internet of Things
Primarily focused on	General Industry	Telecom Industry, Automobile	IoT Hardware Manufacturer	General Industry

OWASP INTERNET OF THINGS (IOT) PROJECT

The concept of OWASP Internet of Things project provides a better understanding of the security issues associated with IoT to the manufactures, developers, and consumers. It also enables users to make better security decisions in any context while building, deploying, or assessing IoT technologies. (Ref. to OWASP)

The OWASP IoT Top 10 lists things to avoid when building, deploying, or managing IoT systems or devices, including:

Weak, Easily Guessable, or Hard-coded Passwords	Insecure Network Services	Insecure Ecosystem Interfaces	Lack of Secure Update Mechanism
Use of Insecure or Outdated Components	Insufficient Privacy Protection	Insecure Data Transfer and Storage	Lack of Device Management
Insecure Default Settings	Lack of Physical Hardening		

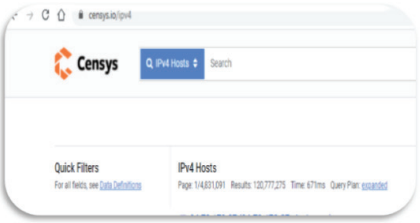
IOT VULNERABILITIES PROJECT (IOT ATTACK SURFACE MAPPING)

VULNERABILITY	ATTACK SURFACE	SUMMARY
Username Enumeration	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to collect a set of valid usernames by interacting with the authentication mechanism
Weak Passwords	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to set account passwords to '1234' or ▪ Usage of preprogrammed default passwords
Account Lockout	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to continue sending authentication attempts after 3-5 failed login attempts
Unencrypted Services	▪ Device Network Services	▪ Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
Two-factor Authentication	▪ Administrative Interface ▪ Cloud Web Interface ▪ Mobile Application	▪ Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner
Poorly Implemented Encryption	▪ Device Network Services	▪ Encryption is implemented however it is improperly configured or is not being properly updated, e.g. using SSL v2
Update Sent Without Encryption	▪ Update Mechanism	▪ Updates are transmitted over the network without using TLS or encrypting the update itself
Update Location Writable	▪ Update Mechanism	▪ Storage location for update files is world writable potentially allowing firmware to be modified and distributed to all users
Denial of Service	▪ Device Network Services	▪ Service can be attacked in a way that denies service to that service or the entire device
Removal of Storage Media	▪ Device Physical Interfaces	▪ Ability to physically remove the storage media from the device
No Manual Update Mechanism	▪ Update Mechanism	▪ No ability to manually force an update check for the device
Missing Update Mechanism	▪ Update Mechanism	▪ No ability to update device
Firmware Version Display and/or Last Update Date	▪ Device Firmware	▪ Current firmware version is not displayed and/or the last update date is not displayed
Firmware and storage extraction	▪ JTAG / SWD interface ▪ In-Situ dumping ▪ Intercepting a OTA update ▪ Downloading from the manufacturers web page ▪ eMMC tapping ▪ Unsoldering the SPI Flash / eMMC chip and reading it in a adapter	▪ Firmware contains a lot of useful information, like source code and binaries of running services, preset passwords, ssh keys and more

Source: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

TOP SEARCH ENGINES FOR INTERNET OF THINGS (IOT)

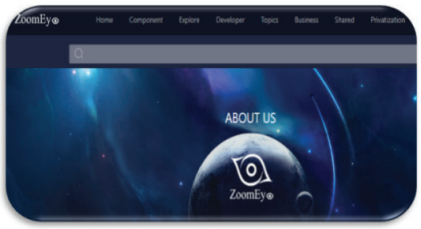
Thingful Search Engine



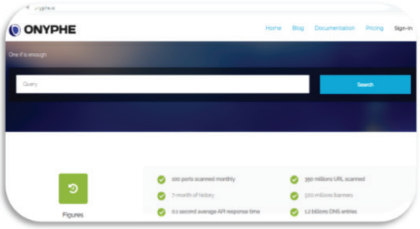
Censys Search Engine

FOFA Search Engine

Shodan Search Engine

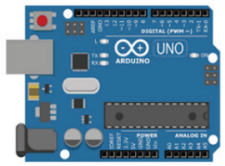


ZoomEye Search Engine

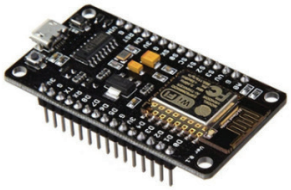


ONYPHE Search Engine

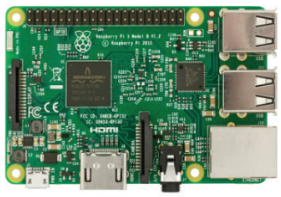
TOP HARDWARE PLATFORMS FOR INTERNET OF THINGS (IOT)



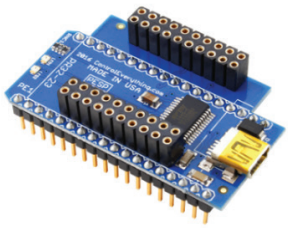
Arduino



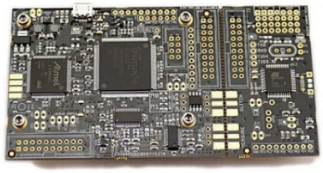
NodeMCU ESP8266



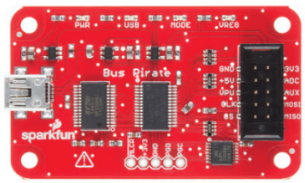
Raspberry pi



Adafruit Huzzah ESP8266



ChipWhisperer



buspirate

HackRF One

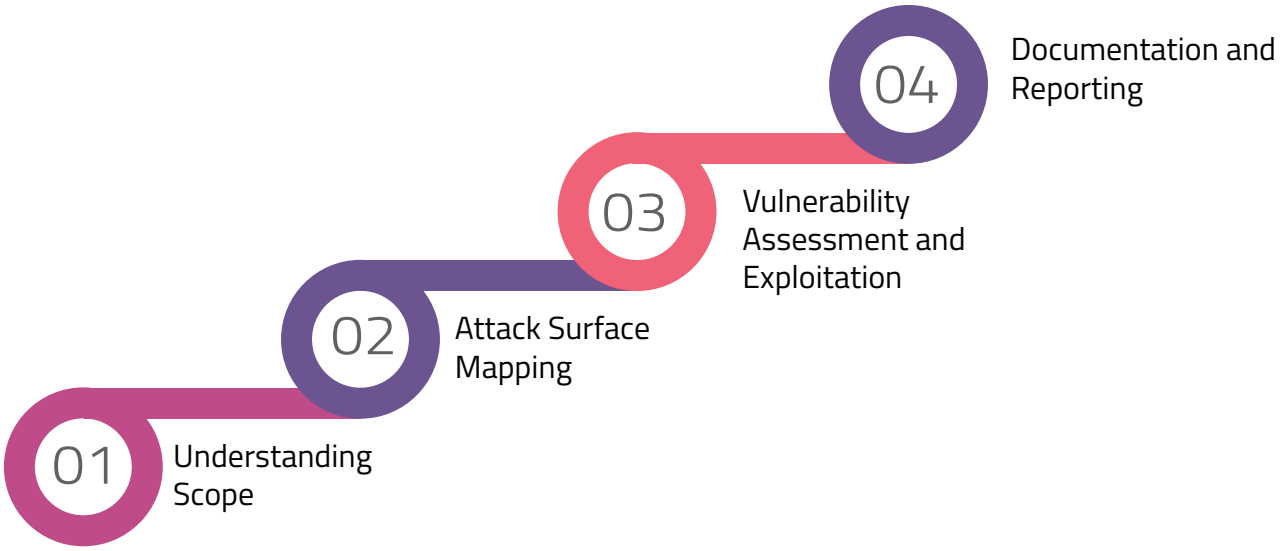
IOT ATTACK VECTOR

Below is a list of several attack vectors that make IoT Devices vulnerable and can be used to exploit them:

Firmware Running on The Device (UEFI, Filesystem, Bootloaders)	Network & Port Probe	Device Hardware	Device Radio and Network Communication
Mobile, Web and Other Back-End Interface	Authentication/ Authorization	Cloud, API	

WHAT IS IOT PEN-TESTING?

An IoT penetration test is the security assessment and exploitation of various modules or components present in an IoT device solution to help make the device more secure. IoT pen-testing solution includes network testing, API monitoring, and application testing.



The first phase of IoT pen-testing is to map the entire attack surface of the solution, followed by identifying security risks and performing exploitation, which is then followed by post exploitation. The testing determines with an in-depth technical report.

IOT PEN-TESTING METHODOLOGY

Internal communications Protocols like UART, I2C, SPI and more	Open ports	JTAG debugging	Exacting Firmware from EEPROM or FLASH memory
Tampering			

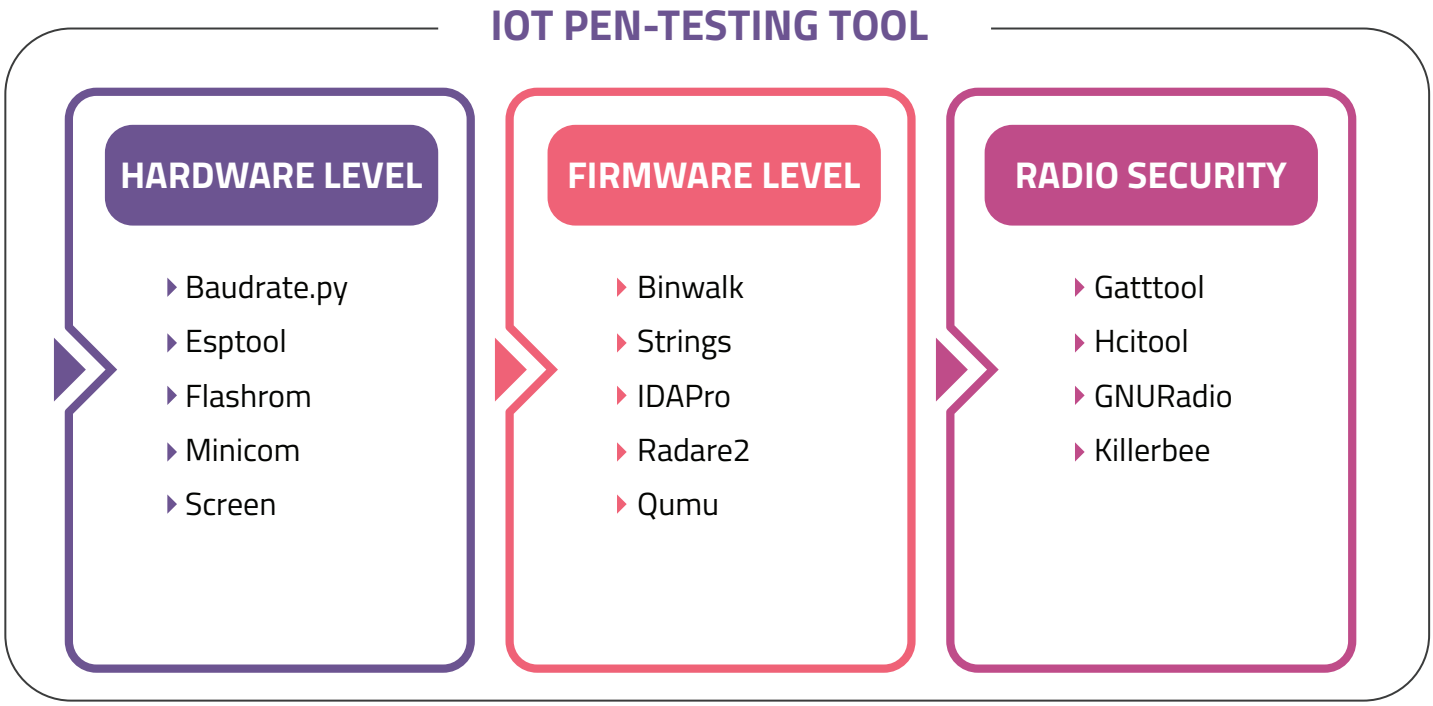
JTAG Exploitation

UART Port

Dumping Flash Memory

IOT PEN-TESTING TOOLS

There are several open sources as well as commercial tools available that can perform IoT Pen-Testing. Few of popular ones are listed below and for more of such tool can be found on the Internet.



INDUSTRY-WISE IOT PEN-TESTING

IoT Penetration Testing can be performed across the following industries:

Smart Home Automation	Medical / Healthcare	Aviation	Industrial Control Systems
Wearable IoT Devices	Energy/Utility	Automotive	Retail
Enterprise IoT			

POPULAR OPERATING SYSTEMS FOR IOT PEN-TESTING

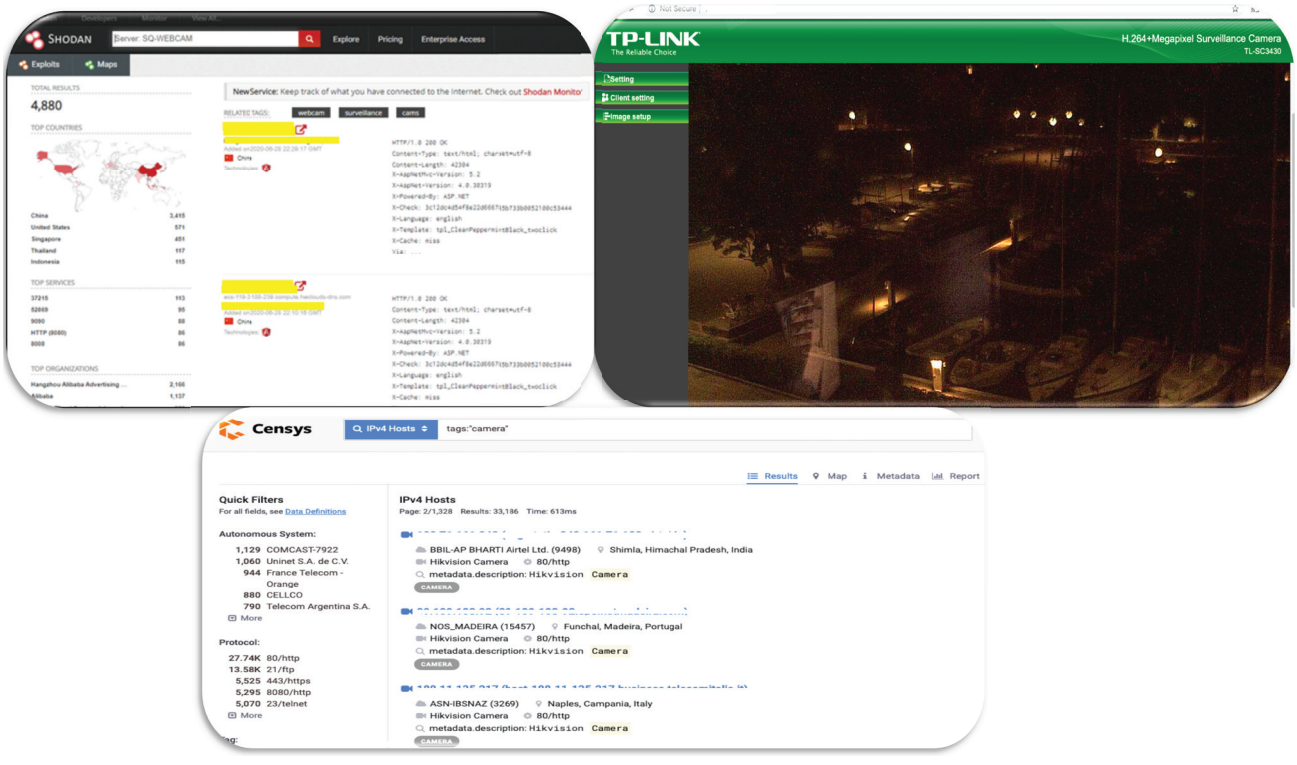
Kali Linux	AttifyOS v3.0	Instant GNU Radio	Ubutnu Best Host Linux for IoT's - Use LTS
IoT-PT OSv1	EmbedOS	ParrotOS	

COMMON IOT PORTS USED BY IOT DEVICES

SERVICE	PORT	IOT DEVICE TYPE
SSH	Port 22	*Includes IoT
HTTP	Port 80	Mainly web apps but includes common IoT devices, ICS, and gaming consoles
TELNET	Port 23	ALL
SIP	Port 5060	All VoIP phones, video conferencing
HTTP_Alt	Port 8080	SOHO routers, smart sprinklers, ICS
TRo69	Port 7547	SOHO routers, gateways, CCTV
Applications	Port 8291	SOHO routers
Telnet	Port 2323	ALL
HTTP	Port 81	*Can include IoT: Wificams
SMTP	Port 25	*Can includes IoT: Wificams, Game consoles
Rockwell	Port 2222	ICS
HTTP_Alt	Port 8081	DVRs
WSP	Port 52869	Wireless chipsets
HTTP_Alt	Port 8090	WebCams
UPnP	Port 52869	Wireless chipsets
Applications	Port 37777	DVRs
UPnP	Port 37215	SOHO Routers
Applications	Port 2332	Cellular gateways
Rockwell	Port 2223	ICS
Secure SIP	Port 5061	VoIP phones, video conferencing

FIND VULNERABLE WEBCAMS ACROSS THE GLOBE USING SHODAN

Shodan is an advance search engine to find vulnerable webcams across the globe which are indexed in its database. Many of them either have no credentials or default credentials which can be seen in the below image and can be access in just one click over IP or url.



FIRMWARE ANALYSIS

WHAT IS IOT FIRMWARE

Firmware is a software code programmed on a hardware device. It offers the necessary instructions on how the device communicates with the other computer hardware.

WHAT IS IOT FIRMWARE ANALYSIS & METHODOLOGY?

Firmware analysis is a complicated and hectic job of hunting firmware vulnerabilities with deep research and uncountable vulnerability scan. This process helps efficiently determine security risks that can affect your business legal and financial status and your reputation.

Firmware for Internet of Things devices can cover malicious code or security bug, which are already being used in devastating attacks. Firmware analysis is the best approach for finding embedded files and executable code, vulnerabilities, hard coded credentials, private keys, certificates and more. Below is the procedure for Automated Firmware Vulnerability Analysis.

Get the Firmware	Extract the Firmware	Run Firmware analysis tool	Ubutnu Best Host Linux for IoT's - Use LTS

HARD CODED CLOUD CAMERA CREDENTIAL DUMPING FROM FIRMWARE IMAGE

As per OWASP IoT Top 10 many of IoT Device's firmware have very weak, easily guessable password or credentails which put them at high risk resulting compromised security. Refer to the example given below:

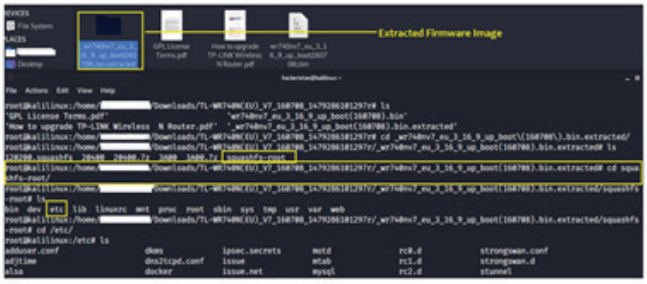
HUNTING ROOT PASSWORD FROM CLOUD ROUTER FIRMWARE IMAGE

As per OWASP IoT Top 10 many of IoT Device has been found with serious vulnerabilities in over a dozen wireless routers and access points with the help of an open-source framework that can be used to perform dynamic security analysis on embedded firmware.

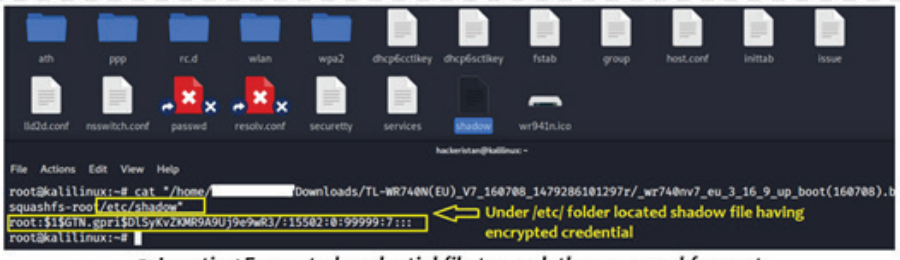
1. Finding Firmware

2. Download Firmware

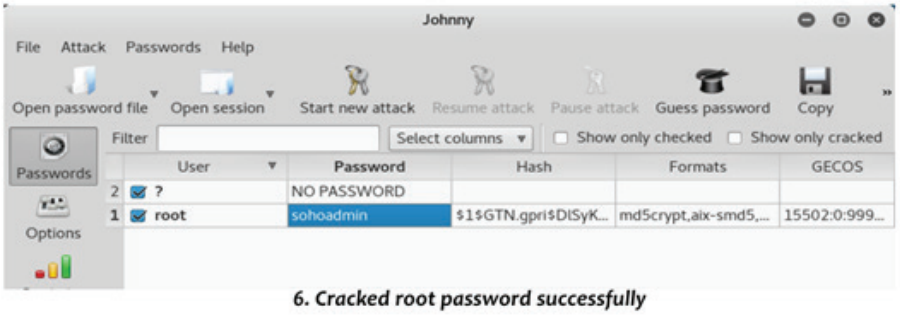
3. Extracting firmware image



4. Extracted firmware image and found squashfs-root file system



5. Locating Encrypted credential file to crack the password for root



6. Cracked root password successfully

HACKER'S RADAR CAN TRACK A FLIGHT

The RTL-SDR can be utilized as a super low-cost real time air radar. Modern planes use something termed an ADS-B (Automatic Dependent Surveillance-Broadcast) Mode-S transponder, which periodically broadcasts location and altitude information to air traffic controllers (ATC).

A home aircraft radar system can be created utilizing ADS-B signals received by RTL-SDR.

Flight Tracked at Radar near Bangalore, India Airport

Aggressive mode enabled for tracking signals at Flight Radar

Tracked Flight Detail in real time

HEALTHCARE IOT DEVICES ARE AT HIGH RISK

Healthcare Industry has now moved to the direction of Internet of Medical Things (IoMT). As per research 87% of healthcare organizations will have adopted IoT technology and by end of the year 2020 it is expected to reach 650 million IoMT devices.

Global WannaCry cyberattack in 2017 was able to proliferate due to failure of patching, Check Point's research also confirms the risk of legacy systems to patient data. WannaCry attack impacted more than a one third of the UK National Health Service trusts, forcing the cancelation of about 7,000 appointments.

The researchers found that in many scenarios IoT devices are easy for hackers to target, putting massive storage of patient data at risk. The researchers have especially noted major vulnerability issues with IoT devices.

There are various Smart Healthcare IoT Devices which are indexed in Shodan, Censys and many more such IoT Search engines that provide one search facility to hackers to find those Medical IoT Devices in the world and target them easily. For example, DIACOM (Digital Imaging and Communications in Medicine), which uses default port 104/TCP and records its presence with existing known vulnerabilities on Shodan for 38,011 device count and on the other side where this service was customized and run over port 2345/TCP. The count of connected device that are exposed to the internet is 99,872.

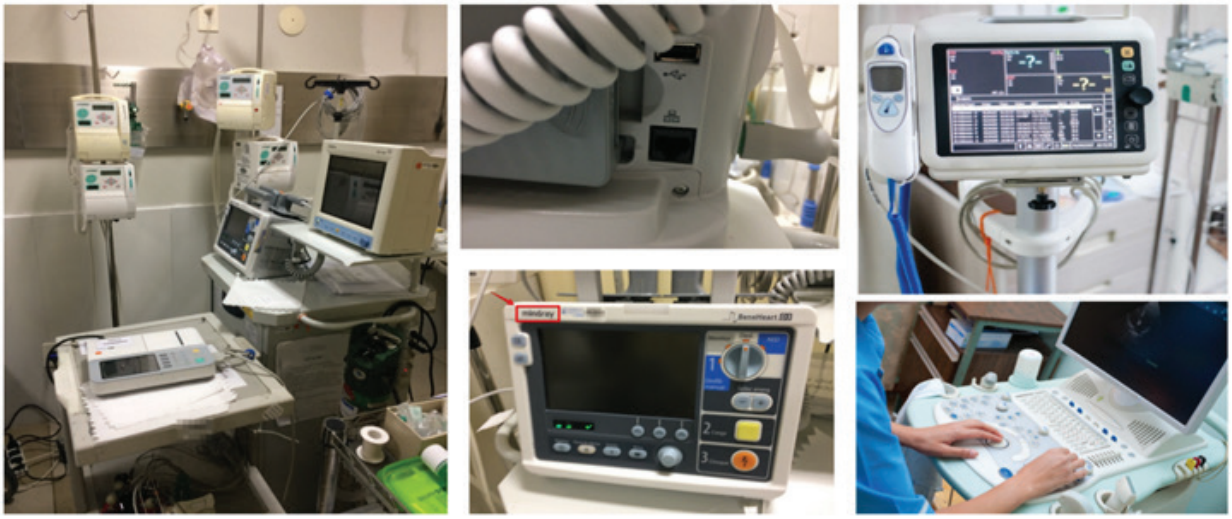
```
root@kalilinux:~# shodan stats --facets vuln port:104
Top 10 Results for Facet: vuln
cve-2017-15906                  1,024
cve-2018-15919                  1,016
cve-2016-10708                      9
cve-2016-0777                       9
cve-2014-1692                       9
cve-2012-0814                       8
cve-2010-5107                       8
cve-2011-5000                       7
cve-2011-4327                       7
cve-2010-4755                       6

root@kalilinux:~# shodan stats --facets vuln port:2345
Top 10 Results for Facet: vuln
cve-2017-15906                  1,081
cve-2018-15919                    773
cve-2016-10708                    525
cve-2014-1692                     336
cve-2016-0777                     318
cve-2011-5000                     296
cve-2011-4327                     296
cve-2012-0814                     295
cve-2010-4755                     288
cve-2010-5107                     281
```

Found list of medical devices like DIACOM indexed in Shodan Database working over port 104 & 2345 along with vulnerability they got.

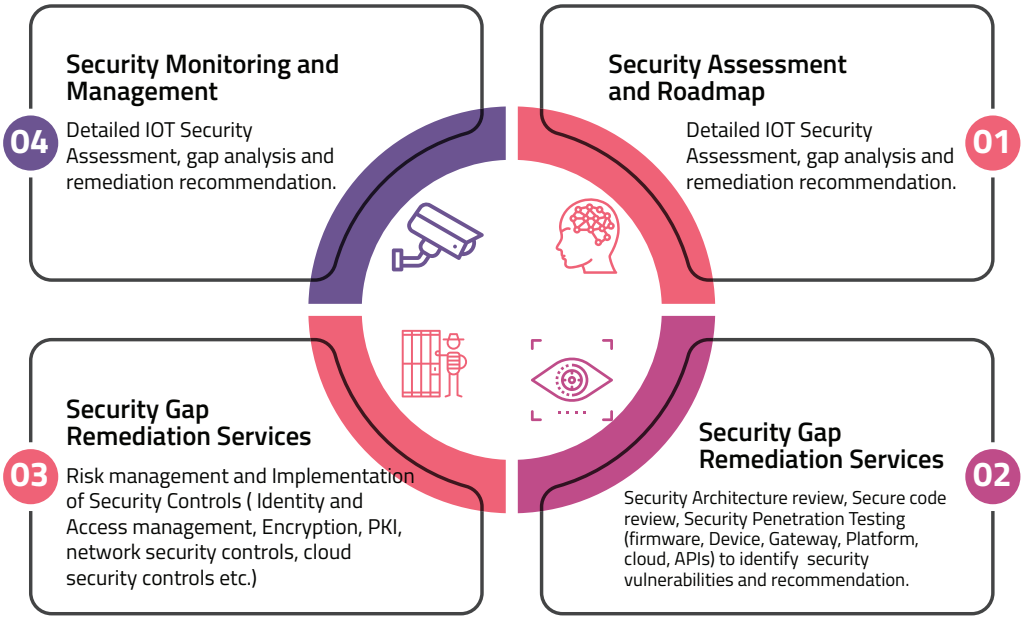
```
File  Actions  Edit  View  Help
root@kalilinux:~# shodan count port:104
38011
root@kalilinux:~# shodan count port:2345
99872
root@kalilinux:~#
```

Count list of medical devices using port 104 & 2345 which are exposed to internet via Shodan

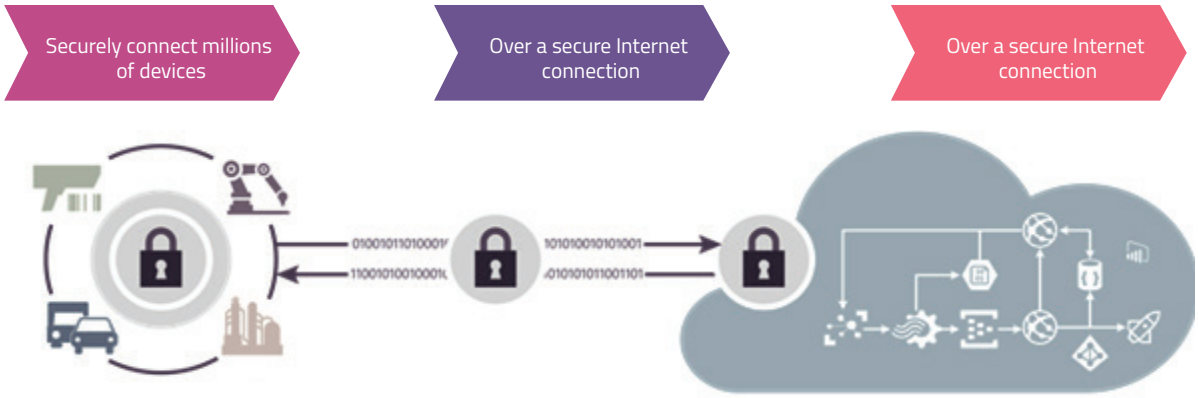


"Healthcare corporations must be well aware of the vulnerabilities or security bug that come with these IoT devices that enhance their chances of a data breach,". Network separation is the best practice that permits IT Security professionals in the healthcare sector the confidence to adopt new digital medical solutions, while offering another tier of security to network and data security, without compromising performance or reliability."

IOT SECURITY – OUR SERVICES / SOLUTIONS



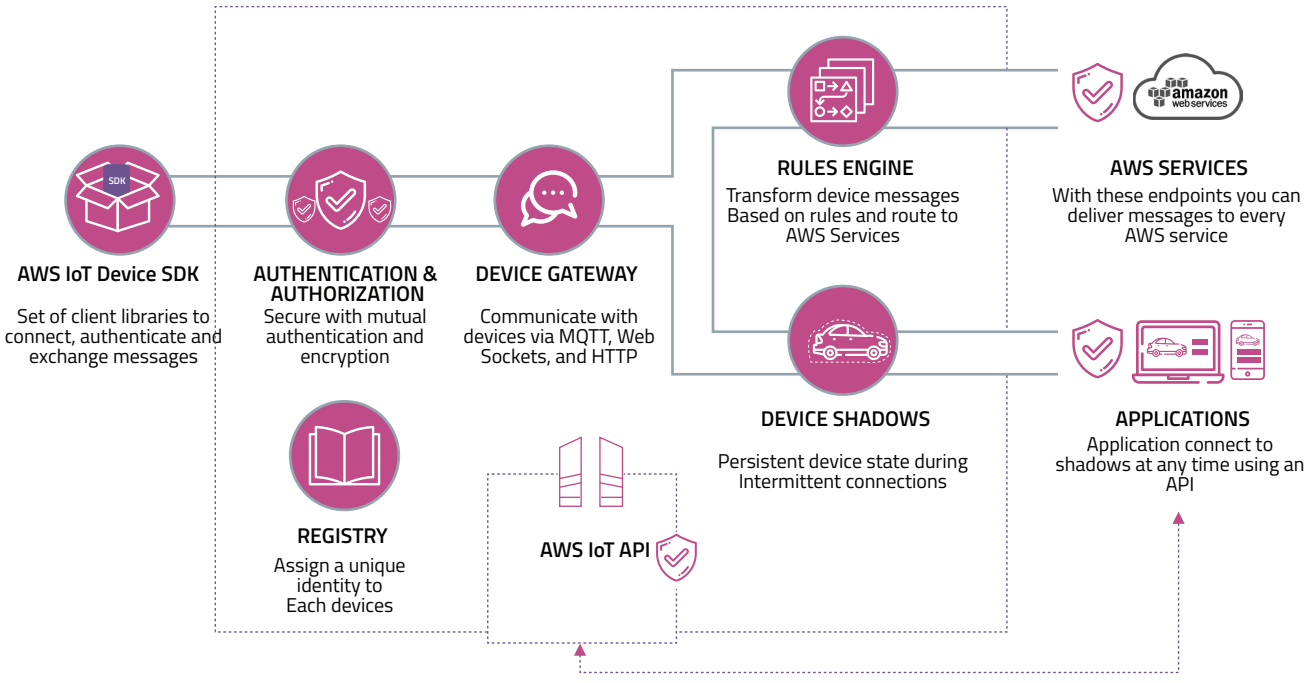
AZURE IOT SOLUTION ACCELERATORS



Device Security
Device Provisioning and Authorization

Connection Security
X.509/TLS-Based Handshake and Encryption

Cloud Security
Azure Active Directory Key Vault Policy-Based Access Control



INTERNET OF THINGS (IOT) THREAT MODEL – STRIDE

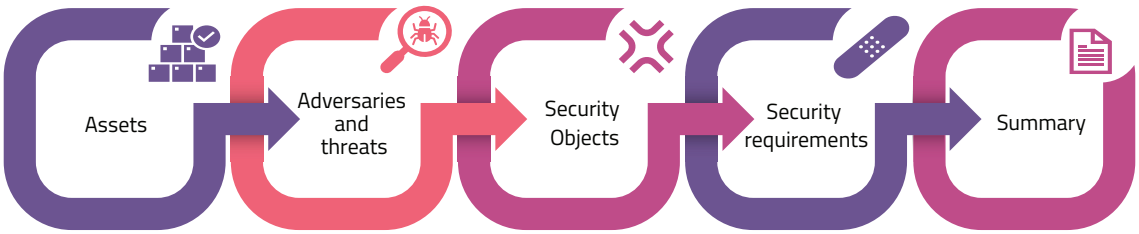
IoT devices are the most preferred target for the cybercriminals. Innovators must secure their assets and consumers from these emerging threats. While planning an Operating environment, security might be the least of one's concerns given the restrictions one faces from the cost management perspective. This however, can prove hazardous to the infrastructure that you are building thus putting the companies reputations and your job at risk.

In order to design-in security, Platform Security Architecture (PSA) suggests designers and manufacturers start by evaluating the operating environment and understand and document the ways each device could be attacked. It is a practice known as Threat Models and Security Analyses (TMSA).

The TMSA will draw attention to critical security concerns which need to be addressed and challenged to consider important issues, such as:

What are the most valuable assets?	What are the potential threats to a device?	What type of attack do you need to defend against?
How severe are the threats?	What countermeasures could be implemented?	What are the security requirements?
How does a device meet its security requirements?		

FIVE STEPS TO DESIGN SECURITY INTO YOUR NEXT IOT DEVICE



Now, the threat model can be used, and in this case, it facilitates in identify and classify the threats to an IoT device. The STRIDE model helps in detecting security gaps against each entry point to determine the security threats. STRIDE stands for

Information Disclosure

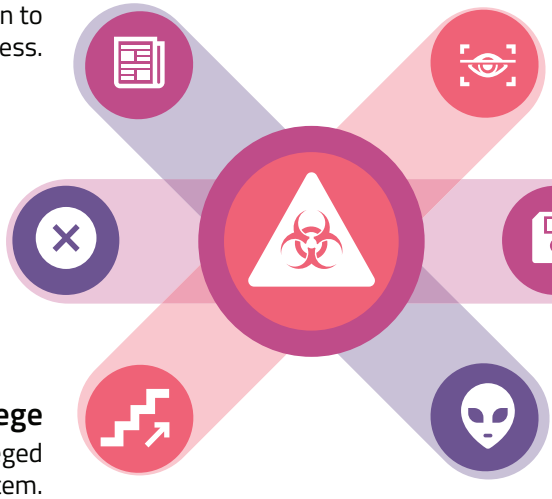
- Exposure of Information to individuals not supposed to access.

Spoofing Identity

- Illegally accessing and then using another user's authentication information.

Denial of service

- Deny service to valid users.
- Threats to system availability and reliability.



Tampering with Data

- Malicious modification
- Unauthorized changes

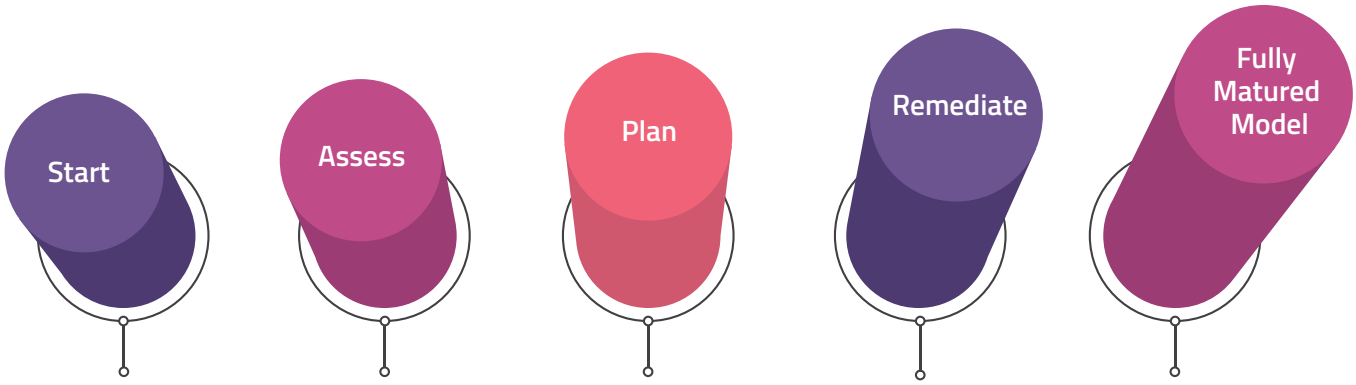
Elevation of privilege

- Unprivileged user gains privileged access to compromise the system.
- Effectively penetrated and become part of the trusted system.

Repudiation

- Deny performing a malicious action.
- Non-repudiation refers to the ability of a system to counter repudiation threats.

HOW CAN WE HELP IN IOT SYSTEM SECURITY?



Start

- IoT architecture review
- Understand Business dependency on IoT
- Existing process document review
- IoT Security Awareness Sessions to Management
- Remediation Project plan.

Assess

- Assess endpoint identification, authentication & authorization process
- Third Party Risk Management
- Assess level of RoT (Root of Trust)
- Review API security process
- Review IoT Encryption process
- Review VAPT & patching Remediation strategy & roadmap.

Plan

- Establish RoT principle
- Create policy, procedures & guidelines
- Incident response structure
- Data protection technical control implementation
- Risk assessment & Mitigation plan
- Threat & vulnerability management

Remediate

- Policy and process review
- Incident Management capability
- Patch Management
- Routine VAPT
- Responsibility & ownership
- Periodic audits and assessment
- Periodic training & awareness

Fully Matured Model

- Fully Mautured Model

BEST PRACTICES TO PROTECT IOT SYSTEMS AND DEVICES

Incorporating security at the design phase	Use strong authentication and authorization	Use of PKI and digital certificates
Provide for firmware Security updates/patches	API security	Identity Management
Hardware & Network security	Network Access Control	Use strong Encryption and Security protocols in IoT Devices
Security gateways	Integrating teams	Consumer education

CONCLUSION

IoT security is fired by lack of industry signed standards, but few IoT security frames exist in which no single user agreed to the frame. The IoT feature differs from one organization to another according to its needs. Apart from security, the variation of IoT standards leads to interoperability between them. So, all IoT consumers must ensure that all the security issues must be updated with the security fixes before installation to have a high standard of security with multilayer encryption or multilayer firewall.

AUTHOR INFO

Vikas Kumar is a techno-savvy profession with 8.5 years of experience in Security Operation Center (SOC), Cyber Forensics, Web Application and Network vulnerability management also certified with CEH, ECSA, CHFI, ACISE, ITILv4 certifications. He is currently part of Infrastructure Management and Security Services business unit of Happiest Minds Technology Pvt. Ltd. He is primarily responsible for uncovering threats, vulnerabilities and security risks as Information Security Specialist focusing on threat intelligence and investigation of advanced cyber-attacks. He is also involved and contributing to design new security solutions. Vikas is an active member of EC-Council, HackTheBox, TryHackMe & Nullcon organization.