Internet of Things (IoT) Security Guidelines

CONTENTS

INTRODUCTION

Internet of Things or (IoT) is a blazing point these days. However, what exactly is IoT? An explanation in the simplest way is that it could be regarded as an internet connects virtually between everything that is present in the surroundings, and it can be monitored and operated online. It can depict a situation in which everything that encompasses the surroundings is prepared and made to do consequent interactions with each other without any human-to-machine or inter-human contact.

Technically, IoT is the network of vehicles, physical objects, buildings, devices, and some other elements that are embedded with software, network connectivity, electronics, and sensors, allowing these objects to exchange and collect data. This innovative solution enables objects to be remotely sensed and controlled across current network infrastructure, which creates opportunities for more direct integration between the computer-based and physical world systems. This results to accuracy, improved efficiency, and economic benefit.

When the Internet of Things is augmented with actuators and sensors, the technology will become an instance of the more general form of cyber-physical systems. Through that, it also encompasses technologies like smart homes, smart cities, smart grids, and intelligent transportation. Everything can be uniquely identified with its embedded computing system. However, it can also inter-operate within the current internet infrastructure. Professionals have estimated that the Internet of Things will consist of nearly 50 billion objects in year 2020.

The “things” in IoT can be referred to as a large range of devices like biochip transponders on farm animals, heart monitoring implants, automobiles that have built in sensors, field operation devices that assist the firefighters in the “search and rescue” operations, electric clams in the coastal waters, or DNA analysis devices to monitor pathogen/environment/food. These devices are collecting useful data through the help of many different current technologies, and then flow the data between other devices autonomously.

Existing market examples include dryers or washers that use Wi-Fi for monitoring remote and smart thermostat. Other than the wide variety of new application areas for the internet connected automation to expand into, Internet of things has also been expected for generation of great amount of data from diverse locations, which are quickly aggregated; thus, increasing the necessity for better store, process, and index these data.

APPLICATIONS OF INTERNET OF THINGS

In accordance to an advisory corporation and technology research, there is going to be more than 25 billion devices on the IoT by year 2020. Another research has estimated that around 30 billion of devices are going to be connected to IoT wirelessly. As per a latest study and survey done, a great number of technology professionals, engaging internet users who responded, agreed with the notion that the IoT, wearable and embedded computing, will have beneficial and widespread effects by the year 2025. As such, it is clear that the Internet of Things will consist of a great number of device connected online.

The integration with the internet is implying that devices will be using an IP address to be a unique identifier. However, because of the limited address space of IPv4, which enables for 4.3 billion unique addresses, the objects in the Internet of Things will need to use IPv6 in order to accommodate the greatly wide address space needed. The objects in Iot are not going to be the only devices that have sensory capabilities, but is also providing actuation capabilities. To a great extent, the future of IoT will not be possible without the support of IPv6, and the global adoption of IPv6 in the next several years will consequently be important for the successful development of the Internet of Things in the future.

The capability of networking embedded devices with limited memory, power resources, and CPU means that Internet of Things (IoT) finds applications in almost any field. These systems may become in charge for the collection of information in settings, which range from factories and buildings, to natural ecosystems; thus, finding applications in field of urban planning and environmental sensing. However, IoT systems could furthermore be responsible for the performing actions, not only sensing things.

For instance, intelligent shopping systems are able to monitor the purchasing habits of particular users in a store through tracking their mobile phones. These users may be provided with special offers on their favorite products, or even place of products that they need, wherein their fridge has conveyed automatically to the phone. Some other examples of actuating and sensing are being reflected in applications that deal with energy management, heat, and electricity.

Other applications provided by IoT include allowing extended home automation and home security features. The concept of the Internet of “living” things was proposed in order to describe networks of biological sensors, which are able to use cloud-based analysis. This is to enable the users to study DNA and many other molecules. All of these advances are adding to the countless list of the applications of IoT. With this innovative solution, one will be able to control the electrical devices that are installed in his/her home, and at the same time, sorting out his/her files in the office. His/her water will be warm once he/she get up in the morning for shower.

All the credit goes to smart devices making up the smart home. Everything can be connected with the help of internet. Nonetheless, the application of Internet of Things is not only restricted to these areas. Other people specialized use of IoT could also exist. Some of these products include the media, infrastructure management, environmental monitoring, energy management, manufacturing, home and building automation, and medical and healthcare systems. Based on the app domain, the products of IoT can be broadly classified into various categories, which include smart home, smart environment, smart enterprise, smart wearable, and smart city.

BENEFITS OF INTERNET OF THINGS: LEVERAGING THE POWER OF TECHNOLOGIZING EVERYTHING FOR BUSINESS AND EVERYDAY LIFE

Internet of Things of IoT has been popping up in more conversations across the whole supply chain, and more businesses are turning IoT professionals for guidelines about how to make the most out its benefits. The internet has radically changed how the world will communicate. Simple information an activities became available instantly, which finally led to creating IoT. This allows identification of possible issues and great accuracy across the processes of supply chain. In several cases, human input and intervention will be totally eliminated. Take a closer look about how Internet of Things is changing the supply landscape when it comes to shipping processes, trend analysis, equipment functionality, payments, and invoicing.

1. **Shipping Processes** – Across the order fulfillment process, delays, inefficiencies, and ample chances for problems exist. IoT is able to reroute the instructions for truck driver, facilitate new ways to get products delivered, or make changes to automated delivery systems. For instance, one can use IoT for controlling automated delivery of products through unmanned aerial vehicles or the UAV.

   By identifying the problems and inefficiencies before they occur, the total expense to the supply chain will be reduced. Moreover, the use of robotics in the order fulfillment, particularly the processes of item picking, will be able to help in fostering a faster purchase-to-delivery timeline. As a result, businesses are going to grow faster, and get their customer base expanded.

2. **Machine functionality** – Most of the manufacturing processes are heavily relying on use of the machinery. Every robotic, belt or convey, or moving item has to contain a motor for powering the movements of the machine. Thereby, simple factors like operating temperature, hydraulic pressure, and frequency are affecting the efficiency of the respective machine. At its core, the Internet of Things (IoT) serves as a way to gather information regarding a process, but applications of IoT will be able to detect possible problems within a machine before the machine would falter.

IoT can identify the exact cause of the problem and provide detailed instructions about how one can make a proper repair, as well as helping ensure that machines will maintain functionality by means of stopping production when maintenance is necessary. This can be in the form of signaling maintenance workers to have the machine checked out, or the IoT can upload new firmware into the system, which is going to correct the issue of the machine.

3. **Trend analysis and recommendation** – One of the greatest advantage of the Internet of Things (IoT) is that it is capable of collecting and analyzing data, even though, analyzed collection of data is useless by itself. The actual advantage of data collection occurs when the resulting analysis has made a recommendation about how they can improve the processes of supply chain. The software in IoT is the driving force behind analysis and recommendation of data, and it may be likened to AI creation.

   The system is going to determine what occurs, what trends will become prevalent, and how the respective company will be able to improve the outcome automatically. This may become involved in the shipping of merchandise to the customers, fulfillment of order, collecting debts, tracking merchandise sent from customers in the reverse logistics processes, or enacting a change in the manufacturing-environmental conditions in order to improve the workflow.

4. **Automated transfer of data** – When customers place an order, the Internet of Things (IoT) will allow automated information transmission. This process was already deployed in vending machines in particular companies in California. They are using IoT to help them in monitoring the temperature of the vending machines, monitoring inventory, and detecting thieves. In the future, this innovative solution may enable vending machines to recognize dropping inventory, recognize product delivery, place orders for more products, and generate a payment to the respective supplier.

If this example has been expanded into the supply chain of other niche industries, the chances on how the Internet of Things can impact daily business becomes endless. Hospitals will be able to place new orders for supplies before the current stocks become scare automatically, which will be improving patient outcomes, and foster better nationwide health.

IoT already exists in several hospitals in which electronic medical records are identifying the problems in test results and generate a phone call to the respective physician and nurse for the certain patient.

Internet of Things has changed, changing, will continue to change the world, most particularly supply chain processes. Through the benefits of IoT integration into the current processes becoming clearer, more organizations and businesses will be working towards expanding IoT capabilities today.

FRAMEWORK ASSESSMENT OF INTERNET OF THINGS

Designing a safe IoT solution will depend on a number of security considerations. Among the most significant consideration is the use of a secure IoT framework to build one's ecosystem. Using a safe framework will ensure that developers will not overlook security considerations and enables for speedy application development. A framework ideally contains security components baked into the framework in such a way of providing security by default that developers do not need to think about it. This will free the architects and developers and help them focus on the capabilities and features without having to burden their development efforts with security considerations or errors.

There is a vendor agnostic set of evaluation criteria, which architects and developers may use for the measurement of relative security strengths of the IoT development frameworks. This has to serve as a useful benchmark and motivation vendors in producing more robust IoT development frameworks, so as to address the various security issues. The evaluation criteria have been broken down into 4 distinct sections. These sections represent usual IoT system archetypes. Every section has particular security related concerns, which are outlined in the evaluation criteria or framework for that section. These sections are as follows:

1. **Edge** – It is the actual physical device making up the IoT ecosystem. Keep in mind that in different deployments, the edge is heterogeneous and this means that it is made up of any number of device types with different operating systems, communications resources and capability, hardware, or networking. An ideal IoT framework will be able to provide cross platform components in order for that edge code to be deployed anywhere from a normal metal, to an embedded OS, to a mobile operating system, to a completely blown personal computer, and so on.

   The framework considerations for IoT's edge component include:

   - Strong logging – The framework has to offer robust logging, which include security event logging. The log events must be customizable and have to report sensitive events in a format that is usable for managers, operators, and end users.

- Update verification – Updates must be delivered through a secured channel and must be verified after download to make sure that updates are legitimate. Binary checking and signing, and update hashes being delivered over an encrypted and verified channel make sure that malicious updates will not be installed on a device.

- Storage encryption – Sensitive data on the edge is liable to exposure and theft unless it is stored with appropriate security considerations.

- Communications encryption – The encrypted communications have to occur end-to-end every time possible. Remember that several communications can pass through a barrier such as load balancer or gateway, and it can influence the end-to-end encryption.

  Also included in the edge component consideration are no default passwords, offline security features, cryptographic identification capabilities, automatic version reporting and updates, strong local authentication, owner and device authentication, defensive capabilities, transitive ownership considerations, configurable root trust store, secure web interface, and secure M2M capabilities.

2. **Cloud –** The cloud component of the Internet of Things (IoT) ecosystem is referred to the ecosystem's management portion and central data aggregation. It will usually consist of a data storage layer, ecosystem management, reporting and analytics, and more.

   The framework considerations for cloud component include:

   - Authentication – The cloud component enables for complex authentication, which include multi-factor authentication. The interface has to include anti-account enumeration mitigation feature and brute force.

   - Secure web interface – Cloud needs to be built through technology that can bake solutions to usual web application vulnerabilities in the code.

   - Encrypted storage – The cloud component is usually the system of aggregation and record for the whole deployment.

- Secure authentication credentials – In any form, such as IDs, passwords, device, and more, it has to be hashed and salted properly, before the storage.

- Audit capability – It is important to track communications to make sure their appropriate timeframe and delivery. It has to provide mechanism to ensure delivery of targeted messages to particular edge components.

  Other considerations for this component are stack security considerations, ensuring ecosystem segregation, defensive capabilities, extension or plugin verification, automatic update verification, data classification segregation and capabilities, and security event alerting and reporting.

3. **Gateway** – This component usually support weak edge devices, or enable edge devices a bridge networks to cloud components. They can serve as a communications aggregation, controlling bottleneck and enabling for an easy interface between an insecure yet trusted local network, as well as a secured connection to the untrusted public internet. With that, there are also some framework things to be considered, such as:

   - Storage – The gateway can serve as a point of failure in the ecosystem and has to store only the minimum amount of information in an encrypted format if possible.

   - Alerting and logging – The component will be having access to a great volume of traffic and must be able to alert and log based on event logging.

   - Service denial and replay attack mitigation – The gateway must be able to resist and detect attacks from the edge, which include replay, spoofing, and excessive communications.

4. **Mobile –** Mobile interfaces in Internet of Things (IoT) deployments vary in integration and capabilities. Several mobile applications are merely providing limited data reporting from particular edge devices, and others enable for the manipulation of edge components, and still, others are providing a cloud management abilities and complete view analytics.

Through that, the framework considerations to be made include the following:

- Local storage security considerations – The framework has to be mindful of the sometimes limited storage security on mobile devices.
- Strong audit trail of mobile interactions – Since the mobile device may fall into malicious hands, it is important that you keep a security audit trail of mobile app interactions with the ecosystem.
- Encrypted communications channels – Mobile devices are specifically prone to use in encrypted communications and hostile networks, so they have to be the framework default.

  Multi-factor authentication – Mobile devices have extended capabilities of performing multiple factors of authentication. Biometrics and sensors have to be supported by the framework for the mobile platform's extended security checking.

INTERNET OF THINGS SECURITY VULNERABILITIES

The benefits of the internet are really countless and inarguable. One of the best things about this particular modern technology is its inherent abilities to serve us in every course, be it on learning, business and in every single thing that you can think of. Now that we are already in the 21st century where the modern ad advanced technology is very vital, internet of things will always be important in terms of connectivity, sending and receiving of data. Just like the other valuable assets out there, the information and data that we put online must be regarded as a very valuable asset too to any organization that needs an effective and suitable protection against any possible types of threats such as virus and hackers. The internet of things refers to devices other than tablets, smartphones and computers that communicate, connect, and transmit information between or each other via internet.

The Internet of things can offer a number of benefits to all consumers and there are a lot of innovative companies out there that already sell connected devices, sensors, apps, services and many more unlike the things that we have ever seen before. Though that is the case, businesses and consumers alike need to consider the protection and security regarding internet of things, too, after all it is very important to protect each consumer's very sensitive data from any unauthorized access, hackers or thieves. In the world of internet of things, the risk is not just to the information or data but beyond the security dimensions that we considered before with the fact that hackers are now highly modernized too. Here, a certain insecure connection can give access to a hacker not only to the confidential data that are transmitted by the device but also to everything else right there on a certain user's network. If a home automation system is not secure, a hacker can override the settings in order to unlock all the doors. It can really be disturbing to think that a hacker can remotely recalibrate one's medical devices such as a heart monitor or an insulin pump.

When it comes to protection and security, the advanced technology is definitely ever-changing. Despite the numerous benefits of internet of things, with the increased connectivity between the internet and devices, you must expect that there will also be a number of privacy and security risks that may be such a pain in the neck. The following are the OWASP IoT Top 10 Vulnerabilities:

INSECURE WEB INTERFACE

This can be possibly present when issues such as lack of account lookout, account enumeration, or weak credentials are present. This is very much prevalent as the intent here is to have a certain interface exposed mainly on the internal networks, however, the threats from the internal users can be as significant as the threats that are from the external users. The issues regarding the web interface are just quite easy to discover when you manually examine the interface long with the automated testing tools in order to identify issues like cross-site scripting, account lockout and session management.

When an insecure web interface is not addressed in real time, it can result in a great corruption or data loss, and as well as lack of accountability, or a denial of access which can only lead to a complete device takeover. Its impact also in the business can lead to a highly compromised devices as well as compromised customers. With this being said, it is very important that you know if your web interface is secured all the time. The following are ways on how to check an insecure web interface:

- Determine if the default password and username can be changed during the initial product setup
- Determine if a particular user account is locked out right after 3 to 5 failed log-in attempts
- Determine if the valid accounts can be possibly identified using a password recovery mechanism or a new user pages.
- Review the web interface for issues like cross-site request forgery, cross-site scripting, and SQL injection.

Ways on how to make your web interface completely secure:

An insecure web interface can result to a very serious problem that can impact not only your brand or company but can compromise your customers as well. It is very essential that for you to know a secure web interface strictly requires the following:

- Default passwords and usernames to be changed right during the initial setup.

- Ensuring that the password recovery mechanisms are totally robust and don't supply any attacker with data or information which indicates a valid account.
- Ensuring the web interface is not at risk or susceptible to SQLi, CSRF, or XSS.
- Ensuring that the credentials are not susceptible or exposed in both the external or internal network traffic.
- Ensuring that weak passwords are literally not allowed.
- Ensuring the account lookout right after 3 to 5 log-in attempts.

INSUFFICIENT AUTHENTICATION OR AUTHORIZATION

This is another security threat that occurs when a certain website permits an attacker to have an access with sensitive contents or functionalities without having authenticating it properly. A good example of this is the web-based administration tools of websites that provide an access to a number of sensitive functionalities. Depending on the particular online resource, the said web applications must not be directly accessible without strictly requiring the user to verify their own identity properly. In an insufficient authorization/ authentication issue, the attacker uses a weak password, insecure password recovery mechanisms, lack of granular access control or poorly protected credentials in order to have access to a particular interface. The said attacker can come from an internal or external user. It is very good to remember that an authentication may not be that effective or sufficient when the passwords that are used are weak or are poorly protected.

An insufficient authorization or authentication can possibly result in corruption or data loss, denial of access, lack of accountability and as well as to a complete compromise of the user accounts and of the device. In terms of business, it can lead to compromised devices and user accounts and all the data can be modified, stolen or deleted. In order for you to know if your authorization or authentication is effective and sufficient, you can check it by:

For insufficient authentication

- Attempting to use only simple passwords like “1234 “. It can be an easy and fast way to determine if its password policy is bound and sufficient to all kinds of interfaces.
- Reviewing the network traffic in order to determine if the credentials are transmitted in valid and clear text.
- Reviewing all the requirements around that password controls such as password history check, password complexity, password expiration and the forced password reset for the new user.
- Reviewing if re-authentication is needed for the sensitive features.

For insufficient authorization

- Reviewing the different interfaces in order to determine if the interface allow for the separation of roles. Let's say, all features will be open or accessible to the administrators but the users, on the other hand, will have a more limited set of the features that are available.
- Reviewing the access controls as well as the testing for a privilege escalation.

Effective ways on to make your authorization/ authentication even better:

- Always ensure that strong passwords will always be required.
- Ensure that the granular access control is always in place, if necessary.
- Ensure that all the credentials are properly secured or protected.
- Implement 2 factor authentication when possible
- Ensure that the password recovery mechanisms are always secure
- Ensure the re-authentication will always be a requirement for the sensitive features
- Ensure that the options are completely available for/ when configuring the password controls.

INSECURE NETWORK SERVICES

Insecure network services may be prone or susceptible to a buffer overflow attack or any attacks that can create a denial of service condition which may make the device inaccessible to its user. These attacks against the users may be facilitated when an insecure network services are present or available. This particular problem can be detected with the help of the automated tools like fuzzers and port scanners. Here, the attackers use the vulnerable network services to access or attack a certain device or to bounce the attacks off a device. These attacks can come from internal or external users and if they are not addressed immediately or are not prevented, these may result in corruption or data loss as well as denial of service and facilitation of attacks on some other devices.

To check for the presence of an insecure network service, you can try the following ways:

- Determine if the insecure network service exists by reviewing the device for an open ports with the use of a port scanner
- When you have already identified the open ports, each can be checked or tested by using any number of automated tools that works on looking for any DoS vulnerability or any vulnerabilities which are related to UDP services. You can also look for vulnerabilities that are related to fuzzing attacks or buffer overflow.
- Review the network ports in order to ensure that they are completely necessary and as well as if there are any ports that are exposed right to the internet via UPnP.

Ways to secure your network services:

- Ensure only the necessary ports are being exposed to the internet and are made available.
- Ensure the services are not susceptible or vulnerable to any fuzzing attacks or buffer overflow, as well as to DoS attacks that can just impact or affect the device itself or the other devices or users right on the local network and other networks.
- Ensure the network services or ports are not being exposed to the internet via UPnP, for example.

LACK OF TRANSPORT ENCRYPTION AND TESTING

This allows the communication to be possibly exposed to any untrusted 3rd parties which provides a certain attack vector to completely compromise the web application and steal the sensitive information. Here, the attackers use lack of transport encryption to access or view the data that is being passed over a network. The attack can be from an internal or external user and it is very prevalent on networks, particularly the local networks, as it is quite very easy to assume that their traffic will not be that widely visible. In the case of the local wireless networks, misconfiguration of the wireless networks can make the traffic visible very much visible to any person within the range of the wireless networks. If this is not prevented or is not addressed, this problem may result in great data loss, and depending in the information or data that were exposed, it can also possibly lead to a complete compromise of the user accounts and of the device itself.

Checking for lack of transport encryption includes:

- Reviewing for the network traffic of a certain device, its possible mobile applications and any cloud connections in order to determine if there are any information that is passed in a valid and clear text
- Reviewing the possible use of TLS or SSL to ensure that it is up to date and is properly implemented
- Reviewing the possible uses of any kind of encryption protocols to ensure that they're accepted and recommended.

Ways on how to use a sufficient transport encryption:

- Ensure that the data is encrypted using protocols like TLS and SSL while transiting networks.
- Ensure that the other industry standard encryption techniques are used to protect the data during the transport if the TLS or SSL are not accessible or available.
- Ensure only the accepted encryption standards that are being used and avoid the use of propriety encryption protocols.

PRIVACY CONCERNS/ TESTING

Here, the attackers use multiple vectors like lack of transport encryption, insufficient authentication or insecure network services to access or view personal data which are not properly secured or are being collected unnecessarily. The collection of this personal data along with the insufficient protection of the data can possibly lead to a compromised user's personal data. IN checking for privacy concerns, you must:

- Identify the data types that are collected by a device, the mobile applications and cloud interfaces.
- Collect only the necessary things to perform at its proper function.
- Review the persons who have access to it and determine if the data can be anonymized or de-identified.
- Data if a data retention policy is required or in place.

How to prevent or minimize privacy concerns:

- Ensure only the data which is critical to the device's functionality.
- Ensure that the collected data is de-identified or anonymized as well as protected with encryption.
- Ensure that the device and its components is properly secure personal data or information
- Ensure that only the authorized individuals can have access to important information and there is a retention limits that are set for all the collected data.
- Ensure that there is a notice and choice that is provided for end-users if the information collected is more than what is actually expected from a certain product.

INSECURE CLOUD INTERFERENCE

Insecure cloud interference is present when the account enumeration is possible or when the easy to guess credentials are used. Usually, this can easily be discovered by simply reviewing the cloud interface connections and determining if the SSL is actually in use or by using the reset password mechanism in order to identify the valid accounts, which can lead to the account enumeration.

Basically, the attackers use multiple vectors like insufficient authentication, account enumeration, and lac of transport in order to get an access to the controls or data through the cloud website. The attacks usually come from internet and this could lead to compromise the control and user data over the device. The data could be modified or stolen and the control over the devices can be assumed, which could definitely harm your brand and customers as well.

So, is your cloud interface completely secure? In order to check for an insecure cloud interface, one should do the following:

- Determine if the default password and username can be changed during the initial setup of product.
- Determine if a specific account of user can be locked out after 3 to 5 failed login attempts.
- Determine if the valid user accounts can possibly be identified using the mechanisms such as password recovery or via new user pages.
- Review the interface issues such as cross site request forgery, cross site scripting and SQL injection.
- Review the entire cloud interfaces for any kind of vulnerabilities including the could-based web interfaces and API interfaces.

How can you secure your cloud interface? In order to secure a cloud interface it requires the following:

1. The default passwords and ideally, the default usernames to be changed during the initial setup.
2. Ensure that the user accounts can't be enumerated by using any functionality like the password reset mechanisms.
3. Ensure that accounts will lock out after 3 or 5 failed login attempts.
4. Ensure that the cloud-based web interface isn't susceptible to the SQLi, XSS or CSRF.
5. Ensure that the credentials aren't exposed throughout the internet.
6. If possible, implement a two-factor authentication.

INSECURE MOBILE INTERFACE

Just the same with insecure cloud interface, an insecure mobile interface is usually present in mobile application interfaces when weak passwords are made, no 2-factor authentication is being implemented, and no account lockout mechanism is featured.

The simple solution for this vulnerability is to do exactly what a mobile interface lacks; ,make strong passwords, implement two-factor authentication, and implement an account lockout feature after several failed login attempts.

Usually, the attackers uses numerous vectors like account enumeration, lack of transport encryption and insufficient authentication in order to get an access on controls or data through the mobile interface, which could also lead to compromising the user control and data over the mobile devices.

So, is your mobile interface secure? In order to check if it is, you need to identify the following:

- Determine if the default password and username can be changed during the initial setup of mobile product.
- Determine if there's an account lockout feature after 3 to 5 failed login attempts.
- Determine if the valid accounts can be identified through the use of mechanisms like password recovery or the new user pages.
- Review whether the credentials are visible while being connected to the wireless networks
- Review whether the 2-factor authentication option is available.

To secure a mobile interface, it requires the following:

1. Changing of default usernames and passwords during the initial mobile product setup.
2. Ensuring that the user accounts can't be enumerated through the use of functionalities like the password reset mechanism.
3. Ensure an account lockout after several failed login attempts.
4. Ensure that the credentials are completely hidden during the connection with wireless networks.
5. Implement the 2-factor authentication as much as possible.

INSUFFICIENT SECURITY CONFIGURABILITY

Insufficient security configurability is a kind of vulnerability present when the users of device have no or limited ability to alter their security controls. This is usually apparent when the device's web interface has no available options for creating the granular permissions for user or for instance, forcing the use of very strong passwords. The manual review of web interface as well as its available options will be the one to reveal these deficiencies.

Usually, the attackers took advantage of the granular permissions in order to access the data or the controls of device. They could also take the advantage when there's a lack of encryption options as well as lack of password options in order to perform their other attacks, which can compromise the data or the device itself. The attacks can potentially come from any user of device, whether accidental or intentional.

Is your security configurability sufficient? In order to check, simply do the following:

- Review the device's administrative interface for the options in order to strengthen its security like forcing of strong password creation.
- Review its administrative interface for the capability of separating the admins users from the normal users.
- Review the encryption options administrative interface.
- Review the options on administrative interface in order to enable a secure logging for several security events.
- Review the administrative interface in order to enable the notifications and alerts to the end users for the security events purpose.

In order to improve your security configurability, it would require the following:

1. Ensure the ability of separating the normal users from the administrative users
2. Ensure the ability of encrypting data in transit or at rest.
3. Ensure the ability of forcing the strong password policies
4. Ensure the ability of enabling the logging of security events
5. Ensure the ability of notifying the end users of the security events.

INSECURE SOFTWARE/FIRMWARE

The devices' lack of ability to become updated shows security vulnerability on its own. The devices should always be capable of updating themselves when the vulnerabilities or security issues are discovered, and the software/firmware updates can also become insecure when the updated files as well as the network connection that are delivered are not completely protected. The software/firmware can also become insecure if they contain sensitive hardcoded data like credentials. The security issue regarding the software/firmware are somewhat easy to be discovered by simply inspecting the amount of traffic during the update in order to check for the encryption, or by simply using a hex editor in order inspect the updated files for the interesting formation.

The insecure software/firmware attackers usually use multiple vectors like capturing the updated file through the unencrypted connection, the updated files itself isn't encrypted or they're capable of performing their own malicious update through DNS hijacking. Depending on the update methods as well as the device's configuration, the attack would potentially come from local internet or network, which could lead to compromise of user data, attack against other devices and control over the devices.

So, how would you know if your software/firmware is secure? First and foremost, it's very important to note that the devices should be capable of updating and perform regular updates themselves. If they are, checking for insecurities on updates should include:

- Reviewing of the updated files for the exposure of its sensitive information in the human readable format for those who use hex editor tools.
- Reviewing of the production updated files for the proper encryption through the use of accepted algorithms.
- Reviewing of the production updated files in order to ensure that it's properly signed.
- Reviewing of the method used for communication during the transmission of update.

- Reviewing of the cloud updated service in order to ensure that the encryption methods for transport are up-to-date and configured properly and also the service itself isn't vulnerable.
- Reviewing of the device for the proper validation of the signed, updated files.

In order to secure your software/firmware, you need to do the following:

1. Ensure that the device is capable of updating and can perform regular updates
2. Ensure that the update files are encrypted through the use of several accepted methods for encryption.
3. Ensure that the updated files are transmitted through the use of encrypted connection.
4. Ensure that the update is verified and signed before your allow the update to be applied or uploaded.
5. Ensure that the update server is completely secured.

POOR PHYSICAL SECURITY

The poor physical security is present in the device when the attacker is capable of disassembling the device easily to get an access in the storage medium or any data store on the medium. Poor security is also present when the USB ports or any other external ports can possibly be used in order to get an access on the device using the features that are intended for the maintenance or configuration.

Anyone who has a physical access on the device can be a threat agent and they may use several vectors like SD cards, USB ports, and other external storage means in order to get an access on the operating system and probably, any kind of data that are stores on the device.

Is your physical security sufficient? In order to check if it is, you need to do the following:

- Review how easy your device can be disassembled and your data storage mediums can be removed or accessed
- Review the usage of any external ports in order to identify if the data can be accessed even without disassembling the device.
- Review several physical external ports in order to determine if all of them are needed for proper function of device.
- Review the administrative interface in order to determine if the external ports like USB can be used for deactivation.
- Review the administrative interface in order to identify if the admin capabilities can be narrowed to the local access only.

In order to physically secure your device, you need to do the following:

1. Ensure that the data storage medium can't be removed easily
2. Ensure that the stored data is completely encrypted even at rest
3. Ensure that any external ports can't be used in order to get an access in your device.
4. Ensure that the device can't be disassembled easily.
5. Ensure that the product is capable of limiting the admin capabilities.

CONCLUSION

IoT and big data go hand in hand. Within a very short period, connected sensors are able to produce great masses of information. In order to make all those data actionable and meaningful, manufacturers have to take advantage of the right reporting tools and business intelligence. They also have to find ways of looping their findings into product design and engineering. Because of that, there has to be close connection between analysis, data gathering, and product lifecycle management or PLM systems.

Anywhere and anytime, manufacturers are using complicated and expensive machinery as a key asset production, the connected sensors in the global IoT is able to report on materials, output, and key performance and quality metrics. Teams of people would no longer need to travel in order to visit the production sites for recording their findings on manual basis. Data from the IoT can draw instant attention, followed by corrective and timely action, such as maintenance, repair and replacement.

In the future, whether it is 2020 or 2025, Internet of Things will become the most important part of one's life, for it is going to connect various sources of information such as cars, sensors, and mobile phones in an even tighter manner. The number of devices connecting to the internet increases. These billion of components are consuming, processing, and producing information in various environments, which include airports, logistic applications, and factories, along with the work and daily lives of people. IoT is the upcoming technology with countless benefits and particular assumed drawbacks. However, those drawbacks can be transformed into benefits by little bit of more research and system advancement for it will become the most efficient part of people's lives in the near future.