Internet of Things
Risks & Mitigation
Table of contents

1. Cyber Security Overview
   1.a Abstract

2. Insecurity in the Internet of Things
   2.a Introduction
   2.b IoT Security Threat Map
   2.c IoT Security Issues
   2.d IOT Privacy Issues
   2.e Mitigation

3. Making a secure thing

4. Conclusion
Cyber Security Overview

1a. Abstract

Today’s cyber security landscape is an ever-changing environment where the greatest vector of attack is our normal activities, E-mail, Surfing, etc. The adversary can and will continue to use Mobile apps, E-mail (phishing scam), the web (redirects) and other tools of our day-to-day activities to get intellectual property, personal information, and other sensitive data. Hactivists, criminals, and terrorists use this information to gain un-authorized access to systems and sensitive data. Hactivists commonly use this information that is gathered during attacks to support and convey messages that support their agenda. According to Symantec, there were 163 new vulnerabilities associated with mobile computing, 286 million unique malware variants, a 93% increase in web attacks, and 260,000 identities exposed in 2010. McAfee reported that during the first two quarters of 2011 there were 16,200 new websites with malicious reputations, and an average of 2,600 new phishing sites appeared each day.

We have also seen the proliferation of new technologies like Internet of Things into our day-to-day activities. New smart phones and tablets have become as common as the home computer. Technologies like IoT are considered as future technology & new technology means new vulnerabilities.

Insecurity in the Internet of Things

1a. Introduction

The Internet of Things is connecting more devices every day, and we’re headed for a world that will have 24 billion IoT devices by 2020. That’s more than 4 devices for every human on earth. The Internet of Things first came to us on PCs. Then it moved to smart phones, tablets, smart watches, and TVs. But now it’s coming to all of our everyday devices that fall under the IoT umbrella. The Internet of Things (IoT) has become a ubiquitous term to describe the tens of billions of devices that have sensing or actuation capabilities, and are connected to each other via the Internet. The IoT includes everything from wearable fitness bands and smart home appliances to factory control devices, medical devices and even automobiles. Security has not been a high priority for these devices until now. There has been a lot of discussion regarding the hacking of devices and systems to obtain information and data. However, just as critical are cyber-attacks against the devices themselves - attacks which take over control of the device and cause them to operate in dangerous and insecure ways. Late last year, a group of hackers took down a power grid in a region of western...
Ukraine to cause the first blackout from a cyber attack. And this is likely just the beginning, as these hackers are looking for more ways to strike critical infrastructure, such as power grids, hydroelectric dams, chemical plants, and more.

2b. IoT Security Threat Map

Source: Beecham Research
3b. IoT Security Issues

Insecure Web Interface
To exploit this vulnerability, attacker uses weak credentials or captures plain text credentials to access web interface. The impact results in data loss, denial of service and can lead to complete device take over.

Insufficient Authentication/Authorization
Exploitation of this vulnerability involves attacker brute forcing weak passwords or poorly protected credentials to access a particular interface. The impact from this kind of attack is usually denial of service and can also lead to compromise of device.

Insecure Network Services
Attacker uses vulnerable network services to attack the device itself or bounce attacks off the device. Attackers can then use the compromised devices to facilitate attacks on other devices. This vulnerability was exploited by hackers that used 900 CCTV cameras globally to DoS attack a cloud platform service.

Lack of Transport Encryption
A lack of transport encryption allows 3rd parties to view data transmitted over the network. The impact of this kind of attack can lead to compromise of device or user accounts depending upon the data exposed.

Privacy Concerns
Hackers use different vectors to view and/or collect personal data which is not properly protected. The impact of this attack is collection of personal user data.

3. IoT Privacy Issues

Too Much Data
The sheer amount of data that IoT devices can generate is staggering. This creates more entry points for hackers and leaves sensitive information vulnerable.

Eavesdropping
Manufacturers or hackers could actually use a connected device to virtually invade a person’s home. German researchers accomplished this by intercepting unencrypted data from a smart meter device to determine what television show someone was watching at that moment.

Consumer Confidence
Each of these problems could put a dent in consumers’ desire to purchase connected products, which would prevent the IoT from fulfilling its true potential.
4. Mitigation

Manufacturers of IoT devices should ensure that they implement basic security standards at the very least:

- Use SSL/TLS-encrypted connections for communication
- Mutually check the SSL certificate and the certificate revocation list
- Allow and encourage the use of strong passwords
- Require the user to change default passwords
- Do not use hard-coded passwords
- Provide a simple and secure update process with a chain of trust
- Provide a standalone option that works without internet and cloud connections
- Prevent brute-force attacks at the login stage through account lockout measures
- Secure any web interface and API from bugs listed in the OWASP List of Top Ten Web vulnerabilities
- Implement a smart fail-safe mechanism when connection or power is lost or jammed
- Where possible, lock the devices down to prevent attacks from succeeding
- Remove unused tools and use white listing to only allow trusted applications to run
- Use secure boot chain to verify all software that is executed on the device
- Where applicable, security analytics features should be provided in the device management strategy

Unfortunately, it is difficult for a user to secure their IoT devices themselves, as most devices do not provide a secure mode of operation. Nonetheless, users should adhere to the following advice to ensure that they reduce the risk of these attacks:

- Use strong passwords for device accounts and Wi-Fi networks
- Change default passwords
- Use a stronger encryption method when setting up Wi-Fi networks such as WPA2
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Be careful when buying used IoT devices, as they could have been tampered with
- Research the vendor’s device security measures
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available
- Use devices on separate home network when possible
- Ensure that an outage, for example due to jamming or a network failure, does not result in a unsecure state of the installation
- Verify if the smart features are really required or if a normal device would be sufficient
Making a secure thing

Building protection into the device itself provides a critical security layer - the devices are no longer depending on the corporate firewall as their sole layer of security. In addition, the security can be customized to the needs of the device. Security must be considered early in the design of a new device or system. Support for secure boot or device tamper detection requires specific hardware capabilities, so this capability must be considered prior to that decision. Since many embedded devices are deployed outside of the standard enterprise security perimeter, it is critical that security be included in the device itself.

Conclusion

This paper has presented framework for developing & deploying Secure Internet of Things. I have put my views base on the articles available on internet as well research published by various agencies.

Many of today’s modern embedded devices and systems are complex connected devices charged with performing critical functions. Including security in these devices is a critical design task. Security features must be considered early in the design process to ensure the device is protected from the advanced cyber-threats they will be facing now as well as attacks that will be created in the future. These are the steps to make your things secure and help create the Internet of Secure Things.
Get in touch

TATA TELE BUSINESS SERVICES
Market leaders with the widest range of products and solutions.

| Collaboration | Connectivity | Cloud & SaaS | IoT Solutions | Marketing Solutions | Security Solutions |

Call 1800 266 1800
Email dobig@tatatel.co.in
Visit www.tatateleservices.com

Find us on

Author Name: Tata Tele Business Services