Unit - VI

Security in IoT

6.1 Introduction

6.2 Vulnerabilities of IoT

6.3 Security Requirements

6.4 Challenges for Secure IoT.

6.5 Threat modeling

6.6 key elements of IoT security:-

6.6.1 Identity establishment

6.6.2 Access control

6.6.3 Data & message Security

6.6.4 Non-repudiation & availability

6.6.5 Security model for IoT

6.6.6 challenges in designing IoT applns

6.6.7 lightweight cryptography

6.1) Introduction:-

Securing the IoT nlw has always been a major issue. In routine security assessment, flaws are discovered in s/w, even in the old codes which are well-used. Several IoT appliances/ devices cannot be patched with security fixes as a result almost all devices will be at risk.

Moreover, IoT Sensors which collects the data from these IoT Devices are also amazing 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.

6.2) Vulnerabilities of IoT:-

- Weak, guessable passwords:-
  Most IoT devices come with preset credentials that are provided by the manufacturer. These default credentials are publicly available and can be easily broken through brute-force attacks.
- Unsecured nlw services:-
  One of the core features of IoT devices involves networking

capabilities that allow endpoints to communicate amongst themselves over a secure internet conn^{n}.

- Unhealthy IoT ecosystems:-
  When IoT devices are integrated with centralized mgmt platforms and legacy systems, users can unknowingly introduce security vulnerabilities at the appln layer.
- Inefficient update mechanisms:-
  To prevent IoT devices from being compromised, companies must be able to send real-time update to each endpoint as soon as they are made available.
- Lack of privacy protections:-
  IoT devices often collect & store user's personal info which may be compromised if hackers are able to bypass built-in security features.
- Improper data tranfer & storage:-
  Even the most robust IoT equipment can be exploited if users fail to encrypt data within their IT ecosystems.

6.3) Security Requirements:-

- Best Secure Coding Practices should be followed:-
  Developers must take steps to ensure that device & services do not contain

Vulnerabilities in the implementation.
- Use of TLS for all nlw communicⁿs:
  All commⁿs on a networking stack with a medium that is shared with other device not part of this deployment must use at least TLS 1.0, and should use at least 1.2.
- Verified firmware updates:-
  All firmware updates must be deployable on a large scale. In particular, there must not be any step requiring per-device manual intervention.
- Strong Authentication mechanisms:-
  All access to configuration settings, firmware updates & sensitive data in any device or service must be protected by strong authentication.
- Unique MAC Addresses:-
  At all times that a device is present on a wired ethernet or wifi nlw, it must use a unique mac addⁿ.
- No comm with third-party servers:-
  Device & services must not communicate with any third-party server outside of the google nlw, except for explicitly approved connⁿs.
- Bluetooth Security:
  Device supporting Bluetooth must support Bluetooth 4.0 or

higher.

- Sync clocks with NTP:- All device clocks must be synced to a n/w time protocol server.
- No external N/W connectivity:- Devices & services must not provide n/w connectivity that could bypass n/w firewalls.
- Use of Non-Wifi Wireless Interfaces:- many IoT devices make use of Non-Wifi wireless interfaces in the 900 MHz or 2.4 GHz ISM bands, including technologies like 802.15.4.

6.4) IOT Security Challenges:-

1) The Rise of Botnets:-
In recent years, there has been an increase of botnets among IoT devices. A botnet exists when hackers remotely control internet-connected devices & use them for illegal purposes.

2) More IOT Devices:-
A few years ago, security professionals were focused solely on protecting mobile devices & computers.

3) Lack of Encryption:-
Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security

Challenges:

4) Outdated legacy Security:-
In addn to the vulnerabilities of the IoT devices, the other concern is with interconnected legacy systems. In enterprise with a growing number of IoT devices, legacy tech might seem out of place.

5) Weak Default Passwords:-
many IoT devices come with original default passwords that are weak. Although it is recommended that you change the pass, some IT leaders fail to take this simple step.

6) Unreliable Threat Detectn methods:-
Enterprises have numerous methods of detecting data breaches, which involve spotting common indicators, monitoring user activity, and other security protocols.

7) Small Scale attacks In IoT:-
Although Security professionals are focused on preventing large scale attacks, it is actually the small scale attacks that could be among the more serious IoT security challenges.

8) Phishing Attacks:-
Phishing is already a security concern across all enterprises technologies.

9. Inability to Predict Threats:-
Security professionals need to be proactive in order to prevent IoT security breaches before they occure.

10. Infrequent updates:-
S/w update is one way that IT professionals ensure that computers and mobile devices are as secure as can be.

11. IoT Financial-Related Breaches:
With some enterprises using IoT devices for electronic payments, there is always a risk for a hacker to breach and steal the money.

12. User Privacy:-
Enterprises must protect user data.

6.5) Threat Modeling:-
- Threat modeling is a method of optimizing nw security by locating vulnerabilities, identifying objectives, and developing counter-measures to either prevent or mitigate the effects of cyber-attacks against the system.

• Need of Security Threat modeling:-
- Just how bad is the cyber-security situation that we need to create things like threat modeling to help combat it?

- Cybercrime has exacted a heavy toll on the online community in recent years, as detailed in this piece by Security Boulevard, which draws its conclusions from several industry sources.
- As a result of these troubling statistics, spending on cyber-security products & services is expected to surpass $1 trillion by 2021.

Threat Modeling Methodologies:-

There are as many ways to fight cybercrime as there are types of cyber-attacker. For instance, here are 10 popular threat modeling methodologies used today.

1.) STRIDE:-

- **Spoofing:**
  An intruder posing as another user, component, or other system feature that contains an identity in the modeled system.
- **Tampering:**
  The altering of data within a system to achieve a malicious goal.
- **Repudiation:**
  The ability of an intruder to deny that they performed some malicious deed.
- **Information Disclosure:-**
  Exposing protected data to a

User that isn't authorized to see it.

- Denial of service:-
  An adversary uses illegitimate means to exhaust service

2> DREAD:-
- Proposed for threat modeling, but microsoft dropped it in 2008 due to inconsistent ratings.
- Open stack and many other organizations currently use DREAD.
- It's essentially a way to rank and access security risk in 5 categories:-
  - Damage potential
  - Reproducibility
  - Exploitability
  - Affected users
  - Discoverability

3> P.A.S.T.A:-
- This stands for process for Attack simulation & threat Analysis. a seven step, risk centric methodology.
- It starts a dynamic threat identification, enumeration & scoring process.
- One experts create a detailed analysis of identified threats, developers can develop a asset-centric mitigation strategy by analysing the app'n through an attacker-centric

4) Trike:-
- Trike focuses on using threat models as a risk mgmt. tool.
- Threat models, based on requirements models, establish the stakeholder "acceptable" level of risk assigned to each asset class.

5) VAST:-
- Standing for Visual, Agile, and Simple Threat modeling, it provides actionable OIPs for the specific needs of various stakeholders such as app'n architects & developers, cyber security personnel, etc.

6) Attack tree:-
- The tree is a conceptual dig. showing how an asset, or target, could be attacked, consisting of a root node, with leaves & children nodes added in.
- Child nodes are conditions that must be met to ~~false~~ make the direct parent node true.

6.6 Key Elements of Security:-

6.6.1) Identity establishment:-
- Identity mgmt. concerns the unique identification of objects, and authorized then validates the identity relationship betn two parties.
- The CERP report recognizes that further research is needed in the 'development', convergence &

interoperability of technologies for identification & authentication that can operate at a global scale.'

6.6.2> Access Control :-
- It has been recognised that there is a need to exercise access control over at the edge of the nw in the device or, at least, a local access controller for the device.'.
- Access control requires comm^n between entities to request and grant access.
- There are various models for access control such as Discretionary Access Control; role-based access control & attribute-based access control.

6.6.3> Data & Msg. Security :-
- Data privacy is a requirement for data to be available only to authorized users.
- Data privacy is about keeping data private rather than allowing it to be available in the public domain.
- An organization can have data that is private to be organized such as the minutes of mgnt. meetings & financial

- For an individual there is a little chance of data privacy if there is not a legal framework in place to penalize offenders who breach this privacy.
- Data protectn laws oblige organizatn to ensure the privacy & the integrity of this data.

6.6.4> Non-repudiatn & availability:
- Non-repudiatn is the securing service for point-to-point commn's.
- Process by which an entity is prevented from denying a transmitted msg.
- So when the msg is sent, receiver can prove that initiating sender only sent that msg.
- Sender can prove that receive got msg.
- Availability is ensured by maintaing all h/w, repairing immediately where required.
- Also prevent bottleneck occurrence by keeping emergency backup power systems.
- And guarding against malicious actions like Denial of Service (DOS) attacks.

6.6.5> Security Model for IOT:-
- This is huge problem as sensitive information is now available to every intern, contractor or "coasting through their tenure until they

take a new job at your biggest competitor" employee with new access.
- This scenario makes plain the big dependency on a Data Security approach & data classification more in the IoT & organizations

6.6.6) Challenges in designing IoT appln's:
- Connectivity:-
- Connectivity is the first concerning issue, i.e. how to connect devices to the internet & the cloud computing platform.
- For eg., if you need to develop a smart home device, such as an online toaster, you may access a Li-Fi home router or a ZigBee/Z-wave IoT router.

- Security & Privacy:-
- IoT Security has always been controversial issue.
- The first challenge to be considered is that security & privacy of IoT are fundamentally diff. from the new security that we're known.

- Flexibility & Compatibility:-
- As the IoT pattern is continously changing, you must ensure that your product can support future technologies.