Comprehensive study of Communication Security in the Internet of Things (IoT) in Healthcare

Group Members: Ambarish Ravindran (Group leader), Nitesh Gupta (Deputy leader), Ravi Nihalani, Vaishnavi Barla, Ting Chen, Sneha Manjunatha, Hanumantha Narayana Harish Pendela, Maitrayee Pingale, Nikhil Lohia and Sushant Sakolkar.

INTRODUCTION

Motivation:

The advent of IoT is changing the face of healthcare in numerous ways. Though IoT can revolutionize the way doctors and patients interact in a healthcare ecosystem, the security of the IoT healthcare architecture seems to raise eyebrows and limits its capabilities. The recent attacks on IoT healthcare systems has raised questions about whether the benefits of this architecture outweigh its applicability.

Goals:

This Project Report is a detailed study of security in IoT healthcare systems based on the layered architecture of IoT. The project report focuses on security in three important layers: Perception Layer, Network Layer and Application Layer. We have adopted a **top-down approach** to understand and critique how security measures are implemented in each of these layers. Through this comprehensive understanding, we look to compare and contrast the security implementation changes constantly being made on IoT healthcare systems.

Scope:

The scope of this project is focused on addressing the security considerations of ensuring that doctors and patients receive the correct information at the right time, and most importantly in a secure manner. To do this, we have focused on security considerations across three layers namely, the Perception Layer, the Network Layer and the Application Layer. We have looked at pros and cons of approaching a security concern in healthcare security from different angles. Our mail area of focus is categorizing and answering questions in security of healthcare across three domains: **What work has been done, what are our major findings, and what is the current work being done and how does it compare to previous work.**

The project begins with an understanding of security in each of the specified layers in IoT healthcare systems and further goes on to enumerate these concerns in detail based on the above classification.

PROJECT RESULTS

Application Layer Security in IoT Healthcare

I. INTRODUCTION

The Application Layer deals with the high-level functions of programs that may utilize the network. User interface and primary function live at this layer. Doctors access and keep track of patient information using IPads and all hospitals these days have monitors that display patient queue information. All functions not pertaining directly to network operation occur at this layer. [1] - Applying the OSI seven-layer model to Information Security.

Suppose that we apply good security through the underlying layers (1 and 2 layer), with physical isolation (layer 1), private VLANs (layer two), and firewalls with tight packet filter policies (layers 2 and 3). But then we are deficient on our application layer security (layer seven, and often layers six and five), using unpatched server software and poorly written application and script code.

II. THREATS

Following are the threats to application layer:

- One of the prime threats at the Application Layer is poor or non-existent security design of the basic function of an application
- Some applications may insecurely handle sensitive information by placing it in publicly accessible files or encoding it in “hidden” areas which are trivially displayed, such as in the HTML code of a web form.
- Programs may have well-known backdoors or shortcuts that bypass otherwise secure controls and provide unauthorized access.

III. SECURITY

The following steps have been in practice **(current research findings)** to make the application layer safer.

A. Use methods from applications

From the higher levels, outside of the model, user input is a significant threat from both deliberate and accidental standpoints. Doctors may provide unexpected input into the application environment, which if not handled properly could lead to crashes or other unexpected behavior. The unsuspecting hapless physician may cause his application to crash or otherwise fail. A malicious user may be able to use bugs and program flaws to attack and gain access to personal patient data.

B. Use Hardware Security

On the hardware front, Intrusion Detection Systems (IDS) can observe data traffic for known profiles of network activity that can indicate probes for vulnerable applications or an imminent or ongoing attack, as well as detecting the presence of undesirable application traffic that may involve confidential patient information being transmitted to a third-party. Many current host-based firewall systems also include the means to control the access of applications to the network to ensure that only the authorized doctor can gain access to the relevant patient file.

Area of special interest: Cisco has two Cisco IronPort® solutions for email security. It offers an Email Security Appliance (ESA), or as a cloud solution, Cloud Email Security (CES). These solutions provide industry-leading cloud-, virtual-, and appliance-based email security. [2] - Healthcare Security by Cisco, White Paper.

IV. CURRENT RESEARCH IN WEARABLES AND SENSORS

WBAN (Wireless Body Area Network) is the latest trend in technology to monitor the patient's health record remotely using wearable sensors. A high level of system security and privacy plays a key role when protecting this data from intruders who wish to steal patient information for personal benefits.

Architecture of WBAN:
a. Intra-WBAN communication: The communication is done confined to the sensors on the body.
b. Inter-WBAN communication: Communication to the access points and this is where the problem arises.

Security Concerns and measures to be taken:
The **medical conditions of an individual should not reach his/her insurance company** as they may find ways to void the coverage. Public humiliation, losing a job and mental instability are other such examples why security is necessary. Intruders can pass on false information by intercepting an unsecure channel and this can cause unforeseeable problems. The following requirements are outlined as: Data Confidentiality, Data Integrity, Data Freshness, Network Availability, Data Authentication, Secure Management, Accountability etc.
Current Security Measures:

- TinySec represents as a solution to attain link layer encryption and authentication of the data in biomedical sensors networks.
  Biometrics is widely used to secure communication.
- Bluetooth and wireless security protocols for secure patient information transfer.
- Hardware security and encryption techniques.

Security measures to be taken in the future:

- DoS or DDoS attacks are often cited as being at the root of security vulnerabilities in a routing protocol. Malicious information can be inserted via the router. Connecting these WBAN networks with mobile devices require further challenges and research.
- Trust management between the nodes is also a very big issue. There must be dependable, distributed cooperation between network nodes for a wireless healthcare application to operate properly.

Network Layer Security in IoT Healthcare

I. INTRODUCTION

Once the patient information is entered on a device by the concerned medical practitioner, it is necessary to ensure that it is transported and stored securely. This transfer of confidential information is made possible by the Network Layer. Additionally, when the doctor accesses patient information, it is vital that no other third-party can gain access to the system at the same time through processes such as eavesdropping or man-in-the-middle attack.

II. ATTACKS ON NETWORK LAYER

Attacks on the network layer specifically occur in two forms i.e.: protocol- and layer-specific compromise.

1) Standard Protocol Compromise: An attacker deviates from standard protocols (application and networking protocols) and acts maliciously to threaten service availability, message privacy, integrity, and authenticity.

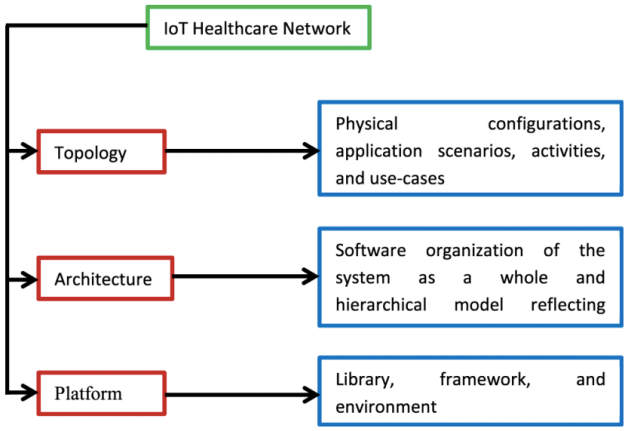

Fig 1. IoT Healthcare Network Security

2) Network Protocol Stack Attack: As shown in Fig. 1, each layer of the protocol stack proposed by the IETF working group for the IoT network has different types of vulnerabilities that an adversary may exploit to launch malicious activities. To improve the performance of IoT healthcare networks with respect to security, longevity, and connectivity under varying environmental conditions, security should be ensured at each layer of the protocol stack.

Connectivity Standards: Enabling IoT Devices to Work Together

Standards represent an inherent challenge for any environment in which a large number of complex devices need to communicate with each other—which is exactly the case for the IoT in healthcare.

Fortunately, standards organizations are working now to create guidelines for wireless communications between monitoring devices and with care providers [1].

III. IOT HEALTHCARE NETWORK CHALLENGES, OPEN ISSUES AND POSSIBLE INTEGRITY ISSUES:

In terms of the design approach, an IoT healthcare network can be of one of **three fundamentally different types: data-, service-, and patient-centric architectures.**

- In the data-centric scheme, the healthcare structure can generally be separated into objects based on captured health data.
- In a service-centric scheme, the healthcare structure is allocated by the assembly of characteristics that they must provide.
- In the patient-centric scheme, healthcare systems are divided according to the involvement of patients and their family members they consider for treatment. In this regard, answering the question of what network type is appropriate for IoT-based healthcare solutions becomes an open issue. [2]

Possible Solutions for Network Layer Information Integrity:

Firstly, establish a four-level security architecture

- Level 1: Network access security: This level is mainly responsible for protecting the radio-link and providing users with security access. Its mechanisms include the integrity protection and ciphering.

- Level 2: Network domain security. This level mainly protects the wire-line networks and enables them to exchange data in a safe manner.

- Level 3: User domain security. Here the scope is between the USIM and the mobile equipment. It would include the mutual authentication of the USIM and the mobile equipment, before they can access each other, using a secret PIN.

- Level 4: Application domain security. The level enables applications information exchanged in the user equipment and the backend network in a security manner [2].

Secondly, enhance the key management

Various keys play a critical role in the working of the overall security mechanism. They are responsible for monitoring the operation of the network and quickly identifying a possible integrity attacks and threats [2].

IV. CURRENT RESEARCH

1. Secure End to End key establishment protocol for resource constrained healthcare sensors in context of IoT

In order to mitigate the security issues in IoT based healthcare applications one needs a secure and powerful network infrastructure.
We need an end to end key establishment protocol which is lightweight for a resource constrained devices and still provides same security functionalities like the unconstrained one's. According to this protocol, the heavy cryptographic operations are offloaded to the neighboring trusted devices.

2. Secure Patient Information Transfer Method through Delegated Authorization

The idea is to propose a secure transfer method of patient information collected from IoT devices among hospitals via a delegated user trusted by the patient using an access token issued by a token repository.

Security Principle: Delegated Authorization [3].

Issue: Any authorized medical personnel can access patient information collected from IoT devices and stored on hospital servers which could lead to leakage of personal information.

Solution: Patient appoints a delegated user to initiate transfer of patient information from Hospital A to Hospital B. Here the delegated user initially receives an access token from Hospital A when the patient registers the delegated user into Hospital A's network. Now, when the patient is admitted to Hospital B and requires his/her information to be transmitted from Hospital A to Hospital B, the delegated user then initiates a request by authenticating himself/herself(using his/her mobile phone) and sending his/her access token to Hospital A along with the information about Hospital B. Hospital A verifies this access token, and encrypts patient's information using the public key of Hospital B. Hospital B decrypts this information using its own private key.

Per the author, only a delegated user can initiate/access patient information collected from various IoT devices by adding an extra layer of security (using access tokens) above the IoT security communication protocols that are used to authenticate and authorize a user.

Name	Definition
Resource Owner(RO)	A patient who saves medical and healthcare information with Hospital A
D-User	An authorized user in trust relationship with RO.
Hospital A	A hospital that constantly saves patient information.
Hospital B	A hospital visited by patient in an urgent situation.
Token, Key Repository	Where Token or Key is stored
Mobile Authenticator	Mobile phone authentication service provider

Table 1: Definitions of terms used in the above scenario

Perception Layer Security in IoT Healthcare

I. INTRODUCTION
The patient information is entered by the doctor and the data is securely transmitted to a storage unit. But, we also must ensure that the end-devices connected to the network are secure. This is where Perception Layer Security comes into picture.

II. CURRENT RESEARCH
1. An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things:
Security areas/techniques proposed [4]:
ECC-based authentication and the attribute-based access control policy.

It defines an Attribute-based Access Control policy and ECC-based mutual Authentication, these methods were introduced to ensure that only the authorized user are given access to certain data or resources. A security analysis was made on few of the following factors:

a. Provide mutual authentication
b. Mitigate DoS attack
c. Defend against node capture attack

2. Current Status, Challenges and Prospective Measures of Perception Layer Security

The perception layer forms the physical layer and is often known as the Sensor Layer. This layer collects data from the sensors and actuators. The 8 general security features that the perception layer of IoT must have are: Confidentiality, Integrity, Availability, Authentication, Light weight solutions, heterogeneity, policies and key management systems.

The security issues specific to perception layer of IoT are:

- strength of wireless signals,
- interception of sensor nodes by attackers and
- the inherent nature of network topology.

There exist three state-of-art security measures as follows that address the specific features and security goals of perception layer IoT.

(1) A mutual authentication scheme for IoT between platforms and terminal nodes.

(2) A lightweight authentication protocol, which ensures mutual authentication between RFID readers and tagged items without introducing large overhead, to secure RFID tags.

(3) ID authentication at sensor nodes. It is a one-time one cipher method based on request-reply mechanism, implemented by using a pre-shared matrix between the communicating parties.

III. SECURITY ISSUES AND SOLUTIONS

Perception layer is divided into perception node and perception network where node is used to get the data while perception network sends the data to its respective destination.

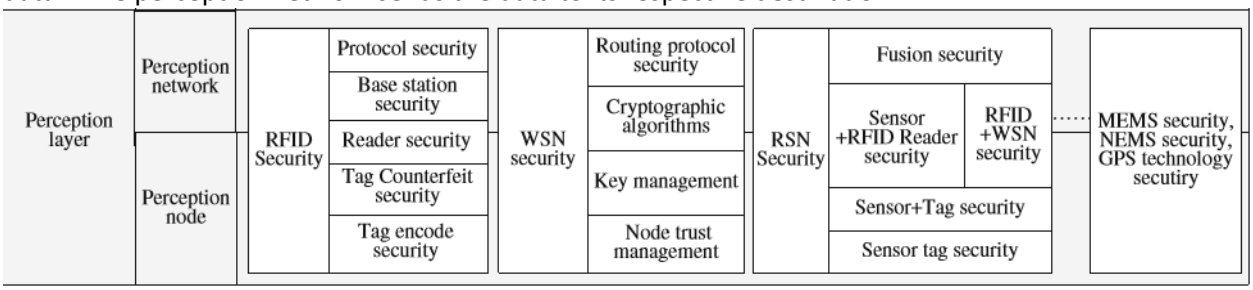

Fig 2. Perception Layer architecture

RFID - Radio frequency identification uses electromagnetic fields to automatically identify and track tag attached objects. This is widely used but it has a lot of problems to it too.

1. There is currently no uniform encoding standard for RFID tag. This may cause problem in reading process. The most influential standards are UID (universal identification) standards and the solution is to use a single standard across the world.
2. There might be collisions when multiple RFID tags transmit data which may cause read error near the reader. The solution to this is to use anti-collision techniques such as Slot, Aloha etc.
3. Low cost tags lead to RFID's limited resources like less storage and weak computation power. Hence it has to be careful about its data privacy and location privacy by using cryptographic techniques and make sure that hackers cannot access the location on the go [5].

References:

[1] David Niewolny Healthcare Segment Manager, Freescale Semiconductor - NXP Whitepaper.
[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, no. , pp. 678-708, 2015.
doi: 10.1109/ACCESS.2015.2437951
[3] J. Park, S. Je, S. Jung and S. Jung, "A secure patient information transfer method through delegated authorization," *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, 2016, pp. 56-60.
doi: 10.1109/ICTC.2016.7763434
[4] Ye, Ning, et al. "An efficient authentication and access control scheme for perception layer of internet of things." (2014).
[5] Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for*. IEEE, 2015.

Papers already read:

[1] The Internet of things for healthcare: A Comprehensive Survey
http://ieeexplore.ieee.org/document/7113786/references
[2] Information Integrity and its protection in networks
http://ieeexplore.ieee.org/document/5303237/
[3] Intel Security
https://www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks.pdf
[4] An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things: Security areas/technique
http://repository.up.ac.za/bitstream/handle/2263/39762/Ye_Efficient_2014.pdf?sequence=1
[5] Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7412116

A gist of papers to read in the future:

[1] Gil, David et al. "Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services".
[2] Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li. "Internet of Things in Industries: A Survey".
[3] Hande Alemdar, Cem Ersoy. "Wireless Sensor Networks for healthcare: A Survey".

Time Table (for next three weeks):

[1] **Focus on protocols** that ensure secure transportation of patient information and their implementation in IoT Security – Harish, Ravi, Ambarish and Maitrayee

[2] Security threats and their solutions for **application layer devices used by medical practitioners** for accessing information such as X-ray monitors, IPads and other medical equipment connected to software – Nikhil, Nitesh and Sushanth.

[3] How **perception layer devices are connected to each other** at the physical layer and how these devices communicate with other layers by transmitting packets securely – Sneha, Vaishnavi and Ting.