Journal of Software Engineering and Applications, 2017, 10, 174-193
http://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Security Framework for Managing Data Security within Point of Care Tests

Sivanesan Tulasidas, Ruth Mackay, Chris Hudson, Wamadeva Balachandran

College of Engineering, Design and Physical Sciences, Brunel University, Uxbridge, UK
Email: eepgsst@brunel.ac.uk

How to cite this paper: Tulasidas, S., Mackay, R., Hudson, C. and Balachandran, W. (2017) Security Framework for Managing Data Security within Point of Care Tests. *Journal of Software Engineering and Applications*, **10**, 174-193.
https://doi.org/10.4236/jsea.2017.102011

Received: November 3, 2016
Accepted: February 21, 2017
Published: February 24, 2017

Abstract

Point of Care (PoC) devices and systems can be categorized into three broad classes (CAT 1, CAT 2, and CAT 3) based on the context of operation and usage. In this paper, the categories are defined to address certain usage models of the PoC device. PoC devices that are used for PoC testing and diagnostic applications are defined CAT 1 devices; PoC devices that are used for patient monitoring are defined as CAT 2 devices (PoCM); PoC devices that are used for as interfacing with other devices are defined as CAT 3 devices (PoCI). The PoCI devices provide an interface gateway for collecting and aggregating data from other medical devices. In all categories, data security is an important aspect. This paper presents a security framework concept, which is applicable for all of the classes of PoC operation. It outlines the concepts and security framework for preventing security challenges in unauthorized access to data, unintended data flow, and data tampering during communication between system entities, the user, and the PoC system. The security framework includes secure layering of basic PoC system architecture, protection of PoC devices in the context of application and network. Developing the security framework is taken into account of a thread model of the PoC system. A proposal for a low-level protocol is discussed. This protocol is independent of communications technologies, and it is elaborated in relation to providing security. An algorithm that can be used to overcome the threat challenges has been shown using the elements in the protocol. The paper further discusses the vulnerability scanning process for the PoC system interconnected network. The paper also presents a four-step process of authentication and authorization framework for providing the security for the PoC system. Finally, the paper concludes with the machine to machine (M2M) security viewpoint and discusses the key stakeholders within an actual deployment of the PoC system and its security challenges.

Keywords

Point of Care Testing, Data Security, Security Framework, Threat Model

1. Introduction

With the exponential rise in clinical devices such as PoC systems [1], clinical network security has become a major issue for biomedical teams and health care organizations [2]. Because of the need for multiplexed detection of viral infections without any easy access to a lab, management of future outbreaks become more involved with the compact portable point of care test devices [3]. Based on the "State of the Internet report" published by Akamai, Port 80 was the top targeted port by advisories in US [4]. In addition, Port 443 [5] based attacks were seen primarily in Indonesia [4]. Port 80 is for the application based on Hyper Text Transfer Protocol (HTTP) and use of port 443 for the applications based on the Secure-HTTP (HTTPS). Targeting ports 80 and 443 implies that the advisories were targeting web-based applications (both HTTP and HTTPS) which are very popular among smartphone users. Smartphones use medical applications based both on the web as well as device specific applications. Clinical instruments and devices such as a PoCT that connect via the smartphone have grown more than 60% in 2012 [2]. As more devices are added, there is an increasing concern with respect to security of the data transmitted in a clinical setup.

The PoC device systems can be classified into three broad categories as shown in **Figure 1**. The categories are testing, healthcare monitoring and alert and interfacing with existing other health monitoring devices. All the classes of the devices need to have strategies and processes to deal with the security concerns.

The current ways of providing security are specific to applications. The IoT related security proposal are available. There is a method for authentication process which is applicable to IoT is described [6]. A proposal for secure communication protocol specifically for the healthcare IoT has been discussed [7]. A security framework for general to address IoT security issues has been outlined [8]. There is need to authenticate the user and the system and the methods and processes are evolving [9]. A method for preventing energy depletion security attacks with ZigBee is explained [10]. A review of security challenges and exiting architectures in the fast growing IoT system has been documented [11]. The important need for having a holistic security framework is mentioned [12]. Though the cloud based storage for medical data is convenient, the accessing of data from the cloud has security issues and the data must be accessed securely [13]. The IoT security can be accomplish in many ways including having the HW and biometrics defense [14]. The challenges of developing m-Health securely for defending privacy of the user community is one of the key aspects in interconnected medical systems [15]. It is very crucial to have security systems to work with multiple interconnected systems that may use multiple communication technologies [16]. There is a need to enhance security of communication links any IoT type of systems for preserving patient's anonymity [17].

Therefore it is important to have a security framework independent of communication technologies and medical applications with flexible enough to use universally. The security framework presented may be used within a hospital network scenario or any other healthcare clinical establishment in which a PoCT

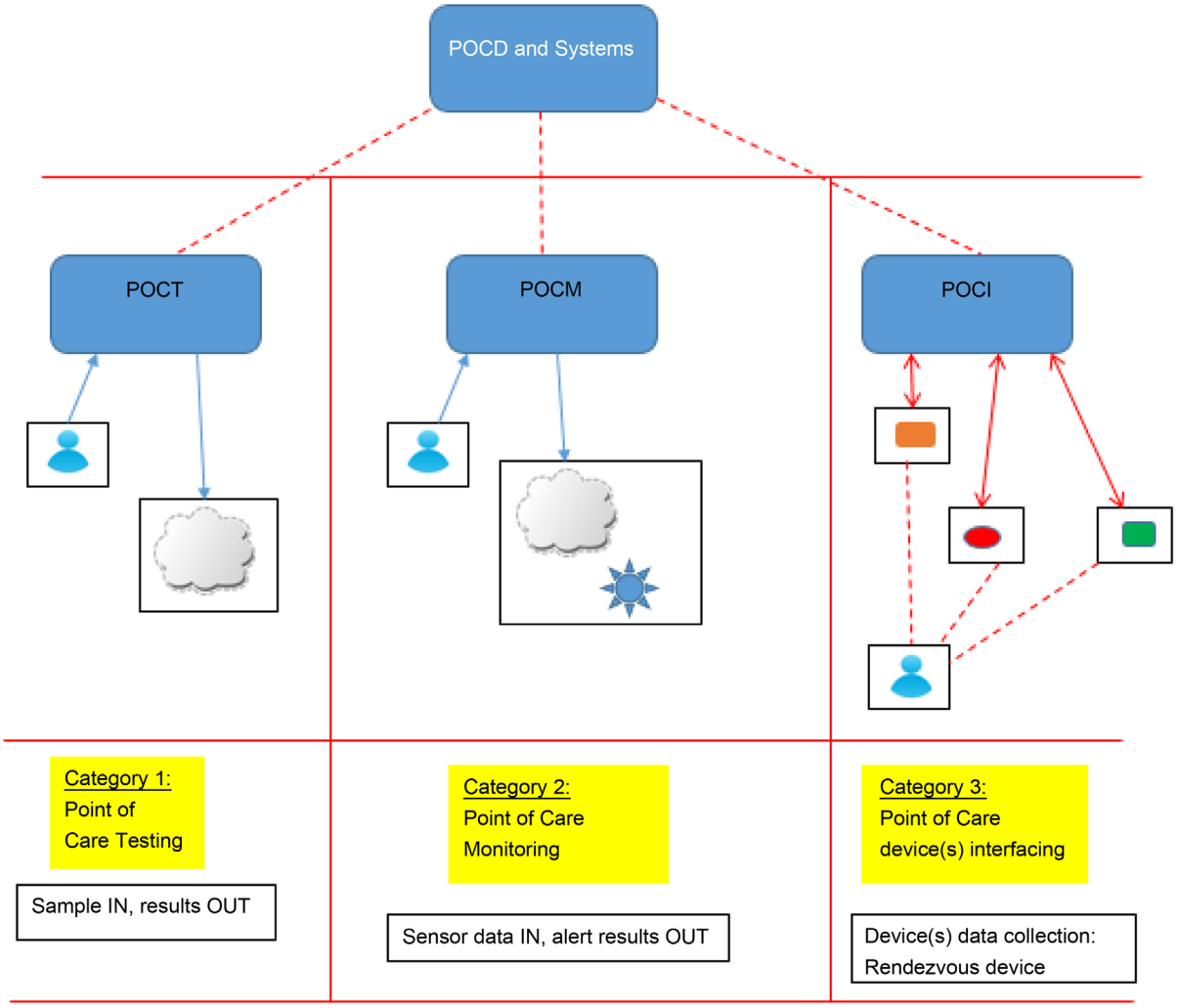

Figure 1. Device usage categories.

is carried out remotely. This paper provides a security framework that can be used in the context of the PoCT devices, system, and networks. The framework is independent of SW and HW of the PoC device.

2. PoCT Configurations

2.1. Architecture Layering

There are three high-level layers as shown Figure 2. The P-Node represents a PoCT device; the G-Node represents a smartphone or another device used for accessing the PoCT device, and the P-Cloud represents the data collection end-point. The three layers outlined here form the basis for security portioning.

Consider the following POC configurations or operational scenarios:

1) The P-Node communicates with the P-cloud without any intermittent gateway entities such as smartphones.

2) Integration of the P-Node and the G-Node as one single unit; *i.e.* the G-Node, which is a smartphone, has all the required sensors and control built-in to conduct the PoCT processes.

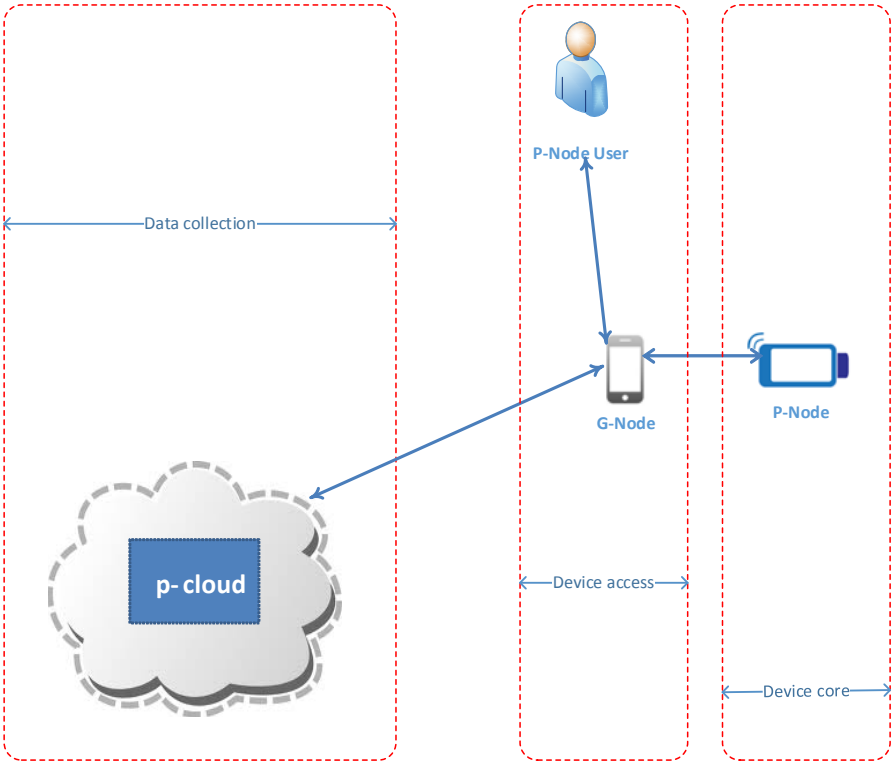

Figure 2. High-Level architecture layers.

In the first case, the PoCT device and associated infrastructure combined provide security functionality. In the 2nd case, the G-Node together with the associated infrastructure assures security. In both instances, a layered model requires a partition strategy that protects all components in the network (PoCT devices, network equipment, secure gateway and secure clouds). This layering approach provides physical security for the end to end system. The layering approach needs to be architected dependent upon the PoC device deployment.

2.2. Security Layering

The designers and architects provide the layering security architecture for the PoC device and PoC service infrastructure. The system implementers of the PoC device and the service providers must ensure that updated security technologies and security products are used to secure data on the PoC device and its associated network infrastructure.

A management layer for managing administrative functions and organizational policies ensures that the patient uses the PoC deployment securely. Service operators involved in PoC deployment use the management layer to configure security and privacy policies on the PoC infrastructure.

As shown in **Figure 3**, all the partitioned layers of security coexist to provide secure data transfer between key entities (P-Node, G-Node, and P-Cloud).

3. Definition of Asset in PoC

Within the PoC domain, an asset is the value of data collected from patients

during PoCT. A threat model ([18] [19]) aids understanding of any potential threat scenarios and threat agents who are deemed likely to carry out a threat. For threat modeling with respect to PoC, a threat modeling tool shows the threat paths for the PoC system.

Attack Tree for PoC System

An attack tree [20] [21] has been built for analyzing the PoC system security implications. This attack tree is shown in **Figure 4**.

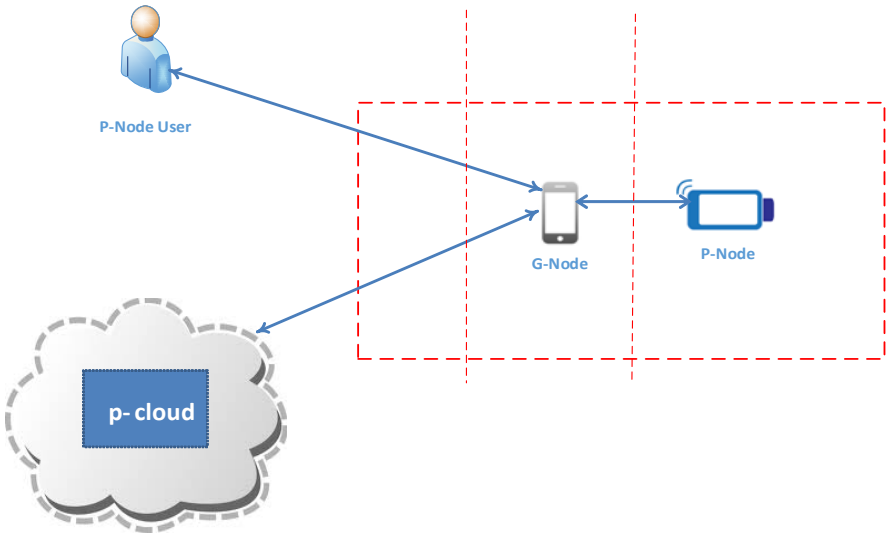

Figure 3. Secure layering of the basic architecture.

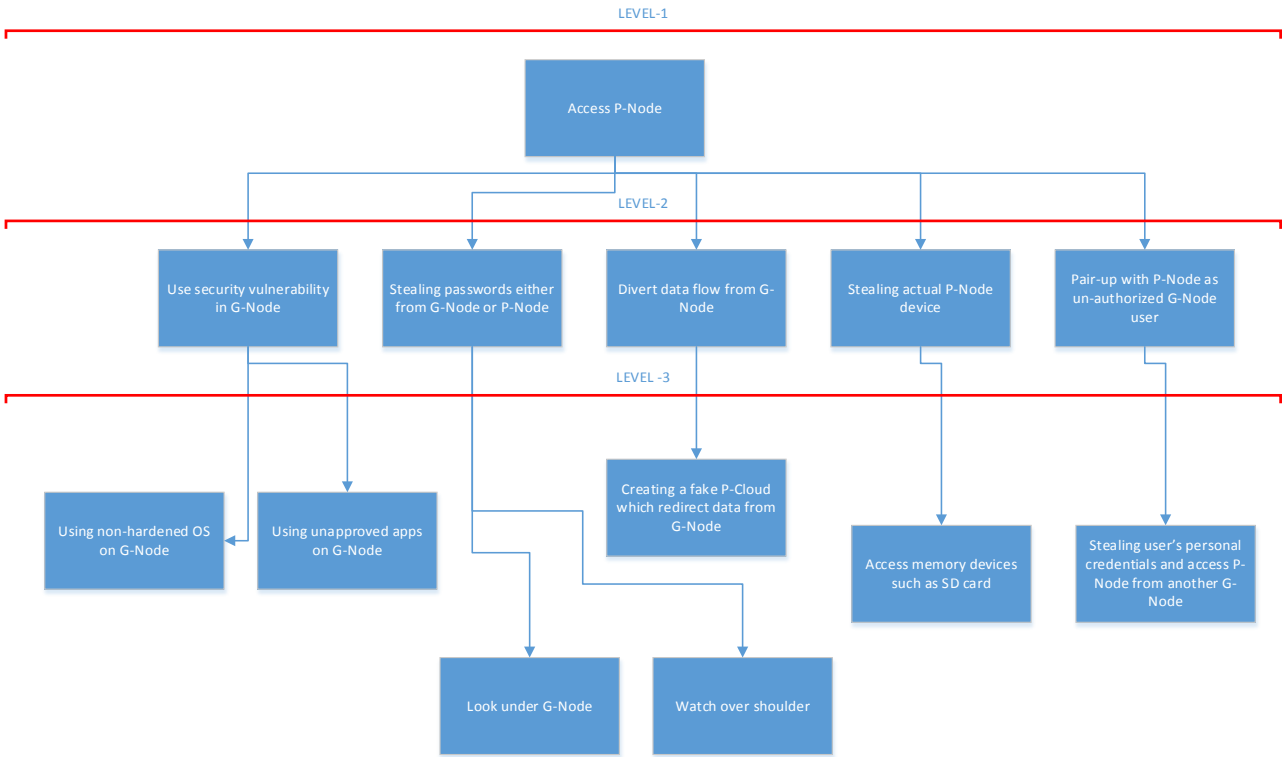

Figure 4. Threat path tree (attack tree).

The Freeport scanner shows that the ports have been configured as filtered (using open source tool [22]: "Network Mapper", also known as "Nmap"). The state is either defined as, open, and filtered, closed or unfiltered. Open means that an application on the target machine is listening for connections or packets on that port. Filtered means that a firewall, filter, or another network activity is blocking the port. Therefore, Nmap cannot determine whether it is open or closed. The closed ports have no application listening to them (*i.e.* they are available to use), and an application can open them at any time [23]. Ports are identified as unfiltered when they are responsive to the Nmap probes. However the Nmap cannot determine whether they are open or closed [23].

The setup configuration used to experiment with the tool is shown in **Figure 5**. **Figure 6** displays the configuration of the Nmap tool. **Figure 7** shows the output of a sample scan run.

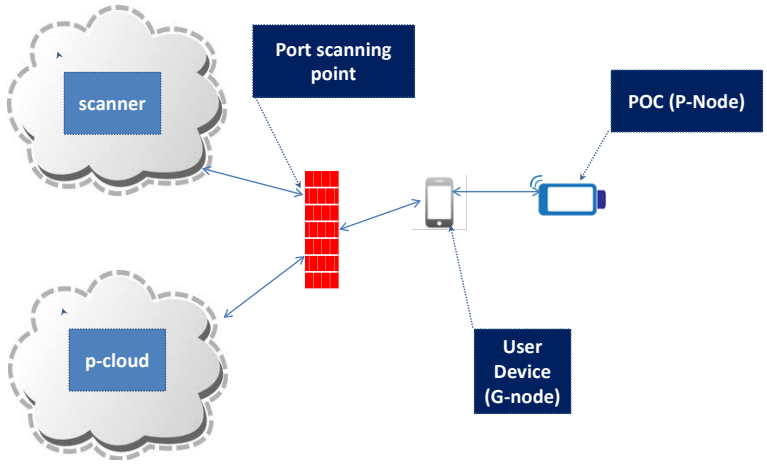

Figure 5. Port scanning setup.

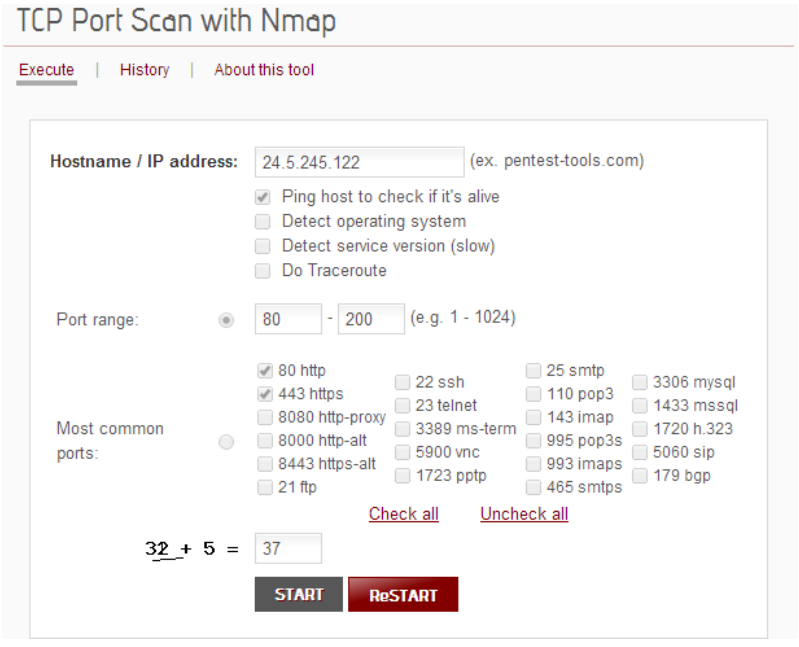

Figure 6. Configuration of port scanning tool.

4. Use Cases

In the PoC domain, an intruder targets applications, run on the P-node or G-Node which range from web application attacks, client-side attacks, and buffer overflow attacks [24].

4.1. Web-Based PoC Access

Web-based applications are one of the ways in which application developers create smartphone applications that will be used to control the P-node. One of the mechanisms to secure web applications is to apply well-known security hardening patches for web servers and provide adequate network protection.

Figure 8 shows the application of the Web server that was running on the

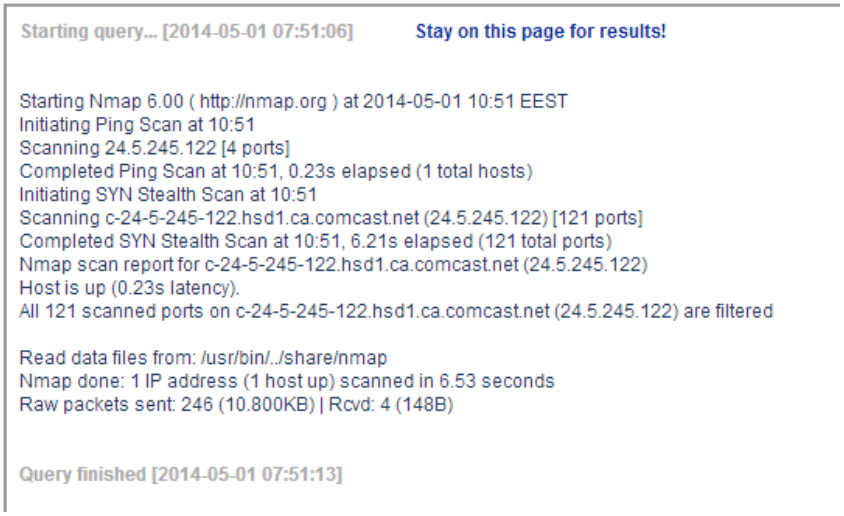

Figure 7. Scanned results.

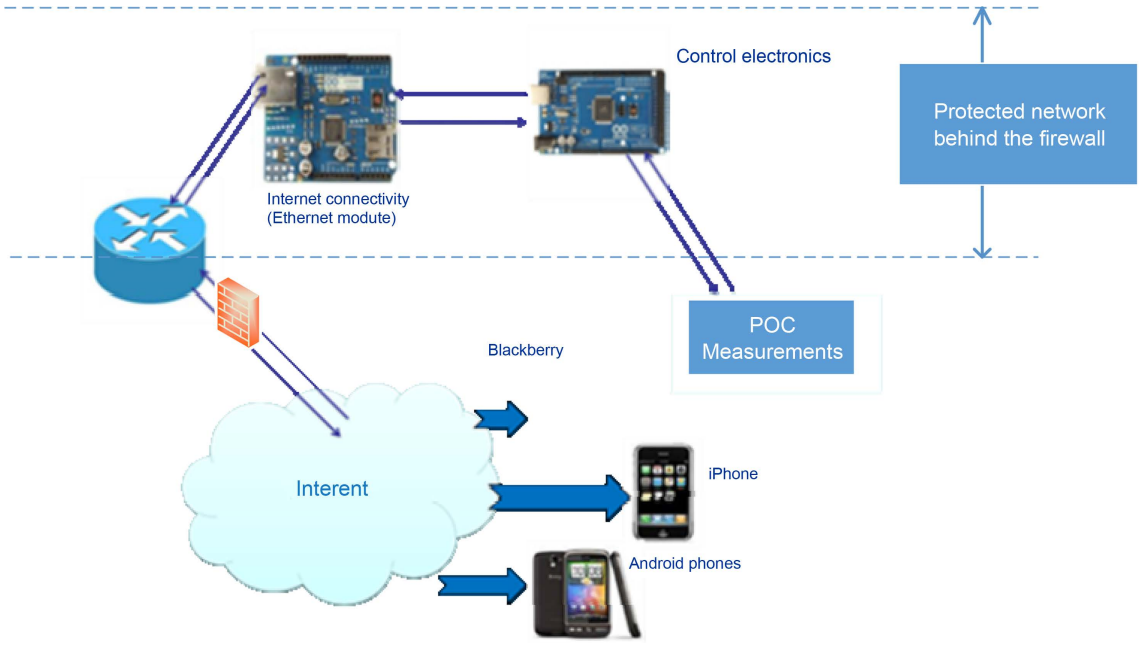

Figure 8. Embedded Web server with PoC.

PoC device. The PoC device was situated behind a firewall and a router. This configuration is an example of a protected network behind a firewall.

Web browsers are a readily available feature on any smartphone. An embedded web server was implemented in the PoC device, and a public Internet IP address was provided (via port forwarding at the router) for access to the web server. The smartphone was able to obtain the IP address to look at the PoC measurement data using the embedded web browser.

Common web application attacks such as cross-site scripting, SQL injection, XML injection and command injection are also applicable to PoC systems. Any HTTP request from the smartphone may be subject to these common web attacks.

4.2. Cross-Site Scripting

In the cross-site scripting (XSS) attack in the context of PoC access, malicious instructions can be sent to the smartphone browser. A standard browser cannot distinguish between valid code and a malicious script, and it accepts user input without validation. The main goal of the XSS is to steal information that is retained by the browsers. Therefore, it is necessary to have an approved browser that is configured to run PoCT web applications. The standard browsers available on the smartphones are not advisable for accessing medical applications. There are secure frameworks available for developing secure mobile embedded browsers [25]. There are many techniques has been developed to secure browsers for data transfer [26]. Applications such as MedCheck [27] are needed on the smartphones for PoC applications. For developing embedded secure web servers, an architecture similar to Sizzle platform is required in securing PoC web servers [28].

4.3. SQL Injection

By entering an incorrectly formatted e-mail address, an attacker attempts to analyze whether the input is being validated. Then the attacker will use SQL statements to collect data from the database. This illegal, unauthorized access of data can be prevented if all the fields are validated in the HTTP website code. To ensure that the data field validation is implemented, a mandatory requirement must be created. This requirement will be implemented and tested before the deployment of the web application.

4.4. XML Injection

HTML instructs the browser to display text in a particular format. XML carries data instead of indicating how to display it using a predefined set of tags, mostly defined by the user application. If the website that does not filter user data, it will be prone to XML tag injection. This process will modify data stored in the P-Cloud database. By implementing the requirement for data filtering, the XML injection attacks can be prevented.

A compromised G-Node will lead attacks on the web server that resides with-

in the PoC device. An attacker can gain access to the operating system on the PoC device via the infected G-Node. One of the HTTP header fields is called a referrer field that indicates the site that generated the web page. Attackers can modify this field to hide the fact it came from another website (a website similar to PoC web server); a modified web page hosted from attacker's computer. The accept-language field is another HTTP header; some web applications pass contents of this field directly to database (P-Cloud). This field could be used to inject SQL commands to get patient data.

4.5. Client-Side Attacks

So far the attacks related to the web applications have been discussed. Server-side attacks and client-side attacks also target vulnerabilities that exist in client applications. Examples of a client side attack are that the client application interacts with a compromised server or the client initiate a connection to the server, which could result in an assault.

The security of the G-Node, *i.e.* the client computer, can be compromised simply by viewing a web page. Attackers can inject content into the vulnerable web server and gain access to server's operating system.

4.6. Malware Attacks

Malware is software [29] that enters a computer system without the owner's knowledge or consent. These are spread through computer viruses and worms [30]. Trojans, rootkits, logic bombs and backdoors are all forms of malware. Malware with a profit motive includes botnets, spyware, adware, and keystroke loggers.

Social engineering [31] is a means of gathering information for an attack from individuals. Types of social engineering approaches include phishing [32], impersonation [33], dumpster diving [34], and tailgating.

Malware can be downloaded to the G-Node without the knowledge of the user. Attackers develop a zero pixel frame to avoid visual detection and embed an HTML document inside the main document. When the browser used by the G-Node downloads a malicious script, it instructs the G-Node to download malware. Therefore, it is very critical that the G-Node must be loaded with suitable anti-malware software to detect any malware downloads.

4.7. Cookies and Attachments

Cookies store user-specific information on the G-Node. The cookies are used to identify repeat visitors such as travel websites to store user's travel itinerary and personal information provided when visiting a site. Only the Web site that created the cookie can read it.

There are a number of types of cookie used. Website users create a first-party cookie when they visit a website. Website advertisers use a third-party cookie to record user preferences. A number of cookies will also be used when a web-based PoC application is accessed on the G-Node. A few scenarios which involve the

use of cookies are outlined; a session cookie is stored in the RAM and expires when the browser closes. The G-Node records a persistent cookie on its drive, and the persistence cookie does not expire when the browser closes. A secure cookie is used when a browser visits the server over a secure connection, which is always encrypted. A flash cookie uses more memory than a traditional cookie, and it cannot be deleted through browser configuration settings. Given this wide range of cookie types, cookies pose security and privacy risks and if stolen it can be used to impersonate a user and can, therefore, be exploited by attackers to steal data from the G-Node.

Session hijacking is a malicious process used by an attacker to impersonate a user by stealing or guessing the session token when the G-Node communicates with the web server. To prevent this kind of attacks the G-Node to P-node and the G-Node to P-Cloud links must be encrypted using well-known encryption algorithms.

Buffer overflow is an anomaly in the software code where the buffer boundaries are not checked during data writing. An attacker uses any buffer overflow to steal data by attempting to store data in RAM beyond boundaries of fixed-length storage buffer, which cause data overflow into adjacent memory locations. This attack may cause the G-Node or the P-Node to stop functioning and open an unintended pathway in which the attacker can change the "return address", to redirects to an address containing malware code.

4.8. Denial of Service (DoS)

The DoS attempts to prevent the system from performing normal functions by pinging a flood attack, therefore sending a large number of echo request messages, which in turn overwhelms web server. It is possible to send a ping request and alter the original IP address, thus mimicking the target G-Node; therefore an attacker can acquire specific responses from all the devices connected to the network.

Dangerous attack types include the SYNC flood attack and the DDoS (Distributed DoS [35]) attack. In the SYNC flood attack, the attacker takes advantage of procedures for establishing a connection.

In the DDoS, the attacker uses many zombie G-Nodes (G-Nodes connected to the Internet that has been compromised by a hacker) to flood a device with requests from non-existence IP addresses. The source of the attack is impossible to identify and, therefore, cannot be blocked.

In order to prevent any of the security attacks described above (see **Figure 9**), the PoC network requires a separate entity for security management [36] [37]. The separate entity is a network element (S-Node) for monitoring security. The S-Node is a specific kind of node which needs to be updated with all the latest security signatures of known vulnerabilities. DoS attacks can be prevented [38] by utilizing a static IP address (that are known to an administrative domain) plan for PoC system deployments. Even if an attacker imitates the DoS attack, this can be easily detected with the static IP configuration.

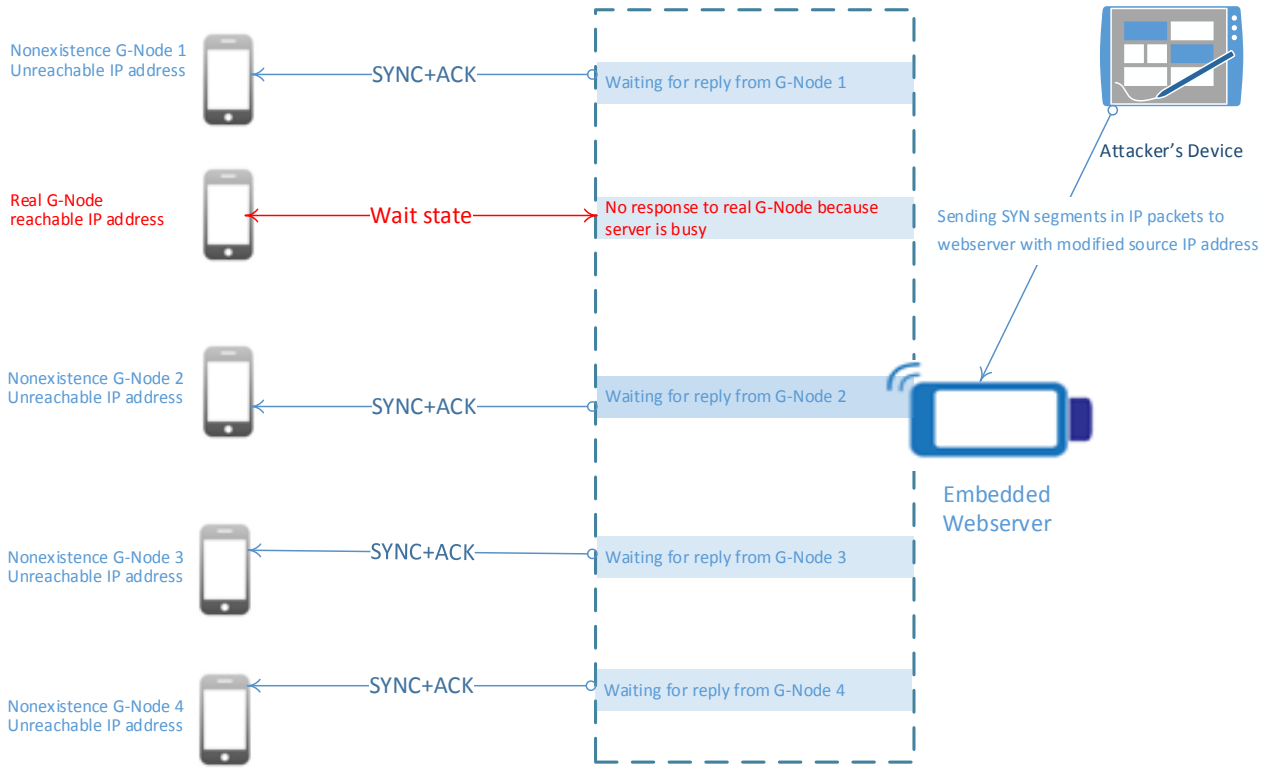

Figure 9. Distributed Deniyal of service (DoS) attacks.

5. Security Framework

There are many approaches available for providing security (mainly for identity and data protection) for the PoC system environment. Methodologies and techniques already exist for providing information protection in the industry. A list of few notable methodologies are listed here; a biometric-based identification, user identification based on behavioral analytic process (including the Big Data approach), challenge and response mechanism and the multi-attribute access process. The method used is to establish a trust relationship with the PoC system network nodes, especially the P-Node, G-Node, and P-Cloud. Two main approaches are outlined in the following sections. Two main approaches are outlined in the following sections.

5.1. The Protocol Used between the G-Node and the P-Node

A communication protocol can be used to help accomplish data security. In a closed system, the protocol format can contribute in providing security protection for the asset, which is the data collected during PoC testing. Any violators will not be able to determine the data unless if they have got hold of the protocol format.

5.2. Security Mechanism-1 (Challenge and Response Based)

As shown in Figure 10, it is assumed that the network connectivity between the three main nodes has been established. At this point, the G-Node attempts to

start a PoCT process using a native application or a web-based application. The OPCODE for START in section 5.1 is used to begin the assay process by the user. A security challenge is sent to the G-Node from the PoC device to list the operational capabilities of the PoC. These interactions are shown as by #1 in Figure 10. The user device (which is the G-Node) will respond with a list of known operational codes that are provisioned by the operator. The PoC device selects a subset of OPCODEs from the received list and queries the G-Node for the last known list of OPCODEs. This particular information must come from the P-Cloud. If the G-Node has the authorization to retrieve information from the P-Cloud, then it can obtain the requested OPCODEs. This interaction is depicted by #2 in Figure 10.

Once the history of the operational codes is retrieved from the P-Cloud, the G-Node informs the PoC with the OPCODEs list. If the data matches the records in the PoC device, then the user is allowed to continue the interaction with the PoC for testing. Figure 11 shows a summary of the interactions.

5.3. Security Mechanism-2 (Behavioral Based)

In this method, the user is first authenticated with the G-Node by the standard methods such as the G-Node device password and network password in order to access services. Step 1, shows the process of user authentication with a gateway in Figure 12.

The next step (shown as Step 2: Application authorization) involves establishing a security relationship with PoC app authorization server. The PoC application authorization server is responsible for providing approvals for the G-Node users to use a particular application or a set of PoC applications. The application

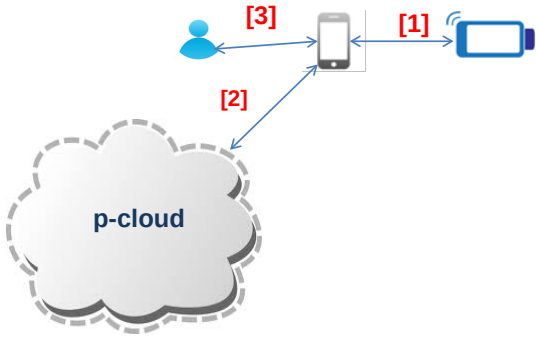

Figure 10. Interaction of messaging mechanism.

POC: [1] Tell me about my operational abilities
User device: [1] Responds with list of known OPCODEs
POC: [1] Will chose a subset of OPCODEs and ask when was the last time the OPECOE (s) was (were) used
User device: [2] Connects to p-cloud to get the last known time info for the requested OPCODE(s)
User device: [1] Informs POC with requested *OPCODE-usage time* record.
POC: [3] Will allow the operation from the user if the *records match* the stored values

Figure 11. Interaction summary.

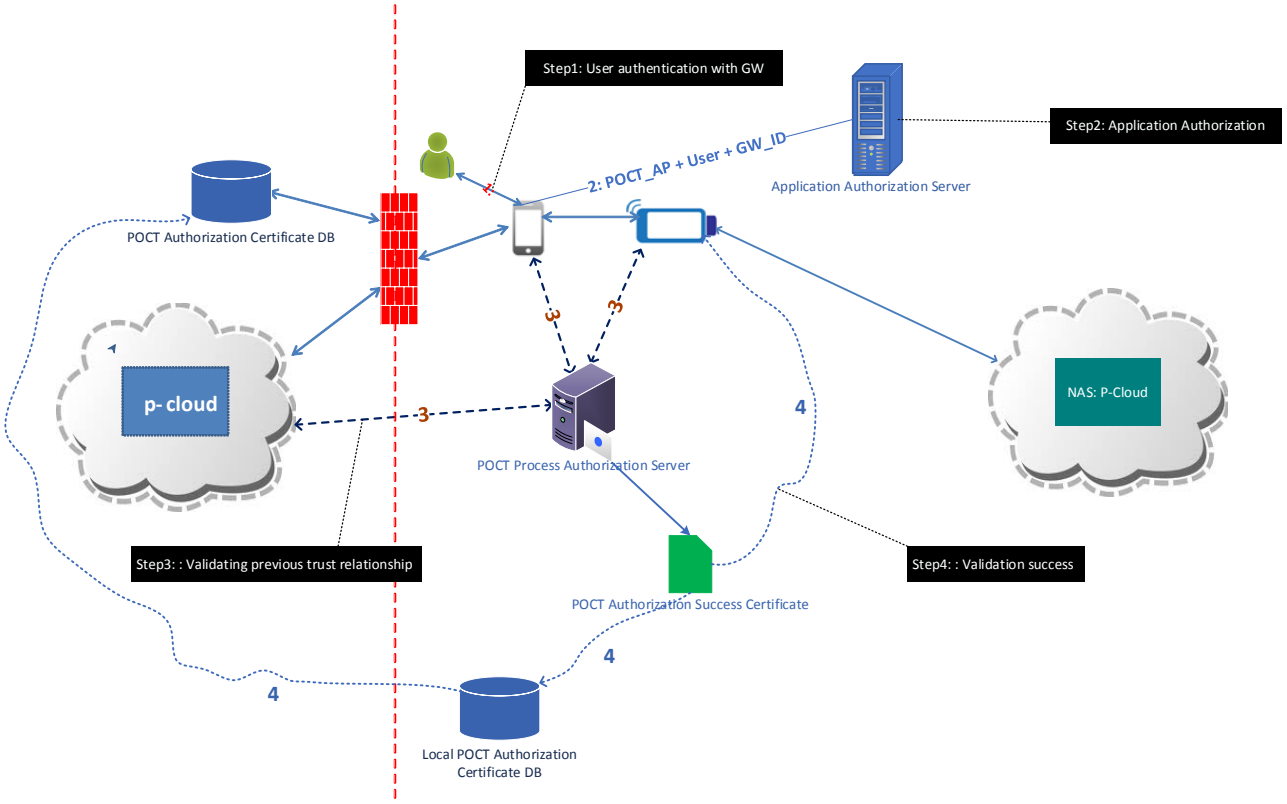

Figure 12. Security mechanism: behavioral-based.

authorization process is triggered when user attempt to start a PoC application from the G-Node (via G-Node user interface).

The authorization process requires few metadata attributes that are related to actual data. There are metadata attributes available that can be used for the authorization process (e.g. an identifier for the PoC application, a user identification parameter such as SIM card and MEID [39] or IMIE [40] of the G-Node). These data attributes must be validated by the PoC application server prior to PoC testing. The purpose of step 3 (validation of previous trust relationship) are an assertion, and validation of the relationships existed between P-Cloud, G-Node, and PoC device, prior to the current test. This process is very similar to the security mechanism in section 5.2.

An entity called PoCT process authorization server is introduced. The purpose of the authorization server is to manage who can execute certain assay types on the PoC. The server is responsible for creating a PoCT authorization success certificate, which is an outcome of the record of the validation process for step 3. Step 3 can be modified using Big Data techniques to identify the user.

6. M2M Security in PoCT

Deployment and operation of PoC systems are encompassed by cellular or short range communication M2M [41] technology. The cellular M2M system differs from current cellular networks in three important ways.

The cellular network services today are typically offered by a single service

provider who owns the distribution of devices with the SIM card distribution, device provisioning, network infrastructure, and service delivery for voice and data services. On the other hand with the cellular M2M, multiple operators and network vendors offer services. These players have limited business relationships among them.

For example, in the case of entities involved in providing M2M solutions for power metering are the utility company that provides application, cellular access network provider, meter manufacturer, and end-user. These entities do not necessarily trust each other. Hence providing a security implementation in this environment is very challenging.

Secondly, M2M communication does not have intensive data transmission that could lead to lower financial earnings for the players involved. Fewer economic outcomes lead to less interest in implementing a security related layer that is not very cost effective for business survival.

Thirdly, unlike cellular phones, smartphones, or wireless-enabled laptops, M2M devices are often unattended and are subjected to a higher risk of malicious mischief and misuse. However, in the case of PoCT, there is a user who has ownership of the PoC device.

This dynamics between the main stakeholders suggests that the current security mechanisms in place today for mobile devices in the cellular networks are not appropriate for M2M applications.

The device manufacturer and the M2M service providers may not have a business relationship or predefined mutual trust. The users may buy devices on the open market. In the case of PoC market, there are authorized drug stores or authorized medical devices dealers who are involved in the sales and marketing of the devices and services. In the medical applications such as the PoC, the PoC device user may not even be aware of the existence of a virtual network operator who is providing the service on behalf of the owner of an organization that owns a PoCT application. However, securing usage of the application is critical to all stakeholders.

6.1. Trust Relationships between POC System Entities

Table 1 shows the business relationships involved in M2M service delivery for a PoCT. This scenario is applicable for PoCT at home as well as in the hospital. A health care or medical institution acquires PoCT devices from a vendor company and distributes these to the end-users (end-consumers, the patients) who have subscribed to the service. The health care institution owns and deploys the PoCT devices in the premises or hospitals of the end-consumers. The medical institution subscribes to the M2M service from an M2M service provider for PoCT data collection and device management. The M2M service providers are usually the telecom carriers (operators, e.g. AT & T [42]). The M2M service provider, in turn, has business relationships with network providers (e.g. Ericsson [43]) for the use of the bandwidth for transmission of data. The table below shows the various entities and the relationships between them. A similar table is

Table 1. Main players and security relationships.

	What role does this entity play	PoCT Device Users	PoCT Device	Network Providers	M2M operators	PoCT Application Providers (Health Care service providers)
PoCT Device Users	Subscribe to health care service providers	-	-	-	-	-
PoCT Device	PoCT capable with wireless enabled module	PoCT device is configured with user's smartphone	-	-	-	-
Network Providers	Provides wireless communication (cellular and connectivity)	*No direct relationship*	Certifies wireless modules in the PoCT device	-	-	-
M2M operators	Home network for PoCT devices and interface with multiple transport network providers	*No direct relationship*	*No direct relationship*	Roaming?	-	-
PoCT Application Provider	Health Care service providers	PoCT device user subscribes to POCT service	PoCT Device ownership and deployment	*No direct relationship*	PoCT Application Provider gets wireless services from M2M operator	-
PoCT device vendor	Makes PoCT device with wireless module	*No direct relationship*	Makes PoCT device with wireless module	*No direct relationship*	*No direct relationship*	Delivers PoCT device with wireless module

used to describe the metering service [41].

Given the above summary, note that the complexity of the PoC M2M ecosystem is strongly characterized by diverse business and trust relationships, which cannot be accurately predicted during the design of security solutions. For this reason, security protocol design for M2M systems has to assume inherently that the M2M service provider may not have trust relationships with other stakeholders in the ecosystem. Therefore a collection of suitable security strategies for the case of M2M is required along with design recommendations for appropriate security solutions in the context of the PoCT system design.

6.2. Security Compromising Scenarios

The PoCT devices can be misused for their access capabilities by attackers pretending to be the back-end application server. A scenario, where such an attack could be of some economic value to the attacker, is the selling of PoCT data or using the PoCT device to gain control over other devices or systems. By pretending to be the PoC application server, attackers can penetrate other barriers and reach other business applications (such as mobile banking applications) on the user's devices. The PoCT devices (G-Node and P-Node) must be protected from unauthorized entities trying to establish communications to and from the devices.

The data collected from the M2M enabled PoCT devices are sensitive in nature. For example, the data may contain information that can be used against the user by insurance organizations. Thus, the (M2M security) PoCT security solution must be such that it is not possible to acquire information about the stored data by eavesdropping at any point within the network. The security framework in section 4 ensures prevention of any such attempts to access the network in an

unauthorized way.

Identity information can be correlated with other data such as the location of data of the network elements from which the identity data is retrieved to discern some patterns. In the case of PoC, it is important that the identity of the end-customer is not available from a public database [41]. Therefore, the device should not transmit unencrypted data relating to the user identity [41]. Well-known, robust encryption mechanisms must be used, rather than reinventing new algorithms [44].

Low-cost health care devices such as heart rate monitors are required to send data collected by a server in a single data connection session. This design can be easily compromised by clever adversaries [41]. The proposed architecture model in Section 5 encourages multiple communication sessions to be established with the main network entities before the data access is granted.

The PoCT device is a non-mobile entity in the system. Moreover, by physically accessing the device without authorization causes three main problems. Firstly the data can be taken from the SD card. Secondly, the credentials from the UICC (Universal Integrated Circuit Card or SIM card) can be taken if the PoCT has a cellular access interface. Thirdly, since there is no need for the hand-offs (device mobility is not required) to different base stations or radio access network, the intruder easily identify the associated network and hence the device identity.

It is essential that appropriate SLA (service level agreements) between all stakeholders (**Table 1**) involved being in place prior to system deployment and this must include security as one of the main items. The integrity of data stored in the PoCT device after the testing process can be tampered. It is possible to masquerade as another PoCT device and upload incorrect data to the P-cloud.

6.3. Core Security Requirements for POC M2M

Based on the scenarios discussed above, a list of core security requirements can be formulated [45].

Authentication: Mutual authentication procedures need to be carried out by the PoCT device and the PoCT operator network before initiating PoCT testing and the data transfer.

Confidentiality: Unauthorized data eavesdropping must be prevented between the application server and the PoCT device.

Data Integrity: Unauthorized data manipulations or modifications must be prevented between all entities in the PoCT system.

Exclusive Access: The PoCT device must use only authenticated PoCT applications that are available from the apps provider's apps marketplace, and the network operator should prevent any other use.

Identity: The identity of the PoCT device or the user must not be revealed to any intruders in the event of security compromises.

6.4. Bootstrapping Requirements for POCT Device Deployments

The bootstrapping process can be defined as initial processes that must be run

before the PoCT device can be used for PoC testing [46]. The PoCT device ecosystem is complex in nature which involves security relationships that must be established between the four key stakeholders (PoCT Device Users, PoCT Device, Network Providers, M2M operators and PoCT Application Provider). During the bootstrapping process, the trust relationships between the four main entities must be established successfully. The scalability of the PoCT devices deployment is a major factor as the ecosystem expands with the growth of the PoCT device users. Registering of the PoCT device on a network needs to comply with the 3 GPP standards [47] (including specialized requirements specified by the network providers and the operators [48]). The bootstrapping process will start after the successful network registration. Due to business reasons, the application provider, or the PoCT user may change operators, and the bootstrapping process must ensure forward and backward compatibility between the network operators keeping the network boundary agreements intact.

7. Conclusions

In this paper security mechanisms are discussed that can be used for three main PoC configurations (PoC for testing, PoC as the patient monitoring device and PoC as an interfacing device). It should be noted that the security mechanisms discussed here do not depend on the mentioned configurations; this applies to PoC operation and systems in general.

An attack tree model is presented considering the main assets that are required to be secured including the collected data. Port scanning results are presented (using Nmap process) given that the constructed asset tree in a real scenario where the PoC is used within a secure in-house environment. The purpose of showing the process is to emphasize the need for the port scanning process for security validation of the PoC system on a continuous basis. Any applications within the PoC system can potentially create security violations if they are conducted without security guidelines for developing PoC applications. A rigorous process for accepting any PoC applications must be in place along with a security monitoring center for PoC installations.

The security concerns that are applicable to any web based system that is very much applicable to PoC web-based systems. The use of embedded web server within the PoC is discussed with potential security vulnerabilities such as cross-site scripting, SQL injection, XML injection and command injection.

Given that fact the vulnerabilities issues in the PoC system are unavoidable, methods (security framework) for managing security risks have been discussed. The communication protocol developed (close communication) for the PoC system is the first defense process for securing the data asset. Two kinds of security mechanisms have been discussed, challenge and response based and data behavioral based. All the methods discussed here are independent of communication technologies and Radio Access Technologies such as 2G, 3G, and 4G.

Finally, M2M security that applies to PoC is discussed. The PoC system is a good example of the M2M communication environment. The PoC deployment

depends on a successful working relationship between multiple stakeholders (or entities); PoCT device users, PoCT device, network providers, M2M operators, PoCT application providers and the PoCT vendors (OEMs). The key M2M requirements for successful PoC device deployment have been mentioned. The PoC M2M security is a complex issue, which needs not only a technology collaboration but also requires political harmony among the main organizations involved.

References

[1] Tulasidas, S., Mackay, R., Craw, P., Hudson, C., Gkatzidou, V. and Balachandran, W. (2013) Process of Designing Robust, Dependable, Safe and Secure Software for Medical Devices: Point of Care Testing Device as a Case Study. *Journal of Software Engineering and Applications*, **6**, 1-13. https://doi.org/10.4236/jsea.2013.69A001

[2] Boswarthick, D., Elloumi, O. and Hersent, O. (2013) Securing Networks through the Internet. Health Management Technology. https://www.healthmgttech.com/securing-networks-through-the-internet.php

[3] Ymeti, A., Nederkoorn, P.H.J., Dudia, A., Subramaniam, V. and Kanger, J.S. (2009) Rapid, Ultrasensitive Detection of Microorganisms Based on Interferometry and Lab-on-a-Chip Nanotechnology. *Proceedings of the International Society for Optical Engineering*, **7306**, 73060J-1-73060J-7. https://doi.org/10.1117/12.818466

[4] Akamai's State of the Internet Q1 2014 Report. https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q3-2014.pdf

[5] TCP and UPD Ports. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

[6] Srinivas, J., Mukhopadhyay, S. and Mishra, D. (2017) Secure and Efficient User Authentication Scheme for Multi-Gateway Wireless Sensor Networks. *Ad Hoc Networks*, **54**, 147-169. https://doi.org/10.1016/j.adhoc.2016.11.002

[7] Han, K.-H. and Bae, W.-S. (2016) Proposing and Verifying a Security-Enhanced Protocol for IoT-Based Communication for Medical Devices. *Cluster Computing,* **19**, 2335-2341. https://doi.org/10.1007/s10586-016-0669-3

[8] Huang, X., Craig, P., Lin, H. and Yan, Z. (2016) SecIoT: A Security Framework for the Internet of Things. *Security and Communication Networks*, **9**, 3083-3094. https://doi.org/10.1002/sec.1259

[9] Karimian, N., Wortman, P.A. and Tehranipoor, F. (2016) Evolving Authentication Design Considerations for the Internet of Biometric Things (IoBT). *Proceedings of the* 11*th IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, Pittsburgh, 1-7 October 2016, 1-10. https://doi.org/10.1145/2968456.2973748

[10] Cao, X., Shila, D.M., Cheng, Y., Yang, Z., Zhou, Y. and Chen, J. (2016) Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks. *IEEE Internet of Things,* **3**, 816-829. https://doi.org/10.1109/JIOT.2016.2516102

[11] Custodio, V., Herrera, F.J., López, G. and Moreno, J.I. (2012) A Review on Architectures and Communications Technologies for Wearable Health-Monitoring Systems. *Sensors,* **12**, 13907-1346. https://doi.org/10.3390/s121013907

[12] Cam-Winget, N., Sadeghi, A.-R. and Jin, Y. (2016) INVITED: Can IoT Be Secured: Emerging Challenges in Connecting the Unconnected.

[13] Wang, H., Li, K., Ota, K. and Shen, J. (2016) Remote Data Integrity Checking and

Sharing in Cloud-Based Health Internet of Things. *IEICE Transactions on Information and Systems,* **E99-D**, 1966-1973. https://doi.org/10.1587/transinf.2015INI0001

[14] Guo, Z., Karimian, N., Tehranipoor, M.M. and Forte, D. (2016) Hardware Security Meets Biometrics for the Age of IoT. 2016 *IEEE International Symposium on Circuits and Systems*, Montreal, 22-25 May 2016, 1318-1321. https://doi.org/10.1109/ISCAS.2016.7527491

[15] Ding, D., Conti, M. and Solanas, A. (2016) A Smart Health Application and Its Related Privacy Issues. 2016 *Smart City Security and Privacy Workshop*, Vienna, 11-14 April 2016, 1-5. https://doi.org/10.1109/SCSPW.2016.7509558

[16] Attila, A., Garai, A. and Pentek, I. (2016) Common Open Telemedicine Hub and Infrastructure with Interface Recommendation. *IEEE* 11*th International Symposium on Applied Computational Intelligence and Informatics*, Timisoara, 12-14 May 2016, 385-390. https://doi.org/10.1109/saci.2016.7507407

[17] Seo, S. Preserving Patient's Anonymity for Mobile Healthcare System in IoT Environment. Vol. 5.

[18] SDL Threat Modeling Tool. http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx

[19] El-Hadary, H. and El-Kassas, S. (2014) Capturing Security Requirements for Software Systems. *Journal of Advanced Research*, **5**, 463-472. https://doi.org/10.1016/j.jare.2014.03.001

[20] AttackTree. Isograph. http://www.isograph.com/software/attacktree/

[21] ThreatModeler Archives. http://myappsecurity.com/threatmodeler/

[22] Nmap-Free Security Scanner for Network Exploration & Security Audits. http://nmap.org/

[23] Chapter 15. Nmap Reference Guide. http://nmap.org/book/man.html

[24] Application and Network Attacks. http://sl.sierracollege.edu/cis147/TextBook/CIS147-TextbookChapter3.pdf

[25] Malik, M. and Agrawal, D.P. (2012) Secure Web Framework for Mobile Devices. 2012 *IEEE Globecom Workshops*, Anaheim, 3-7 December 2012, 781-786. https://doi.org/10.1109/GLOCOMW.2012.6477674

[26] Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Co-Located with the 16th ACM Computer and Communications Security Conference, Proceedings of the ACM Conference on Computer and Communications Security.

[27] Weingart, S.N., Hamrick, H.E., Tutkus, S., Carbo, A., Sands, D.Z., Tess, A., Davis, R.B., Bates, D.W. and Phillips, R.S. (2008) Medication Safety Messages for Patients via the Web Portal: The MedCheck Intervention. *International Journal of Medical Informatics*, **77**, 161-168. https://doi.org/10.1016/j.ijmedinf.2007.04.007

[28] Gupta, V., Millard, M., Fung, S., Zhu, Y., Gura, N., Eberle, H. and Shantz, S.C. (2005) Sizzle: A Standards-Based End-to-End Security Architecture for the Embedded Internet. 3*rd IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, 8-12 March 2005, 247-256. https://doi.org/10.1109/PERCOM.2005.41

[29] Malware-Malicious Virus Code Detection. http://us.norton.com/security_response/malware.jsp

[30] Ciampa, M. Guide to Network Security. http://www.academia.edu/21604648/Comp_TIA_Security_Guide_to_Network_Securit_-_Mark_Ciampa

[31] What Is Social Engineering? Definition from WhatIs.com. http://searchsecurity.techtarget.com/definition/social-engineering

[32] What Is Phishing? Definition from WhatIs.com. http://searchsecurity.techtarget.com/definition/phishing

[33] Impersonation. https://technet.microsoft.com/en-us/library/cc961980.aspx

[34] What Is Dumpster Diving? Definition from WhatIs.com. http://searchsecurity.techtarget.com/definition/dumpster-diving

[35] Understanding Denial-of-Service Attacks. US-CERT. https://www.us-cert.gov/ncas/tips/ST04-015

[36] Geva, M., Herzberg, A. and Gev, Y. (2014) Bandwidth Distributed Denial of Service: Attacks and Defenses. *IEEE Security & Privacy*, **12**, 54-61. https://doi.org/10.1109/MSP.2013.55

[37] Rontti, T., Juuso, A.-M. and Takanen, A. (2012) Preventing DoS Attacks in NGN Networks with Proactive Specification-Based Fuzzing. *IEEE Communications Magazine*, **50**, 164-170. https://doi.org/10.1109/MCOM.2012.6295728

[38] DHCP Consumption Attack and Mitigation Techniques White Paper. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_Paper_C11_603833.html

[39] Mobile Equipment Identifier. http://en.wikipedia.org/wiki/Mobile_equipment_identifier

[40] 3GPP TS 22.016: International Mobile Equipment Identities (IMEI) (2009).

[41] Boswarthick, D., Elloumi, O. and Hersent, O. (2012) M2M Communications: A Systems Approach. Wiley, Hoboken, 221-240. https://doi.org/10.1002/9781119974031

[42] AT&T M2M Solutions. Machine to Machine. M2M Communications. http://www.business.att.com/enterprise/Family/mobility-services/machine-to-machine/#fbid=-7OUq7Bu73_

[43] Machine-to-Machine Products. Ericsson. http://www.ericsson.com/ourportfolio/products/machine-to-machine-products?nav=productcategory002

[44] Wen, J., Severa, M., Zeng, W., Luttrell, M. and Jin, W. (2001) A Format-Compliant Configurable Encryption Framework for Access Control of Multimedia. 2001 *IEEE 4th Workshop on Multimedia Signal Processing*, Cannes, 3-5 October 2001, 435-440.

[45] Boswarthick, D., Elloumi, O. and Hersent, O. (2012) M2M Communications: A Systems Approach. Wiley, Hoboken, 233. https://doi.org/10.1002/9781119974031

[46] M2M Communication: A System Approach. Section 8.3.5.

[47] Compliance Guides for Small Businesses. FCC.gov. https://www.fcc.gov/encyclopedia/compliance-guides-small-businesses

[48] Safe for Network Certification. Verizon Wireless. https://odi-device.verizonwireless.com/Info/Open%20Development%20Device%20Docs/Certification%20Process%20Documentation/ODDeviceCertificationProcess.pdf