computers

Article

Exploring a New Security Framework for Remote Patient Monitoring Devices

Brian Ondiege [1,*], Malcolm Clarke [1] and Glenford Mapp [2]

[1] Department of Computer Science, College of Engineering, Design and Physical Sciences, Brunel University London, London UB8 3PH, UK; malcolm.clarke@brunel.ac.uk

[2] Department of Computer Science, School of Science and Technology, Middlesex University London, London NW4 4BT, UK; g.mapp@mdx.ac.uk

* Correspondence: brian.ondiege@brunel.ac.uk; Tel.: +44-7547-311336

Academic Editor: Paolo Bellavista
Received: 26 September 2016; Accepted: 17 February 2017; Published: 24 February 2017

Abstract: Security has been an issue of contention in healthcare. The lack of familiarity and poor implementation of security in healthcare leave the patients' data vulnerable to attackers. The main issue is assessing how we can provide security in an RPM infrastructure. The findings in literature show there is little empirical evidence on proper implementation of security. Therefore, there is an urgent need in addressing cybersecurity issues in medical devices. Through the review of relevant literature in remote patient monitoring and use of a Microsoft threat modelling tool, we identify and explore current vulnerabilities and threats in IEEE 11073 standard devices to propose a new security framework for remote patient monitoring devices. Additionally, current RPM devices have a limitation on the number of people who can share a single device, therefore, we propose the use of NFC for identification in Remote Patient Monitoring (RPM) devices for multi-user environments where we have multiple people sharing a single device to reduce errors associated with incorrect user identification. We finally show how several techniques have been used to build the proposed framework.

Keywords: telehealth security; telemedicine security; remote patient monitoring security

1. Introduction

Remote patient monitoring (RPM) refers to using technology for monitoring of patients from their own homes, which is aimed at increasing access to quality care and decreasing costs of healthcare delivery [1].

The term cybersecurity is defined by the FDA as the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient [2].

Healthcare has become a key target for cybercriminals. For example, a recent report showed that 94% of healthcare organisations had been targeted by cybercriminals; this included attacks on medical devices [2]. Therefore, in the USA, the FDA has been mandated with the responsibility to ensure safety, effectiveness, and security of medical devices in the country [2].

A healthcare cyber threat report released in February 2014 by Norse and SANS involving study of malicious traffic aimed at healthcare organisations in the US during a one-month period, reported 49,917 unique attacks across more than 700 devices, with 375 US based healthcare organisations compromised and compromised devices ranged from mail servers, firewalls, and radiology software [3]. The Norse and SANS report also reported an incident where an attacker compromised a dialysis machine and tried to purchase goods online using a fraudulent credit card number [3]. This opportunistic attack can easily put the patient using the dialysis machine in danger if it was to malfunction [4]. These findings suggested that RPM systems can be attacked remotely and this can endanger patients' lives [5]. In addition, it is also highly likely that the potential attackers track activities and health information of RPM devices over a certain period of time, which highlights the issue of patients' privacy.

In addition, the literature shows that criminals can steal medical records and impersonate patients [6]. To address the issue of cyberattacks, some organisations such as the National Health Service (NHS) trusts in England need to have adequate training programmes in place to ensure their personnel are protected against cyber threats [6].

Therefore, failure in maintaining cybersecurity and effectively dealing with cyber threats can not only result in medical devices getting compromised but also can result in data losses, integrity, and availability, which can lead to potential risks to patients' lives [7]. Therefore, it is essential that healthcare providers that use medical devices should not rely on device manufacturers to ensure security of devices but they should also take steps to safeguard patient information within their networks [7]. In addition, healthcare providers need to ensure that antivirus software and firewalls are updated, report any medical device security flaws, and monitor any unauthorised use on their network [8].

2. Legislation on Health Data Encryption

For protecting personal health data, there is a comprehensive set of legislations including regional, national, and international legislation. For example, the US legislation such as the HIPAA [9], amended in 2014, European legislation such as the European Directive 95/46/EC (European Community, 1995), and UK legislation such as the Data Protection Act 1998 [10] apply to electronic as well as paper approaches of health record management. These legislations address some of the issues and protect the privacy and security by specifying penalties to individuals breaching the legal barriers. For example, the HIPAA specifies up to 10 years' imprisonment for selling patient's health records when sensitive material about a person's health issues are exposed and social damage is done, legislation can be applied [9]. However, there is no way to revoke the information or to restitute the individual. Therefore, technological means to enforce privacy protection and prevent security and privacy breaches are of extreme significance.

3. Issues in Currents RPM Devices

Telehealth research shows that one of the main gaps in RPM architecture research is that the issue of security is not considered, because the researchers are not familiar with it [11]. These findings suggest that telehealth and Remote Patient Monitoring (RPM) devices could provide a perfect playing field for opportunistic security attacks. In addition, the current RPM devices are limited in terms of the number of users that can use each device at a given time and only the person who is being monitored is allowed to use the device [12,13]. Therefore, should another person use the same device, then an incorrect reading will be sent to the patient record [13,14].

The findings in the literature have identified that there is little empirical evidence on how security is implemented in RPM devices, or if it has been done it has been done poorly [11]. In addition, none of the studies conducted so far have addressed the issue of how best to implement security on RPM devices due to lack of standards that define interoperability [15]. Most of the studies have assumed the role of security to be the responsibility of medical device manufacturers [15].

The additional problem in the current architecture of RPM devices included the issue of verification of the person using the device because the measurement is not supervised at home and the device does not have a mechanism for identification and authentication [16]. Therefore, if the patient's ID is not verified then, once again, incorrect data may be placed in the patient's record with the possibility of incorrect diagnosis and incorrect treatment [12,13,16].

Therefore, there is a need to address a number of the key questions in the RPM device architecture [14], as follows:

- How can a clinician trust the data measured by a patient at home if it is not supervised and the patient is in a multi-user environment?
- How can patients use RPM devices while ensuring their privacy and controlling the use of information in a simple intuitive way?

If more than one person uses the same device without identification there is a likelihood of the wrong measurement being transferred to the wrong user which can lead to the user getting the wrong intervention.

To address these issues, an appropriate identification technique inbuilt in RPM devices can be beneficial in settings such as care homes for the elderly and households that have two or more people suffering from the same chronic disease, as it will cater for a large number of users to be monitored and thus reduce costs associated with having multiple devices. However, with the current architecture this possibility is limited [13].

A review of current ISO/IEEE 11073 family of standards shows that these standards do not provide any scheme to ensure security of data exchange but assume that data exchange is secured by other means, for example when data is passing through a secure transport channel [17]. In addition, review of ISO/IEEE11073 PHD standards reveals that these standards bring the possibility to record medical data related to patient ID but do not define how the mapping is going to be achieved and leave mapping out to the design manufacturers as this in not within the scope of these standards [15]. Additionally, the ISO/IEEE 11073 PHD standards permits agents to record data; however these agents (e.g., BP monitor, weighing scale, insulin pump) are not connected to a manager (e.g., cell phones, personal computers, personal health appliances, and set top boxes) and the standards permit managers to request all stored data [15]. Therefore, without proper mapping and an appropriate identification technique to identify the patient, a situation can arise where managers will not be able to verify which readings belong to them. Further security issues can arise when managers are infected with malware, which have the ability to change data formats.

4. Threats and Risks

The key users of PHDs include users such as patients, healthcare professionals, caregivers, and technicians and there are a number of security threats and risks involved in the use of PHDs, which are summarized in Table 1.

Table 1. Summary of security threats and risks in PHDs.

Threat and Risk	Examples
Human Issues	**Usability** Since a PHD and the managing software are used by the user/patient, they need to be as user friendly and as easy to use as possible. Since this technology is for the elderly and some of them might have other disabilities, the system must adhere to usability and accessibility guidelines. Research shows that humans are the weakest link in the security chain and many attacks in computer systems are through social engineering [18]. For example, using a covert channel to deceive a healthcare provider employee to gain access to a person's medical record.
Missing information about how to use a PHD	Placing the blood pressure cuff incorrectly might lead to misleading results and wrong medical treatment being triggered [19]. Therefore, detailed and user oriented manuals and descriptions of PHDs are necessary.
PHD technical failure	Threats and risks also might arise from technical failures of PHDs, which might vary from a device sending wrong or no data to communication limitation or even complete breakdown. This can have an impact on availability.

Table 1. *Cont.*

Threat and Risk	Examples
PHD abuse	**Agent device abuse** Device might be stolen and switched by a compromised agent that either deliberately provides wrong data that will trigger wrong treatment or intercepts patient and medical data [20]. **Abuse of device manager software** For technical reasons, wireless communication is much more likely to be compromised, which is similar to misuse of agent devices, and the transmitted information could either be altered and entered into the communication channel [18,21]. **Manager to telemonitoring server abuse** Device fraud and manipulation are possible abuse cases. For example, eavesdropping, which is common to attackers since data from various devices have already been merged and formatted for transmission [18,21]. **Telemonitoring server abuse** Many abuse cases transpire within healthcare provider organisations where a large number of users and devices access large amounts of user/patient-specific data through many process steps [18]. The wide range of applications or devices in the healthcare organisation has many targets for attacks and setups for abuse; hence, any component might be tampered with, every transport channel snooped, data manipulated or even deleted, which creates issues of availability when patient data is needed. Therefore, appropriate access control need to be put in place.

Threat Modelling

Threat modelling methodology involves optimisation of Network/Application/Internet security through identifying objectives, threats, and defining countermeasures to mitigate the effects of the threat [22]. Threat modelling plays a vital part of the Security Development Lifecycle (SDL) process because it helps in identification of system vulnerabilities and threats and helps in establishing appropriate mitigation techniques [23]. Thus, threat modelling can be used in medical devices to optimise mitigations through identification of threats and vulnerabilities to a specific device from an organisation supply chain that can harmfully affect the safety of the patient [7]. The threat modelling tool can be used to detect security threats and vulnerabilities in other remote controlled devices. To display security design flaws and vulnerabilities and threats in in the current PHDs, the present study uses the Microsoft Threat Modelling Tool (version 2016, Microsoft Corporation, Redmond, WA, USA) to show a threat model of a blood pressure monitor (Figure 1).

In Figure 1, the patient is represented as a user, the blood pressure monitor represents the agent device, the smartphone represents the manager, and the telemonitoring represents the server.

Table 2 below represents the report produced from threat modelling software with additional modification.

Table 2. Current threats and vulnerabilities in Bluetooth (BTCommands) Interaction.

Threat	Category	Description	Requirement
Potential data repudiation	Repudiation	Smartphone claiming it did not receive data from a source outside the trust boundary.	Digital signatures can be used to counter this threat. Therefore, it is important to have audit trails from the source, indicating time and the summary of the data received.
Spoofing the blood pressure process	Spoofing	The blood pressure monitor may be spoofed by an attacker and this may lead to information disclosure by smartphone.	With lack of authentication mechanism to identify the destination would mean that this attack would likely occur. Encryption can also be used in preventing information disclosure.

Table 2. *Cont.*

Threat	Category	Description	Requirement
Spoofing the smartphone process	Spoofing	The smartphone may be spoofed by an attacker and this may lead to information disclosure by smartphone.	With lack of authentication mechanism to identify the source would mean that this attack would likely occur.
Elevation using impersonation	Elevation of privilege	Smartphone may be able to impersonate the context of blood pressure monitor in order to gain additional privilege.	Access control
Elevation by changing the execution flow in smartphone	Elevation of privilege	An attacker may pass data into smartphone in order to change the flow of program execution within smartphone to the attacker's choosing.	Encryption and access control

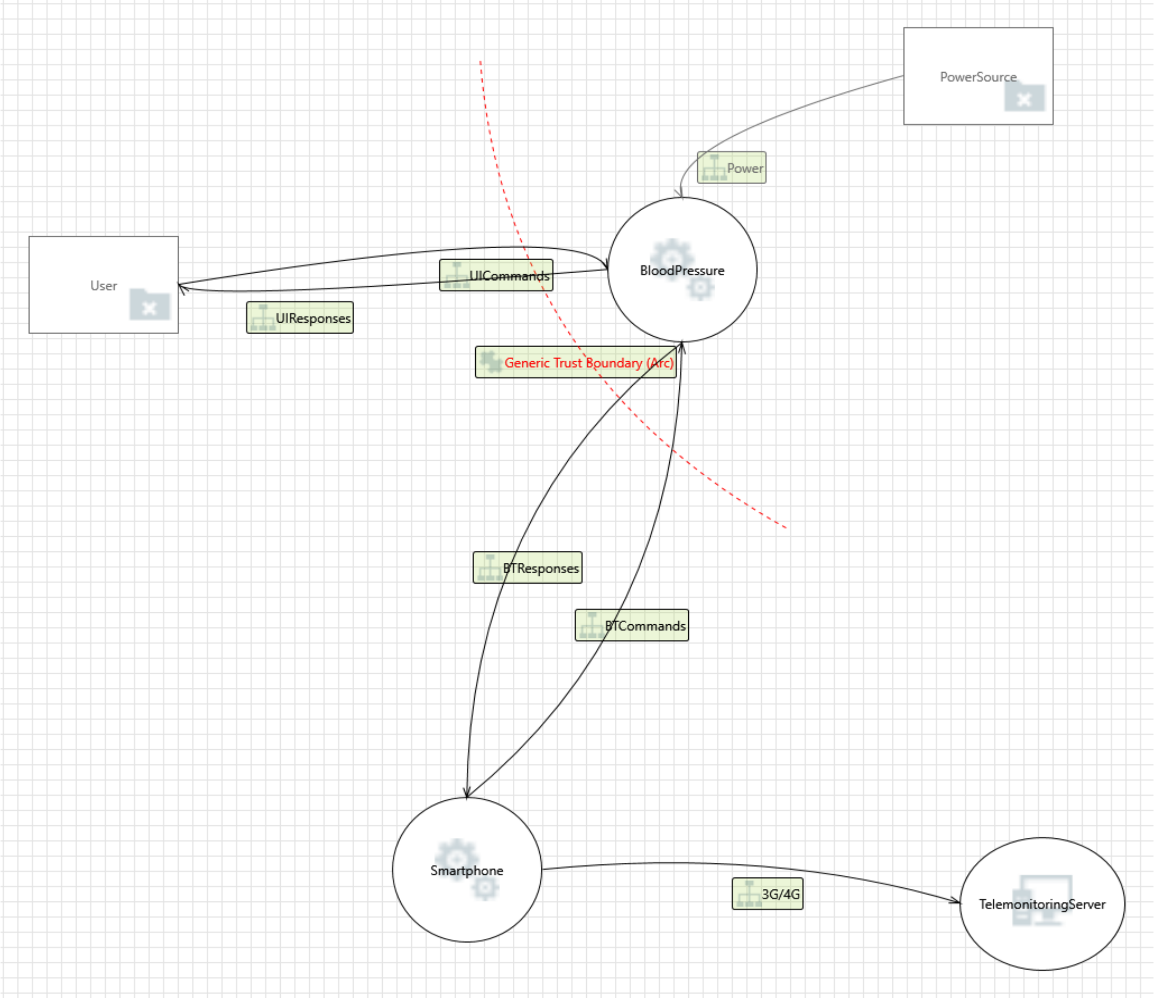


Figure 1. Blood pressure threat model.

Information displayed in Table 2 can be used for mitigation purposes and in prevention of threats and vulnerabilities identified in the threat model.

5. Security Models

Other frameworks which have been proposed by other authors [24,25] provide analysis required for secure health. Although there is some significance in these frameworks, the authors believe that a new framework is required that incorporates the functionalities of these frameworks, in contexts of major entities such as, cloud infrastructure, applications, and cognitive capabilities of elderly as they are the largest beneficiaries of RPM. Therefore, these frameworks are able to serve as reference models.

United4health functional model provides detailed analysis of how to implement end to end security in an RPM architecture.

The next section looks at United4Health security model and its description.

5.1. United4Health Telehealth Functional Model

A study conducted by [26] on security for United4Health telehealth trial system for chronic obstructive pulmonary disease (COPD) patients project provided analysis of security in RPM devices. Although their functional model has not been implemented in RPM, it provides a detailed overview of the security requirements for security in RPM. In their functional model they recommended the use of PINs for identification of the patient, considering this technology is for the elderly who might have cognitive impairments, this approach would not be practical for them, the authors further add that, when the users forget their PINs they have to place a call to the nurses supporting the service to support them, this approach will not be practical in the real world. Additionally, they do not address the issue of a multi-user environment, where users have to share a single device.

Therefore, there is need for an identification solution that incorporates other aspects of disability for the elderly so that any technology presented to them is easily acceptable. In the [26] study other security aspects are ignored, which are fundamental in delivering quality of care to the patient such as:

- Device authentication

  This threat occurs when an unauthenticated device is introduced into an RPM ecosystem. Device authentication will ensure that only authorised devices are allowed in the network. In healthcare, diseases such as diabetes rely on accurate measurements for treatment, if a device is lost or is replaced with a rogue device and then introduced into the ecosystem, there are high chances of it sending the wrong reading, which will trigger the wrong treatment that might endanger the patient's life [20].

- Data availability

  This are measures taken to ensure that data continues to be available at a required level of performance in situations ranging from normal to a disaster. Without appropriate security measures in the telemonitoring server and the manager device, it is highly likely that data can be made unavailable or be compromised. This model does not address the issue of data availability.

- Manager device security

  Security issues can arise when managers are infected with malware, which have the ability to change data format. The authors of United4Health (United4Health—project aimed to exploit and further deploy innovative telemedicine services implemented and trialed under the RENEWING HEALTH project [26]) failed to mention on security requirements of the manager device which is very crucial.
  Figure 2 below shows the United4Health telehealth system functional model.

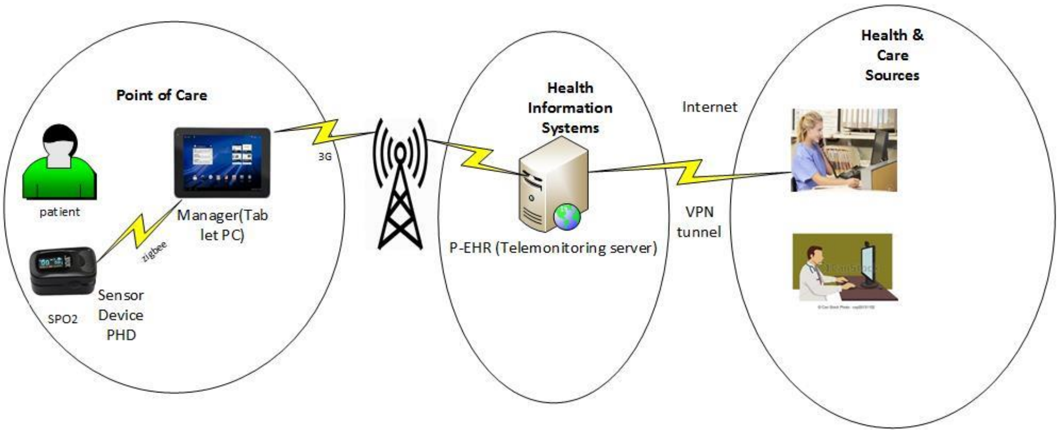


Figure 2. United4Health system. Source: United4Health [26].

- Point of care

  The patient takes their readings from the SpO2 sensor device which communicates the measurement through a wireless Bluetooth device to the manager device. The data from the SpO2 is stored in a local database on the manager device. The manager device then transmits the data to the HIS infrastructure. The patient authenticates themselves using a PIN on the manager device. A username and PIN is used to identify the patient.

- Health Information service

  From the manager device, the data is transmitted and stored in a PEHR. Clinicians and carers can access the data through a telehealth service which provides web based information.
  Uses HTTPS for providing end to end encryption communication between the manager device and the PEHR. The unique device identifier of the manager device and the corresponding symmetric key known to the PEHR is used for authentication and for establishing bidirectional session encryption.

- Health care and sources

  Different organizations, clinicians, and care professionals get access to the data from the patients. This can be viewed through a web-portal containing details of the data being monitored from the HIS infrastructure. It uses a role based access control for the users of the system.
  United4health functional model provides a detailed overview of the security requirements of the RPM system.

5.2. The New Security Framework for RPM Devices

The researchers propose a security model for RPM devices (Figure 3), which offers the most comprehensive security framework proposed so far. The construction of the proposed framework is drawn from guideline in literature and the threat model used. Therefore, the proposed framework provides an essential ground for understanding and examining security in RPM.

Various components of the proposed security model for RPM devices are described below.

5.2.1. Home Area Network

Since the proposed technology is for the elderly, usability plays an important role, from switching on the device to patients identifying themselves to the device with their NFC tags and sending the BP readings, the sequence and prompts need to be easy to follow. For improving usability, a few prompts have also been proposed to ensure that it is easy to learn and follow.

How It Will Work

A patient identifies themselves using their NFC tag on the NFC reader, then they take their blood pressure. The system will then check if the patient or the carer has been assigned the capability of sending the BP reading, if yes, then the system will allow the sender to send the BP readings.

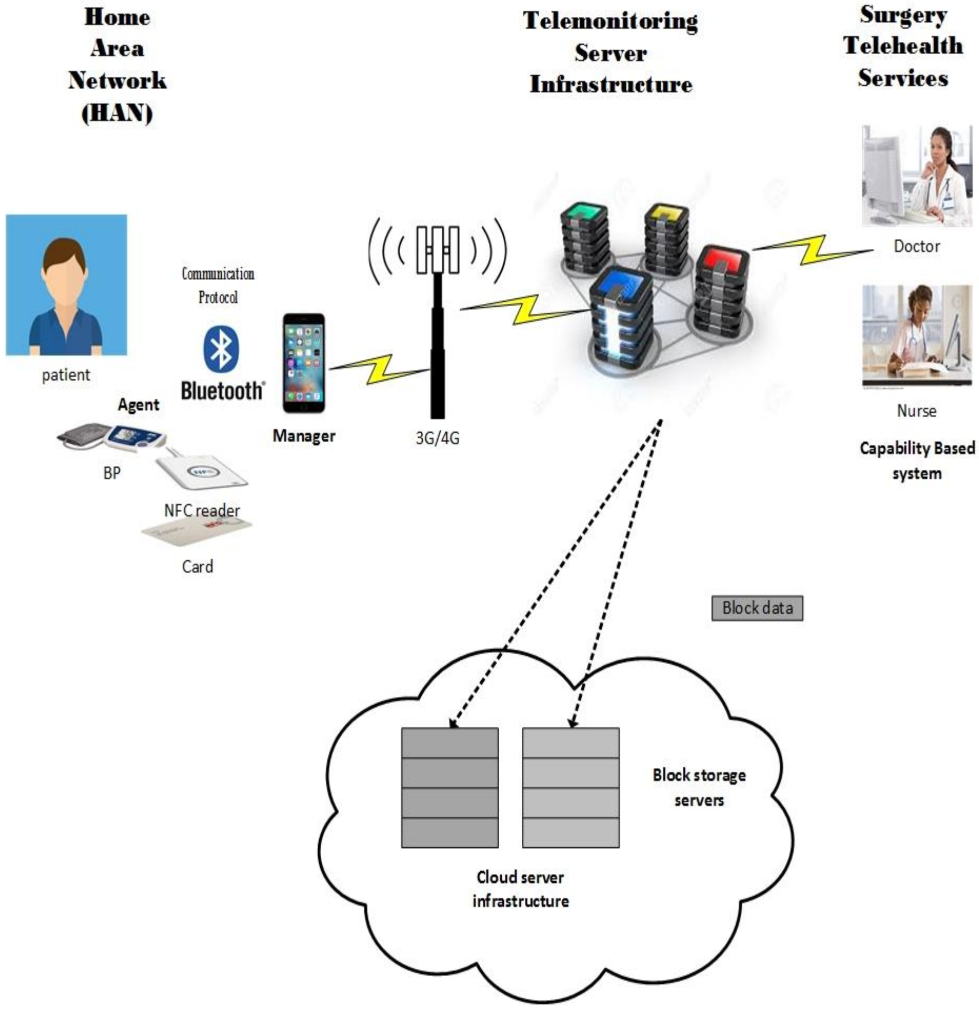


Figure 3. Security model for RPM devices.

A Capability-Based System for the Secure Use of NFC

A capability is a software construct that specifies the right of its holder to invoke operations on a defined system object via a communications port [27]. Identification with NFC alone is not sufficient; therefore, there is need for a solution that will increase the security within the NFC framework. This study proposes the use of a capability-based system to enhance security for tele-monitoring systems because the NFC_ID and the PHD device ID can be changed or tampered with either while in storage or in use; thus, resulting in misdiagnosis or fatality [13]. In addition, this study proposes the use of different NFC tags such as, cards, key fobs, and wristbands among the users for distinction purposes. In an environment such as home, errors such as using the wrong tag are likely to occur. Clear marking and using picture icons representing different sexes can play a significant role in mitigating tag mix-up errors. Currently, a trial is being conducted with a modified blood pressure monitor incorporated with NFC with elderly patients who are couples living within the same household and suffering from hypertension.

The capability based system only authenticates registered devices and in case a rogue device is introduced in the eco-system an alert will be raised, which will prevent the device from sending its readings.

It is imperative to highlight that the IEEE 11073 PHD standards does not specify security requirements of the manager device whereas the current study proposes that security requirements for a manager device need to be defined because the manager device is vulnerable to security threats and this can be seen from the threat model Table 2. The proposed framework used the threat model in Figure 1 to identify existing threats in RPM devices. The proposed framework offers mitigation techniques that can be used in preventing threats in existing devices. The threat modelling tool is useful in identifying security threats and vulnerabilities.

The manager device is vulnerable to malware, which can corrupt and change the data format. An anti-virus can be used in protection against malware and viruses. In addition, the threat model identified spoofing and repudiation threat between agent manager communication. Therefore, it is important that the sender identity is verified and use of digital signatures can be used to prevent issues of non-repudiation.

5.2.2. Telemonitoring Server Infrastructure

The data collected from patients using PHDs is stored in the telemonitoring server at the clinic/hospital monitoring the patients. Security at the telemonitoring server is very important because it ensures confidentiality, availability, and privacy of the patient's health records and without appropriate security measures the telemonitoring server can be vulnerable to security attacks. To ensure availability of data in case the telemonitoring server gets compromised, this study proposes storage of data in the cloud.

Asymmetric keys can be used in establishing session encryption, which utilises Public Key Infrastructure (PKI).

In addition, digital certificates can be issued and validated by a Certification Authority (CA) in authentication of managers and telemonitoring server.

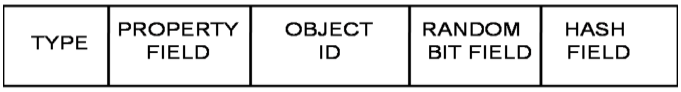
5.2.3. Cloud Server Infrastructure

The current study proposes cloud infrastructure for ensuring availability and security of PHR/EHR. The proposed file system will be a distributed file system that encrypts all the data blocks. The data blocks will be replicated and placed randomly on a number of cloud block storage servers [27]. However, it is worth to note that each country will have different jurisdictional requirements on data security. In order to improve security, the meta-data part of the file will not be stored in the cloud. The meta-data is protected so that in case an intruder manages to decode a block of data, it would still be very difficult to read the whole file. The new file system is shown in Figure 3. The blocks of data are encrypted using AES 256-bit encryption the recommended encryption algorithm by the NHS in the UK [28].

The proposed system fulfils the HIPAA requirements for security of patients' data.

5.2.4. Surgery Telehealth Services

In the surgery/clinic, different people might have access to patient records; therefore, there is a need to protect the privacy and confidentiality of a patient's health records. Only authorized personnel with the right access rights depending on their job roles should be allowed to have access to these records. Therefore, the current study proposes the use of a capability based system because capabilities allow to run a role-based mechanism so restrictions can be based on the roles of different people within the healthcare system such as doctors, nurses, technicians, and administrators [27]. Capabilities offer a cleaner set of protection mechanisms in a role-based systems since capabilities for a given role can be managed together. In addition, capabilities are better at providing better support for multi-role situations. Because of the large quantities of data to be managed, capabilities are now being used to secure objects compared to using Access Control Lists (ACLs). Therefore, in the proposed model, each entity must have a capability, for example people, devices and infrastructure all must have capabilities. Capabilities can also be used to provide restrictions, data access, and resources to personnel based their roles. Figure 4 presents the new format that will be used to present the capabilities.



TYPE	PROPERTY FIELD	OBJECT ID	RANDOM BIT FIELD	HASH FIELD

Figure 4. New capability format. Source: [27].

The address space of IPv6 affords the prospect to design a capability ID based system for users, applications, devices, and cloud infrastructure. Objects and their properties are identified by the use of capabilities. Capabilities therefore need to be carefully managed and need to be protected against being created or changed in an inappropriate manner.

- The Type Field: This field is used to specify the type of object capability that is being used. Types could include cloud providers, cloud platforms, users, applications, etc.
- The Property Field: This field is used to define the properties of the object.
- The Object ID: This field is used to uniquely identify the object.
- The Random Bit Field: This field helps to uniquely identify the object.
- The Hash Field: The Hash field is used to prevent the casual tampering of capabilities.

A capability based system provides additional security by restricting access to data, people, and devices.

Communication between the telemonitoring server and the surgery telehealth service is secured using HTTPS protocol. HTTPS is only used for encryption of messages within the surgery telehealth services. Access control and authentication is done by the capability based system at the surgery (clinic) telehealth service.

With an increase in the number of people getting chronic diseases, we are seeing cases of people living within the same household suffering from the same disease, therefore, its significant to address the current limitation in RPM devices. The proposed model not only provides security but it looks at the limitations currently faced by RPM devices by proposing an identification technique (NFC) that would be suitable for the elderly with cognitive impairments. NFC will be an ideal identification technique in a multi-user environment where people are sharing a single RPM device.

With telehealth still in its infancy stages it faces a threat of counterfeiting and the proposed framework using capability based system can be able to authenticate devices within its eco system. Counterfeit devices pose a threat as the standards used in manufacturing them are unknown and this can pose a serious threat to the patient, if the device is uncalibrated and sends the wrong readings which can trigger the wrong treatment to the patient.

The current standards such as the IEEE 11073 do not address the issue of patient identification even though they say mapping is possible they do not define how it is going to be achieved. For this to be achieved there is a need of an interoperable standard that can define patient identification. Future work can be done to define an interoperable standard that will allow patient identification to be added on RPM devices.

6. Conclusions

Security is becoming an issue of major concern and for telehealth to be successful, security has to be a top priority. Technologies such as NFC have been proposed in this study to address the issue of multi-user device patient identification. The RPM security model will help in mitigating security vulnerabilities and threat in an RPM ecosystem and possibly improve security. For telehealth to be widely accepted, issues such as usability need to be made a top priority considering that this technology is used by the elderly.

Acknowledgments: We wish to declare that there are no known conflicts of interest associated with this publication and there has been no financial support for this work that could have influenced its outcome.

Author Contributions: Brian Ondiege conceived and designed the paper; Malcolm Clarke was the principal supervisor, provided guidance on the manuscript; Glenford Mapp contributed on additional aspects of security. Additionally, Glenford Mapp contributed to revisions of the paper. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cafazzo, J.A.; Leonard, K.; Easty, A.C.; Rossos, P.G.; Chan, C.T. Bridging the self-care deficit gap: Remote patient monitoring and hospital at home. In *Electronic Healthcare*; Springer: Berlin/Heidelberg, Germany, 2009.
2. Food and Drug Administration (FDA). *FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*; FDA: Silver Spring, MD, USA, 2013.
3. Norse SANS Institute. Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. Available online: https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735 (accessed on 22 February 2017).
4. GS1. Global Standards Pave the Way for Unique Device Identification (UDI). Available online: http://www.gs1.org/docs/healthcare/GS1_UDI_Position_Paper.pdf (accessed on 20 February 2017).
5. Jacob, J.A. Hackers Could Threaten Home Health Monitoring Devices. Available online: http://www.healthbizdecoded.com/2013/09/hackers-could-threaten-home-health-monitoring-devices (accessed 24 February 2017).
6. Fadilpašić, S. NHS Trusts Lack Cyber-Attack Protection. Available online: http://www.itproportal.com/2015/12/08/nhs-trusts-lack-cyber-attack-protection/#ixzz46ejhsgiS (accessed on 8 January 2016).
7. Food and Drug Administration (FDA). *Postmarket Management of Cybersecurity in Medical Devices Draft Guidance for Industry and Food and Drug Administration Staff*; FDA: Silver Spring, MD, USA, 2016.
8. Doctors Remote Patient Monitoring: Real-Time Patient Data, Real Liability Risks. 2016. Available online: http://www.thedoctors.com/KnowledgeCenter/PatientSafety/articles/Remote-Patient-Monitoring-Real-Time-Patient-Data-Real-Liability-Risks (accessed on 8 January 2016).
9. HIPPA. Health Insurance Portability and Accountability Act of 1996. Available online: https://www.healthit.gov/sites/default/files/rules-regulation/health-insurance-portability.pdf (accessed on 27 July 2016).
10. Data Protection Act 1998. Available online: http://www.legislation.gov.uk/UKPGA/1998/29/contents (accessed on 27 July 2016).
11. Garg, V.; Brewer, J. Telemedicine security: A systematic review. *J. Diabetes Sci. Technol.* **2011**, *5*, 768–777. [CrossRef] [PubMed]
12. Continua Health Alliance. *Recommendations for Proper User Identification in Continua Version 1—PAN and xHR Interfaces*; Continua Health Alliance: Beaverton, OR, USA, 2008.
13. Ondiege, B.; Clarke, M.; Mapp, G. Exploring Security of Remote Patient Monitoring Devices Using NFC Technology for Identification of the Frail Elderly. In Proceedings of the 8th International Conference e-Health, Funchal, Portugal, 1–3 July 2016.
14. Vavilis, S.; Petkovi, M.; Zannone, N. Impact of ICT on Home Healthcare. In Proceedings of the IFIP International Conference on Human Choice and Computers (HCC 2012), Amsterdam, The Netherlands, 27–28 September 2012.
15. Kliem, A.; Hänsel, J.; Hovestadt, M.; John, M.; Kao, O. Towards self-organization of networked medical devices. In Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Toulouse, France, 5–9 September 2011.
16. Ondiege, B.; Clarke, M. Healthcare Professionals Perception on Information Security. In Proceedings of the 5th International Conference on Internet Technologies & Society, Taipei, Taiwan, 10–12 December 2014.

17. IEEE Standards on Cybersecurity. Available online: http://theinstitute.ieee.org/benefits/standards/ieee-standards-on-cybersecurity (accessed on 22 February 2017).
18. Part 10103: Nomenclature—Implantable device, cardiac. Available online: https://shop.austrian-standards.at/Preview.action;jsessionid=BD0A395AEB0CBA9629F4007A60E72462?preview=&dokkey=521755&selectedLocale=en (accessed on 22 February 2017).
19. Pickering, T.G.; Hall, J.E.; Appel, L.J.; Falkner, B.E.; Graves, J.; Hill, M.N.; Jones, D.W.; Kurtz, T.; Sheps, S.G.; Roccella, E.J. AHA Scientific Statement: Recommendations for blood pressure measurement in humans and experimental animals, part 1: Blood pressure measurement in humans. *Hypertension* **2005**, *45*, 142–161. [CrossRef] [PubMed]
20. Petković, M. Remote Patient Monitoring: Information Reliability Challenges. In Proceedings of the 9th International Conference on Telecommunication in Modern Satellite, Cable, and Broadcasting Services (TELSIKS '09), Nis, Serbia, 7–9 October 2009.
21. Gibbs, M.; Quillen, H. The Medical-Grade Network: Helping Transform Healthcare. Available online: http://www.cisco.com/web/strategy/docs/healthcare/07CS1034_HC_Whitepaper_r5.pdf (accessed on 12 December 2016).
22. OWASP. Category: Threat Modelling. Available online: https://www.owasp.org/index.php/Category:Threat_Modeling (accessed on 7 July 2016).
23. *SDL Threat Modeling Tool*, version 3; Microsoft Corporation: Redmond, WA, USA, 2008.
24. Pah, W.; Williams, P.A.; Maeder, A.J. A Conceptual framework for secure mobile health. *J. Int. Soc. Telemed. eHealth* **2013**, *11*, 44–51.
25. Patient Privacy in a Mobile World: A Framework to Address Privacy Law Issues in Mobile Health. Available online: http://www.trust.org/contentAsset/raw-data/03172beb-0f11-438e-94be-e02978de3036/file (accessed on 22 February 2017).
26. Gerdes, M.; Fensli, R. End-to-end Security and Privacy Protection for Co-operative Access to Health and Care Data in a Telehealth Trial System for Remote Supervision of COPD-Patients. In Proceedings of the 13th Scandinavian Conference on Health Informatics, Tromsø, Norway, 15–17 June 2015.
27. Mapp, G.; Aiash, M.; Ondiege, B.; Clarke, M. Exploring a New Security Framework for Cloud Storage Using Capabilities. In Proceedings of the IEEE 8th International Symposium on Service Oriented System Engineering (SOSE), Oxford, UK, 7–11 April 2014; pp. 484–489.
28. NHS Information Governance. *Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information*; NHS Information Governance: Leeds, UK, 2008.