A Secured Healthcare Platform for Remote Health Monitoring Services

Rajesh Kannan Megalingam, Sarathkumar KS, Vishnu Mahesh Kumar
rajeshkannan@ieee.org, sarath.ks60@gmail.com, vishnumahesh93@gmail.com
Amrita School of Engineering, Amrita Vishwa Vidyapeetham University, Kollam, India

Abstract — Health monitoring systems play a pivotal role in modern day healthcare. People nowadays opt for remote health monitoring services. Typical health monitoring systems use a compact device like a mobile phone to extract the data from the sensors and send them to the server. Research has shown that the health data or Electronic Health Records (EHR) are vulnerable to interception. This is due to the fact that the use of mobile devices to facilitate the transfer of the data to the server affects the security by limiting the implementation of encryption algorithms. Our system consists of a Raspberry Pi which records health data like the heartbeat and pulse rate of a patient and sends them to the server which will be monitored by the doctor. The system consists of a server side which enables the doctor to generate the EHR (Electronic Health Record) of a patient. In order to enhance the security of the system, we have implemented a password authentication key exchange mechanism based on zero knowledge password proof. Unlike normal authentication mechanisms, Zero Knowledge proof does not exchange the device credentials in order to authenticate. Instead, in a system using Zero knowledge proof, a prover proves to the verifier that it is in possession of a secret, without actually revealing what the secret is. An analysis of this protocol has also been done by simulating various security attacks like replay attack and phishing, thereby testing its resilience against such threats.

Index Terms—Health Monitoring Systems, Electronic Health Records, Security, Authentication, Zero Knowledge

I. INTRODUCTION

Investors in healthcare industry believe that remote health monitoring services are going to change the way people will ever perceive health services. In order to increase the business turnover hospitals and doctors are slowly switching over to remote health monitoring services owing to the fact that costs incurred will be low for better chronic care management. People in rural areas do not get reasonable healthcare because of either unavailability or inadequacy if available. When it comes to the technical security of a healthcare system, most products do not exhibit an exceptional performance. Similar to the theft of important user data such as usernames and passwords which can prove harmful, theft of health data handled by health monitoring systems can also have adverse effects. In some cases, it would compromise the whole security setup of the system. One cannot allow that to happen. In a typical remote health monitoring system, there will be a sensor circuit attached to the patient's body, which will measure the patient's vital signs like heartbeat and send it to a host device which in turn will send the data to the server to be monitored by the medical faculty. Depending upon various factors like portability and system type, the host device used in the system might be different. Some systems might use a mobile device, some might use a PC (where portability is not a relevant issue). Similarly, the measures adopted in each system to secure the medical data will also vary. In our work, we present a Zero Knowledge Password Proof based approach for authentication implemented on a health monitoring system, which can be implemented even on portable systems which use a mobile device as a host

II. PROBLEM DEFINITION

A normal web application uses SSL/TLS protocol in order to secure its data transmission process. In such a scenario with a typical client server architecture, both client and server machines will use a PC and a normal server respectively. In such cases, the portability of the system becomes an issue. But they can be helpful to bedridden patients where mobility of the system is not a concern. Since a normal PC can act as the host in such cases, adequate security measures like encryption mechanisms can be implemented. But in portable health monitoring systems, where the host must be at the person of the patient at all times, custom machines cannot be used. Obviously, we will have to switch to a smaller device with resource constraints to act as a host. Although this achieves portability, it deteriorates the security of the system compared to the previous one. In addition to that, most health monitoring systems lack a proper authentication mechanism. Not much work has been done in this regard. Healthcare systems have not yet been perceived much from a security point of view. But insecure transmission of health data can spawn serious consequences. At DEFCON 2014, a security conference, the researchers from Aries security were able to extract personal health data, usernames, passwords and other information from the DEFCON attendees within the distance of the team's hardware. This kind of an attack proved that health monitoring systems and gadgets are vulnerable to threats. Normal authentication mechanisms transfer the credentials of the device in order to authenticate successfully. Our work focuses on a health monitoring system that will monitor the patients vital signs remotely through a host device which uses a different approach to achieve successful authentication i.e. without exchanging the credentials.

III. RELATED WORKS

[1] discusses about a health monitoring system which when mounted on a patient or a victim will transmit the vital signs of the patient through an ad-hoc wireless network. It

is basically an off-the shelf health monitoring system. Our work, on the other hand emphasizes on the security aspect of a health monitoring system.[2] describes a four-step pre-analytical conceptual study of the reliability aspect of an e-Health monitoring system. It proposes techniques for integrating the physical layer hardware with the application layer interface as the system presents a need to expand so as to optimize the best design of a reliable e-Health monitoring system. [3] tries to solve the problem of mobility and portability of health monitoring systems by proposing a three level decentralized intelligent framework to develop a smart and mobile health monitoring system that shares and analyzes patient data. Although these works stand fairly close to ours in terms of the medical domain, none of the above focus on the security aspect of the system which is the emphasis of our work.

IV. SYSTEM DESCRIPTION

Our system consists of two divisions. First being the remote health monitoring system and second being the authentication protocol. The remote health monitoring system comprises of a raspberry pi which will act as the host device. It will accept readings of vital signs from the sensors that are attached to the patient's body. Then the Raspberry Pi will transmit the medical data thus aggregated to the remote server using the Zero Knowledge based authentication protocol. The authentication protocol used is based on a concept called Zero Knowledge Password Proof. Conventional authentication mechanisms transmit the device credentials between the host and the server which increases the chances of interception. Instead of this approach, what Zero Knowledge Password Proof does is rather than transmitting the credentials, it performs some operations based on these credentials, the output of which will be some numbers which even intercepted will be meaningless.

The system also has a server side which presents the data received from the Raspberry Pi on the patient side to the doctor in the form of an Electronic Health Record (EHR) along with the aggregated medical data like the vital sign readings so that it can be monitored by them. This server side is in the form of a web application for the ease of use.

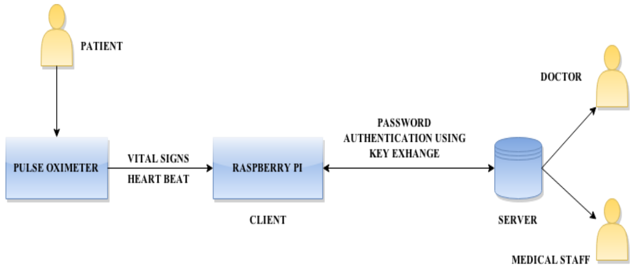


Fig. 1. System Architecture

V. ALGORITHM

This section explains the protocol based on Zero Knowledge Password Proof that we designed. The client which will be a mobile device and the server authenticate using this protocol. The protocol consists of the following steps:

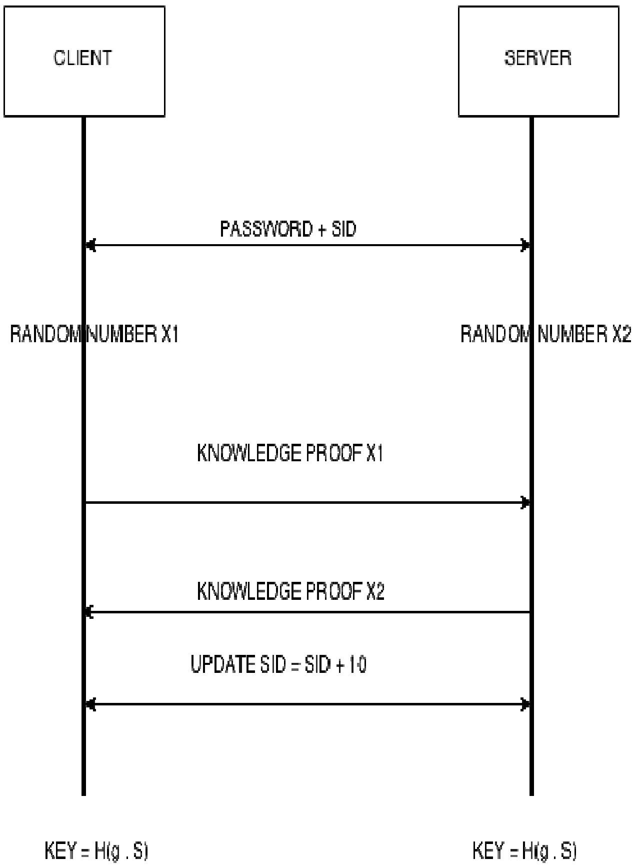
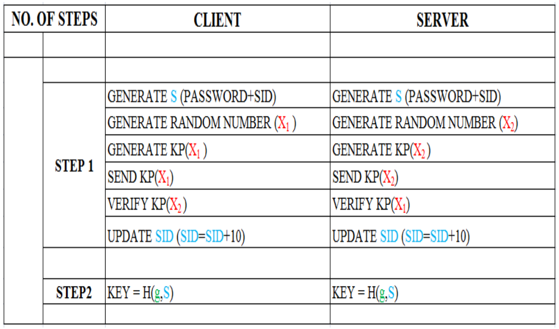


Fig. 2. Control Flow

- In this scenario, 'G' denotes a subgroup of 'Z_p^*' prime order. 'g' denotes a generator in 'G'. Both sender and receiver agree on (G,g).
- The client and server will contain the password and a common session ID (SID). Both the client and the server will combine the password and SID.
- In the first step, the client will generate a random number X_1 and a knowledge proof of it followed by the server generating a random number X_2 and its knowledge proof.
- In the next step. client sends its knowledge proof to the server and the server also sends its knowledge proof to the client.

- After verifying their respective knowledge proofs, both client and server increment their session ID by a certain common factor. In this case we have used a value of 10.
- In the final step, a key is generated by hashing the combination of 'g' and 'S'.



NO. OF STEPS	CLIENT	SERVER
STEP 1	GENERATE S (PASSWORD+SID)	GENERATE S (PASSWORD+SID)
	GENERATE RANDOM NUMBER (X_1)	GENERATE RANDOM NUMBER (X_2)
	GENERATE KP(X_1)	GENERATE KP(X_2)
	SEND KP(X_1)	SEND KP(X_2)
	VERIFY KP(X_2)	VERIFY KP(X_1)
	UPDATE SID (SID=SID+10)	UPDATE SID (SID=SID+10)
STEP2	KEY = H(g,S)	KEY = H(g,S)

Fig. 3. Steps involved in core algorithm

As described above, before the final step, there is a process which involves generation of a knowledge proof at both ends. In the field of cryptography, an interactive proof of knowledge more commonly known as a knowledge proof is a way in which one of the two parties involved in communication say a client, is able to prove to the other involved party say a server that it is in possession of a secret. Zero Knowledge Proofs achieve this by having a prover prove to the verifier that it is in possession of a secret without ever revealing what the actual secret is. The following steps describe how the knowledge proof is generated and verified:

- In this scenario, for the sake of explanation, we will explain as to how the knowledge proof of X_1 is generated.
- Initially, the client has values 'g' which as described in the preceding paragraph denotes a generator in 'G' which is a subgroup of prime order 'Z_p^*', 'g^ X_1' and 'X_1'.
- In the first step, the client generates a random number 'v'.
- In this step, a hash 'h' based on the values of 'g', 'g^v', 'g^ X_1' is generated.
- The first element of a pre-initialized array ZKP i.e. ZKP[0] is assigned the value of 'g^v' and its second element is assigned the value 'v - X_1.h'.
- This ends the knowledge proof generation phase and this array is sent to the server.
- After the server receives the array ZKP, the second element of the array is assigned into a variable 'r'.
- Then, the expression 'g^r * g^(X_1.h)' is evaluated. If this is reducible to obtain the value 'g^v', then the knowledge proof received is genuine.

  The expression is :

$$g^{r} * \; g^{x1\,.h}$$

This can be reduced to :

$$g^{v\,-\,x1\,.\,h} * \; g^{x1\,.\,h}$$

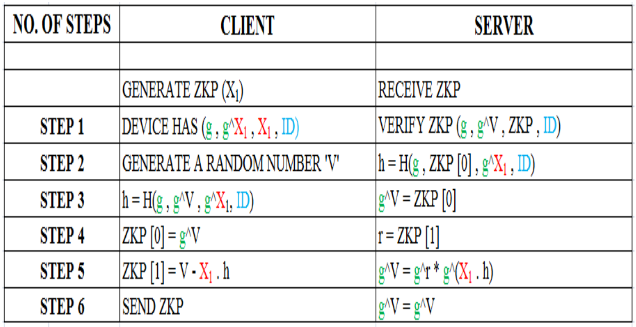
{ since r = v - X_1.h}

Further reducing this equation using the laws of exponentiation, we get :

$$\frac{g^{v}}{g^{x1\,.\,h}} * g^{x1\,.\,h}$$

which equates to :

$$g^{v}$$



NO. OF STEPS	CLIENT	SERVER
	GENERATE ZKP (X_1)	RECEIVE ZKP
STEP 1	DEVICE HAS (g , g^X_1 , X_1 , ID)	VERIFY ZKP (g , g^V , ZKP , ID)
STEP 2	GENERATE A RANDOM NUMBER 'V'	h = H(g , ZKP [0] , g^X_1 , ID)
STEP 3	h = H(g , g^V , g^X_1, ID)	g^V = ZKP [0]
STEP 4	ZKP [0] = g^V	r = ZKP [1]
STEP 5	ZKP [1] = V - X_1 . h	g^V = g^r * g^(X_1 . h)
STEP 6	SEND ZKP	g^V = g^V

Fig. 4. Steps involved in Knowledge Proof Generation

VI. ANALYSIS

In this section, we present a brief overview on our authentication protocol's computational performance along with its comparative analysis with similar methods. First, we will describe two prime attacks that our algorithm is resilient to:

Replay Attack : In case of a replay attack, a third party intercepts a genuine transmission and then uses it again repeatedly to gain access. This kind of an attack is normally carried out as part of an IP substitution attack.

In case of such attacks, the most suitable countermeasure is to use unique session tokens, which will be rendered invalid right after the session for which it was created expires. Our approach involves combining the password and the session ID and then creating its hash before authenticating. Unlike encryption, hashing is a non reversible process. Encrypted cipher text can be decrypted back to plain text with the help of the key which was used to encrypt. But that is not the case with hashing. A hash cannot be used in any way to obtain the original text. So in case any malicious third parties succeeds in intercepting the hash or even the password, it will be pointless since neither the password nor the session ID can be obtained from it. Our algorithm uses SHA-1 for hashing which produces a 160 bit hash value. Simulation of replay attack on our algorithm several times (1000 cases) using previously captured packets could not authenticate successfully.

Phishing : A phishing attack is a type of security attack which involves stealing vital credentials by masquerading as a trusted entity. As discussed in previous paragraph, the interception of a hash alone is not enough to authenticate successfully. This is why we added an additional security measure by using Zero Knowledge Proofs. Successful reception of the genuine hash along with successful verification of the knowledge proofs are mandatory to authenticate.

Zero Knowledge :If the statement is true, the verifier, in this case the receiver will not know anything other than the fact that the statement is true. Password and session ID details are secured using Zero Knowledge approach.

JPAKE : JPAKE (Password authenticated key exchange using juggling) is a similar protocol which also exploits the functionalities provided by the Zero Knowledge Proof. But it is computationally expensive algorithm expensive in terms of both space and time. It involves performing exponentiation of random numbers generated which produces extremely large results. On a 2.33 GHz system running Mac OS X, the time was 75 ms, whereas our algorithm on a 2 GHz processor machine running Windows operating system took 27 ms to execute. This is the mean obtained from 100 test cases.

Parameters	No of Test Cases	Result
Replay Attack	1000	No authentication
Phishing	100	No authentication
Execution Time	100	27ms (mean value)

Table 1. Analysis Results

VII. CONCLUSION

In this paper, we presented a platform which enables the devices which operate as a part of remote health monitoring systems to communicate in a secure manner. The protocol that we devised is based on the concept of Zero Knowledge Password Proof. As an experimental setup, we implemented this protocol on Raspberry Pi and the results were analyzed. Since the main advantage of our approach for being a Zero Knowledge based method over other conventional protocols like TLS/SSL is that it does not transfer the vital device credentials like the password over the network to authenticate which reduces its chances of getting intercepted. This is a lightweight protocol which can be incorporated comfortably into any future remote health monitoring systems.

ACKNOWLEDGMENT

We are indebted to the HuT labs and Computer Science and Applications department at Amrita Vishwa Vidyapeetham, Amritapuri Campus for their constant support and guidance for this work.

REFERENCES

[1] Jordan Smalls, Yue Wang, Xi Li, Zehuang Chen, and K. Wendy Tang, "Health Monitoring Systems For Massive Emergency Situations"

[2] Ahmed Alahmadi and Ben Soh, “A Four-Step Pre-Analytical Conceptual Study Towards a Reliable Smart Mobile E-health Monitoring System Design”

[3] Ahmed Alahmadi and Ben Soh, “A Smart Approach Towards a Mobile E-Health
Monitoring System Architecture”

[4] Feng Hao and Peter Ryan, "Password authenticated Key exchange by Juggling"

[5] William Stallings, "Cryptography and Network Security"

[6] Atul Kahate, "Cryptography and Network Security "

[7] Azzedine Boukerche, and Yonglin Ren, "A Secure Mobile Healthcare System using Trust-Based Multicast Scheme"

[8] Honggang Wang, Dongming Peng, Hsiao-Hwa Chen, Ali Khoynezhad, "Resource-Aware Secure ECG Healthcare Monitoring through Body Sensor Networks"

[9] Ming Li, Wenjing Lou, Kui Ren, "Data Security and Privacy in Wireless Body Area Networks"

[10] Jinyuan Sun, Yuguang Fan, Xiaoyan Zhu, "Privacy and Emergency Response in E-Healthcare Leveraging Wireless Body Sensor Networks"

[11] Linkie Guo, Chi Zhang, Yuguang Fang, " A Privacy Preserving Attribute Based Authentication System for Mobile Health Networks"