ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment

[1] R.Poornimadevi, [2] P.Valvarasi, [3] M.Ambika, [4] A.K.Punitha
[1][2][3] Final Year Student, [4] Assistant Professor
[1][2][3][4]Department of Cse, Sengunthar College of Engineering, Tiruchengode

***Abstract* – Implantable medical devices (IMDs) are man-made devices, which can be implanted in the human body to improve the functioning of various organs. The IMDs monitor and treat physiological condition of the human being (for example, monitoring of blood glucose level by insulin pump). The advancement of information and communication technology (ICT) enhances the communication capabilities of IMDs. In healthcare applications, after mutual authentication, a user (for example, doctor) can access the health data from the IMDs implanted in a patient's body. However, in this kind of communication environment, there are always security and privacy issues such as leakage of health data and malfunctioning of IMDs by an unauthorized access. We propose a new secure remote user authentication scheme for IMDs communication environment to overcome security and privacy issues in existing schemes. We provide the formal security verification using the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. We also provide the informal security analysis of the proposed scheme. The formal security verification and informal security analysis prove that proposed scheme is secure against known attacks**

1. INTRODUCTION

Implantable medical devices (IMDs) monitor and treatphysiological conditions within the body of a patient. Different types of IMDs such as brain neurosimulator, pacemaker, gas-tric implant and cochlear implant provide remote monitoring M. Wazid is with the Center for Security, Theory and Algorithmic Research,International Institute of Information Technology, Hyderabad 500 032, India(e-mail: mohammad.wazid@research.iiit.ac.in).
A. K. Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India(e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in). (Corresponding au-thor: Ashok Kumar Das.)N. Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala 147 004, India (e-mail: neeraj.kumar@thapar.edu).
M. Conti is with the Department of Mathematics, University of Padua,Padua 35122, Italy (e-mail: conti@math.unipd.it).
A. V. Vasilakos is with the Department of Computer Science, Electrical andSpace Engineering, Lulea University of Technology, Lulea 971 87, Sweden(e-mail: th.vasilakos@gmail.com).and treatment to patients with severe medical conditions. Thepervasiveness of IMDs is growing continuously, for example,25 million US citizens reliant on them for their day to day lifecritical functions [1]. The global IMDs market was valued at$72, 265 million in 2015, and is projected to reach $116, 300million by 2022, registering a compound annual g rowth rate(CAGR) of 7.1% from 2016 to 2022 [2]. Information and communication technology (ICT) facilitates the information exchange of IMDs and provides them capabilities to com-municate with each other. IMDs have the ability to send the collected health related data of a patient to the nearby controller node (CN) using the communication technologies such as bluetooth, zigbee and infrared transmission. CN is more powerful node as compared to IMDs as it has more communication range, processing power and storage capability. CN is connected to the Internet using an access point. A user (for example, a doctor) can access the data of an IMD via CN after successful mutual authentication.However, in such kind of communication environment, there are several security and privacy related issues such as replay attack, man-in-the middle attack, impersonation attacks and privileged-insider attack [3], [4], [5], [6].

A. Motivation

An attacker can exploit the vulnerabilities in the IMDs, which can cause negative medical effects on the health of the patient. Such effects are commonly known as adverse events [7]. According to the report available in [8], the vulnerability in an implanted insulin pump could be exploited by a hacker (a remote malicious user) which can cause an overdose of insulin to the diabetic patients. The overdose of insulin could then cause hypoglycemia (low blood sugar level) which in extreme case becomes a diabetic shock to the patient. Therefore, security of IMDs becomes a serious concern so that an illegal party can not

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

attack the IMDs implanted in a patient's body. Hence, there is a strong need to design a secure remote user authentication scheme for IMDs by which the controller node of a patient's IMDs and a user (for example, a doctor) can mutually authenticate each other. At the end, both entities establish a secret session key shared between them for their future secure communications. To address such an important issue for IMDs communication environment, we propose a new secure remote user authentication and key agreement scheme.

B. Main Contributions

The contribution of this paper is manyfold:

• We propose a new lightweight three-factor remote user authentication scheme for implantable medical devices in which the controller node of the implantable medical devices of a patient and remote user can authenticate each other.

• The security analysis shows that the proposed scheme is secure. In addition, we test the formal security verification of the proposed scheme using the widely-accepted AVISPA tool to show the proposed scheme is also secure against the replay and man-in-the middle attacks.

• We provide the practical implementation of the proposed scheme using the widely-used NS2 simulation tool to measure the impact of the scheme on network performance parameters such as end-to-end delay and throughput.

C. System Models

The following two models are considered to describe and analyze the proposed scheme in the paper. Network Model: The network model for the (IMD)scommunication environment shown in Figure 1 is used in the proposed scheme. In the given model, we have different types of IMDs, such as brain neurosimulator and gastric simulator,which are implanted in a patient's body. There is a controller node (CN) which collects data from all IMDs using wireless communication technologies (for example, bluetooth, zigbee and infrared transmission). CN is connected to the Internet through an access point. The users can access IMDs through CN. Suppose there is a user (for example, a doctor) Ui wants to access the data from the controller node belonging to a set of implantable medical devices. In this scenario, we need authentication between Ui and CN. attacker A can then have the opportunity to eavesdrop, modify or delete the exchanged messages during the transmission in order to tamper the communicated data. A can also physically capture CN and can extract the stored information by using the power analysis attacks [11], [12] as these devices are non-tamper resistant. However, all IMDs are implanted inside the body of a patient, and hence, there is a rare possibility of physical capturing of IMDs from a patient's body. We further assume that the trusted authority (TA) is fully trusted party in the network, which is responsible for pre-deployment of IMDs and the user registration phase as described in SectionIII.

D. Structure of the Paper

The rest of the paper is organized as follows. In SectionII, we discuss the existing related authentication schemes proposed for IMDs. The various phases of the proposed scheme are discussed in Section III. The security analysis of the proposed scheme is provided in Section IV. The formal security verification of the proposed scheme using the widely- accepted AVISPA tool is given in Section V. The performance comparison of the related existing schemes and the proposed scheme is provided in Section VI. The practical demonstration of the proposed scheme using the widely-accepted NS2 simulation tool is also provided in Section VII. Finally, the paper is concluded in Section VIII.

EXISTING SYSTEM

Existing system lightweight three-factor remote user authentication scheme for implantable medical devices in which the controller node of the implantable medical devices of a patient and remote user can authenticate each other. The security analysis shows that the proposed scheme is secure. In addition, we test the formal security verification of the proposed scheme using the widely-accepted AVISPA tool to show the proposed scheme is also secure against the replay and man-in-the middle attacks.

DISADVANTAGES

•No improved Energy Efficiency

•Discovered routes by these algorithms may neither be energy-efficient nor be reliable.

PROPOSED SYSTEM

Implantable medical devices (IMDs) are man-made devices, which can be implanted in the human body to improve the functioning of various organs. We propose TSEOAP based on cooperation and routing operation and attacker detection, prevention .we detail the techniques and the contributions in trust-based security in TSEOAP. We present trust-based analysis of the OLSR protocol using trust specification language and we show how trust-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

based reasoning can allow each node to evaluate the behavior of the other nodes. After the detection of misbehaving nodes. we propose solutions of prevention and countermeasures to resolve the situations of inconsistency, and counter the malicious nodes. We proposed cryptography based security mechanism to security algorithms like ECC Security Algorithm. ECC is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Improving encryption and decryption aspects of the algorithm, which is already exist and creates the way for an excellent security.

Advantages:
•Trusted nodes and perfect IDSs'
•Reduces the IDSs' active time as much as possible without compromising on its effectiveness.
•Maximizing the lifetime of the network and achieved security level significantly.
•Overall energy consumption is reduced and increases network performance.

MODULES DESCRIPTION

1. MANET(IMD) Network Deployment

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

2.Data Communication

This Module is developed to MANET networks data communication and aggregation process. The radio and IEEE 802.11 MAC layer models were used. The network based data processing or most expensive and data communication level on their performance on the network. Multiple sources create and end sending packets; each data has a steady size of 512 bytes.

3.Trust Computation

To make a security decision with the computed trust value, we need to estimate how much risk is affordable for each ongoing task. In other words, a threshold of trust value (Threshold) needs to be defined for each task. Such threshold trust value may be varied depending on the security requirement of each ongoing task. By comparing the computed trust value and the threshold trust value, it is easy to see whether the trustee node satisfies the trust requirement or node.

Trust computation based attacker detection

T^{d}_{ij} -Trust value

I and j nodes

α-positive value

B-negative value

Trust value=10/10 +8=10/18 =0.5 **Formula :**

$$T^{d}_{ij} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$$

4.TSEOAP

This module is developed to propose TSEOAP based on cooperation and routing operation and attacker detection ,prevention .we detail the techniques and the contributions in trust-based security in TSEOAP. We present trust-based analysis of the TSEOAP protocol using trust specification language and we show how trust-based reasoning can allow each node to evaluate the behavior of the other nodes

5.ATTACK PREVENATATION MODEL

Generation of key is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.
Now, we have to select a number 'd' within the range of 'n'.Using the following equation we can generate the public key
Q = d * P
'd 'is the random number that we have selected within the range of (1 to n-1). 'P' is the point on the curve.
'Q' is the public key and 'd' is the private key.

ENCRYPTION

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from;

[1 – (n-1)].

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

DECRYPTION

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

5. Performance Analysis Result

This module is developed to improve Wireless network performance

Throughput Ratio

Packet Delivery Ratio

Average End-to-End Delay

Energy Consumption

CONCLUSION

The use of IMDs facilitates the remote monitoring of the health of a patient. The IMDs specially improve the quality of life of elderly people, who other has problem to move easily.A doctor can provide them remote consultation on the basis of their health data, which is collected by the help of IMDs. However, wireless communication raises serious threats in the IMD deployment. In this paper, we proposed a remote user authentication scheme through which a user (a doctor) and a controller node can mutually authenticate each other and establish a session key for their future secure communication.Apart from that the pairwise key establishment between a controller node and its IMDs is also provided in the proposed

scheme for the secure communication between them. The computation and communication costs of the proposed scheme are comparable with the existing related schemes. In addition, the proposed scheme also provides better security and more functionality features, such as password and biometric update phase, dynamic controller node and IMD addition phases, as compared to other existing related schemes.

ACKNOWLEDGMENTS

We thank the anonymous reviewers and the Associate Editor for their valuable feedback on the paper which helped us to improve its quality and presentation.

REFERENCES

[1] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39, 2008.

[2] R. Thakur, "Implantable Medical Devices Market is Expected to Reach $116, 300 Million by 2022, Globally – AlliedMarketResearch,"http://www.prnewswire.com/news-releases/implantable-medical-devices-market-is-expected-to-reach-116300-million-by-2022-globally—allied-market-research-613835833.html.

[3] C. S. Jang, D. G. Lee, J.-w. Han, and J. H. Park, "Hybrid Security Protocol for Wireless Body Area Networks," Wireless Communications and Mobile Computing, vol. 11, no. 2, pp. 277–288, 2011.

[4] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," IEEE Communications Magazine, vol. 53, no. 1, pp. 71–77, 2015.

[5] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based Access Control for Implantable Medical Devices," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009), Chicago, USA, 2009,pp. 410–419.

[6] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga,"Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting," in 3rd International Workshop on Trust-worthy Embedded Devices, Berlin, Germany, 2013, pp. 35–42.

[7] C. Camara, P. P. Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," Journal of Biomedical Informatics, vol. 55, pp. 272 – 289, 2015.

[8] J. Finkle, "J & J warns diabetic patients: Insulin pump vulnerable to hacking," http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps eidUSKCN12411L.Accessed on February 2017.

[9] D. Dolev and A. C. Yao, "On the security of public key protocols,"IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208,1983.

[10] M. L. Das, "Two-factor user authentication in wireless sensor networks,"IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086–1090, 2009.

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of 19th Annual International Cryptology Conference (CRYPTO1999), LNCS, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[13] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun,"Proximity-based Access Control for Implantable Medical Devices," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009), Chicago, USA, 2009,pp. 410–419.

[14] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga,"Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting," in Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices, Berlin, Germany, 2013, pp. 35–42.

[15] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72– 83, 2015.

[16] D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti, and S. S. Yeo,"Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21,no. 1, pp. 49–60, 2015.

[17] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," IEEE Systems Journal, pp. 1–12, 2016, DOI: 10.1109/JSYST.2016.2544805.

[18] X. Li, J. Niu, S. Kumari, F. Wu, and K. K. R. Choo, "A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city," Future Generation Computer Systems, 2017, DOI: 10.1016/j.future.2017.04.012.

[19] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R.Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," Computer Networks,2017,DOI:10.1016/j.comnet.2017.03.013