e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 11, October-2019

Security System Approach With pressure Sensor

Prof. Kanu Patel, Prof. Jitendra B Patel

Assistant Professor, IT Department, BVM Engineering College, V.V.Nagar
Lecturer, CE Department, K.D Polytechnique, Patan

Abstract *— The increased usage of smart wearable in various applications, specifically in health-care, emphasizes the need for secure communication to transmit sensitive health-data. practically, where multiple devices are carried by a person, a common secret key is essential for secure group communication. In this paper, we present a novel solution to generate and distribute group secret keys by exploiting on-board accelerometer sensor and the unique walking style of the user, i.e., gait. We propose a method to identify the suitable samples of accelerometer data during all routine activities of a subject to generate the keys with high entropy. In our scheme, the Smartphone placed on waist employs fuzzy vault, cryptographic practical applications. Suitable construct, and utilizes the acceleration due to gait, a common characteristic extracted on all wearable devices to share the secret key. We implement our solution on commercially available off-the-shelf smart wearable's, measure the system performance, and conduct experiments with multiple subjects. Our results, and is suitable for demonstrating that the proposed solution has a bit rate of 750 bps, low system overhead, distributes the key securely and quickly to all legitimate devices we have presented our novel protocol for group secret key generation and secure key distribution for multiple smart wearable devices. Our solution leverages the accelerometer sensor available on the off-the-shelf wearable devices and the unique walking characteristics of the user. We have presented a method to detect the suitable samples of sensor data dynamically to ensure the generation of the secret keys with good entropy during different activities. The secure key distribution process extracts the acceleration due to gait on all the smart devices and exploits this as a common characteristic to share the keys using the fuzzy vault. The solution is implemented on real wearable devices.*

Keywords: Arduino, IoT

I. INTRODUCTION

RECENTLY, the rapid advances in smart wearable device technologies have led to their increased usage impersonalized health-care, fitness, sports applications, etc. As a result, wearables like smart glass, smart watch, and wristbands have become an integral part of the Internet of Things (IoT).A recent survey by Forbes [1] states that the wearable industry is expected to grow to USD $6 billion in the next few years. Typically, the smart devices exchange sensitive health information over wireless medium e.g., Bluetooth Low Energy(BLE), which is vulnerable to many types of attacks such as eavesdropping, tampering the packets, and injecting malicious commands The above discussion underscores that securing communications between smart wearable's is crucial. To ensure confidentiality, the messages exchanged by these devices can be encrypted using a secret key known a priority the legitimate devices. The traditional cryptographic key establishment mechanisms are computationally complex and hence are infeasible for the resource-constrained devices. In addition, in practical scenarios, the devices need to establish keys in an ad hoc manner where a trusted entity for key distribution/management (e.g., PKI) is not always available. Therefore, a very lightweight, reliable and fast key generation/sharing mechanism is desirable for smart personal wearables. The devices need to generate the secret keys dynamically and renew them periodically to provide strong protection from privacy leakage and node compromise.

II. LITERATURE REVIEW

Sr. No.	*Paper Name*	*Author Name*	*Published Year*	*Advantages*	*Disadvantages*
1	*Next generation pressure sensors in surface micro machining technology*	*G. Lammel ; S. Armbruster ; C. Schelling ; H. Benzel ; J. Brasas ; M. Illing ; R. Gampp ; V. Senz ; F. Schafer ; S. Finkbeiner*	*2005*	*Useful in Sacrificial layer technology for fabrication.*	*Requires high budget.*

2	*Development of a novel carbon nanotube based printed and flexible pressure sensor*	*Dinesh Maddipatla ; Binu B. Narakathu ; Mohammed M. Ali ; Amer A. Chlaihawi ; Massood Z. Atashbar*	*2007*	*The capability of the sensor to distinguish between varying applied pressures were investigated based on its capacitive response.*	*Less flexible to wear.*
3	*Foot plantar pressure measurement system using optical sensor*	*Tanapon Keatsamarn ; Chuchart Pintavirooj*	*2009*	*Provides health care monitoring, and wireless communication.*	*Foot pressure measurement is only for classifying disorders of the foot and designing insole for individual person.*
4	*Fatigue estimation using foot pressure sensors*	*Isamu Tanaka ; Shuhei Terada ; Ryuichi Tsuchiya ; Dai Hanawa ; Kimio Oguchi*	*2012*	*Fatigue detected using wearable sensor.*	*Fatigue level cannot be quantified.*
5	*Investigation on developing of a piezoresistive pressure sensor for foot plantar measurement system*	*Fairuz Rizal Mohamad Rashidi ; Omar Hussein ; W. Z. W. Hasan*	*2013*	*Is useful in helping medical examiner to detect any pressure abnormality.*	*Complicated to design.*
6	*Low cost and customized plantar pressure analyzer for foot pressure image in rehabilitation foot clinic*	*K. Petsarb ; C. Apaiwong ; C. Phairoh ; R. Rattanakajornsak ; Y. Kajornpredanon ; S. Daochai*	*2015*	*Effective tool to analyse a foot pathology and disorder in foot care.*	*Power Consumption is high.*
7	*Design and simulation of new micro-electromechanical pressure sensor for measuring intraocular pressure*	*M. Shahiri-Tabarestani ; B. A. Ganji ; R. Sabbaghi-Nadooshan*	*2016*	*Intraocular pressure sensors are important in detection and treatment of an incurable disease.*	*High cost.*
8	*A Low-Cost and Highly Integrated Fiber Optical Pressure Sensor System*	*F. Ceyssens ; M. Driesen ; K. Wouters ; R. Puers*	*2016*	*Cost-effective.*	*Less flexible.*

9	*Sitting posture recognition using screen printed large area pressure sensors*	*Jawad Ahmad ; Henrik Andersson ; Johan Sidén*	*2017*	*The sensor system provides wireless communication and a Windows based GUI is developed that allows real-time presentation of pressure data by means of a pressure map.*	*Complicated to design.*
10	*New electromagnetic transduction micro-sensor concept for passive wireless pressure monitoring application*	*M.M. Jatlaoui ; F. Chebila ; I. Gmati ; P. Pons ; H. Aubert*	*2017*	*This approach is based on electromagnetic transduction principle, which can be used for long distance covering pressure measurement.*	*This communicati on is focused only on the pressure measuremen t cell.*

III. EXISTING SYSTEM

Group key generation and sharing among wearable's has received very little attention in the literature due to the underlying challenges is difficulty in obtaining a good source of randomness to generate strong cryptographic keys, and finding a common feature among all the devices to share the key.

.

IV. SURVEY OF PROPOSED SYSTEM

We propose a method to identify the suitable samples of accelerometer data during all routine activities of a subject to generate the keys with high entropy. In our theme, a Smartphone placed on waist employs fuzzy vault, a cryptographic construct, and utilizes the acceleration due to gait, a common characteristic extracted on all wearable's device to share the secret key. We implement our solution on commercially available off-the-shelf smart wearable, measure the system performance, and conduct experiments with multiple subjects.
Our results demonstrate that the proposed solution has a bit rate of 750 bps, low system overhead, distributes the key securely and quickly to all legitimate devices, and is suitable for practical applications.

ADVANTAGES OF PROPOSED SYSTEM:

1.Our solution does not require a stored seed, or any pre shared secret for key generation and sharing among the devices.
2. Our energy-efficient scheme helps to perform continuous authentication of all the body-worn devices by establishing the group secret key without any user intervention, a desirable feature for all personal health-care devices.
3.Our protocol can be used for secure automated pairing, i.e., authentication and secret key sharing. Current pairing mechanisms require additional IO devices or Out Of Band (OOB) sensors [20] to input keys or passwords to share the initial key
4.Our method enables dynamic key generation and periodic key renewal, enhancing the overall security of personal smart devices.

V. SYSTEM ARCHITECTURE

Fig.: System Architecture

VI. CONCLUSION AND FUTURE WORK

In this project, we have presented our novel protocol for group secret key generation and secure key distribution for multiple smart wearable devices. Our solution leverages the accelerometer sensor available on the off-the-shelf wearable devices and the unique walking characteristics of the user. We have presented a method to detect the suitable samples of sensor data dynamically to ensure the generation of the secret keys with good entropy during different activities.

Future scope

The secure key distribution process extracts the acceleration due to gait on all the smart devices and exploits this as a common characteristic to share the keys using the fuzzy vault. The solution is implemented on real wearable devices.

VII. REFERENCES

[1] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical Devices," in Proc. ACM SIGCOMM Conference, 2011.
[2] G. Revadigar, C. Javali, W. Hu, and S. Jha, "DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices," in Proc. 40th IEEE Conference on Local Computer Networks (LCN), 2015.
[3] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks," in Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2013.
[4] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks." IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, pp. 60–68, Jan 2010.
[5] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie- Talkie: Motion-Assisted Automatic Key Generation for Secure On- Body Device Communication," in Proc. ACM/IEEE Conference onInformation Processing in Sensor Networks (IPSN), 2016.
[6] C. Hennebert, H. Hossayni, and C. Lauradoux, "Entropy Harvesting from Physical Sensors," in Proc. ACM Conference on Security andPrivacy in Wireless and Mobile Networks (WiSec), 2013.
[7] B. Mjaaland, P. Bours, and D. Gligoroski, "Gait Mimicking – Attack Resistance Testing of Gait Authentication Systems," in Proc. Norwegian Information Security Conference (NISK), 2009.
[8] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections Between Smart Artefacts," in Proc. 3rd International Conference on Ubiquitous Computing (UbiComp), 2001
[9] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices," IEEE Transactions on Mobile Computing, vol. 8, no. 6, pp. 792–806, Jun 2009.
[10] D. Bichler, G. Stromberg, M. Huemer, and M. L¨ow, "Key Generation Based on Acceleration Data of Shaking Processes," in Proc. 9th InternationalConference on Ubiquitous Computing (UbiComp), 2007.

