Secure Mutual Self-Authenticable Mechanism for Wearable Devices

Nnabuike Eya[1], Trust Mapoka[1], Simon Shepherd[1], Raed A Abd-Alhameed[1], Issa Elfergani[2] and Jonathan Rodriguez[2]
[1]*School of Electrical Engineering and Computer Science, University of Bradford, UK*
[2]*Instituto de Telecomunicações, Averi, Portugal*

Abstract

Due to the limited communication range of wearable devices, there is the need for wearable devices to communicate amongst themselves, supporting devices and the internet or to the internet. Most wearable devices are not internet enabled and most often need an internet enabled broker device or intermediate device in order to reach the internet. For a secure end to end communication between these devices security measures like authentication must be put in place in other to prevent unauthorised access to information given the sensitivity of the information collected and transmitted. Therefore, there are other existing authentication solutions for wearable devices but these solutions actively involve from time to time the user of the device which is prone to a lot of challenges. As a solution to these challenges, this paper proposes a secure point-to-point Self-authentication mechanism that involves device to device interaction. This work exploits existing standards and framework like NFC, PPP, EAP etc. in other to achieve a device compatible secure authentication protocol amongst wearable device and supporting devices..

1. Introduction

The statistics on mobile wearable communication is alarming, by 2017 the shipment of mobile wearables is projected to reach 70 million and the market value of mobile wearable device was estimated to be $1.5 in 2014[1]. According to [2], 97 million wearable devices generated 15 petabytes of monthly traffic in 2015. Mobile wearable communication is fast becoming a new communication paradigm and mobile wearable device can be said to use up a reasonable amount of bandwidth due to the nature of its application which is basically collect, store, interpret, transmit and exchange these data (information) over the internet or amongst other supporting wearable devices. For instance, mobile health wearables measure, monitor or collect biomedical information from patients or user in real time and this information is transferred to the hospital for clinical diagnosis and may be there a need for emergency response could be established. This medical information is accessed or shared by more parties than the picture painted already, parties like the government, Medical staff, researchers, insurance companies etc. as the case may be. One of the obvious challenges of wearables is the limited communication range and attempts are being made to address this challenged and this has exposed wearables to security and privacy challenges.

Most wearable devices are not stand-alone device as they are more useful when they transmit sensed or collected data since most of them cannot process these data. These wearables collect, store, interpret, transmit and exchange these data (information) over the internet or amongst other supporting wearable devices. Depending on the application of the mobile wearable they store or collect data such as temperature, blood pressure, activity tracking, heart rate etc. to interpret and make recommendations based on these data collected these wearables need to share or transmit this data to other supporting device or application. The security of the transmitted information needs to be guaranteed from point of sending to intended receiver due to the sensitive nature of information transmitted which could be of commercial value, military high secret information or a patient's medical record or health status etc. Due to the peculiar characteristic of these mobile wearable there are some communication challenges, peculiar characteristics like limited memory (there is need to transmit to an external device), limited CPU power (there is need to transmit to another device that would process collected data), mobility (transmition needs to be via a secure channel), limited battery life (there is a limit to the computation these devices can take), connectivity range (very limited range of connectivity, there is need for communication with other device), limited user and device interaction etc.

The high possibility of these wearables communicating with other device have attracted some security challenges because the stored data or content in transit needs to be protected from unauthorised access, for example, a patient's medical record is private and should only be access by authorised persons depending on the situation. In a situation of an emergency and a patient's wearable is meant to communicate with his hospital or an ambulance via the internet or any other means, the device needs to confirm that this information gets to the authorised authority and the authority or hospital needs to confirm that the information is coming from their patient. A secure identification and authentication mechanism is essential for the privacy

and security of the information shared between the wearable device and other supporting device or application. This authentication mechanism is meant to request, obtain and verify credentials of parties before granting access to sensitive data.

Most authentication solutions present today tend to treat the wearable as a token to authenticate other device [3, 4], some other solutions are meant for scenarios where the device is authenticating with participating sensors within the same Body Area Network (BAN), some others authenticate the users or would need the physical intervention of the users in other to authenticate communicating devices. In the light of this authentication challenge, this work proposes a secure identification and authentication mechanism that can authenticate with supporting devices remotely with no intervention of the user. Most authentication mechanisms require another device may be a mobile phone to forward the received data from the wearable to other supporting device but the proposed mechanism here the wearable device authenticates directly against from one point to another and another without the mobile phone acting as a tunnelling device.

RFID technologies, NFC are common technologies for wearables adopted in other to secure or grant authorised access to information but these technologies have limitations which is one of the main reason why this work proposes the use of contactless smart cards (CSCs). Considering the size of wearable, CSCs is a small device with a more sophisticated computing power with a very limited read range which reduces the chances of eavesdropping, unlike RFID tags with more read range. The power challenge face by these mobile wearable devices makes CSCs a preferable option due to its Non-volatile memory.

The rest of this work is divided into four (IV) sections with subsections within each section: Section two (II) gives a brief review of previous related technologies, highlights some possible user identification and authentication threats when using a mobile wearable device, it also explains some authentication techniques meanwhile section three (III) categories and explains some of the major security and communication requirements for wearables, while section four (IV) introduces the proposed design while the concluding part of this work tends to validate the design and suggest future work.

This section presents related work and briefly introduces the technologies to be adopted in the proposed design.

2. Related work and Technologies

Wearable devices could be defined as lightweight devices with limited storage, constrained computation and communication abilities hence, its size that is worn by users in other to perform specific task mainly sensing and observation [11]. Wearable technologies are electronic technologies that are designed to be worn on the body and equipped with scanning, sensory and communication capabilities. The communication capabilities are such that the wearable device communicates with a supporting device to interpret or display captured data in real time due to the limited communication range.

In the last ten (10) years, the technological market has witnessed the influx of wearable device with major players like Fitbit, Apple, Samsung, Garmin etc. flooding the market with different wearable technologies with applications that range from fitness to health. These devices come in different shapes and sizes and could be worn as wristwatches, earphones and as a part of our clothing as well [31, 32]. This influx has been fuelled by a lot of factors ranging from consumers demand to the low cost of sensors and technologies used for the manufacturing of wearables, not to mention that all wearable are cheap. Another major reason that has encouraged the vast deployment of wearable technology is the success that has been recorded over the years. These successes have been recorded in different works of life ranging from medical, entertainment, emergency, sport and fitness etc. and in the nearest feature wearable would become part of our lifestyle.

As mentioned earlier when the word authentication meets wearable devices, what comes to mind is the use of wearables as an authentication device as seen in the few technologies mentioned in [5] Smart jewellery, Smart Watches etc. [6] proposes a transient authentication (TA) used in securing mobile devices, this authentication mechanism comes as solution to the evident characteristic security challenges with mobile devices. Mobile devices have become more expensive by the day and the physical security has become more difficult due to the size and the value of these devices have increased due to the nature of data that they carry. In the light of this TA model was proposed not only to secure the mobile device but also provides convenience. In TA the wearable device acts like a token that constantly attest the users and authenticates him as well, this protects the information stored in the device and save the user from authenticating at all time which can be a bit frustrating for users. In the same vein, SEPIA (Secure-PIN-Authentication-as-a Service) [7] used cloud-connected wearables as an authentication device to protect ATM and POS terminals. Here, the wearable is used as a QR code scanner which the user would scan from the screen of the POS terminal in order to obtain a one-time-password that would be used for the transaction.

Recent research efforts have focused on improving the connectivity range of wearable

devices using more powerful personal devices (e.g., mobile phones or tablets) as intermediate devices. However, this new communication method also opens up new security challenges that should be addressed, which involve protecting wearable devices from both malicious intermediate devices and unauthorised access attempts from other entities residing on the Internet.

2.1. Smart Watches

In [5] smart watches were mentioned as an authentication device. Wristwatches are worn by most people for different purposes other than keeping time, based on this the authors exploits the fact that the capabilities of the smart watch interacting with the user, more storage capabilities unlike the iButton, higher processing power etc. all these capabilities are requirements for a more secure authentication device. There have also been proposed mechanisms or technologies that have not treated wearables as authentication device rather has attempted to propose a solution to the access control challenges in mobile wearables. [8] Presents a data authentication mechanism for the protecting data communication within in a Wireless Body Area Network (WBAN), this mechanism doesn't account for data communication with other supporting devices outside the network which is the case most often.

2.2. Smart Jewellery

The device featured in the article mentioned above as the iButton which could be worn as a jewel and due to human nature, jewels are worn most of the time, therefore, it could be used as a means to provide authentication. The iButton is equipped with a microprocessor that runs on JVM which can communicate with a supporting computer but in this case, the jewellery only stores the information or credentials needed for identification and authentication.

3. Authentication Techniques

Authentication as a process of validating a user's identity using the user's credentials in other to grant access to the user can be achieved in many ways depending on the scenario. Multiple factors may be included for the preservation of sensitive data or data with commercial value. There are quite a number of authentication techniques, mechanism and protocols out there and the research in this area is still very active.

3.1. Message Authentication Code (MAC)

MAC message authentication code, this technique have successfully been used in data authentication [1, 9-11], MAC literally is a code used to authenticate a message in other to verify the sender and protect the integrity of the message by ensuring that the message was not tampered with on transit. This is a very popular authentication technique that has been adopted over the years in other to protect the integrity of data in transit. MAC presents a low-cost authentication for data communication but this can be safer when implemented in a scenarios with very few communicating members because when the more the communicating members the higher the risk of exposure since the secret key would be shared amongst communicating members and trying to manage key sharing (key management) and protection would incur more cost [11]. This mechanism is not the most suitable for mobile wearables that would be performing data communications with a lot of supporting devices.

3.2. Smart Cards

Smart cards are hardware devices used to protect sensitive operations such as electronic payments and access control. They can store sensitive information securely and have cryptographic capabilities.1Smart card characteristics, ranging from physical characteristics to commands to interact with cards, are described in the International Organization for Standards/International Electrotechnical Commission (ISO/IEC) 7816 standard series. Security and commands for information interchange are defined in ISO/IEC 7816–4 [8].

Traditionally, the use of smart cards has been strictly attached to a terminal. Both the terminal and the smart card were involved in the authentication process, working together as a split-supplicant [4]. However, more recent works [9] have proposed using a smart card in an autonomous way (standalone supplicant) where the card is able to take part in the authentication process by itself. This new functionality is based on the Java Card technology, which allows Java-based applications to be run on smart cards, and its autonomy can only be achieved if the smart card has connectivity.

3.3. Kerberos

Kerberos protocol (RFC1510) as a security system was developed in 1988 at the Massachusetts Institute of Technology as an authentication means for secure communication [12]. It has been widely adopted but mainly in a wired network but [13] proposed a Kerberos-based authentication architecture that could be used for authentication in a wireless authentication although its characteristics

have made it unlikely to be used for this design. Kerberos are based on password, which not only makes it's prone to password attacks but not suitable for machine to machine communication scenarios. For a better overview on Kerberos refer to [12, 14, 15].

3.4. Location-Based Authentication

This is a new technique or factor for authentication that uses the physical location of the user to authenticate the user and there are various ways to achieve this like using sensors or GPS receivers. Location-Based authentication is exposed to some challenges such as user mobility and position based security attacks like position targeted spam. Location-based authentication has attracted some research works around it recently and amongst the early authors

3.5. Extensible Authentication Protocol (EAP)

This is a general authentication protocol that provides an interface for specific authentication mechanism. These characteristics have made this the best option for the proposed design since EAP just provides an application with an interface for the main authentication mechanism and EAP can also be used alongside other protocols like PPP/LCP. EAP allows different systems and authentication mechanisms to be used and this gives the user the liberty of choice to include other authentication protocol. This protocol has been used alongside other protocols in cases liked EAP-MD5, LEAP,EAP-TLS (MS) PEAP etc. the list goes on. EAP presents impressive requirements as can be seen in [16]. EAP supports Request, Response, Success, and Failure message following the PPP authentication model.

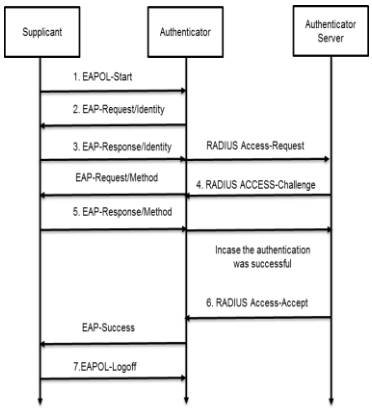

Figure 1. Message exchange procedure of EAP

4. Security Requirements for Wearable Technology

Data security and privacy is a critical issue with wearable devices, data must be stored securely transmitted in a timely manner when needed with no interruption and must be accessed or modified only by authorised users. It is a critical issue because wireless channels for transmitting is not secured due to the fact that anyone can interfere, monitor, or even participate in a communication in a wireless environment as long as they are on the same frequency, basically, wireless technology is more susceptible to security threats than wired. To ensure data security in wearable technology, there are various security requirements which should be considered in any design of security mechanism. The security requirements for wearable devices could be categorised into three depending on the three-tier architecture illustrated below.

Table 1. Security requirements for wearable technology

Wearable Security Requirements	Description
Data Storage Security Requirements	
Confidentiality	All collected data should be stored within a confidential system. Confidentiality also protects the privacy of the data and misuse of the user's identity and this is a key functional requirement.
Integrity	The collected data should be stored in a manner that would assure users that the information has not been tampered with. This is another key functional security requirement that protects unauthorised changes to the data or information stored and also the authenticity of the data.
Availability	This should make sure that anytime that data is needed it could be accessed as and when needed. There should be a secure, effective and efficient channel for communication.
Data Access Security Requirements	
Access Control	Access should only be granted to authorised users to ensure the privacy of sensitive data and also data with commercial value.
Identification	Users must have a form of identification that should be used as credential during authentication and this must be unique to a particular user.
Authentication	Users must be authenticated in order to have access that services or data that is offered. At every occasion or session there should be authentication to verify the claims and identity of users for access to be granted.
Security management Requirements	
Non- Repudiation	This would make sure that parties involved in the in the sending and receiving of content would not have a chance to deny it. The receiver cannot deny receiving the send data and the sender cannot deny sending the data.
Accountability	Every user that is granted access to any service must be accountable and there should be a record of activities that they performed during the period that they had access.
Authorisation	This must be implemented to ensure or approve the activities that users can perform with the data that the access. What action can a user perform and to what extent.

Table 1 shows the three major security requirements for wearables. It is always a challenge to satisfy these various security requirements in wearables due to the practicability, device usability, interoperability and efficiency of these of this device. In most cases, researchers would have to prioritise these security requirements because some

requirements are built around the others which give the reason why this research has been based on the authentication. The importance of authentication in any technology can never be overemphasised, and in this case, it is needed for a secure transmission of data from one device to another.

4.1. Communication Requirements for Wearable Technology

The communication that exist for the design of wearable could be divided in to three depending on the location of the communicating device, on-body communication this is communication between sensors or other supporting device on the body, near-body communication this is communication between intermediate device and the wearables, off-body communication is the communication between the intermediate device and a fixed network infrastructure. These categories are further illustrated in the picture below.

Figure 2. A basic communication architecture for mobile wearables

Short Range Wireless Technology

Short Range Wireless Technology has been the most successful in terms of growth in wireless technology because of its deployment, configuration convenience, low power consumption and peer to peer communication. SRWT have been applied in different areas such as WLAN, WPAN, WBAN and it still remains viable and can be explored further. It has been successful in applications like Machine-to-Machine communications [16], [17, 18], device to device [19, 20] and that influenced the choice of for NFC after reviewing other SRWT as could be seen below.

4.2. Bluetooth

Bluetooth is a wireless standard developed for Short-Range Wireless Technology (SRWT), Bluetooth is an IEEE open standard that uses Frequency Hopping Spread Spectrum Scheme (FHSS) in the transmission of data [21, 22]. Bluetooth is suitable for point-to-point communication devices and has sparked the introduction of other device and technology like Bluetooth headphones, Bluetooth speakers, Bluetooth mouse etc. [23].

4.3. Infrared (IrDA)

Infrared is a form of light that is not visible to the human eye, and it got its nomenclature from the fact that this light goes beyond the visible spectrum and it begins with the colour red (700nm) and the extension spans up to 1000000nm [19]. (IR) is a form of electromagnetic wave that could be found between the visible light and the Microwave with wavelengths between 750nm and 1mm and frequencies between THz and 300GHz [20]. The infrared just like the (Ultrasonic) X-ray is relatively safe because its light particles are harmful to organic breakdown [19, 20]. IR is used in the military for missile weapons due to peculiar characteristics like cost effectiveness, high recognition ability etc. [21].

4.4. Near Field Communication (NFC)

This technology was basically designed for secure payment transactions with its maximum range at about 20cm. Very importantly it enables a safe contactless two-way communication between supporting electronic devices, NFC devices could be said to operate within three operation principles, Peer to Peer where participating devices communicate within a physical proximity in other to exchange files and share information in a timely manner, Card Emulator, here participating devices communicate via common infrastructure while emulating smart cards. Then Tag Reader/ writer, the NFC enabled devices reads information stored on NFC tags that could be embedded within any device.

4.5. Radio Frequency Identification (RFID)

RFID uses radio waves for automatic identification using RFID Tags to store and retrieve information. The RFID consists of three parts, the reader, the tag and the data system. The RFID system could be passive or active depending on its functionalities. RFID is widely used for different applications ranging from supply chain management down to security [22].

4.6. Wi-Fi

Wi-Fi is a terminology that is used to categorize wireless networking devices that conform to the IEEE “802.11b” standard [22]. Wi-Fi Technology over the years since its emergence in the early 1980s has grown to become one of the prominent wireless LAN Standards Wi-Fi could be argued to be a universal, Wi-Fi operated on 2.4 GHz band which is an unlicensed spectrum [23]. Wi-Fi comes with

numerous advantages like ease of use, mobility, ubiquity, mobility, network management etc.[24] and it has got its disadvantages just like every other technology but with ongoing researches.

4.7. ZigBee

ZigBee is a wireless networking technology that was developed by ZigBee Alliance and this technology is meant for short-range applications that work for low-data rate [25]. ZigBee also known as 802.15.4 [26] operates within a personal space of 10m with maximal signal rate of 250 kb/s [27]ZigBee Technology can be used for a variety of applications because of its low price, low power consumption (60mW), Data rate of 250Kbps (2.4 GHz) with distance up to 100m [26, 28-30]. In the medical application, the low range-powered ZigBee can be used in the hospital for monitoring patients and could be used for machine to machine communication and IoT.

Table 2. Properties of Short Range Wireless Technology

Short Range Technology	Frequency	Range	Features	Possible Applications
Bluetooth	2.4 GHz	<10m but with Higher power up to 100m	Low power, Can transmit both voice and data signals	Identity management
Infrared (IrDA)	800 to 1000 µm	<1m	High Speed	Remote control, data transfer
NFC	13.56 MHz	<30cm	Security	Access Control, purchasing, ticketing
RFID	125 kHz, 13.56 MHz, 902 to 928 MHz	<1m	Security	Access control, Inventory, Tracking
Wi-Fi	2.4GHz and 5 GHz	<100m	High Speed, Ubiquity	Broadband,
ZigBee	2.4GHz	<10m[17]	Mesh Network	Patient monitoring, Home automation, Industrial control

5. Proposed Authentication Protocol

The limited communication characteristics of wearable devices have prompted the use of different short range wireless communication technology to transmit the data from level one (1) as shown in the diagram above down to level three (3) for onward processing and storage and this has left a major vulnerability at level (2) because there is an introduction of a broker device which could be a mobile phone or an app or any other supporting device. This broker device even as it serves its purpose of transmitting it could also be the weak point of the communication architecture. In the light of this challenge the proposed protocol presents a mutual authentication mechanism for wearables and their supporting devices.

Due to the characteristics and requirements of mobile wearable, the proposed protocol adopted the functions below to address the preceding challenges and to justify the requirements.

- A size compatible secure mutual authentication protocol that fits with the size requirement of mobile wearables.
- A secure mutual authentication protocol that is compatible with for Short-Range Wireless Technology (SRWT).
- A secure Device 2 Device mutual authentication protocol for participating wearable or supporting device.
- A reliable Inter-Device Imprinting mechanism to create trust amongst participating devices in other to identify the untrusted device.
- A reliable logical capability that classifies data based on their sensitivity to adopt a more suitable authentication measure.
- A secure imprinting mechanism that allows the wearable device to differentiate between trusted and untrusted intermediate devices.

5.1. The following assumptions were made

1. Due to the nature of the secure mutual authentication protocol, the wearable needs to have capabilities of performing cryptographic and logic operations and this is why this research proposed the use of a smart card technology into the wearable to enable these capabilities.
2. The wearable device should have storage capabilities because of the credentials that would be used for identification and authentication and this feature can be achieved using the smart card also.
3. The wearable needs to be embedded with Short-Range Wireless Technology (SRWT) capabilities for transmission and communication with supporting and participating devices and since with the smart card NFC is possible, these two technologies are what informed the unique design of this protocol.

5.2. Proposed Architecture

For most wearable devices to connect to the internet there is the need for a broker device to achieve this and giving the communication range limitation of wearables this device would have to be within the communication range of the wearable device. In other for this communication to be established securely the following steps below needs to be followed.

The broker device and the wearable device needs to establish a communication channel using the NFC protocol. As mentioned earlier this mechanism is built on existing standards and framework.

Due to the computation capabilities of the broker device, it takes up the responsibility of initiating communication between itself, the wearable device and the remote server.

When this communication channel has been established between the wearable and the remote server, the process of authentication begins.
The proposed authentication protocol is based on EAP that way we are able to define our own authentication mechanism.

For the wearable the EAP messages are encapsulated in PPP frames as has been illustrated in [40] the mapping of the PPP headers with the smart card commands, these commands are transmitted using the NFC transmission radio waves between the wearable device and the broker device following the ISO-14443-4 standard.
The broker device unencapsulates the received packets from the wearable device to the EAP level and this would be encapsulated and transmitted over the internet. This could be achieved both ways depending on the origin of the message either from the wearable or from the server. The remote server retrieves the authentication information that was encapsulated by the EAP.

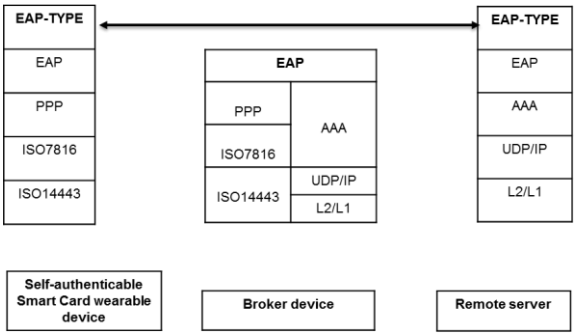

Figure 1. Proposed Authentication Architecture

6. Authentication Procedure

For the proposed authentication protocol, there are two different authentications that will take place. The first would be the authentication of the wearable with the broker device, the second would be the authentication of the broker device and the remote server. N.B due to the fact that these two methods are algorithm independent, the certificate used for the proposed protocol is based on the X509v3 standard where the size of the certificates would solely depend on the key length and the specific algorithm chosen. This case any smart card supported algorithm can be applied depending on the requirements of the application.

6.1. Authenticating the broker device with the wearable device

In authenticating the broker device with the wearable device, bearing in mind the technologies (self-authenticable smart card) included in the wearable as have been described earlier, the first step would involve the wearable device user to register with the broker device and this is achieved by Inter-device Imprinting as described by [43]. Below are the steps followed to achieve or establish a communication channel as illustrated in Figure 4.
1. A communication between the wearable and the broker device is established using NFC
2. A pairing request is sent from the wearable devices to the broker device if this has not been done before.
3. The broker device responds by sending some unique identifiable credential to the wearable device, this could be in the form of IMEI number or a MAC address SSAID etc.
4. The data received is stored in the smart card and it uses the obtained information to create a private and public key.
5. The digital signature and the public key certificate (PKC) are sent from the wearable device to the broker device.
6. Finally, the broker device verifies the signature received and the certificate is stored if the credential is correct. At this point, a confirmation message is sent to the wearable device.
NB. Stored data can be deleted by the wearable device user in an event that there is need to pair another device or a new device.

The illustration above in Figure 2 shows EAP method of authentication during further communication whenever the wearable device wants to communicate with the broker device.
1. To establish a communication channel between the wearable device and the broker device using PPP configuration messages through NFC.
2. An EAP authentication message is sent from the wearable device prompting for an authentication process.
3. A request message is then sent from broker device which includes a random encrypted number with the public key of the wearable device to the wearable device.
4. The wearable device decrypts the received message and sends an EAP response with the decrypted number to the broker device.
5. The broker device sends a confirmation if the received number is correct by cross checking with the stored number.
6. The process is repeated in the opposite direction. Process “3” is achieved using the IMEI number, MAC number or any unique identifiable number of the broker device.

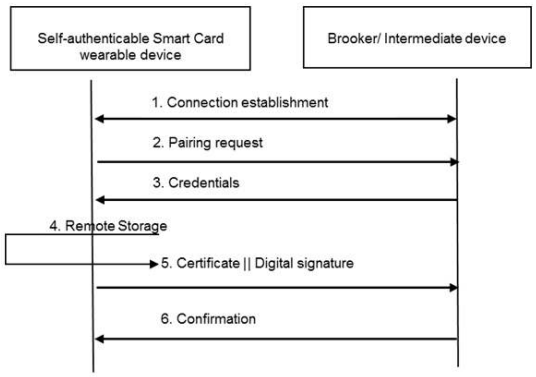

Figure 2. Paring between the wearable device and the broker device

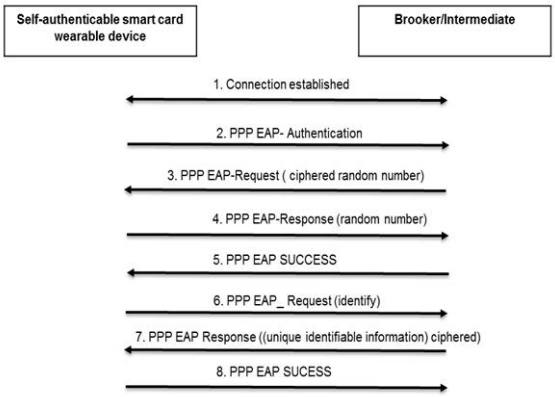

Figure 3. The authentication flow between the wearable device and the broker device

7. Mutual Authentication between the Wearable device and the remote server

For a successful mutual authentication between the wearable device and the remote server using the proposed protocol two assumptions were made.

- The first assumption is that the public key of the wearable device is known by the authentication server.
- The second assumption is that the public key of the remote server is also known by the wearable device

This mutual authentication would be based on a four-round double challenge response.

1. For a communication channel to be established between the wearable device and the broker device, just like other process it uses the PPP configuration message through NFC.

2.The wearable device sends and EAP authentication message to the broker device prompting the start of an authentication process.

3. The broker device sends an EAP request message to the wearable device enabling a start of an authentication process.

4. The wearable device sends an EAP response message with its certificate ID to the remote server, all these are sent through the broker device.

5. The broker device encapsulates the received message and sends it to the remote server.

6. A random number is generated by the remote server “rS” and this number us sent to the wearable device through the broker device.

7. The packet received by the broker device from the remote server is unencapsulated and forwarded to the wearable device.

8. In response, the wearable device generates a random number “rC “and encrypts the “rS” with a private key and in an EAP response encapsulates the digital signature and sends it to the wearable device through the broker device.

9. The broker device encapsulates the received message and sends it to the remote server.

10. To authenticate the wearable device the remote server checks the correctness of the digital signature received, if it is correct it authenticates the wearable device, in turn, it encrypts rC with its private key and in and EAP response encapsulates the digital signature and sends it to the wearable device through the broker device.

11. The EAP packet received from the remote server is encapsulated and sent to the wearable device.

12. To authenticate the remote server, the wearable device checks the digital signature for correctness and if correct it’s authenticated. A SUCCESS message is sent to the remote server in other to confirm the successful mutual authentication.

13.This message is encapsulated by the broker device and sent to the remote server.

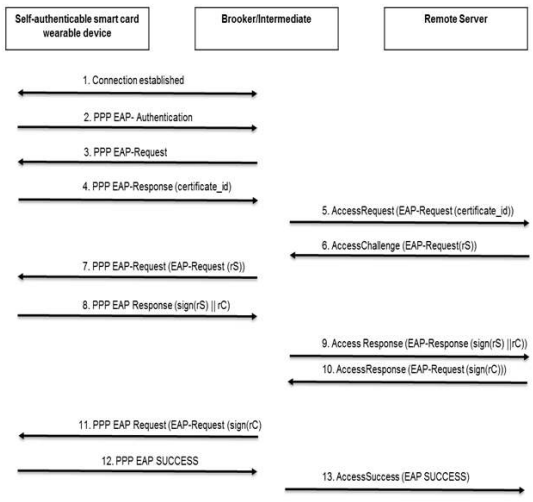

Figure 4. Authentication between the wearable device and the remote server

8. Security Justification

In the proposed authentication protocol as laid out above supports some major functions as would be review below.

I^2 Inter-device Imprinting which is the first functionality is set to establish trust amongst participating devices (the wearable device and the broker device), this process is carried out by the user of the wearable device and this protects the system from all short range communication attacks or threat. This process is only done once because the identifiable credential is stored and for further use.

The second functionality protects the system against spoof attacks and guarantees integrity of the communication. For the second functionality, the identity of the broker device is protected by the previously shared identifiable credential whereas the identity of the wearable device is protected by its private keys by proof of possession in relation to its digital certificate. This protocol enjoys the security properties of NFC communication and Smart card technology.

For the third functionality, the protection of the identities between the remote server and the wearable device lies on the proof of possession of the private key in relations to their digital certificate. These functionalities are possible because of the storage and computational abilities of the smart card as it satisfies the systems security requirements.

9. Conclusion

Wearables over the last few years have become the next big thing when it comes to technology, with medical and health fitness wearables taking the lead. Considering the sensitivity of data and the commercial value of the data transmitted or stored with a wearable device calls for a more secure and robust technology to protect the privacy of these wearable data.

The security of user's medical information or military intelligence must be private and can never be over emphasized and this research work presents a robust authentication protocol for wearable technology, this protocol could be used amongst participating devices within the communication grid. This protocol presents a low overhead cost since the communication would be with different participating devices and at a very high frequency due to the real-time nature of the generated data. This technology is based on a digital signature scheme while authenticating users using a challenge – response mechanism and this is flexible as provides different levels of protection for transmitted packets.

10. References

[1] Moustafa, H., et al., Mobile wearable communications [Guest Editorial]. IEEE Wireless Communications, 2015. 22(1): p. 10-11.

[2] Forecast, C.V., Cisco visual networking index: Global mobile data traffic forecast update 2009-2014. Cisco Public Information, February, 2010. 9.

[3] Sun, D.Z., et al., A new design of wearable token system for mobile device security. IEEE Transactions on Consumer Electronics, 2008. 54(4): p. 1784-1789.

[4] Berney, J.M., User-wearable functional jewelry with biometrics and smartcard to remotely sign and/or authenticate to e-services. 2003, Google Patents.

[5] Al-Muhtadi, J., et al. A flexible, privacy-preserving authentication framework for ubiquitous computing environments. in Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on. 2002.

[6] Nicholson, A.J., M.D. Corner, and B.D. Noble, Mobile Device Security Using Transient Authentication. IEEE Transactions on Mobile Computing, 2006. 5(11): p. 1489-1502.

[7] Khan, R., R. Hasan, and J. Xu. SEPIA: Secure-PIN-Authentication-as-a-Service for ATM Using Mobile and Wearable Devices. in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on. 2015.

[8] Ramli, S.N., et al. A biometric-based security for data authentication in Wireless Body Area Network (WBAN). in Advanced Communication Technology (ICACT), 2013 15th International Conference on. 2013.

[9] Challal, Y., H. Bettahar, and A. Bouabdallah, A taxonomy of multicast data origin authentication: Issues and solutions. IEEE Communications Surveys & Tutorials, 2004. 6(3): p. 34-57.

[10] Krawczyk, H., R. Canetti, and M. Bellare, HMAC: Keyed-hashing for message authentication. 1997.

[11] Ali, S.T., V. Sivaraman, and D. Ostry. Authentication of lossy data in body-sensor networks for healthcare monitoring. in Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on. 2012.

[12] Downnard, I., Public-key cryptography extensions into Kerberos. IEEE Potentials, 2002. 21(5): p. 30-34.

[13] Kâafar, M.A., et al. A Kerberos-based authentication architecture for Wireless Lans. in International Conference on Research in Networking. 2004. Springer.

[14] Neuman, B.C. and T. Ts'o, Kerberos: an authentication service for computer networks. IEEE Communications Magazine, 1994. 32(9): p. 33-38.

[15] Steiner, J.G., B.C. Neuman, and J.I. Schiller. Kerberos: An Authentication Service for Open Network Systems. in USENIX Winter. 1988.

[16] Dantu, R., G. Clothier, and A. Atri, EAP methods for wireless networks. Computer Standards & Interfaces, 2007. 29(3): p. 289-301.

[17] Wu, G., et al., M2M: From mobile to embedded internet. IEEE Communications Magazine, 2011. 49(4): p. 36-43.

[18] Emmerson, B., M2M: the Internet of 50 billion devices. WinWin Magazine, 2010(1): p. 19-22.

[19] Dohler, M., T. Watteyne, and J. Alonso-Zárate. Machine-to-machine: An emerging communication paradigm. in ICST Conference on Mobile Networks Management MONAMI. 2010.

[20] Pyattaev, A., et al. 3GPP LTE traffic offloading onto WiFi Direct. in Wireless Communications and Networking Conference Workshops (WCNCW), 2013 IEEE. 2013. IEEE.

[21] Pyattaev, A., et al. Proximity-based data offloading via network assisted device-to-device communications. in Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th. 2013. IEEE.

[22] Gurczik, G. and M. Behrisch. Modelling and simulating Bluetooth-based moving observers. in Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on. 2015. IEEE.

[23] Lee, J.-S., Y.-W. Su, and C.-C. Shen. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. in Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. 2007. IEEE.

[24] Liu, Y., S. Li, and L. Cao. Application of bluetooth communication in digital photo frame. in 2009 ISECS International Colloquium on Computing, Communication, Control, and Management. 2009. IEEE.

[25] Van Kempen, T., Infrared technology in animal production. World's Poultry Science Journal, 2001. 57(01): p. 29-48.

[26] Al-Zu'bi, M.M., M.A. Khodeir, and M.F. Al-Mistarihi. Modeling and design of an infrared-based identification (IRID) system-tag and reader design. in Information and Communication Systems (ICICS), 2014 5th International Conference on. 2014.

[27] Zhao, G., et al. A study on NSCT based super-resolution reconstruction for infrared image. in TENCON 2013 - 2013 IEEE Region 10 Conference (31194). 2013.

[28] Wang, W. Study on Several Promising Short-Range Wireless Communication Technologies. in Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on. 2008.

[29] Al-Alawi, A.I., WiFi technology: Future market challenges and opportunities. Journal of computer Science, 2006. 2(1): p. 13-18.

[30] Lehr, W. and L.W. McKnight, Wireless internet access: 3G vs. WiFi? Telecommunications Policy, 2003. 27(5): p. 351-370.

[31] Henry, P. and L. Hui, WiFi: what's next? Communications Magazine, IEEE, 2002. 40(12): p. 66-72.

[32] Gomez, C. and J. Paradells, Wireless home automation networks: A survey of architectures and technologies. Communications Magazine, IEEE, 2010. 48(6): p. 92-101.

[33] Baronti, P., et al., Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. Computer communications, 2007. 30(7): p. 1655-1695.

[34] Jin-Shyan, L., S. Yu-Wei, and S. Chung-Chou. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. in Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. 2007.

[35] Lee, J.D., et al. Development of Zigbee based Street Light Control System. in Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES. 2006.

[36] Jong-Won, K., et al. Design of Air Pollution Monitoring System Using ZigBee Networks for Ubiquitous-City. in Convergence Information Technology, 2007. International Conference on. 2007.

[37] Sangeetha, C.P. and C.D. Suriyakala. Performance analysis of IEEE 802.15.4/ZigBee sensor networks using ADAPT algorithm. in Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on. 2014.

[38] Choi, H.S., B. Lee, and S. Yoon, Biometric Authentication Using Noisy Electrocardiograms Acquired by Mobile Sensors. IEEE Access, 2016. 4: p. 1266-1273.

[39] Free, C., et al., The effectiveness of mobile-health technology-based health behaviour change or disease management interventions for health care consumers: a systematic review. PLoS med, 2013. 10(1): p. e1001362.

[40] Torres, J., A. Izquierdo, and J.M. Sierra, Advances in network smart cards authentication. Computer Networks, 2007. 51(9): p. 2249-2261.

[41] Metz, C., A pointed look at the point-to-point protocol. IEEE Internet Computing, 1999. 3(4): p. 85-88.

[42] Fan, C.I., Y.H. Lin, and R.H. Hsu, Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs. IEEE Transactions on Parallel and Distributed Systems, 2013. 24(4): p. 672-680.

[43] Yokoyama, T., K. Iida, and S. Yamaguchi. An architecture of network imprinting for personal but wide area applications. in 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers). 2005. IEEE.

[44] Denning, D.E. and P.F. MacDoran, Location-based authentication: Grounding cyberspace for better security. Computer Fraud & Security, 1996. 1996(2): p. 12-16.

[45] Zhang, F., A. Kondoro, and S. Muftic. Location-Based Authentication and Authorization Using Smart Phones. in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012.

[46] Jansen, W. and V. Korolev. A location-based mechanism for mobile device security. in Computer Science and Information Engineering, 2009 WRI World Congress on. 2009. IEEE.

[47] Bao, L. Location authentication methods for wireless network access control. in 2008 IEEE International Performance, Computing and Communications Conference. 2008. IEEE.

[48] Takamizawa, H. and K. Kaijiri. A web authentication system using location information from mobile telephones. in Proceedings of the IASTED International Conference Web-based Education (WBE 2009). 2009.

