2017

A Novel Method for Bluetooth Pairing Using Steganography

Albahar Marwan Ali

Union of Scientists in Bulgaria

A NOVEL METHOD FOR BLUETOOTH PAIRING USING STEGANOGRAPHY

Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen

University of Eastern Finland, School of Computing, Kuopio Campus,
P.O. Box 1627, FI-70211 Kuopio,
E-mails: Marwana@uef.fi, Olayemo@student.uef.fi, Keijo.Haataja@uef.fi,
Pekka.Toivanen@uef.fi
Finland

Abstract: There are two solutions in data security field for ensuring that only legitimate recipients will have access to the intended data: Steganography and cryptography. These solutions can be used for providing a high level of security. With the exponential growth of challenges in the field of computer security, the use of Bluetooth technology is expanding rapidly to expose many of these challenges on the surface. One of these challenges is the MITM attack during Bluetooth pairing process. In this paper, we will steer the wheel to concoct a novel method based on Steganography to fortify the pairing process and thwart MITM attacks. In the light of this study, a thorough experiment will be conducted based on the proposed method. Moreover, we will provide results of the experiment in order to show the applicability of our novel method. Furthermore, we will sketch some new ideas that will be used in our future research work.

Keywords: Bluetooth pairing process, Decryption, Encryption, MITM attack, SSP, Steganography.

1. INTRODUCTION

Bluetooth [1] is a Wireless Personal Area Network (WPAN) technology, which is capable of transferring data and real-time two-way audio/video providing data rates up to 24 Mb/s. It also allows several devices to be connected to each other without a wired link, using radio waves as a transmission medium at 2.4 GHz frequency band in the free Scientific, Industrial, and Medical (ISM) band and can utilize two different frequency hopping methods: AFH (Adaptive Frequency Hopping) or FHSS (Frequency-Hopping Spread Spectrum) in order to avoid "bad" channels that suffer from interference. Nowadays, AFH is supported in all Bluetooth devices, since it was already released with Bluetooth 1.2 version in November 2003. [1–3]

Different kinds of Bluetooth devices are widely used globally. In fact, already in 2006, the one-billionth Bluetooth device was shipped [4]. Six years later in 2012, the annual Bluetooth product shipments exceed 2 billion and it is expected almost 4 billion Bluetooth product shipments in 2016 alone, thus having 20 billionth Bluetooth device shipped by the end of 2016[4]. Thus, it is extremely crucial to keep all Bluetooth security issues up-to-date. [1–4]

Our results: In this paper, we propose a novel method, which will strengthen the Bluetooth pairing process by employing Steganography in which secret messages and key are hidden in a cover object. Only the key will be sent to the receiver at the first phase and the receiver will reply back to the sender with his key. After both the sender and the receiver sent stego image, which has the key embedded, a shared key will be generated, which is in fact half of the sender's key and half of the receiver's key. In the second stage, the shared key will be verified by both sides. A message will be created at the final stage and integrated into stego image. Indeed, the stego image will be extracted by using the shared key in order to view the message and exchange it to check the originality of the hidden message. Before we inculcate this method in Bluetooth community, there is a need to confirm the confidentiality and integrity. For this reason, we will demonstrate our novel method with experimental figures to ensure its validity. Our results show the feasibility of incorporating Steganography into pairing process to avert any risk of intrusion. Moreover, our method is a viable solution for securing the entire connection. Thus, our method is didactically aiming at drawing a robust pairing model, which can counteract MITM attacks. Furthermore, we will sketch some future research work ideas.

The rest of the paper is organized as follows. Section 2 provides an overview of vulnerability of Bluetooth security mechanism and explains the basics of Steganography. Our novel method is proposed along with experimental results in Section 3. Finally, Section 4 concludes the paper and sketches some future research work ideas.

2. RELATED WORKS

In [12] a new solution is presented, which indeed changes the structure of SSP in which a separate channel is utilized to authenticate the entire connection. The authors, in fact, studied the profound issues with the traditional pairing process (SSP) and proposed some radical changes, which aimed at thwarting MITM attacks. Furthermore, the authors showed a practical experiment in order to confirm the viability as well the applicability of the proposed idea. Finally, their results show an improvement of connection times and prevention of various elements, which empower MITM attacks. [12]

In [13] the authors attempted to add more protection in order to seal the connection by using the traditional pairing process (SSP). An effective countermeasure was proposed along with experimental results by the authors. Indeed, the authors focused on the JW model due to the fact that it is not providing

any protection against MITM attacks. In the proposed method, user intervention was required to complete the pairing process by inquiring about I/O capabilities and then a computational process will follow to fortify the connection. As a conclusion of the paper, the authors stated that the improved JW provided exemplary performance at addressing MITM attacks. [13]

In [14], the authors examined how texts and images can be hidden in mobile phone through Bluetooth. In the paper, the authors proposed a unique steganographic technique that produces a stego image, which looks exactly like the original image in the mobile phone via Bluetooth. The technique is based on the permutation of the XOR operation on secret message and the result is embedded into the Least Significant Bits (LSBs) of the cover image. The authors confirm that this technique provides a high level of security. [14]

In [15], the authors proposed a method in which Steganography is carried out in network protocols using PRNGs (Pseudo-Random Number Generators). The authors of this paper claim that this technique helps to minimize the attacks and information recovery by intruders. The method presents novel steps, which involve encryption of the secret message, Steganographically embedded it into a video, and then compressed it, all to enhance the security of the messages before embedding again into the network packet headers, which can then be extracted at the recipient's side. The authors finally stated that this method is efficient and achieved its goal of ensuring minimum recovery by intruders and thereby countering attacks. [15]

3. VULNERABILITY OF BLUETOOTH SECURITY MECHANISM AND BASICS OF STEGANOGRAPHY

The security of Bluetooth, in fact, is relied on forming a chain of events in which meaningful information will not be supplied to an eavesdropper. Moreover, a particular sequence must govern all events in order to set up the security correctly. A procedure called pairing must be executed when two Bluetooth devices begin communication. As an outcome of this process, two devices form a trusted pair and establish a link key, which is used next for creating a data encryption key for each session. [1–3]

In Bluetooth versions up to 2.0+EDR, a PIN-based (Personal Identification Number) pairing is applied. In fact, this is a personal code that is shared between the two devices to generate different 128-bit keys. When both devices have the same passkey, this will allow devices to create the same shared key to authenticate and encrypt data that is being exchanged between them. Indeed, as PINs are usually comprised of only four decimal digits, the strength of the resulting keys is insufficient to provide protection against passive eavesdropping on communication. In Bluetooth versions up to 2.0+EDR, it has been shown that Man-In-The-Middle (MITM) attacks are feasible on Bluetooth communications [1–3, 5–7].

A new specification added for the pairing procedure called SSP (Secure Simple Pairing) in Bluetooth versions 2.1+EDR and later in which the primary purpose is to

enhance the security of pairing process by attaching shield of protection against MITM attacks as well as passive eavesdropping. Alternatively, SSP applies Elliptic Curve Diffie-Hellman (ECDH) public-key cryptography. For creating the link key, devices utilize public-private key pairs, Bluetooth addresses, and nonces. To fortify the entire pairing process against MITM attacks, SSP requests users to compare two 6-digit numbers or utilizes Out-Of-Band (OOB) channel. SSP uses four distinct association models: Just Works (JW), Passkey Entry (PE), Numeric Comparison (NC), and Out-Of-Band (OOB). However, all these association models are vulnerable to MITM attacks. As it has been shown in [7,10–11,20], several attacks have been reported against Bluetooth pairing process, which opens a debate about the effectiveness of SSP [1–3].

It is obvious that the security of Bluetooth pairing process is not adequately addressed by this current cryptographic method, as previous researches have proven that it is possible for attackers to intercept these messages during key exchange and later retransmit the messages, by sending his own public key to replace the requested one. We believe that introducing steganography into the pairing process during data transfer will be robust against MITM attacks. The use of cryptographic key exchange method during data transmission in Bluetooth network is to enhance the pairing process, a method which is still prone to MITM attacks; however, steganography hide the existence of this process by embedding the keys inside a cover image before transmission to the recipient. The whole key exchange process is unknown to the attacker, because the attacker in this case will not even realise the images contain hidden data, only the recipient will be aware of the content. This is a major uniqueness of our technique.

Steganography is the practice in which secret messages are hidden inside a different digital content, such as image, data file, or audio, which is called the cover object. The process of concealing this secret message into the cover image is carried out before the transmission process and the embedded secret message is extracted by the receiver [14–19].

The basic concept of steganography is to ensure that secret messages are securely transmitted without any doubts. It differs from cryptography, because in cryptography, the secret message is encrypted, making it unreadable, but steganography ensures that the secret message is hidden completely. Figure 1 illustrates the basic concept of steganography, which consists of two basic processes:

1) *Embedding process:* It is carried out by the sender. During the embedding process, there is a secret message, which the sender intends to transmit securely. There is also a cover image into which the secret message will be embedded and there is also a stego key, which enables that only the receiver who has the corresponding decoding key can extract the secret message.
2) *Extraction process:* It is carried out by the receiver. The image generated after the embedding process, called stego image, carries out the secret message. During the extraction process at the destination, the stego image and the corresponding stego key is used to extract the secret message.

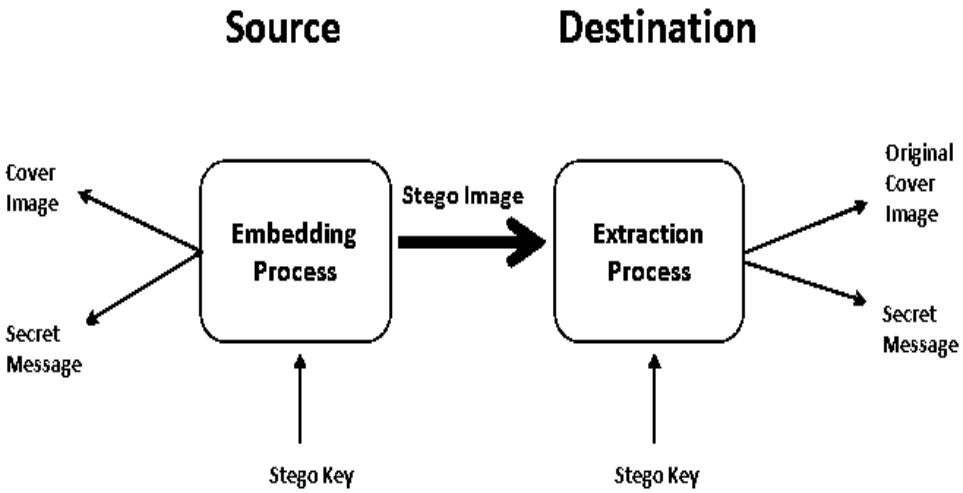


Figure 1. Basic concept of steganography

Steganography can be implemented using numerous techniques. Some common techniques include transform domain technique and the spatial domain technique. In transform domain technique, the secret message is embedded into the coefficients of the image transform used, while in spatial domain technique, the least significant bits (LSBs) of the cover image is replaced by that of the secret bits.[14–18]

As numerous researchers have found out, the current structure of SSP is utterly prosaic against MITM attacks and there is an increasing susceptibility to MITM attacks. For example, one possible attack described in [21] in which legitimate devices will receive false I/O (Input/ Output) capabilities information about each other, inexorably leads to exposing and manipulating users' data. MITM attacks have drawn considerable attention in the last few years. In fact, in this attack, the intruder intercepts the connection between the correspondents. Then, the intruder copies the devices' BD_ADDR (Bluetooth Device Address) values and begins the impersonation process by sending messages to both legitimate devices. The actual attack begins in the first step of SSP by fabricating the exchange of I/O capabilities of each device. Unfortunately, in the traditional pairing (SSP), the device with no necessary hardware to perform a secure association model allows for pairing by using the least secure associate model, which is the JW that does not provide any MITM protection. The attacker will falsify the I/O capabilities of each device once the connection establishes between the legitimate devices. Therefore, the both devices will be forced to use the JW model, which practically leads to a situation in which the attacker can continue his attack without any hassle, because the JW model lacks the adequate scale of complexity. [21]

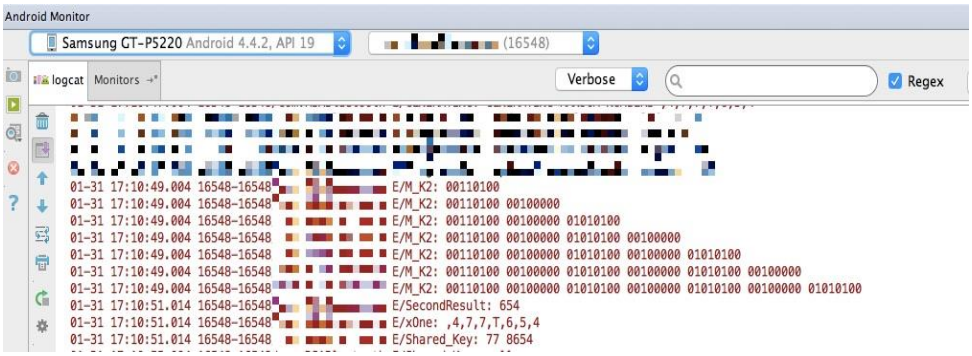
4. OUR NOVEL METHOD

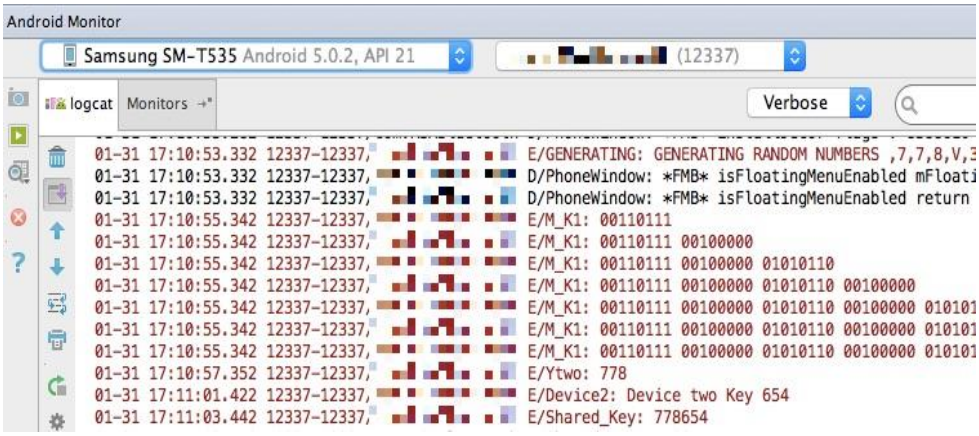
This section presents a comprehensive explanation of our novel method by beginning with an overview of the proposed method and after that distinct phases of the proposed method will be exhibited. Finally, the result of the experiment will be provided.

As the nature of MITM attack, the theory of the attack can seem recondite, thus a persistence of MITM attacks in the Bluetooth pairing brings some damages undoubtedly accrue to the users. For this matter, we conducted this study to ameliorate the security of Bluetooth pairing and thwart the MITM attack by combining steganography. As most of the studies have confirmed, there are two main reasons for MITM attacks to take place during the pairing process. First, lack of the minimum demanded scale of security. Second, lack of mutual verification. Consequently, the gist of our attempt in this study is to design a process, which provides a buffer against the threat of MITM attack and constructs a mutual trust between the devices by including necessary security measures to shield the pairing process. For simulating the process, we used Android Studio with SDK version 23 and tools version 23.0.2.

The method is dedicated for guaranteeing a secure pairing by running through three distinct phases, which will be explained in their occurrence order:

1) In this phase (see Figure 2), a key will be generated and embedded into an image. Then, this key will be sent from the requester to the responder. In the responder side, once the responder receives the image, he will generate his key and send it to the requester. In fact, this process does not require any user interaction.
2) This phase (see Figure 3) is designed to extract the key from the image. Then, another key will be generated based on the requester's key and responder's key. The new key called "Shared_Key" will be utilized in the next phase. To add more strength to this phase, before "Shared_Key" is generated, there will be a verification process of the key. In other words, after the requester obtains the responder key, a request will be sent for checking the key and its originality. All verification processes are assumed to happen internally without any kind of user interaction.





3) This phase (see Figure 4) is the final phase before the successful connection establishment. A message will be embedded into the image. In order to obtain this message, the "Shared_Key" is required as a "Password" to complete the process successfully. As we guarantee a robust vetting process, there will be two requests. First, request to verify the "Shared_Key" between the two devices. Second request is related to the verification of message originality. Noteworthy, the technique used to check the originality of the message is implemented as it shows in the pseudocode below. All verification processes are assumed to happen internally without any kind of user interaction.

```
Requester Message = 0

Responder Message =0

First request {

Embedded the the Requester key into the message

Then

Reference created = 3442  ------ assign to the Requester Message =3442

Embedded the the Responder key into the message

Then

Reference created = 6678------ assign to the Responder Message =6678

}

End
```

Bluetooth communication is steadily expanding in popularity due to the ease of the process of exchanging data between devices. As the usage of Bluetooth grows, the security perils of Bluetooth technology are likely to spawn rapidly. One of the

perils is the pairing process. Since SSP has shown its vulnerability to MITM attacks, the Bluetooth SIG/SEG and several academic researchers have granted significant attention and they are striving to contrive a method that can be an optimal solution. We as academic researchers have analyzed and studied this attack. In this paper, we proposed a new pairing structure that is employing steganography and we feel that it could very well be the optimal solution for securing Bluetooth communications. Based on our results, we can conclude that our method shows high effectiveness at preventing MITM attacks. In addition, it disentangles all factors, which contribute to making the MITM attack feasible. From the verification perspective, our method ensures that all data exchanged will be verified accurately and thus it will result in achieving hassle-free pairing process.

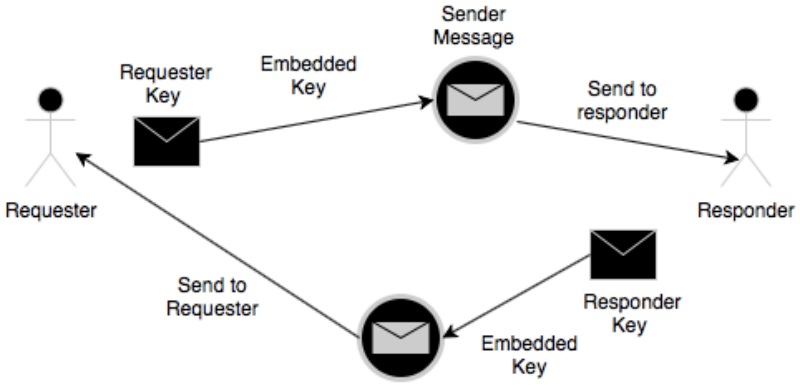


Figure 2. (a). Scheme of first phase of our novel method

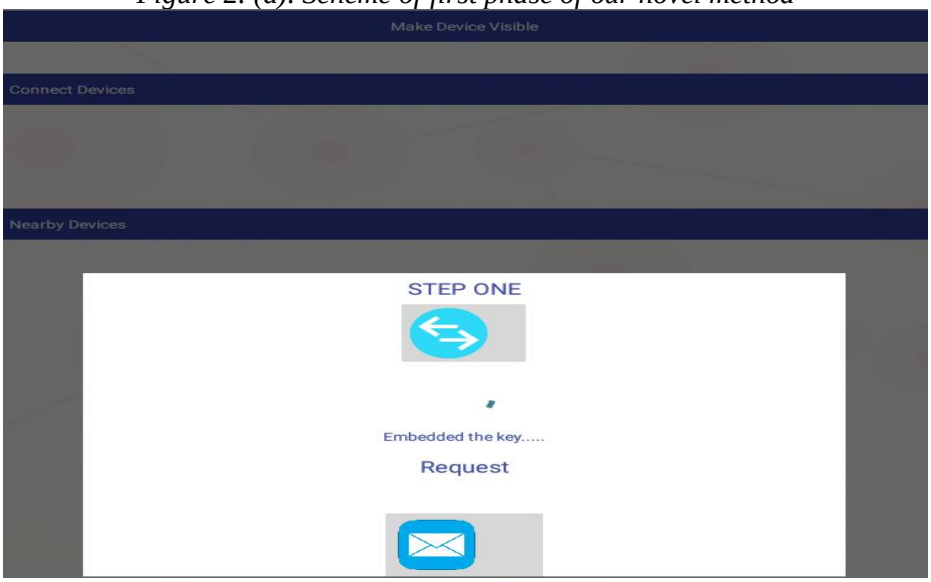


Figure 2. (b). First phase of our novel method

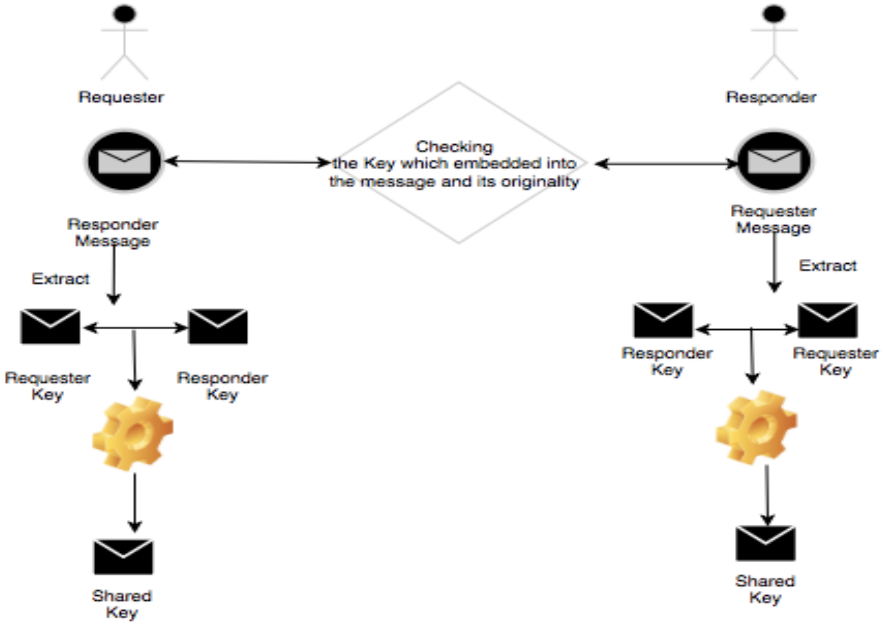


Figure 3. (a). Scheme of second phase of our novel method

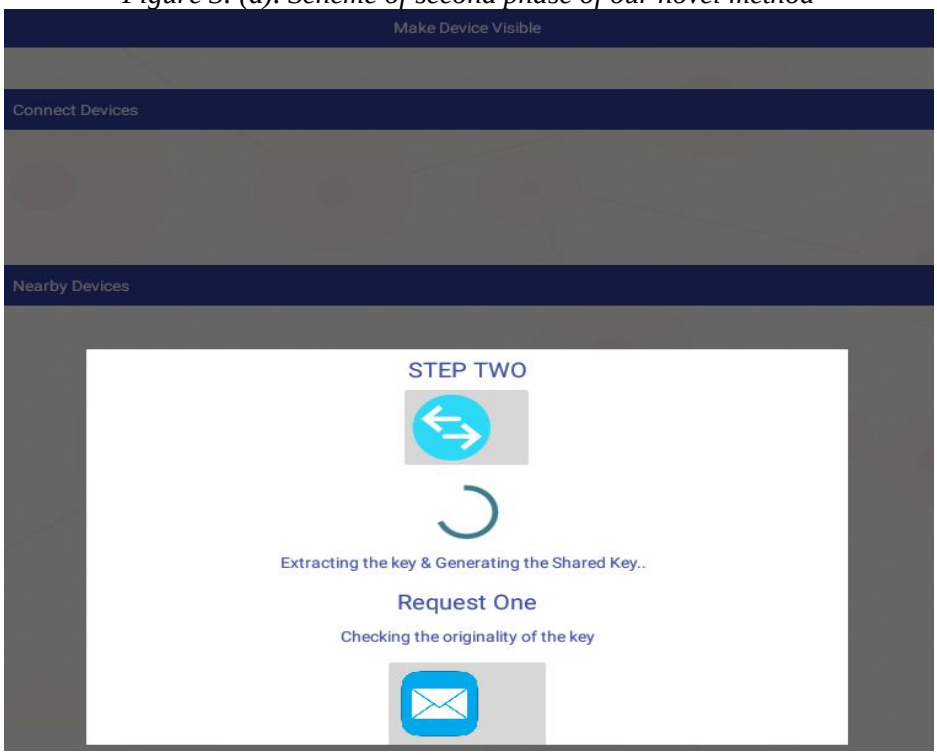


Figure 3. (b). Second phase of our novel method

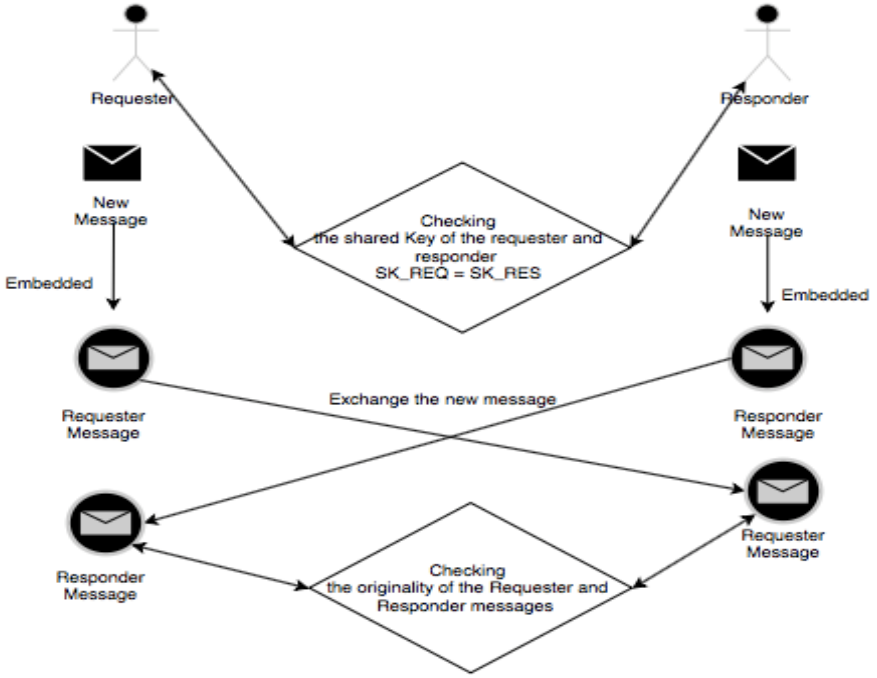


Figure 4. (a). Scheme of final phase of our novel method

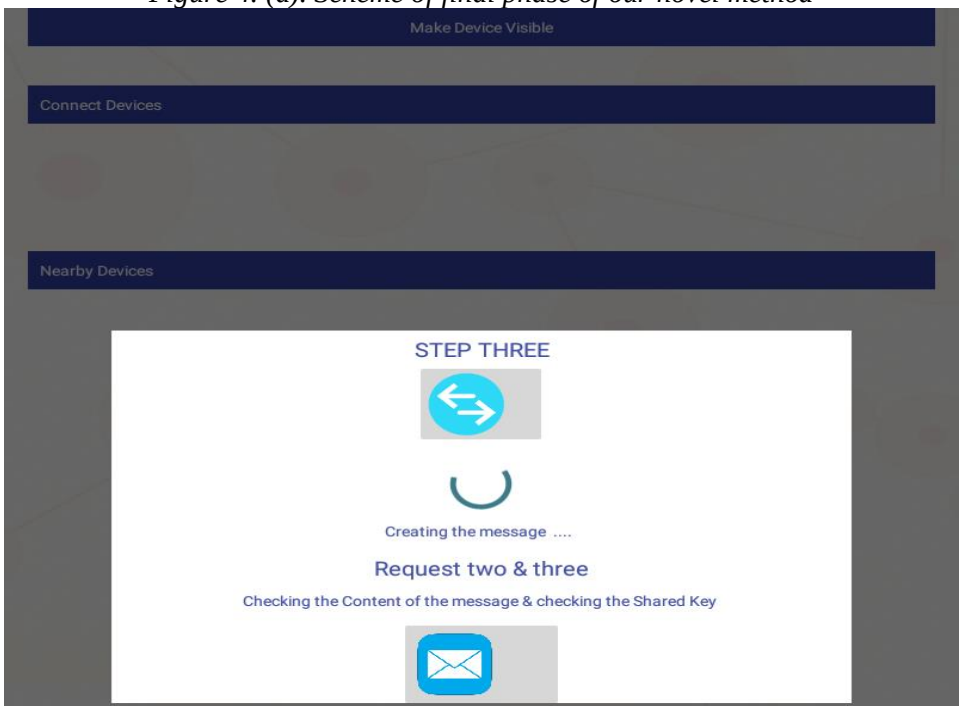


Figure 4. (b). Final phase of our novel method

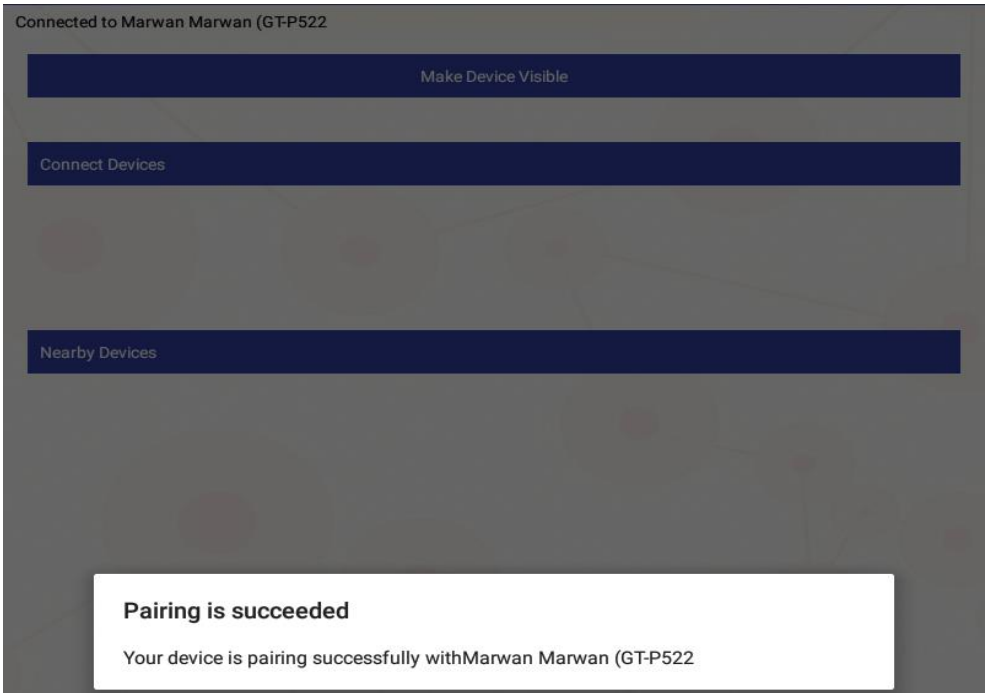


Figure 5. The result of our novel method

5. CONCLUSION AND FUTURE WORK

Our study in this paper clearly shows that most of the countermeasures, which derived from previous studies destined to prevent the threat of MITM attacks during Bluetooth pairing, are somewhat ineffective. In fact, the reason behind that is related to the current structure of SSP. In this paper, we revise the current standard of pairing process and formulate a novel pairing structure based on steganography.

In our novel method, a key and secret message were successfully embedded into an image, whereas a shared key will be generated to extract the secret message from the image. In this way, the pairing process will prevent any interception, because this technique utilizes the information of both the sender and receiver as well as steganography method. Our experimental results clearly show that our method is very efficient and satisfies the requirements for security and robustness for secured pairing process.

To extend our research in the field of computer security, we have some fresh ideas that we will use in our future research work. First, we will propose a hybrid algorithm, which will merge three algorithms in order to present a robust security of data transmission in Bluetooth communication. This hybrid algorithm will be based on RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and TwoFish. In addition, an empirical model will be proposed in order to estimate the risk levels connected with MITM attacks. Positively, this contribution will provide

an extra security layer to achieve a risk-free pairing. By adopting these promising future work ideas, we believe that they will supply remarkable protection against MITM attacks to guarantee a significant level of security for Bluetooth communications.

REFERENCES

[1] Bluetooth SIG, Bluetooth Specifications 1.0A–4.2.[Online]. Available: https://www.bluetooth.com/specifications. [Accessed November 29, 2016].

[2] Haataja K., Security Threats and Countermeasures in Bluetooth-Enabled Systems. Doctoral Dissertation, University of Eastern Finland, 2009.

[3] Haataja, K., K. Hyppönen, S. Pasanen, P. Toivanen, Bluetooth Security Attacks: Comparative Analysis, Attacks, and Countermeasures. SpringerBriefs Book, Springer Verlag, 2013.

[4] Bluetooth SIG, Bluetooth – Our History. [Online]. Available: https://www.bluetooth.com/media/our-history.[Accessed November 29, 2016].

[5] Jakobsson M. and Wetzel S., Security Weaknesses in Bluetooth, *Lecture Notes in Computer Science*, Springer-Verlag, *(*vol.2020*)*, 2001, pp. 176–191.

[6] Kügler D., Man-In-The-Middle Attacks on Bluetooth, *Lecture Notes in Computer Science*, Springer-Verlag, *(*vol.2742*)*, 2003, pp. 149–161.

[7] Levi A., Cetintas E., Aydos M., Koc C., and Caglayan M., Relay Attacks on Bluetooth Authentication and Solutions, *Lecture Notes in Computer Science*, Springer-Verlag, *(*vol.3280*)*, 2004, pp. 278–288.

[8] Suomalainen J., Valkonen J., and Asokan N., Security Associations in Personal Networks – A Comparative Analysis, *Lecture Notes in Computer Science*, Springer-Verlag, (vol.4572*)*, 2007, pp. 43–57.

[9] Hyppönen K. and Haataja K., Niño Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing, *IEEE Third International Conference in Central Asia on Internet, The Next Generation of Mobile, Wireless and Optical Communications Networks*, Tashkent, Uzbekistan, September 26–28, 2007.

[10] Haataja K. and Hyppönen K., Man-In-The-Middle Attacks on Bluetooth – a Comparative Analysis, a Novel Attack, and Countermeasures, *IEEE Third International Symposium on Communications, Control and Signal Processing*, St. Julians, Malta, March 12–14, 2008.

[11] Haataja K. and Toivanen P., Practical Man-In-The-Middle Attacks Against Bluetooth Secure Simple Pairing, *4th IEEE International Conference on Wireless Communications, Networking, and Mobile Computing*, Dalian, China, October 12–14, 2008.

[12] Albahar M., Haataja K., and Toivanen P., Virtual Channel Based Pairing: A New Novel Solution Structure for Bluetooth Pairing, *International Journal on Information Technologies & Security, 4* (vol.8), 2016, pp.51–65.

[13] Albahar M., Haataja K., and Toivanen P., Towards Enhancing Just Works Model in Bluetooth Pairing, *International Journal on Information Technologies & Security, 4* (vol.8), 2016, pp.67–82.

[14] Baker S. and Nori A., Steganography in Mobile Phone over Bluetooth, *International Journal of Information Technology and Business Management (JITBM), 1*(vol.16), 2013, pp.111–117.

[15] Sekhar A., Kumar M., and Rahiman M., A Novel Approach for Hiding Data in Videos Using Network Steganography Methods, Procedia *Computer Science*, (vol.70), 2015, pp. 764–768.

[16] Artz D., Digital Steganography: Hiding Data Within Data, IEEE *Internet Computing*, 3 (vol.5), 2001, pp.75–80.

[17] Joseph A. and Sundaram V., Cryptography and Steganography: A Survey, *International Journal of Computer Technology and Applications (IJCTA),* 3 (vol.2), 2001, pp. 626–630.

[18] Saraireh S., A Secure Data Communication System Using Cryptography and Steganography, *International Journal of Computer Networks & Communications*, 3 (vol.5), 2013.

[19] Mahajan M.T. and Kurhade M.B., Enhance Two-Tier Secure Model of Modern Image Steganography, *International Journal of Computer Science and Mobile Computing*, 5 (vol.3), 2014, pp. 804–806.

[20] Barnickel J., Wang J., and Meyer U., Implementing an Attack on Bluetooth 2.1+ Secure Simple Pairing in Passkey Entry Mode, *IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom'2012),* 2012, pp. 17–24.

[21] Albahar M., Haataja K., and Toivanen P., Bluetooth MITM Vulnerabilities: A Literature Review, Novel Attack Scenarios, Novel Countermeasures, and Lessons Learned, *International Journal on Information Technologies & Security, 4* (vol.8), 2016, pp.25–49.

Information about the authors:

Marwan Albahar: Mr. Albahar received his B.Sc. Degree in computer science from King Faisal University in 2011 and his M.Sc. Degree in computer science from Frostburg State University USA with honor in 2015. Currently, Mr. Albahar is a Ph.D. student at the University of Eastern Finland (UEF). His main areas of research include Computer Networks, Computer Security, Data Mining, Software Quality and Testing, Databases, and Software Engineering.

Olayemi Olawumi: Mr. Olayemi Olawumi is currently a Ph.D. student in the School of Computing at University of Eastern Finland (UEF).He received his M.Sc. Degree in Computer Science in 2012 at UEF. His primary research interests include Computer Networks, Computer Security, Wireless Security, Smart Homes, and Computational Intelligence.

Keijo Haataja: Dr. Keijo Haataja received his Ph.Lic. Degree in 2007 and his Ph.D. Degree in 2009 in Computer Science at the University of Eastern Finland (UEF). His primary research interests include Wireless Communications, Wireless Security, Mobile Systems, Sensor Networks, Data Communications, Computational Intelligence, Intelligent Autonomous Robots, Virtual Reality, and Healthcare IT Systems.

Pekka Toivanen: Prof. Pekka Toivanen received his M.Sc. (Tech.) Degree at Helsinki University of Technology in 1989 and D.Sc. (Tech.) Degree in 1996 at Lappeenranta University of Technology. He has been a full professor in computational intelligence at UEF since 2007. His areas of interest are Computational Intelligence, Image Processing, Machine Vision, and Lossless Compression of Hyperspectral Images.

Manuscript received on 29 November 2016