Adaptive Bluetooth Network for Secure Data Transfer

Swapnil Mishra
SENSE Department, Vellore Institute of Technology University, India

Siraj M.Tamboli
SENSE Department, Vellore Institute of Technology University, India

Abstract – Our nowadays's international is turning into digital and cell. Exploiting the blessings of wireless verbal exchange protocols isn't handiest for telecommunication purposes, but additionally for payments, interaction with wise automobiles, etc. One of the most full-size wi-fi skills is the Bluetooth protocol. Just in 2010, 906 million cellular Bluetooth enabled telephones were bought, and in 2011, there had been greater than 40 million Bluetooth enabled fitness and clinical devices available on the market. Still in 2011, one 0.33 of all new cars produced international protected Bluetooth generation. Security and privacy protection is key inside the virtual international of these days. There are protection and privacy dangers including device monitoring, communique eavesdropping, etc., which may come from flawed Bluetooth implementation with very extreme consequences for the customers. The objective of this paper is to investigate using Bluetooth in m-trade and m-fee fields. The steps undertaken on this paper a good way to come to an offer for a comfortable architecture are the analysis of the nation of the art of the relevant specifications, the existing dangers and the regarded vulnerabilities the related recognized assaults. Therefore, we give first an overview of the general traits of Bluetooth technology these days, going deeper in the evaluation of Bluetooth stack's layers and the safety capabilities presented by using the specifications. After this evaluation of the specs, we examine how acknowledged vulnerabilities were exploited with a comprehensive list of known assaults, which poses extreme threats for the users. With a majority of these elements as background, we finish the paper featuring a design for Secure Architecture for Bluetooth-Enhanced Mobile "Smart" Commerce Environments.

Index Terms – Bluetooth; Mobile Security; Mobile Commerce; Privacy.

1. INTRODUCTION

The Bluetooth wireless is a quick-range communication system (see Table 1) meant to update the cable(s) connecting transportable and/or constant electronic de-vices. The key capabilities of Bluetooth wi-fi era are robustness, low price and device discovery guide. Many functions of the core specification are elective, al-lowing product differentiation.

Created by using telecom vendor Ericsson in 1994, it was originally conceived as a wireless opportunity to RS-232 information cables. In 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed a change association referred to as Bluetooth SIG (Special Interest Group) to put up and sell the Bluetooth well known. From the primary Bluetooth enabled device in 1999 to 2008, extra than 2 billion gadgets were using the Bluetooth era (consistent with a press launch from Bluetooth SIG dated May 2008).

Table 1. Classes of Bluetooth.

Class	Power (mW)	Power (dbM)	Distance (m)	Sample Devices
1	100	20	~100	BT Access Points
2	2.5	4	~10	Keyboard, mouse
3	1	0	~1	Mobile phone

It is therefore clean the excessive degree of pervasiveness and ubiquity of this technology, which justify the want of a deep analysis associated with the State of The Art of its security and privateness functions as well as possible threats and vulnerabilities. Still according to Bluetooth SIG, listed below there are numbers of Bluetooth products worldwide that deliver a clearer photograph of the measurement of this generation:

- 906 million mobile phones offered in 2010, nearly one hundred percentage with Bluetooth generation.
- 171 million laptops shipped in 2010, including 77 percentage with Bluetooth generation.
- More than 50 million game consoles shipped in 2010, together with sixty two percent with Bluetooth era.

- More than 40 million Bluetooth enabled health and clinical gadgets have been already inside the market in early 2011.
- One third of all new vehicles produced international in 2011 encompass Bluetooth technology, growing to 70 percent through 2016, according to Strategy Analytics.

Having said that, it's miles straight away clean the excessive level of pervasiveness and ubiquity of Bluetooth generation, which justify the need of a deep evaluation associated with the State of The Art of its security and private functions as well as feasible threats and vulnerabilities.

2. CURRENT PROBLEM

When connection is made between the Bluetooth devices, an interloper device can be there in one of a kind ways. An intruder can act because the fake device inside the distinct roles. The faux tool can behave as fake slave or fake grasp. Similarly the intruder may be a lively (converting the contents of the information) intruder or passive one (definitely coping the records and sending the identical facts to the some other cease).

It can preserve the connections to the each communicating (unique) tool the only quit (every other cease is considering the intruder as the real one communicating device). Messages despatched with the aid of device A and tool B are shown in figure 1.

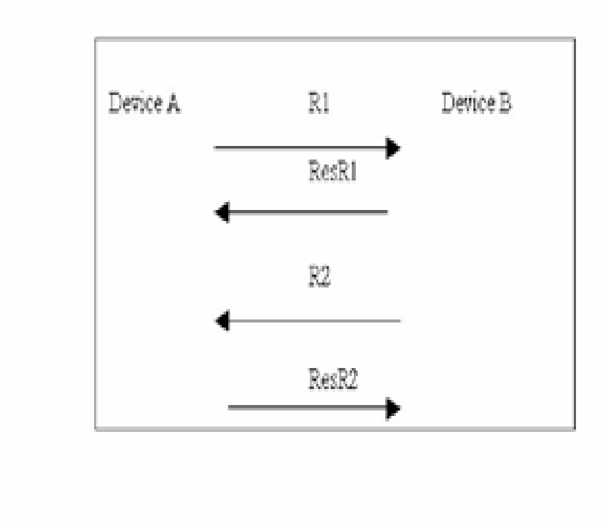


Figure 1 Existing Authentication

In the existing authentication scheme of blue-enamel technology, mutual authentication is executed. First one tool sends the random number for authentication to device second. Then the second tool sends the response and sends some other random range for the verification of first device. Then the primary device sends the response of random range send with the aid of 2nd tool. In this manner the identity of each the gadgets is completed. In rsa, ciphering emerge as at very high speed. It is usefully for stop consumer. Here non-public keys are completely unknown to everyone and also ciphering and decoding set of rules is equal. In rsa technical benefits are as follows:-

- Ciphering and deciphering key are distinct.
- Programming may be accomplished with a polynomial shape.

3. PORPOSED AUTHENTICATION

In this segment, we endorse the solution to remove attacks with the aid of intruder. Here we recommend a Algorithm wherein Bluetooth cope with of both gadgets are used in pairing .In this mechanism following steps are used for pairing.

- First of all we convert BTDA of each devices(Hx1,Hx2) into decimal shape (D1,D2)
- We test if decimal cost of both BTDA (D1,D2) are prime or now not? If it is not a prime no then we exchange it into prime no with the aid of follow a few technique.

After that each BTDA (D1,D2) assigning by means of new identifier (P,Q) for pairing we trade fee of P, Q.

- In RSA Kp. Ks, C ,&P Formula are as follows

  C=(P) Kp Mod N

  P= (C) Ks Mod N

Where

KP is a now not aspect of (P-1) *(Q-1) Ks is calculated by using formulation (KP* KS) Mod (P-1)* (Q-1)=1 Here N=P*Q

P&Q are top No.

BTDA way Bluetooth gadgets deal with C & P are cipher and undeniable textual content

In float chart BTD1 and BTD2 are Bluetooth devices

- After that we Apply RSA algorithm for calculating Kp , Ks, C &P on each Bluetooth Device for in addition calculation
- At the cease Bluetooth devices get same C&P then we get comfy pairing.

Since right here both units contain there BTDA in pairing so 1/3 unit cannot interfere throughout pairing and can't get any information of some other each devices.

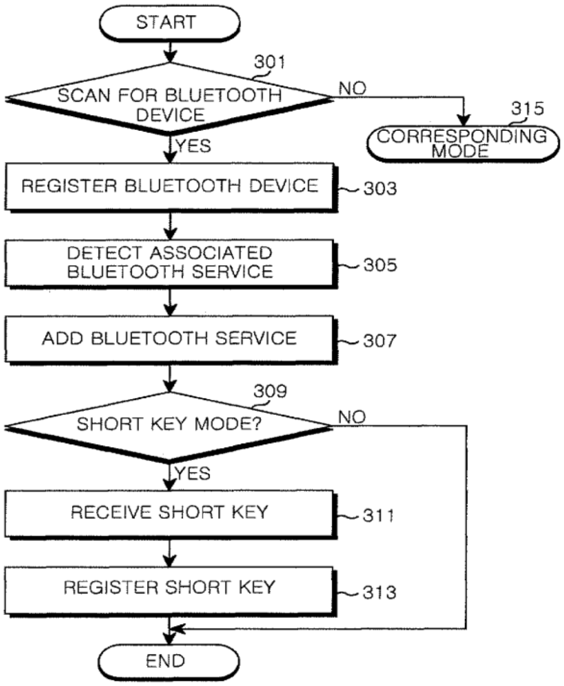


Figure 2 Improved Authentication Method

4. RESULTS AND DISCUSSIONS

With this experimental setup you may send a few textual content messages out of your android phone to arduino and vice versa.

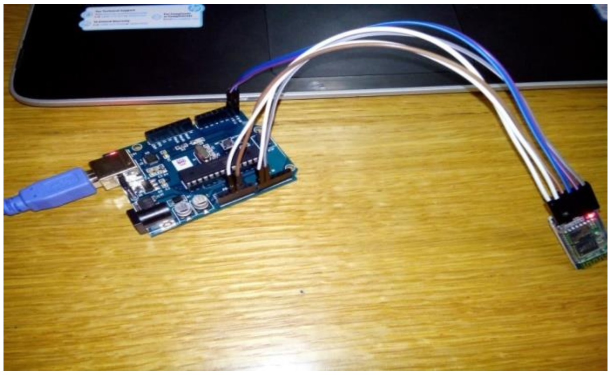
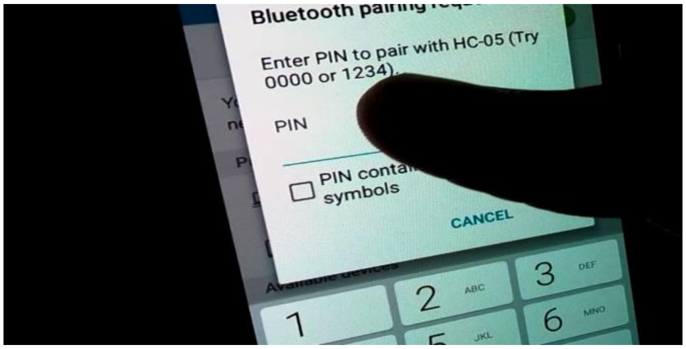


Figure 3 Arduino with HC-05 Connection system

Basically, something you could see on Arduino's Serial Monitor also can be visible on the interface of Bluetooth Application.

Change the baud rate of Bluetooth module. The module needed to be set to baud price of 9600Bd.

Then connect with the Bluetooth module the use of the S2 Bluetooth software. Then write a few text message on smartphone, you may see the same textual content message to your LCD module additionally.



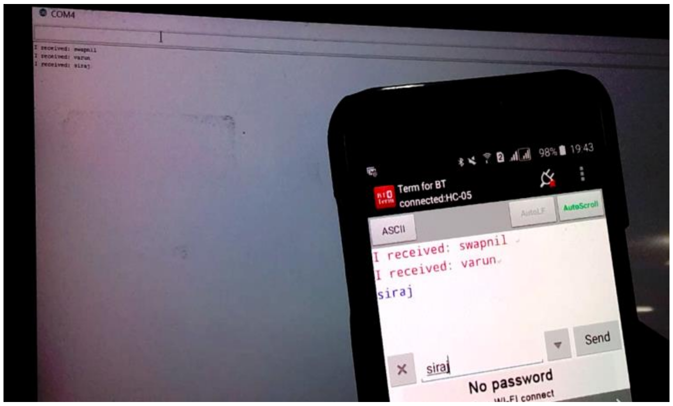
Bluetooth pairing

Enter PIN to pair with HC-05 (Try 0000 or 1234).

PIN

□ PIN contai symbols

Figure 4 Pairing of both Bluetooth



```
I received: swapnil
I received: varun
siraj
```

Figure 5 Transferred text over Bluetooth Network

5. CONCLUSION

We describe the answer to at ease towards the assault on Bluetooth authentication protocol. In the prevailing device the attacker does now not want to wager or obtain a not unusual mystery known to both sufferers a good way to set up these attacks, merely to transfer the information it gets from one victim to the other at some point of the authentication procedure. If an unknown tool wants to make connections or request for a service, then proper authentication is followed through authorization and encryption. We suggest that the authentication system ought to be such that pairing may be emerge as a relaxed manner but some complexity is remain right here. In this system it takes a bit time to begin communication.

REFERENCES

[1] Bluetooth SIG, "Bluetooth Specification." http://www.bluetooth.org/Technical/Specifications/adopte d.htm

[2] Bluetooth SIG, "Bluetooth Special Interest Group." http://www.bluetooth.com/Pages/network-effect.aspx

[3] H. Dwivedi, C. Clarck and D. Thiel, "Mobile Application Security," McGraw Hill, 2010.

[4] Bluetooth SIG, "Bluetooth Specification: Core Versione + EDR," 2004. http://www.bluetooth.org/docman/handlers/DownloadDo c.ashx?doc_id=40560

[5] Bluetooth SIG, “Bluetooth Specification: Core Versione + EDR,” 2007. http://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=241363

[6] Bluetooth SIG, “Bluetooth Specification: Core Versione + HS,” 2009. http://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=174214

[7] Bluetooth SIG, “Bluetooth Specification: Core Versione 4.0,” 2010. http://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737

[8] NIST, “Guide to Bluetooth Security (Draft), Special Pub-blication 800-121, Rev. 1,” NIST, 2011.

[9] W. Stallings, “Wireless Communications and Networks,” 2nd Edition, Prentice Hall, 2004.

[10] S. Hay and R. Harle, “Bluetooth Tracking without Dis-coverability,” 4th International Symposium on Location and Context Awareness, Tokyo, 7-8 May 2009, pp. 120-137. doi:10.1007/978-3-642-01721-6_8

[11] L. Carettoni, C. Merloni and S. Zanero, “Studying Blue-tooth Malware Propagation: The Bluebag Project,” IEEE Security & Privacy, Vol. 5, No. 2, 2007, pp. 17-25. doi:10.1109/MSP.2007.43

[12] “Trifinite Group.” http://www.trifinite.org

[13] M. Herfurt and C. Mulliner, “Remote Device Identifi-cation Based on Bluetooth Fingerprinting Techniques,” Trifinite Group, White Paper, 2004.

[14] C. Gehrmann, J. Persson and B. Smeets, “Bluetooth Secu-rity,” Artech House, Inc., 2004. Kounelis, J. Loschner, D. Shaw and S. Scheer, “Secu-rity of Service Requests for Cloud Based m-Commerce,” 2012 Proceedings of the 35th International Convention MIPRO, Opatija/Abbazia, 21-25 May 2012, pp. 1479-1483.

[15] Kounelis, H. Zhao and S. Muftic, “Secure Middleware for Mobile Phones and UICC Applications,” Mobile Wire-less Middleware, Operating Systems, and Applications, Berlin, 13-14 November 2012, pp. 143-152.

[16] GSMA, “Mobile NFC Technical Guidelines, Version 2.0,” 2007.

[17] NFC Forum, “Bluetooth Secure Simple Pairing Using NFC,” Application Document v1.0, 2011.