Man in the middle attack

Kamal Sai Raj K (E16CSE028),Tirdesh P(E16CSE038)

November 2019

1 Abstract

Man in the middle attack is an attack where the attacker places himself between the client server i.e., all the packets that are sent to server will be routed to the attacker and the attacker will send these to the server, then the packets returned from server to attacker will be routed to the client. The attacker is like a middle person and he can gain sensitive information or manipulate the packets to his will. This attack could also be done by creating fake network that the attacker controls and traffic can be rerouted to a phishing site.The attacker acts a bridge between the client and server.The purpose of this paper is to design a perform a MITM attack in a LAN using ARP spoofing.

2 Introduction

In the age of this modern era, MITM remains as a prevalent network attack due to its simplistic approach. As explained earlier it is just that the attacker will be eavesdropping the communication between the client and server. Most of the MITM attacks were based on wi-fi connections. The attacker/hacker will setup a wifi connection that sounds legit, and he/she just has to wait for the client to fall into his trap by connnecting to this wifi.As soon as the client gets connected to the network, the attacker will start rerouting his packets as a legitimate user and intercepts the information shared in between. One more type of MITM attack is to use spoofing technique to make the client think that he/she is connected to the server but where as in reality the packets are being intercepted by the attacker and transferred in a to and fro motion. ARP being a stateless protocol and without cache having a security mechanism makes the MITM attack using ARP very easy.The mechanism of MITM being spoofing a packet, the attacker/hacker sends the spoofed ARP packets on LAN, to associate his/her own machine mac addess with ip address of other host.The forged packet can also be a ping to host.Now, the traffic originating from host will be sent to the attacker, and he'll be fooling the host/client by acting as a legitimate server.

3 Literature Survey

MITM is named for the game of ball where two people play catch while a third person in the middle attempts to intercept the ball. MITM is also used as a fire brigade attack, a term derived from the emergency process of passing water buckets to put out a fire. In the year 2004, U. Meyer and S. Wetzel presented a report on Universal Mobile Telecommunication System's (UITM) security protocol where the authors discussed about 'men-in-the-middle-attack' on mobile communication (Meyer Wetzel, 2004)[6]. In 2006, Kish published his research in a master listed journal where he showed an encryption method of MITM using Kirchhoff-loop-Johnson (-like)-noise cipher (Kish, 2006)[5]. Hypponen and Haataja (2007)[3], made a research on secure Bluetooth communication and showed their developed system was capable of preventing MITM attack (Hypponen Haataja, 2007). Sun et al., 2018 [10]and Saif et al., 2018[8]; made similar type of researches on updated version of Bluetooth networks security and discussed about new techniques to prevent MITM in two party's communication Sun et al., 2018 [10]and Saif et al., 2018[8]. Ouafi et al. (2008)[7], Callegati et al. (2009)[1], Joshi et al., (2009)[4], Desmedt, (2011)[2] and Sounthiraraj et al., (2014)[9] conducted researches about HTTP security and those researches found MITM as a very serious threat and those also discussed about the prevention techniques Ouafi et al. (2008)[7], Callegati et al. (2009)[1], Joshi et al., (2009)[4], Desmedt, (2011)[2] and Sounthiraraj et al., (2014)[9]

4 Proposed Method

The technique we have used for performing man in the middle attack is ARP poisoning which is one of the most effective strategy to perform man in the middle attack. The insecure nature of the ARP protocol is used in poisoning . Devices using ARP will accept updates at any time which is disadvantageous as unlike protocols such as DNS that can be configured to only accept secured dynamic updates. This simply means that any device can send an ARP reply packet to another host and force that host to update its ARP cache with the new value. Sending a gratuitous ARP means sending an ARP reply when no request has been generated . Few well placed gratuitous ARP packets which are present with malicious intent would result in hosts who think they are communicating with one host, but in reality are communicating with a listening attacker. An attempt which is undetectable to the user is an effective ARP poisoning attempt. ARP poisoning is very effective against wireless networks. By starting an ARP poisoning attack which can further lead to being man in the middle attack, hackers can steal highly-sensitive data from the targeted computers In this attack attackers machine send ARP spoofed packets to victims machine using python scapy script, IP address and the network gateway of the wireless interface, which makes the victim think that attacker machine is the router and also send ARP spoof packets to router to make it think that the attacker machine is the victim. This poisons the ARP table of the victims machine and router. After the script is run then attacker can use packet capturing tools like Wireshark to capture any packet of the victim.

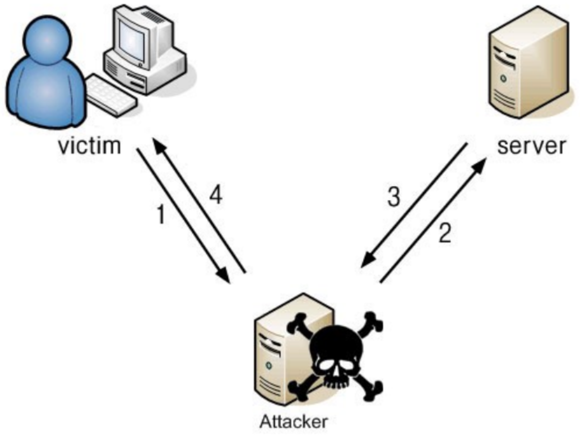


Figure 1: Man in the middle attack

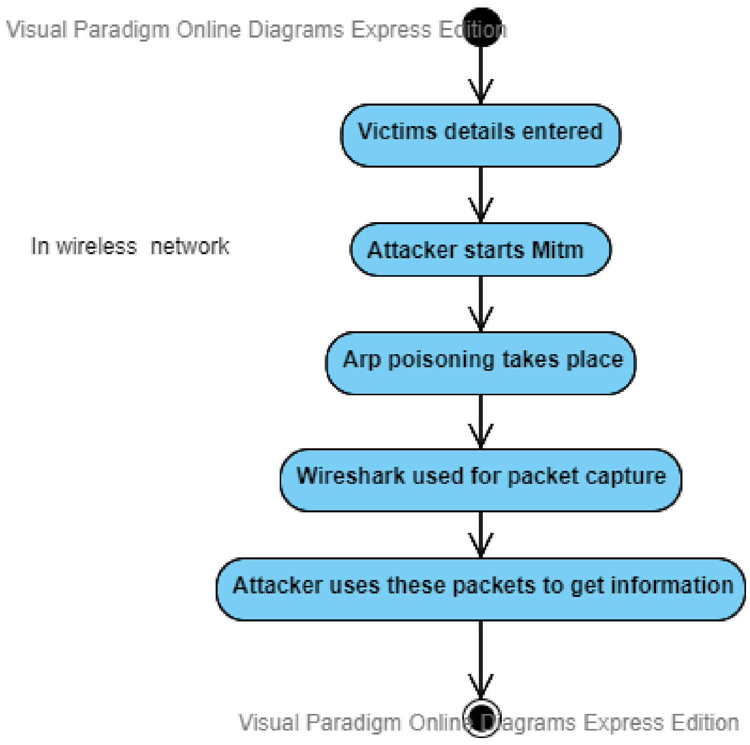

Visual Paradigm Online Diagrams Express Edition
Victims details entered
In wireless network
Attacker starts Mitm
Arp poisoning takes place
Wireshark used for packet capture
Attacker uses these packets to get information
Visual Paradigm Online Diagrams Express Edition

Figure 2: Activity flow

5 Experiments and results

5.1 Dataset and tools information

There isn't a dataset that we have used. But the details of the data that is captured from the victim machine through the attacker machine and is stored in a pcap file which is further analyzed. Attacker Machine : Kali-linux, Tools: python-scapy(used for creating attack), driftnet, urlsnarf, wireshark (used for packet capture). Victim Machine : Windows 10, Tools: Command prompt (to provide input and check test case) ,Browser (to test use case). Smartphone : Wifi-hotspot (to provide network).

5.2 Experiment Setup

The setup consists of two personal computers and a routing device which can provide network which in case we have a taken personal hotspot of a smartphone. One personal computer is the attacker machine which is configured with Kali-linux system and the other is the victim machine which is equipped with Windows.

Steps for Man in the middle attack

1. Once the IP address and the network gateway of the wireless interface of the victim machine are known we can perform the MITM attack. We have created python script file for attack.

2. For checking purposes we have check the ARP table on command prompt of the victim machine. First the ARP table will be configured with routers mac address, in our case that will be the smartphone's mac as it is providing the network.

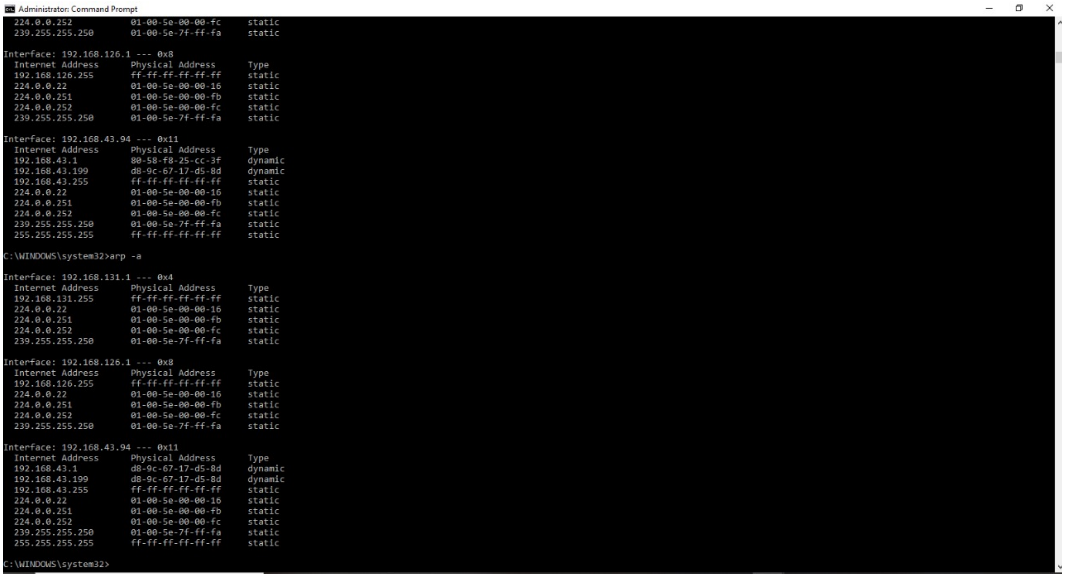
3. We run the attack script on the machine then we wait for some time. Then we check the ARP table on the victim machine which will be changed to attackers mac address. We ensure that port forwarding on the attackers machine to ensure that the victims machine is connected to internet.

4. Now attackers machine has access to all the information to passing from victims machine. We use tools like wireshark to capture these packets and access the information. We can also use tools like driftnet and urlsnarf to get further information.

5.3 Results

First the details are captured of the attacker machine like IP address and Network gateway. Interface : 192.168.41.1,Ip address of the attacker Machine : 192.168.43.94, Attackers Mac address: d8-9c-67-17-d5-8d.

The ARP table is checked before and after the attack is performed.(Fig 3)

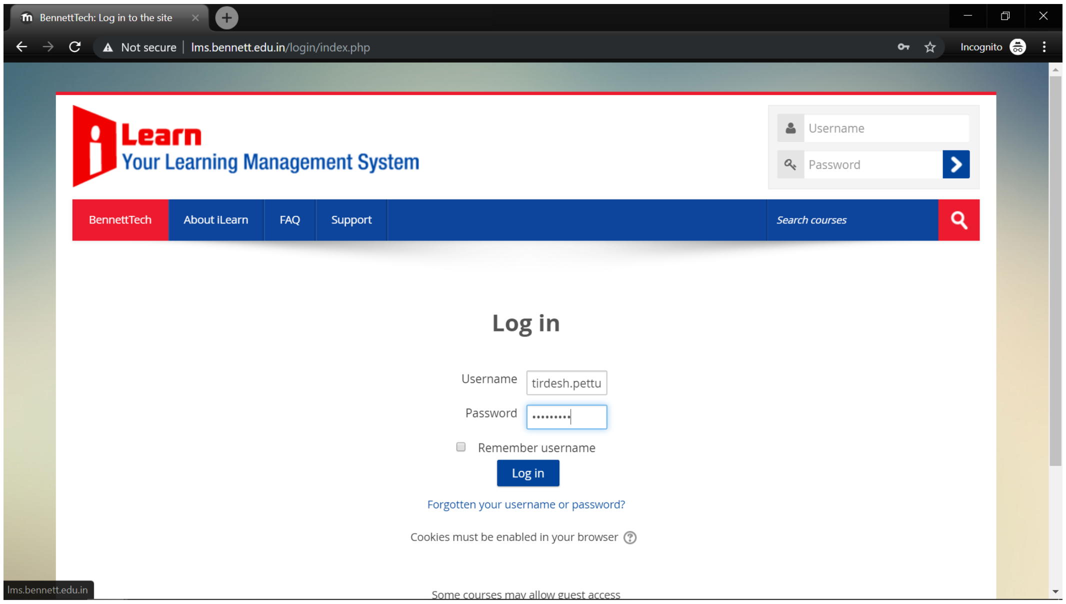


```
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.126.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.126.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.43.94 --- 0x11
  Internet Address      Physical Address      Type
  192.168.43.1          80-58-f8-25-cc-3f     dynamic
  192.168.43.199        d8-9c-67-17-d5-8d     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>arp -a

Interface: 192.168.131.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.131.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.126.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.126.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.43.94 --- 0x11
  Internet Address      Physical Address      Type
  192.168.43.1          d8-9c-67-17-d5-8d     dynamic
  192.168.43.199        d8-9c-67-17-d5-8d     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>
```

Figure 3: ARP table

Now the victim machine thinks the attacker is the router that we can see in the picture above.So the packets that are sent to victims machine are captured by the attacker machine . Now for testing the attack we would like to gather information like login details from a particular website like LMS of Bennett University for instance.(Fig 4)

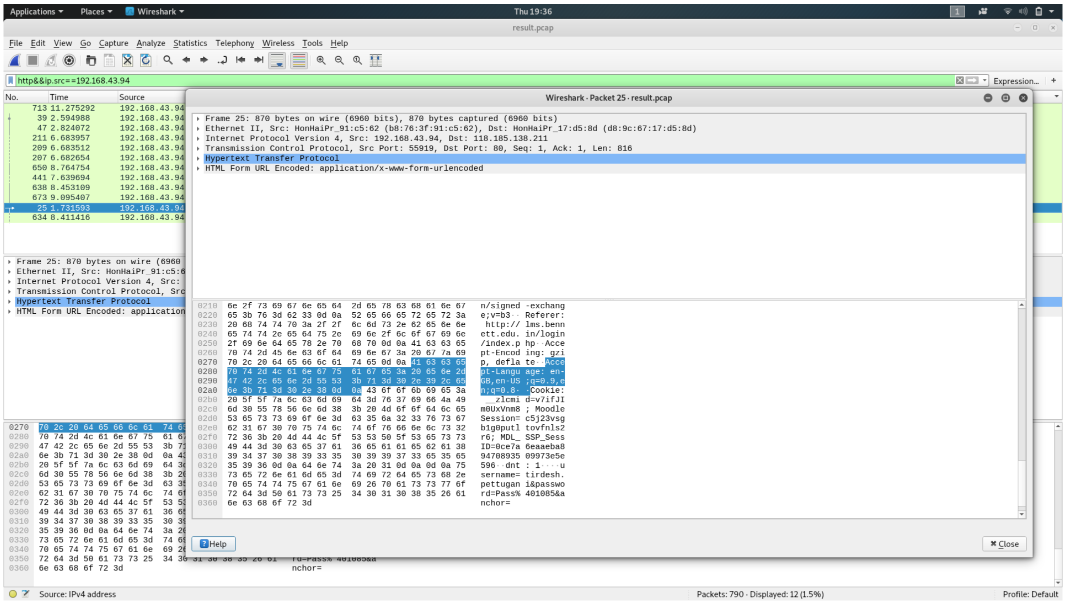
Also the tools used like the Wireshark to capture packets from the victims machine (Fig 5)


BennettTech: Log in to the site
Not secure | lms.bennett.edu.in/login/index.php
Incognito
iLearn
Your Learning Management System
Username
Password
BennettTech
About iLearn
FAQ
Support
Search courses
Log in
Remember username
Log in
Forgotten your username or password?
Cookies must be enabled in your browser
lms.bennett.edu.in
Some courses may allow guest access

Username: tirdesh.pettu

Password: •••••••••

Figure 4: Test case


Applications
Places
Wireshark
Thu 19:36
result.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Wireshark · Packet 25 · result.pcap
Help
Close

```
http&&ip.src==192.168.43.94
```

```
No.   Time       Source
  713 11.275292  192.168.43.94
   39 2.594988   192.168.43.94
   47 2.824072   192.168.43.94
  211 6.683957   192.168.43.94
  209 6.683512   192.168.43.94
  207 6.682654   192.168.43.94
  650 8.764754   192.168.43.94
  441 7.639694   192.168.43.94
  638 8.453109   192.168.43.94
  673 9.095407   192.168.43.94
   25 1.731593   192.168.43.94
  634 8.411416   192.168.43.94
```

```
Frame 25: 870 bytes on wire (6960 bits), 870 bytes captured (6960 bits)
Ethernet II, Src: HonHaiPr_91:c5:62 (b8:76:3f:91:c5:62), Dst: HonHaiPr_17:d5:8d (d8:9c:67:17:d5:8d)
Internet Protocol Version 4, Src: 192.168.43.94, Dst: 118.185.138.211
Transmission Control Protocol, Src Port: 55919, Dst Port: 80, Seq: 1, Ack: 1, Len: 816
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0210  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
0220  65 3b 76 3d 62 33 0d 0a  52 65 66 65 72 65 72 3a   e;v=b3·· Referer:
0230  20 68 74 74 70 3a 2f 2f  6c 6d 73 2e 62 65 6e 6e    http:// lms.benn
0240  65 74 74 2e 65 64 75 2e  69 6e 2f 6c 6f 67 69 6e   ett.edu. in/login
0250  2f 69 6e 64 65 78 2e 70  68 70 0d 0a 41 63 63 65   /index.p hp··Acce
0260  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0270  70 2c 20 64 65 66 6c 61  74 65 0d 0a 41 63 63 65   p, defla te··Acce
0280  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 2d   pt-Langu age: en-
0290  47 42 2c 65 6e 2d 55 53  3b 71 3d 30 2e 39 2c 65   GB,en-US ;q=0.9,e
02a0  6e 3b 71 3d 30 2e 38 0d  0a 43 6f 6f 6b 69 65 3a   n;q=0.8· ·Cookie:
02b0  20 5f 5f 7a 6c 63 6d 69  64 3d 76 37 69 66 4a 49    __zlcmi d=v7ifJI
02c0  6d 30 55 78 56 6e 6d 38  3b 20 4d 6f 6f 64 6c 65   m0UxVnm8 ; Moodle
02d0  53 65 73 73 69 6f 6e 3d  63 35 6a 32 33 76 73 67   Session= c5j23vsg
02e0  62 31 67 30 70 75 74 6c  74 6f 76 66 6e 6c 73 32   b1g0putl tovfnls2
02f0  72 36 3b 20 4d 44 4c 5f  53 53 50 5f 53 65 73 73   r6; MDL_ SSP_Sess
0300  49 44 3d 30 63 65 37 61  36 65 61 61 65 62 61 38   ID=0ce7a 6eaaeba8
0310  39 34 37 30 38 39 33 35  30 39 39 37 33 65 35 65   94708935 09973e5e
0320  35 39 36 0d 0a 64 6e 74  3a 20 31 0d 0a 0d 0a 75   596··dnt : 1····u
0330  73 65 72 6e 61 6d 65 3d  74 69 72 64 65 73 68 2e   sername= tirdesh.
0340  70 65 74 74 75 67 61 6e  69 26 70 61 73 73 77 6f   pettugan i&passwo
0350  72 64 3d 50 61 73 73 25  34 30 31 30 38 35 26 61   rd=Pass% 401085&a
0360  6e 63 68 6f 72 3d                                  nchor=
```

```
Source: IPv4 address          Packets: 790 · Displayed: 12 (1.5%)          Profile: Default
```

Figure 5: Result

6 Limitations

We couldn't successfully implement this on multiple systems as we had lack of computers. Also we couldn't use this on popular websites like google, facebook and many more as the packets captured form these websites are heavily encrypted as we used a website like LMS that uses plain text. Also we couldn't use this on a router that is robust to such type of attacks as we have a personal wifi hotspot in our case.

7 Future Work

We would like to implement this attack in a much larger scale which has more computers and a robust router. We would like to try this out on many other router which are available in public for free. Also we would like to implement a prevention measure that prevents the attack from being happening.

8 Conclusion

We have succesfully completed a MITM attack using ARP spoofing and poisining.We created a personal hotspot and connected two devices on the same network. By spoofing we were able to gain lms access credentials and also the network traffic is captured visualised in wireshark. We also learnt about the vulnerabilities of a system so that the MITM can be performed. We are looking forward to try DNS MITM, SSL MITM and other MITM attacks in the future.

References

[1] Franco Callegati, Walter Cerroni, and Marco Ramilli. Man-in-the-middle attack to the https protocol. *IEEE Security & Privacy*, 7(1):78–81, 2009.

[2] Yvo Desmedt. Man-in-the-middle attack. *Encyclopedia of cryptography and security*, pages 759–759, 2011.

[3] Konstantin Hypponen and Keijo MJ Haataja. “nino” man-in-the-middle attack on bluetooth secure simple pairing. In *2007 3rd IEEE/IFIP International Conference in Central Asia on Internet*, pages 1–5. IEEE, 2007.

[4] Yogesh Joshi, Debabrata Das, and Subir Saha. Mitigating man in the middle attack over secure sockets layer. In *2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, pages 1–5. IEEE, 2009.

[5] Laszlo B Kish. Protection against the man-in-the-middle-attack for the kirchhoff-loop-johnson (-like)-noise cipher and expansion by voltage-based security. *Fluctuation and Noise Letters*, 6(01):L57–L63, 2006.

[6] Ulrike Meyer and Susanne Wetzel. A man-in-the-middle attack on umts. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 90–97. ACM, 2004.

[7] Khaled Ouafi, Raphael Overbeck, and Serge Vaudenay. On the security of hb# against a man-in-the-middle attack. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 108–124. Springer, 2008.

[8] Sohail Saif, Rajni Gupta, and Suparna Biswas. Implementation of cloud-assisted

secure data transmission in wban for healthcare monitoring. In *Advanced Computational and Communication Paradigms*, pages 665–674. Springer, 2018.

[9] David Sounthiraraj, Justin Sahs, Garret Greenwood, Zhiqiang Lin, and Latifur Khan. Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps. In *In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14*. Citeseer, 2014.

[10] Da-Zhi Sun, Yi Mu, and Willy Susilo. Man-in-the-middle attacks on secure simple pairing in bluetooth standard v5. 0 and its countermeasure. *Personal and Ubiquitous Computing*, 22(1):55–67, 2018.