Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 6, September 2017 – www.caeaccess.org

Secure Wireless Communication Protocol: To Avoid Vulnerabilities in Shared Authentication

Varun Shukla
PSIT
Kanpur
Uttar Pradesh, India

Atul Chaturvedi
PSIT
Kanpur
Uttar Pradesh, India

Neelam Srivastava
REC
Kannauj
Uttar Pradesh, India

ABSTRACT
Routers are used to connect both similar and dissimilar LANs. Routers are connected to access points. Access point provides wireless connectivity of a wired LAN. Whenever we consider router or access point for communication, in many cases, they are based on passphrase based security. It can be shown that MITM (Man in the middle attack) based on dictionary attack can be launched very easily and the security of entire network goes down. So we present a cryptographic scheme based on mathematical properties to overcome this problem with various associated advantages.

Keywords
Authentication, Dictionary Attack, Man in the Middle Attack (MITM), Security, Wireless Communication

1. INTRODUCTION
Networks connected by routers and access points are based on passphrase based security. It's all about routers or access points which provide you wireless connectivity of a wired network. Routers connect dissimilar LANs and perform NAT operation that is network address translation and connects with access points to provide wireless connectivity. So if the security of access point is compromised, the security of entire communication is in deep trouble [1][2]. For illustration of this we develop a router connecting two LANs and configure the entire setup and simulate the results for the protocol environment. The setup contains two switches (model 2960), router 2911 and six PCs as end devices or nodes. Switch to router and switch to nodes connection are made accordingly.

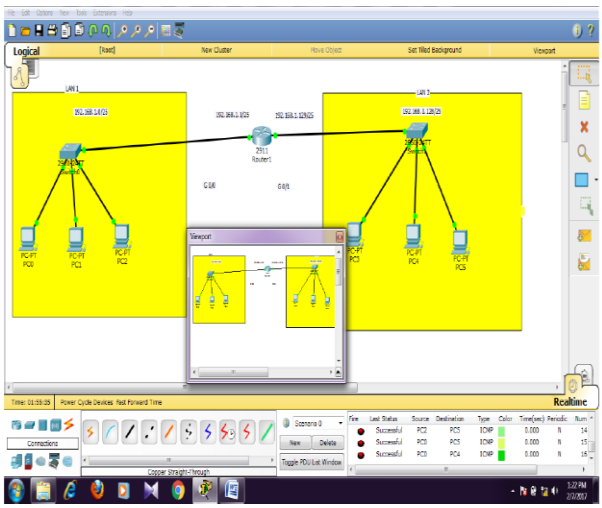

Figure-1: Showing router and switch connections

The address table of this network is as shown below in the table.

Table-1: Denote addresses of the network

S.N	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.10	255.255.255.128	192.168.1.1
PC1	192.168.1.11	255.255.255.128	192.168.1.1
PC2	192.168.1.12	255.255.255.128	192.168.1.1
PC3	192.168.1.200	255.255.255.128	192.168.1.129
PC4	192.168.1.201	255.255.255.128	192.168.1.129
PC5	192.168.1.202	255.255.255.128	192.168.1.129

Here PC0, PC1 and PC2 are connected to LAN1 while PC3, PC4 and PC5 are connected to LAN2. LAN1 and LAN2 both uses switch 2960 named switch0 and switch1 respectively. We have given network address to LAN1 is 192.168.1.0/25 and network address to LAN2 is 192.168.1.128/25. The router is connected to LAN1 via gigabit Ethernet 0/0 port with the corresponding IP address of 192.168.1.1/25 which will be the default gateway for all the PCs of LAN1. Similarly router is connected to LAN2 via gigabit Ethernet 0/1 port with the corresponding IP address of 192.168.1.129/25 which will be the default gateway for all the PCs of LAN2. The link connecting router to these nodes is still down so to make this up we need to perform some programming change to develop the environment for the protocol [3][4]. For link change of LAN 1, we select CLI mode that is command line interface of router. They are as follows.

Table-2: Required programming for router to LAN 1

```
Continue with Configuration dialog?[Yes/No]:N

Press RETURN to get started

ROUTER>

ROUTER> ENABLE

ROUTER#conf t

ROUTER {config}#ip add

ROUTER{config}#interface gigabit Ethernet 0/0

ROUTER{config-if}#ip address 192.168.1.1  255.255.255.128

ROUTER{config-if}#no shutdown

Line protocol on Interface Gigabit Ethernet 0/0 changed state
to up.
```

Similarly for LAN2 we need to perform the similar programming in CLI.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 6, September 2017 – www.caeaccess.org

Table-3: Required programming for router to LAN 2

```
ROUTER#configure t

ROUTER {config}#ip add

ROUTER{config}#interface gigabit Ethernet 0/1

ROUTER{config-if}#ip address 192.168.1.129
255.255.255.128

ROUTER{config-if}#no shutdown

Line protocol on Interface Gigabit Ethernet 0/1
changed state to up.
```

So by this programming on CLI both the links are up and started working and router can provide connection to access points for wireless connectivity.

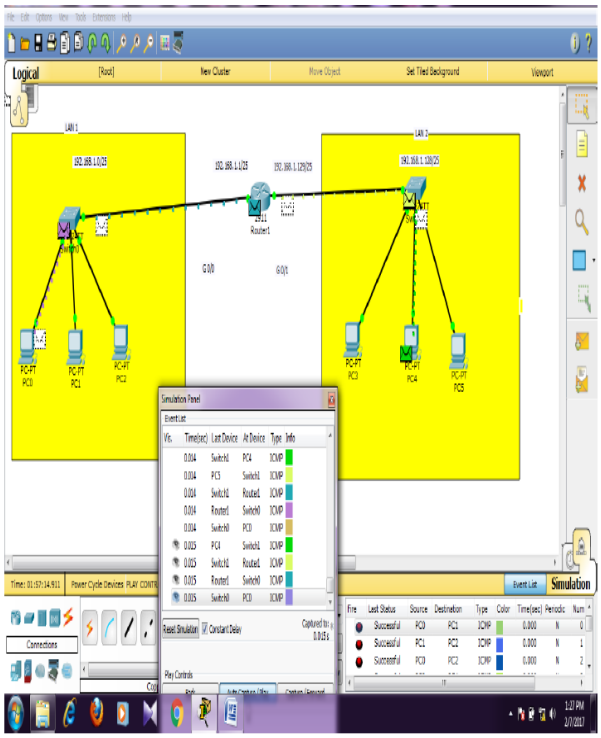

Figure-2: Showing simulation status when all links are up

1.1 Passphrase based Authentication

It can be divided into two broad categories i.e. Open system authentication and shared key authentication. Here we will talk about shared key authentication for our consideration [5][6].

1.2 Shared key authentication

When we want to start the communication process, the mobile phone (or the Computer/Laptop) sends a request for authentication purpose to the corresponding access point. The access point replies with a challenge text to the computer. The computer encrypts this challenge text with the key and sends it back to the access point. The access point decrypts the message and compares it with the original challenge text. If it matches, the access point sends an authentication code to the computer which is obviously accepted by the computer and by this way computer is now a part of the network. The idea is that the entire authentication process is based on the key. If a malicious computer or intruder becomes a part of the network, the security of the entire network is in trouble for the duration of the session or as long as it remains within the range of that access point [7]. This is a series flaw in shared authentication because it is a simple challenge response protocol. The design is vulnerable to dictionary attacks and MITM [8][9][10].

2. PROPOSED SCHEME TO AVOID VULNERABILITY

Here we consider a mobile tries to communicate with an access point which is providing connectivity to a wired LAN. Here authentication is very important to avoid man in the middle attack because an active intruder named Oscar can degrade the performance of the entire network. He may launch a dictionary attack. Oscar knows that the network access is open to everyone means anyone can connect to the network. It means Oscar can launch MITM attack in case of password failure. The proposed scheme is nothing but a cocktail protocol of Diffie-Hellman key agreement with commitment scheme [11]. The commitment scheme has binding and hiding properties. The protocol has two phases to execute i.e. set up phase and communication phase [12].

2.1 Set up phase

We will denote access point by AP and mobile device by MB and intruder Oscar by OS.Let g represents a generator of a group Z_p^* where p is a large prime essential for security. AP and MB selects a and b from this group as their private values (a and b will never transfer anywhere separately) and calculates g^a and g^b . The IP addresses of AP and MB can be used as their identity number denoted as AP_{ID} and MB_{ID} . Now AP calculates $AP_{random} \in \{0,1\}^x$ where x is the length of the string. Similarly MB calculates $MB_{random} \in \{0,1\}^x$. So AP develops $Code_{AP} \leftarrow AP_{ID} \parallel g^a \parallel AP_{random}$. Similarly MB develops $Code_{MB} \leftarrow MB_{ID} \parallel g^b \parallel MB_{random}$. Now it is important to mention here that now AP develops a commitment pair(B, R) in such a way that by sending B, AP can't change its values but MB can't open it also. When AP sends R then only MB can open it. This specific primitives are called as binding and hiding that is $(B, R) \leftarrow commitment(Code_{AP})$ [13].

2.2 Communication Phase

AP sends B to MB and according to the description above, MB can't open $Code_{AP}$ but at the same time AP can't change his choice also. In reply of this, MB sends $Code_{MB}$ to AP. Now AP sends R to MB so that $Code_{AP}$ can be open now. Now AP and MB both perform the authentication $AP_{authentication} = AP_{random} \oplus MB_{random}$ and similarly $MB_{authentication} = MB_{random} \oplus AP_{random}$. Since $AP_{authentication} = MB_{authentication}$, both access point and mobile will recognize each other and look forward for a key agreement for the session. Now AP will calculate $(g^b)^a mod\ p \equiv g^{ab} mod\ p$ and MB will calculate $(g^a)^b mod\ p \equiv g^{ab} mod\ p$ which is the shared secret key for the session [14].

3. SECURITY ANALYSIS

As mentioned earlier, it's a cocktail protocol so it has all the security level which a DH protocol has. The private parameters a and b are never transmit anywhere and to compute a from g^a or b from g^b is discreet log problem which is hard. Now we discuss the security analysis of the

protocol.

3.1 MITM Resist

Suppose Oscar starts the communication as an active intruder with access point. Oscar pretends to be the original mobile device. Oscar sends his commitment value B_{oscar} to AP which is the commitment of calculating the random string OS_{random} where $OS_{random} \in \{0,1\}^x$ and $Code_{OS} \leftarrow OS_{ID} \parallel g^o \parallel OS_{random}$ and sends it to access point. AP will send its code that is $Code_{AP}$ to Oscar. Now Oscar modify the incoming message from access point and send it to MB. In reply MB will send (B, R) pair as usual. Since this (B, R) pair is unique, apart from all the hacking efforts when it comes to authentication stage of the protocol that is $AP_{random} \oplus MB_{random}$, the streams will not match. So this authentication failure provides resistance against MITM and there is no chance of further exchanging of parameters for key sharing [15].

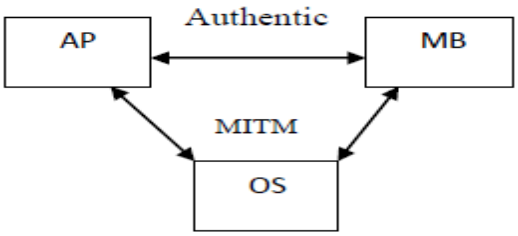

Figure-3: Showing possible MITM connection between access point and mobile device

3.2 Probability of Brute Force

Since the success of authentication depends on the selection of random strings, the only chance of Oscar's success is when OS and MB select same bit stream. So probability of brute force is $P_{brute\ force} = 2^{-x}$. The selection of $x = 16\ bits$ gives us $P_{brute\ force} = 2^{-16}$ which is 0.0000152587890625 which is negligible. One can understand that the probability will approach zero if one selects $x = 64\ bits$.

3.3 No Collision Protocol

The commitment primitives (B, R) are ideal in our assumption. It indicates that the binding primitive B is unique for $Code_{AP}$ in a manner so that $B = B_{oscar}$ is never possible (until $Code_{AP}$ is not known). The same security consideration applies for R because (B, R) are the primitives of commitment pair [16].

3.4 Security of DH protocol

The private selected values a and b are never transmitted anywhere. The only chance of intruder's success is possible if he calculates a from g^a or b from g^b which is not possible as DH discreet log problem is secure [17].

3.5 No dictionary attack

Since in every run, protocol is bounded with the commitment primitives which are based on random string value so the dictionary attack is not possible [18].

4. ASSOCIATED ADVANTAGES

4.1 Security Equivalent to OTP

In the protocol run, the transmitter and receiver selects random string which is responsible for the development of commitment primitives. This random selection provides security equivalent to OTP (one time pad) which is assumed strongest in cryptography [19][20].

4.2 Savings of computational overheads

In case of authentication failure($AP_{authentication} \neq MB_{authentication}$) , protocol will not run further and the session declines. It will save computational resources in all those cases where authentication is not provided [21].

4.3 Enhances security level

As discussed above, the protocol provides security level of one time pad. This security level further enhanced with the hardness of DH protocol as to calculate a from g^a or b from g^b is hard and computationally infeasible [22].

4.4 Extension of the protocol

We have proposed the protocol for two parties but the idea can be extended to group communication protocol since the calculation is simple but the security level is very high. Any communication scenario whether it is EHR (Electronic health record) system or military battlefield where authentication and security is prime concern, the protocol can be utilized [23][24].

5. CONCLUSION

The protocol can beat dictionary attack and MITM. Since the success probability is very less, brute force attack is not possible. Here we are achieving security of one time pad (OTP) which is unbeatable. Once we make sure that the Wi-Fi access of wired network is safe, it always help us to achieve cryptographic goals. The customization of the protocol is user dependent as length of string x determines the probability of successful attack. In case of heavy traffic load or in peak hours user can enhance the security level by increasing the value of x and otherwise, moderate value of x is good enough for security.

6. FUTURE SCOPE

The proposed scheme has a very rich future scope. We have proposed point to point protocol that can be extended to group communication as well. The protocol run time can also be shown so that the comparison can be made with existing schemes in this category. The calculation related to computational overheads can be shown because mobiles and wireless access devices are battery powered where power consumption is a key issue.

7. REFERENCES

[1] P.Mackenzie, More efficient password-authentication key exchange, Cryptographers track at the RSA conference (CT-RSA) Springer, 2001, 361-377.

[2] R.Morris, K.Thompson, Password security: A case history, Magazine communications of the ACM, volume 22, issue 11, New York, USA, 1979, 594-597.

[3] Cisco IOS configuration fundamentals command reference, American headquarters, Cisco sytem Inc., USA, 2010. http://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.pdf

[4] Cisco security appliance configuration guide using ASDM, version 6.2, American headquarters, Cisco system Inc., USA, 2009. http://www.cisco.com/c/en/us/td/docs/security/asdm/6_2/user/guide/asdmconfig.pdf

[5] J. R. Walker, Unsafe at any key size, an analysis of the

WEP encapsulation, IEEE Document 802.11-00/362, 2000.

[6] N.Borisov, I.Goldberg, D.Wagner, Intercepting mobile communications: The insecurity of 802.11, Proceedings of the 7th annual international conference on mobile computing and networking, MobiCom'01, Italy, 2001, 180-189.

[7] T.Pank, M.Cho, K.G.Shin, Enhanced wired equivalent privacy for IEEE 802.11.wireless LANs, CSE-TR, 469-02, 2002. https://www.cse.umich.edu/techreports/cse/02/CSE-TR-469-02.pdf

[8] M.Agarwal, S.Biswas, S.nandi, Advanced stealth man-in-the-middle-attack in WPA2 encrypted Wi-Fi networks, IEEE communications letters, volume 19, issue 4, 2015, 581-584.

[9] W.Stallings, Cryptography and network security, principles and practices, fourth edition, Prentice Hall, 2005.

[10] A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press Inc., USA, 2001.

[11] W.Diffie, M.Hellman, New directions in cryptography, IEEE transactions on information theory, volume 22, issue 6, 644-654.

[12] I.B.Damgard, T.P.Pedersen, B.Pfitzmann, Statistical secrecy and multi bit commitments, IEEE transactions on information theory, volume 44, issue 3, 1998, 1143-1151.

[13] V.Shukla, N.Srivastava, A.Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (WTLS), IEEE Uttar Pradesh section international conference on electrical, computer and electronics engineering(UPCON), 2016.

[14] A.Chaturvedi, N.Srivastava, V.Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications(IJCA), Foundation of computer science(FCS), volume 126, number 5, New York, USA, 2015, 35-38.

[15] V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless (Mobile) communication in an EHR system using cryptography, Communications on applied electronics (CAE), Foundation of computer science (FCS), volume 3, number 3, New York, USA, 2015, 16-21.

[16] C.Tang, D.Pei, Z.Liu, Z.Yao, M.Wang, Perfectly hiding commitment scheme with two-round from any one-way permutation. https://eprint.iacr.org/2008/034.pdf

[17] I.F.Blake, T.Garefalakis, On the complexity of the discreet logarithm and Diffie-Hellman problems, Journal of complexity-science direct, volume 20, issue 2-3, 2004, 148-170.

[18] P.Wang, Y.Kim, V.Kher, T.Kwon, Strengthening password-based authentication protocols against online dictionary attacks, proceedings of ACNS'2005, LNCS 3531, Springer-Verlag, 2005, 17-32.

[19] One time pad encryption, the unbreakable encryption method, Mils electronic. http://www.cryptomuseum.com/manuf/mils/files/mils_otp_proof.pdf

[20] S.Arora, B.Barak, Computational complexity: A modern approach, first edition, Cambridge university press, New York, USA, 2009.

[21] J.Liu, K.Kumar, Y-H.Lu, Trade off between energy saving and privacy protection in computation offloading, IEEE international symposium on low power electronics and design (ISLPED), USA, 2010.

[22] H-C.Chen, H.Wijayauto, C-H.Chang, F-Y.Leu, K.Yim, Secure mobile instant messaging key exchange protocol with one-time-pad substitution transposition cryptosystem, IEEE conference on computer communication workshops (INFOCOM WKSHPS), USA, 2016.

[23] The office of the national coordinator for health information technology, Guide to privacy and security of electronic health information, version 2.0, 2015.https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

[24] A. A. Yavuz, F.Alagoz, E.Anarim, A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption, Turkish journal of electrical engineering & computer sciences, volume 18, number 1, 2010.