A Study of Authentication Scheme for Wireless Access Network using APEA Framework

Kavita R. Wagh
Computer Engineering
S. N. D. College Of Engineering And Research Center
Yeola , India
Kavita.wagh1989@gmail.com

Prof. I. R. Shaikh
Computer Engineering
S. N. D. College Of Engineering And Research Center
Yeola , India
imran.shaikh22@gmail.com

***Abstract*—**In case of wireless access networks significantly changes the way we live and work, bringing us closer anywhere at any time. Security, privacy, accountability, and efficiency issues are of most concern in such networks. because of need and importance, little research has been conducted on designing accountable and privacy-preserving authentication schemes for wireless access networks, and this motivates us to develop an authentication framework, namely APEA using Attribute Based Encryption, that defines new form of APEA while Existing version of APEA integrates a key management protocol, where key transfer mechanism is more complicated , time consuming and less secure In our proposed approach attribute based encryption does is that, it effectively binds the access-control policy to the data and the users(clients) instead of having a server mediating access to files. An effective approach to simultaneously achieve the four goals without involving any trusted third party. However, with the requirement of wireless area network security solution, this paper presents the various techniques on WAN authentication with certain constraints and analyzes their strengths and weaknesses.

***Keywords**: APEA, Authentication, Privacy, Trusted third party, Wireless Access Network , Attribute Based Encryption .*

*****

I. INTRODUCTION

The fast development of wireless technologies has led to everywhere network accesses through smart phones, laptop, PCs, mobile devices etc. This provides users unauthorized access to network-based applications such as e-commerce, e-learning, and social networking. However, the security and privacy risks introduced by such technology development are also exceptional, from unintended disclosure of sensitive information by inexperienced or non-vigilant users, due to ease of wireless signal interception, to the rapidly evolving sophistication of surveillance gadgetry [1].Wireless technology is widely spread everywhere in the real world and has a biggest contribution to mankind. However, with the vitality of wireless architectures, security protocols are vulnerable to attackers outside the system, failure in wireless connectivity and machine failures. Protocols must be streamlined to combat with these abnormal conditions. In this paper, a review of an existing protocols are given. Achieving security is of most disquiet in the use of wireless access networks. First, due to the open and distributed nature of wireless access networks, it is important to enforce network access control

to handle malicious attacks. Second, it is also vital to provide ample user privacy, particularly in contexts such as banking, commercial transactions, and e-healthcare. Privacy means not only hiding the user's true identity, but also securing the linkage among the transactions of the same unknown user. Third, user accountability must be provided since fraudulent user behaviors and insider attacks should be audited under the permission of the law authority. Fourth, each access point (AP) should be capable of verifying a large number of access requests in a timely manner so that connections of roaming users are not forced to terminate.

II. WIRELESS ACCESS NETWORK

It is a Type of network mainly based on wireless technology.

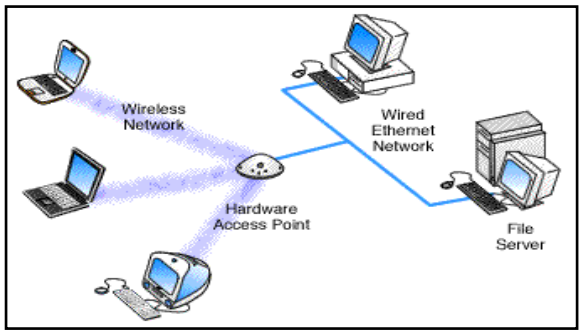

Figure 1. Wireless Access Network

Small businesses can experience many benefits from a wireless network, including:

- Convenience:- Access your network resources from any location within your wireless network's coverage area or from any WiFi hotspot.
- Mobility:- You're no longer tied to your desk, as you were with a wired connection. You and your employees can go online in conference room meetings, for example.

- Productivity:- Wireless access to the Internet and to your company's key applications and resources helps your staff get the job done and encourages collaboration.
- Easy setup:- You don't have to string cables, so installation can be quick and cost-effective.
- Expandable. You can easily expand wireless networks with existing equipment, while a wired network might require additional wiring.
- Security:- Advances in wireless networks provide robust security protections.
- Cost:- Because wireless networks eliminate or reduce wiring costs, they can cost less to operate than wired networks.

Various attacks on wireless access network:

1. Wormhole attack:

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways; the attacker can also still perform the attack even if the network communication provides confidentiality and authenticity, and even if the attacker does not have any cryptographic keys.

2. Jamming/Interference :

Wireless interference basically means disruption of one's network. This is a very big challenge especially owing to the fact that wireless signals will always get disrupted. Such interference can be created by a Bluetooth headset, a microwave oven and a cordless phone. This makes transmission and receiving of wireless signals very difficult. Wireless interference can also be caused by causing service degradation so as to make sure that one denies complete access to a particular service. Jamming can also be used in conjunction with an evil twin.

3. Evil twin

A wireless evil twin mainly comes into play when criminals are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network. Coming up with an evil twin is very simple since all one need to do is purchase a wireless access point, plug it into the network and configure it as exactly as the existing network.

4. War driving:

War driving is a way that bad guys use so as to find access points wherever they can be. With the availability of free Wi-Fi connection and other GPS functionalities, they can drive around and obtain a very huge amount of information over a very short period of time. One can also use some special type of software to view all the different access points around one. With this information, an individual is in a position to come up with a very large database which he or she can use to determine where he or she can gain access to a wireless signal.

5. Bluejacking:

Blue jacking is a kind of illegal activity that is similar to hacking where one can be able to send unsolicited messages to another device via Bluetooth. This is considered spam for Bluetooth and one might end up seeing some pop-up messages on one's screen. Bluejacking is possible where a Bluetooth network is present and it is limited to a distance of ten meters which is the distance a Bluetooth device can send a file to another device.

6. Bluesnarfing

Bluesnarfing is far much more malicious than Bluejacking since it involves using one's Bluetooth to steal information. This is where a Bluetooth-enabled device is able to use the vulnerability on the Bluetooth network to be able to get into a mobile device to steal information such as contacts and images. This is a vulnerability that exposes the weakness and vulnerability with the bluetooth network. This is an act that creates some very serious security issues since an individual can steal a file from one if he or she knows it.

7.War chalking

War chalking is another method that was used so as to determine where one could get a wireless access signal. In this case, if an individual detected a wireless access point, he or she would make a drawing on the wall indicating that a wireless access point has been found. However, this is not currently used.

So to provide security against all this attacks it is necessary to apply some access policies to available data.

III. LITERATURE SURVEY

Existing security research on wireless access networks considered privacy and has lead to a number of new and efficient protocols, most of them assumed that there is a trusted third party which manages all keying materials so that no secured information and privacy details can be loose. Unfortunately, with the trusted third party, the security system suffers from the key escrow problem and the single point of failure. An enemy can break the security measures of the whole system by compromising the trusted third party. It is thus desirable to achieve security and privacy preservation without involving any trusted third party. Another issue that has not been adequately addressed in the literature is to provide accountability along with privacy, which are two seemingly contradictory goals.

In recent years, a number of authentication frameworks have been proposed for wireless access networks [2]–[10]. Among them, only a few achieve authentication. For example, a simple and typical way to construct authentication mechanisms is to use symmetric-key cryptography due to its low computation complexity [2]–[4]. However, they are vulnerable to the-man-in-the-middle attacks by scoundrel APs. As a result, user privacy is at risk. Another drawback is that their support of user privacy commonly suffers from

an inbuilt scalability problem. That is, to identify only one single user privately, the user registration center must check all keys in its own database with user testimonial, which makes the process undistrustly impractical. An example is the Extensible Authentication Protocol-Authentication and Key Agreement, which is used in wireless access networks (e.g., the Third- Generation Partnership Project) for authentication and session key distribution.

A common approach to maintain user privacy is to update a user's credentials regularly [5]–[8]. However, this means that a user can still be tracked during the validity period of a credential. The choice of the validity period poses a difficulty. With a long validity period, an adversary can gather substantial information. On the other hand, with a short validity period, a malicious user can send multiple messages without being detected. Moreover, this approach requires each user to store a large number of pseudonyms and certifications, which means that a revocation scheme is difficult to implement. Another kind of approach is delegation-based authentication, such as the protocol in [9] and [10]. The advantage of this method is that it has low computation cost. However, the anonymity property cannot be easily achieved. We observe that none of the available privacy-aware cryptographic primitives (e.g., standard digital signature, blind signature, group signature, ring signature, and their extensions) can be directly applied to achieve the aforementioned goals.

From the given analysis, it is clear that, until now, no efficient privacy-preserving authentication protocol for wireless access networks has been proposed, let alone protocols also supporting accountability. Moreover, most of existing authentication methods rely on the existence of a trusted third party, such as the home location register [3], [9] and home server [4], [10], [11], but the establishment and maintenance of this entity in a distributed environment is not trivial.

IV. SYSTEM ARCHITECTURE

TRUST AND KEY MANAGEMENT MODEL

In APEA, users are organized in groups. Each user group is a collection of users based on certain aspects of their nonessential attributes user. APEA using Attribute Based Encryption is designed based on the trust and key management model shown in Fig. 1. It typically involves four kinds of network entities: NO, APs, user group managers, and groups of users. Since our protocol does not rely on the existence of a trusted third party, the trust of all entities is limited. Users do not directly register with the NO; instead, each group manager subscribes to the NO on behalf of its group members. The NO produces the group private key and partial group public key but keeps the group private key secretly. Upon receiving a registration request from a group manager, the NO distributes the partial group public key to this user group. Then, the group manager generates full group public key and returns it to the NO. Subsequently, the NO delivers the group public key to each AP. To access the network, each user requests the member secret key and group public key from his/her group manager. In this system more security is preserved. And Reduces time required to decrypt irrelevant data.

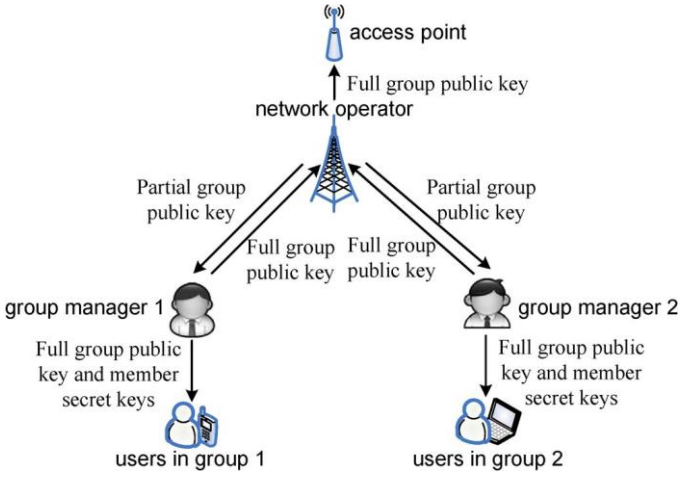

Fig. 1 Trust And Key Management model

V. ACKNOWLEDGMENT

I would like to express my special thanks to all those people who have helped me to complete this work. I am very grateful to my guide, Prof. I. R. Shaikh And PG Coordinator Prof. V. N. Dhakane Computer Engineering, SND College of Engineering & Research Centre, Yeola, Nashik for his guidance, encouragement and the interest shown in this project. He has continuously helped and encouraged me in my work.

REFERENCES

[1] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmissionfor cluster-based wireless sensor networks," *IEEE Trans. Parallel Distrib.Syst.*, vol. 25, no. 3, pp. 750–761, Mar. 2014.

[2] Y. Tsai and C. Chang, "SIM-based subscriber authentication mechanismfor wireless local area networks," Comput. Commun., vol. 29, no. 10,pp. 1744–1753, Jun. 2006.

[3] H. Tsai, C. Chang, and K. Chan, "Roaming across wireless local area networks using SIM-based authentication protocol," Comput. StandardsInterfaces, vol. 31, no. 2, pp. 381–389, Feb. 2009.

[4] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authenticationscheme with smart cards for wireless communications," Comput.Commun., vol. 34, no. 3, pp. 367–374, Mar. 2011.

[5] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficientand robust pseudonymous authentication in VANET," in Proc. VANET,2007, pp. 19–28

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "FLIP: An efficient privacypreservingprotocol for finding like-minded vehicles on the road," in Proc.IEEE Globecom, 2010, pp. 1–5.

[7] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "AEMA: An aggregatedemergency message authentication scheme for enhancing thesecurity of vehicular Ad Hoc networks," in Proc. IEEE ICC, 2008,pp. 1436–1440

[8] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security frameworkFor VANETs," in Proc. VANET, 2006, pp. 94–95.

[9] Z. Lu and J. Zhou, "Preventing delegation-based mobile authenticationsfrom man-in-the-middle attacks," Comput. Standards Interfaces, vol. 34,no. 3, pp. 314–326, Mar. 2012.

[10] C.-C. Chang and H.-C. Tsai, "An anonymous and self-verified mobileauthentication with authenticated key agreement for large-scale wirelessnetworks," IEEE Trans.Wireless Commun., vol. 9, no. 11, pp. 3346–3353,Nov.2010.

[11] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authenticationprotocols for anonymous wireless communications," IEEE Trans.Wireless Commun., vol. 9, no. 1, pp. 168–174, Jan. 2010

[12] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authenticationwith conditional privacy for wireless networks," IEEE Trans.Comput., vol. 62, no. 3, pp 616–622 Mar. 2013.

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacypreservingprotocol for vehicular communications," IEEE Trans. Veh.Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007

[14] "An Accountable, Privacy-Preserving, and Efficient Authentication Frameworkfor Wireless Access Networks" Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, and Mohsen Guizani, IEEE transactions on vehicular technology, vol. 65, no. 3, march 2016 1605.