A Stronger Formal Security Model of Three-party Authentication and Key Distribution Protocol for 802.11i

Tao Wenjun and Hu Bin

Information Science and Technology Institute,Zhengzhou,China
taowenjun515@163.com

Abstract

This paper analyzes the existing formal security models of three-party authentication and key distribution protocol for 802.11i, which are extended BR and Extended CK models. We propose the flaw about the definition of session identifier in Extended CK model and present the limitation of matching conversation defined in Extended BR model .In order to fix these problems and provide a perfect model for provable security protocol, a new stronger formal security model of three-party authentication and key distribution protocol is defined by "efficient AP" according to the rules of 802.11i standard, and we present a new provable secure EAP-TLS protocol in our model. The new formal security model proposes a better method to design provable security three-party authentication and key distribution protocol in WLAN. In addition, this paper also suggests an idea to define the authentication relationships in special application environment.

Keywords: *802.11i, EAP protocol, Provable security, Three-party formal security model*

1. Introduction

As the rapid development of mobile communication, wireless network are widely used in our life. However, the openness of wireless network makes its safety problem has become the focus of our attention.In order to protect the privacy of users, the Wired Equivalent Privacy (WEP) security mechanism was proposed [1]. Unfortunately,the weakness in the 802.11 WEP security mechanism was found by a group from the university of california in 2001.The main reason of these weaknesses is the key scheduling agorithm of RC4. Not long after that, Adam Stubblefield and AT&T announced the first verification of the attack, which were able to intercept transmissions and get unauthorized access to the wireless networks.

In order to strengthen the privacy of WLAN, IEEE 802.11i standard was proposed by the IEEE task group of the 802.11 work group in 2004 [2]. The standard proposes a new set of security mechanisms for wireless networking and solves several problems in WEP:

IEEE 802.11i standard defines a new type of wireless network which is called Robust Security Network. The Robust Security Network brings the concept of security contexts to WLANs. The standard uses 802.1x as the methods of authentication and key management, and defines TKIP, CCMP and WRAP as the three encryption mechanism. The TKIP mechanism is adopted in the RC4 encryption algorithm, which is used to support the existing equipment upgrade firmware and driver method in order to improve WLAN security purposes. CCMP mechanism based on AES encryption algorithm and CCM certification is the realization of RSN mandatory requirements. WRAP mechanism based on AES encryption algorithm and OCB, is an optional encryption mechanism.

With a large number of new technology applyed, the 802.11i standard is thought to be much stronger than the former one and has been widely used. But is it really secure? In this paper we focus on the EAP-TLS protocol of 802.1X, which is the core part of 802.11i to acheive authentication and key distribution. As we know, provable security is an important

method to design security protocols.We consider two existing security models about 802.11i and find out there are still something unsuitable.So a stronger and effective security models is needed to analyze its security formally. Here we propose a new stronger security model for three-party authentication and key distribution protocol in 802.11i standard.

In 2008, a security model of three-party authentication and key distribution protocol Extended CK model was proposed under the transmission frame of 802.11i standard [3]. But the definition of the session identifier(SID) of access point(AP) was uncertain if there was a adversary impersonate AP.So the Extended CK model is not perfect (Actually, the author did not put forward a practical secure protocol in that model). In 2010, an Extended BR model was introduced by Song, etc. [4], in which model the matching session was defined by conversation sequence, however as the definition of matching session didn't consider the relationships between the conversation sequences produced by access point with another two parties, so that the authentication may be unsuccessful. So in order to protect the WLAN, how to improve the security model of three party authentication and distribution protocol are still need us to research more.

This paper suggests that we should consider the special application environment when we use matching sessions to define the authentication relationships, because at least one of the three parties needs to interact with other two parties. For describing the conversation of the special party, we must consider its position and character in the network, otherwise if the adversary impersonate or destroy it, the matching session would be disabled. In the standard of 802.11, AP transmits the messages between clients and servers, so the messages of the AP received and send are similar. We make use of the important character to define the validity of SID and build a perfect security model, at last a new EAP-TLS protocol is proven secure in the new model.

Since the authentication of 802.11i standard is accomplished by 802.1X, so in this section we describe the 802.1X protocol simply. A successful execution of 802.1X protocol is shown as following:

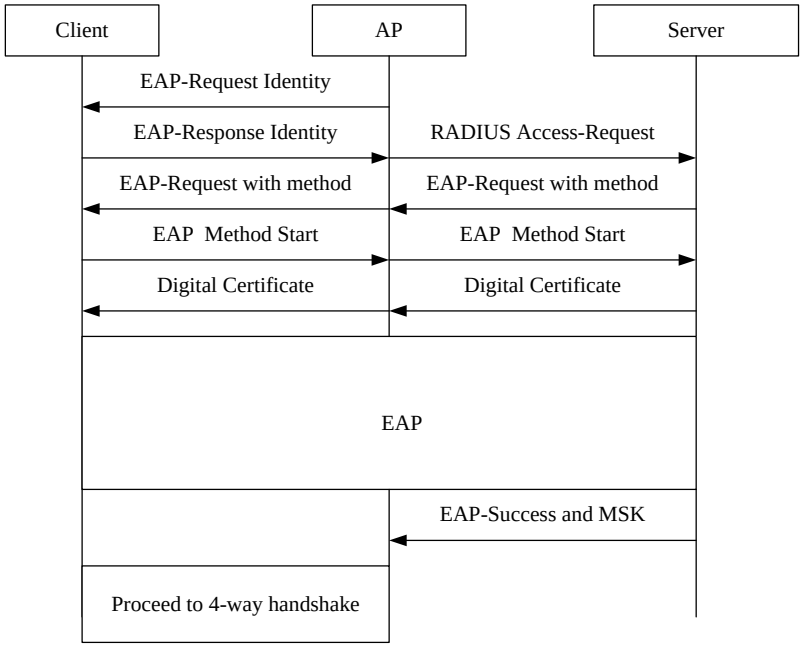


Figure 1. A Successful Execution of 802.1X

Client is connected with AP through wireless network, and AP is connected with server through wired network. The character of AP is encrypted (decrypted) those received messages and send them. The server is setting to authenticate the client. Both client and server have keys (*PKC,SKC*), (*PKC,SKC*) , AP and server share the long-term symmetric key *K*. When 802.1 X authentications are executed, the client and server response identities, EAP method, certificates and start request with each other through AP. The purpose of EAP protocol is to share a master key between client and server and get a mutual authentication between the client and server. After that, the server will send the encrypted master key to AP in order to accomplish the 4-way handshake with client.In this paper,we assume the transmission of *MSK* from server to client have not any information leakage.

In this paper, our research focus our on the EAP protocol, since which is the most important part to achieve authentication and key distribution, and the new formal security model are built on the EAP under the 802.11i standard.

2. Analysis of Security Models of Three-party Authentication and Distribution Protocol

In this section, we introduce the Extended CK model and Extended BR model simply. By lots of analysis of the two security models, we found some imperceptible problem of the two models. One problem is when the AP was impersonated, the SID of AP maybe invalid in the Extended CK model. For the other one, the definition of matching session may result a failing authentication in the Extended BR model.

2.1. Flaw of Definition in the Extended CK Model

In 2008, an Extended CK model was proposed by CAO according to the CK model [5] in the frame of 802.11i standard. The security model defined matching session by session identifier.

Definition1 Let *sid* be the session identifier, P_i, P_j, P_k is the identities of interacting entities. $role \in \{Client, AP, AS\}$ denotes the role entity played in the protocol. After running a protocol *P*, P_i takes session information $(P_i, P_j, P_k, sid_i, role_i)$ as a result , P_j takes corrsponding information $(P_j, P_i, P_k, sid_j, role_j)$, and so P_k gets $(P_k, P_i, P_j, sid_k, role_k)$, if we have $sid_i = sid_j = sid_k$,and $role_i, role_j, role_k$ are different with each other,then these three conversations are called matching sessions.

It's more efficient using session identifier to define the matching session than using conversation sequence. However, as the same as CK model, the Extended CK model still didn't provide the practical definition. The model was just extended from two parties to the case of three parties, and that have not considered the existence and rationality. The Extended CK model supposed all parties get the corresponding SID if the protocol had been executed. But actually, the SID of AP sid_A maybe uncertain if a matching session was completed as Figure 2. At that time, the condition $sid_i = sid_j = sid_k$ in defination 1 maybe confused. We described it in detail as follows:

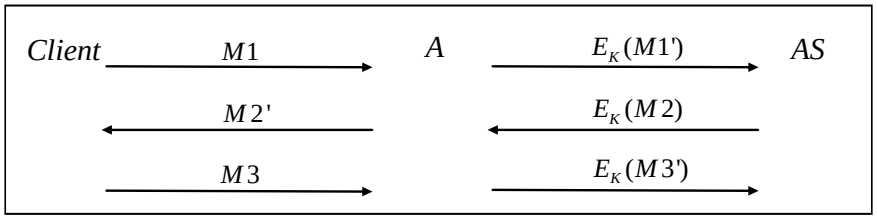


Figure 2. The Case of Uncertain SID in Extended CK Model

Supposing a session has completed like figuer 2, *A* is the adversary who take part in the protocol. Now we try to analyze its security in the Extended CK model. According to the definition of SID, there are $sid_C = H(M1 \| M2' \| M3)$ and $sid_S = H(M1' \| M2 \| M3')$. But what is the SID of AP? We cannot ensure it! That maybe $sid_A = H(M1 \| M2' \| M3)$ or $sid_A = H(M1 \| M2' \| M3')$ or any others. As we know, the SID was used to tag a conversation. It is useless if it is uncertain. So we find out the definition about SID is not suitable, and we have to fix it by analyzing the character of AP. In Section 3, we define the SID of AP according to its working states. If the AP executes correctly, it is efficient, and if the AP was impersonated by adversary, the SID does not exist.

2.2. The Security Problem of Extended BR Model

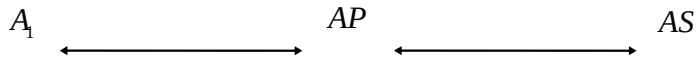
In the Extended BR model, the three-party conversation was formalized as a four tuple $P = (\pi, \phi, \varphi, LL)$, in which π, ϕ, φ are honest conversation execution of client, access point and authentication server. *LL* is the session key agreed between client and authentication server. The adversary is regard as a Probable Turing machine equipped with some oracle $\pi_{i,j}^s$, $\phi_{i,k}^s$ and $\varphi_{j,k}^s$.The adversary can make corresponding query and get the returned value. In order to describe the authentication relationships of parties, we suppose oracles $\pi_{i,j}^s$, $\phi_{i,k}^s$ and $\varphi_{j,k}^s$ produce corresponding conversation sequences $C1, C1'$ and $C2, C2'$. The Extended BR model defines the authentication relationships according to the original BR model [6], which are definition 2 and 3.

Definition 2 If $C1$ is a matching conversation to $C1'$, $C1'$ is a matching conversation to $C1$,and $C2$ is a matching conversation to $C2'$, $C2'$ is a matching conversation to $C2$,we say that $\pi_{i,j}^s, \phi_{j,k}^t, \phi_{j,k}^u, \varphi_{k,j}^v$ is matching session.If an uncorrupted oracle has accepted, but there is not a matching session to it, we call it no matching session.

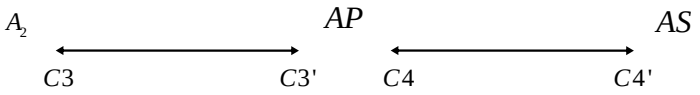
Definition 3 If the probability of no matching session is negligible, then the protocol *P* is secure authenticated.

The definition above is a natural extension of the original BR model. We suggest that there are some problems of definition 2 about matching session . According to definition 2, it is easy to see either client and AP or AP and server can be authenticated with each other. However, we cannot ensure there is an authentication between client and server, which is the

real purpose of EAP protocol. So we can say the definition 2 ignored the relationships between the two matching conversations. For example:

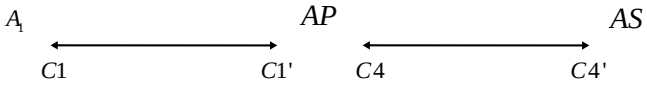


(1)



(2)

The three parties complete two sessions like (1) and (2). they are both matching conversations. Now we construct a new session (3), which is the combination of some parts of (1) and (2). Because $C1$ and $C1'$, $C4$ and $C4'$ and are both matching conversations, according to the definition 2 ,so the new session (3) is matching session. At this time the server treat A_2 as the client who wants to get in the network, but actually A_1 is it. The mistake shows the matching session defined in Extended BR model is limited. We need to fix it in order to avoid some attacks. The best way is not to use conversation sequences to descript the authentication relationships.



(3)

3. The Improved Security Model of Three-party Authentication and Key Distribution Protocol

Based on the analysis of the two security models before, we proposed an improved security model. This model fully considered the character of AP, and solved the problem of SID by defining the efficient AP. A provable secure EAP protocol in our new model achieved mutual authentication and the master key are also secure. Therefore, the new model is very important to analyze and design EAP protocol in 802.11i standard. In this section, we present a concept of "efficient AP" and introduce the adversarial power and security definition in the new model. In addition, we also proved two important properties.

3.1. Adversarial Power

Since the mutual authentication of EAP protocol under 802.11i standard is implemented by encryption and digital signature scheme, so we suppose that the adversary cannot get the long-term symmetric key K and asymmetric privacy key SK of users , because which may result in a forgery to message. In our model, the power of the adversary is described formally as follow:

$execute(A,u)$: The adversary can make execute query to the oracles of all three parties. Once the query $execute(A,u)$ was made, the u-th instance of A was returned. This query impersonates adversary's passive attacks, so that the adversary could get many instances by this query.

$send(A,u,M)$: The adversary can make send query to the oracles of all three parties. The query $send(A,u,M)$ means that adversary sends a message M to the u -th instance of A and

the oracle returns the response of this message. This query impersonates the active attack of adversary.

In the 802.11i standard, client and server try to share a new master key, and then the encrypted *MSK* are delivered from server to AP. In order to make the model simply, we suppose that the security of *MSK* just depends on EAP protocol. The encrypted transmission of *MSK* have no information leakage. Therefore, we define the reveal query as follow:

$reveal(A,u)$: The adversary can make reveal query to the oracles of client and server and reveals a session key of the completed session. We notice there is not a reveal query to AP. This is because AP cannot compute the *MSK* in the execution of EAP protocol.So this notion is suitable.

$test(A,u)$: This query is allowed only once to the completed and fresh oracle, at any time during the adversary's execution. A random bit b is generated; if b = 1 the adversary is given the session key *MSK*, and if b = 0 the adversary is given a random session key. Once the adversary's attack experiment was completed, it output a bit b' as a guess of the real bit b. Now we let $\Pr[b=b']$ denote the probability that the adversary correctly guessed, $Adv_S^P = \Pr[b=b'] - 1/2$ denotes the advantage of the adversary. Well if Adv_S^P is negligible, the adversary cannot get any information of the session key.

We say the adversary before is 3AKE adversary. Actually its power is limited, Since the EAP protocol is implemented by encryption and digital signature scheme, the adversary cannot be supposed to be stronger. But if we try to design the protocol by hard problems, for example the discrete logarithm problem, then we could consider something more, just like the ECK2007 model [7].

3.2. Security Definition

After the Extended BR model analyzed, we find it is limitative to define the SID by conversation sequence. This is because AP always interact with other two parties so that it is hard to separate the messages sequences from client and server. Based on this, in our new model, the SID is used to define the matching session. Then because the messages of AP received and sent are similar. We make use of this character of transmission to define an efficient AP to make sure the SID is valid.

Definition 4 Let AP and server share a symmetric key *K*, encryption scheme *E* and decryption scheme *D*, if at time τ_0, AP received message $M1$ from client ,then at the later time τ_1 sent $E_K(M1')$ to server, and at time τ_2, AP received $E_K(M2)$ from server,then at some later time τ_3 sent $M2'$ to client ,if $(M1 \| M2') = (M1' \| M2)$ we call this AP is efficient.

The SID is used to tag the session when the conversation was completed. In our model, the SID of entity is defined as the connection of messages the entity received and sent. So the SID of client and server are similar with CK model, but the SID of AP has two cases: if the AP is efficient, the SID is defined as before. If not, the AP has not a SID. According to the definition, we can get two important properties.

Property 1 If the session execution proceeds honestly, the client, server and efficient AP get the corresponding session identifier sid_C, sid_A, sid_S , then $sid_C = sid_A = sid_S$.

Proof Because of the definition 4, there must be a sid_A for AP, if the session execution honestly, we must have $sid_C = sid_A = (M1 \| M2')$ that is the connection of the messages interacted between the two parties. Since the messages received and sent by server are $E_K(M1')$ and $E_K(M2)$,we cannot define sid_S as the connection of the two messages directly, but we find if the AP is efficient ,there is $(M1 \| M2') = (M1' \| M2)$,so the SID of server could be $sid_S = (M1' \| M2) = sid_C = sid_A$.

Property 2 If the AP takes part in the session is not efficient. Then the SID of client and server are not equal, that is $sid_C \neq sid_S$.

Proof If the AP is not efficient, then $(M1 \| M2') \neq (M1' \| M2)$ .It must be $M1 \neq M1'$ or $M2 \neq M2'$ .With not loss of generalization, We let $M1 \neq M1'$. At some time τ_i , AP received the message $M1$,that means at earlier time τ_{i-1} the client sent $M1$ .So the $M1$ is a part of sid_C .On the other hand, If At time τ_j , AP sent $E_K(M1')$,that means at later time τ_{j+1} the server received $E_K(M1')$ .So the $M1'$ is one part of sid_C .But we have $M1 \neq M1'$,it is easy to see $sid_C \neq sid_S$.

In our new model, we define the matching session and security as follow:

Definition 5 If the AP is efficient, all of the parties accepted and get the equal session identifier $sid_C = sid_A = sid_S$,we call $\pi_i^C, \pi_j^A, \pi_k^S$ are matching sessions.

Definition 6 The EAP protocol in 802.11i standard is three-party authentication security, if the following three conditions are satisfied.

(1)if $\pi_i^C, \pi_j^A, \pi_k^S$ have a matching session, all is accepted

(2)if $\pi_i^C, \pi_j^A, \pi_k^S$ have accepted, they are matching session

(3)if the AP take part in the conversation is not efficient, neither π_i^C nor π_k^S has accepted

Definition 7 The EAP protocol in 802.11i standard is *MSK* security, if for all 3AKE adversary the following two conditions are satisfied.

(1) the client and server have the same *MSK*.

(2) the advantage is negligible Adv_S^P

4. Protocol and Security Proof

In order to check the validity of the security model, we propose a new EAP-TLS protocol in 802.11i standard, which can be proven secure in the new three-party security model. As shown in following:

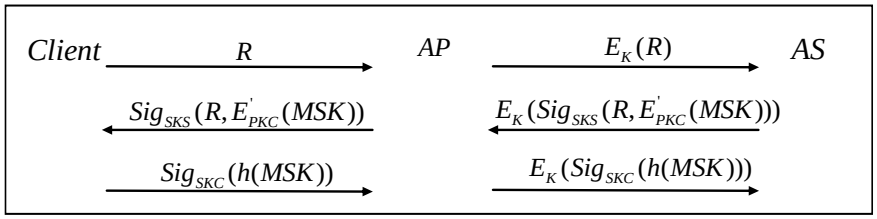


Figure 3. A New EAP-TLS Protocol

The protocol execution proceeds as figure 3: R is picked at random by client and sent to AP. Then it is encrypted by AP using long term symmetric key K and is transfered to authentication server. The server selectes a MSK at random from the session key space and produces a encrypted signature $E_K(Sig_{SKS}(R, E'_{PKC}(MSK)))$, in which $E'_{PKC}(MSK)$ is a public key encryption of MSK. After receiving the delivered message,client checks the signature $Sig_{SKS}(R, E'_{PKC}(MSK))$ and then send its own signature $Sig_{SKC}(h(MSK))$ to AP,where h is a secure hash function. At last AP transfers $E_K(Sig_{SKC}(h(MSK)))$ to server. When the protocol is terminated, the client and server share the same MSK, and we have $sid_C = sid_A = sid_S = H(R \| Sig_{SKS}(R, E'_{PKC}(MSK)) \| Sig_{SKC}(h(MSK)))$.

In this section we also prove the security of the new EAP-TLS protocol. Because our new model defines three-party authentication security and MSK security by definition 6 and 7. So we propose two theorems to prove the new protocol meets either of them .

Theorem 1 If the signature mechanism can not be forged, then the EAP-TLS protocol is three-party authentication secure.

Proof We should prove that the EAP-TLS protocol meets the definition 6. It is easy to see, if the session is matching, all the parties have accepted, so the condition (1) is satisfied. Now let us consider the condition(2):

For a session with efficient AP, there must be $Sig_{SKS}(R, E'_{PKC}(MSK))$ contained in the sid_C and $E_K(Sig_{SKC}(h(MSK)))$ in the sid_S so that the two parties could accept .While the signature is unforgeable, the adversary cannot create these messages. So the messages must be delivered by AP.That means AP had received $E_K(Sig_{SKS}(R, E'_{PKC}(MSK)))$ and $Sig_{SKC}(h(MSK))$ .According to the security of signature and long-term key, the two messages before are also unforgreable, and they must be sent from server and client. Until now, we can find out that:

π_i^C contains the messages $Sig_{SKS}(R, E'_{PKC}(MSK))$ and $Sig_{SKC}(h(MSK))$; π_j^A delivered messages $Sig_{SKS}(R, E'_{PKC}(MSK))$, $E_K(Sig_{SKS}(R, E'_{PKC}(MSK)))$, $Sig_{SKC}(h(MSK))$ and $E_K(Sig_{SKC}(h(MSK)))$;The messages of oracle π_k^S is $E_K(Sig_{SKS}(R, E'_{PKC}(MSK)))$ and $E_K(Sig_{SKC}(h(MSK)))$. According to the randomness of R , MSK and definition 5, We can see $sid_C = sid_A = sid_S$,so that $\pi_i^C, \pi_j^A, \pi_k^S$ are matching sessions.

At last, let's prove the EAP-TLS meets the condition (3) .We suppose there's a session to make oracle $\pi_i^C, \pi_j^A, \pi_k^S$ all accepted when the AP is not efficient, then:

$$sid_C = H(R \| Sig_{SKS}(R, E'_{PKC}(MSK)) \| Sig_{SKC}(h(MSK))),$$
$$sid_S = H(E_K(R') \| E_K(Sig_{SKS}(R', E'_{PKC}(MSK'))) \| E_K(Sig_{SKC}(h(MSK')))$$

According to property 2,if the AP is not efficient, then $sid_C \neq sid_S$ .It must be $R \neq R'$ or $MSK \neq MSK'$.But that means a forgery of $Sig_{SKS}(R, E'_{PKC}(MSK))$ if $R \neq R'$ or a forgery of $Sig_{SKC}(h(MSK'))$ if $MSK \neq MSK'$ .That conflicts with the assumption of signature is unforgreable.So if the AP takes part in the conversation is not efficient, neither π_i^C nor π_k^S has accepted.

Theorem 2 If the hash function, encryption and signature scheme are secure, then the new EAP-TLS protocol is security.

Proof Let the advantage of adversary guessing the toss coin successfully is Adv_S^P .We construct some experiments to prove the adversary cannot get any information about *MSK*.

(1)*Execute Query*: The adversary can make q_e times execute queries at most. Let $Adv_S(b_1' = b_1) = \Pr[b_1' = b_1] - 1/2$ be the advantage of adversary to guess $b' = b$ correctly by these queries. Because the adversary can just get information about *MSK* from $E'_{PKC}(MSK)$ and $h(MSK)$,so we do some experiments as follow:

Experiment 1: A random bit b_{11} is generated, if $b_{11} = 0$, the adversary is given $E'_{PKC}(MSK)$, and if $b_{11} = 1$, the adversary *A* is given $E'_{PKC}(r)$, in which *r* was picked at random in the space of session key. Let b_{11}' is the result guessed by *A* according to the returned value. Let $Adv_S(b_{11}' = b_{11}) = \Pr[b_{11}' = b_{11}] - 1/2$ be the advantage of adversary in this experiment.

Experiment 2: As the same as experiment 1, a random bit b_{12} is generated, if $b_{12} = 0$, the adversary is given $h(MSK)$, and if $b_{12} = 1$,the adversary is given $h(r)$, in which *r* was picked at random in the space of session key. Let b_{12}' is the result guessed by *A* according to the returned value. So $Adv_S(b_{12}' = b_{12}) = \Pr[b_{12}' = b_{12}] - 1/2$ is the advantage of adversary in this experiment.

In Experiment 1 at most q_e times execute queries can be made, because of the secure encryption, the probability that adversary win the game is the probability of *r=MSK*, that means $\Pr[b_{11}' = b_{11}] \leq q_e / |G| + 1/2$. As the same as Experiment 1, if the hash function in Experiment 2 is secure, the probability that adversary win the Experiment 2 is also $\Pr[b_{12}' = b_{12}] \leq q_e / |G| + 1/2$. So that

$$Adv_S(b_1' = b_1) = Adv_S(b_{11}' = b_{11}) + Adv_S(b_{12}' = b_{12}) \leq 2q_e / |G|$$

(2)*Send Query*: At most q_S times send queries can be made. $Adv_S(b_2' = b_2)$ is the advantage to guess $b' = b$ correctly using these queries. That's easy to find out if the adversary can get information about *MSK*, then it can give a forgery of the signature. We make experiment A_1, A_2 as follow:

Experiment A_1:For a fixed *R* ,once the send query was made, the adversary picked MSK_i and SKS_i at random to construct a signature $Sig_{SKS_i}(R, E'_{PKC}(MSK_i))$. Because the send query can be made at most q_S times, the adversary could get a list of signature

List 1. Signature made by adversary impersonating server

MSK_1	..	MSK_i	..	MSK_{qs}
$Sig_{SKS_1}(R, E'_{PKC}(MSK_1))$	..	$Sig_{SKS_i}(R, E'_{PKC}(MSK_i))$	..	$Sig_{SKS_{qs}}(R, E'_{PKC}(MSK_{qs}))$

In the experiment, if signature created by the *i*-th send query was in this list 1, MSK_i would be returned to the adversary, else"$\perp$"was returned.

Experiment A_2 :As the same as Experiment A_1, once the send query was made, the adversary could also get the other list of signature

List 2. Signature made by adversary impersonating client

MSK_1	…	MSK_i	…	MSK_{qs}
$Sig_{SKC_1}(h(MSK_1))$	…	$Sig_{SKC_i}(h(MSK_i))$	…	$Sig_{SKC_{qs}}(h(MSK_{qs}))$

In this experiment, if signature created by the *i*-th send query was in this list 2, MSK_i would be returned to the adversary, else"$\perp$"was returned.

Let the space of asymmetric key(*PK*,*SK*) to client and server is *N*. In Experiment 1, if the signature in the list 1 was forged successfully, there must be a collision of *MSK* and the SKS_i must be selected exactly equal to the real *SKS* .So the probability of adversary to win the Experiment A_1 is $\Pr[MSK_i = MSK_j] \cdot \Pr[SKS_i = SKS_j = SKS]$. In Experiment A_2 ,the situation is the same as Experiment A_1. According to the birthday attack, it is not difficult to see $\Pr[MSK_i = MSK_j] \le 2q_S^2 / G$ and $\Pr[SKS_i = SKS_j = SKS] = 1/N^2$, so that

$$Adv_S(b_2' = b_2) = 2\Pr[MSK_i = MSK_j] \cdot \Pr[SKS_i = SKS_j = SKS] - 1/2 \le 2q_S^2 / (G \cdot N^2)$$

(3) *Reveal Query*: The adversary can make some reveal queries, but we know the *MSK* is picked at random each time, the adversary cannot get any information from the returned value. So we have

$$Adv_S(b' = b) = Adv_S(b_1' = b_1) + Adv_S(b_2' = b_2) \le 2q_e / |G| + 2q_S^2 / (G \cdot N^2)$$

that is negligible.

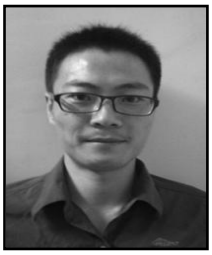
5. Conclusion

This paper analyzes two existing formal security models of three-party authentication and key distribution protocol for 802.11i and show the flaw of them. In order to solve these problems, we present the definition of "efficient AP" using the character of AP under the frame of 802.11i standard. By the efficient AP, a new security model was built and two important properties was given.In order to show the validity of the model, we proposed a new EAP-TLS protocol and proven the security of it. What we need to explain is the new three-party security model discussed in this paper is just suitable for WLAN. As future work, we can research on the three-party security model in specifically environment. Moreover, if we design the protocol using hard problem, the adversary could be stronger.

References

[1] IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications, **(1997)**.
[2] IEEE802.11i. IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements part 1： Wireless LAN Medium Access control(MAC) and Physical Layer(PHY)specifications: Medium Access Control(MAC) Security Enhancements[S]. America, ISO/IEC, **(2004)**, pp. 1-341.
[3] C. Chunjie, "Design and Analysis of Provably Secure Authentication and Key Exchange Protocols", A dissertation Submitted to Xidian University in Candidacy for the Degree of Doctor of Philsophy in Computer Applications and Technology, **(2008)**.
[4] S. Yubo, H. Aiqun and Y. Bingxin, "The provable security formal analysis of 802.11i authentication scheme", Engineering Sciences, vol. 1, no. 12, **(2010)**, pp. 67-73.
[5] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels", Advances in Cryptology EUROCRYPT 2001, Springer-Verlag, **(2001)**, pp. 453–474.
[6] M. Bellare and P. Rogaway, "Advances in Cryptology", CRYPTO'93, Springer, **(1994)**.
[7] B. LaMacchia, K. Lauter and A. Mityagin, "Stronger Security of Authenticated Key Exchange", http://eprint.iacr.org/2006/073.
[8] K. Benton, "The Evolution of 802.11 Wireless Security", INF795-April 18th, 2010 UNLV Informatics Spring, **(2010)**.
[9] Gast and S. Matthe, "802.11 Wireless Networks: the Definitive Guide", Creating & Administering Wireless Networks; Covers 802.11a, G, N & I, Beijing: O'Reilly, **(2007)**.
[10] RFC 2865 - Remote Authentication Dial In User Service (RADIUS), IETF, http://tools.ietf.org/html /rfc2865.
[11] M. F. Finneran, "Voice over WLANs: The complete guide", Boston: Elsevier, **(2008)**, pp. 280-286.
[12] S. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in The Key Schedule Algorithm of RC4", The 8th Annual International Workshop on Selected Areas in Cryptography, London: Springer-Verlag, **(2001)**, pp. 3-25.

Authors



Tao Wenjun was born in 1985. Now he is a master candidate. His research interests are in information security.

Hu Bin was born in 1971. He is a professor and doctor supervisor.His research interests are in information security.