Analysis of Mobile Communication Network Security Situation Based on Multi-factor Node Evaluation

Shang Yanwei, Lin Xijun, Huang Xiaobo

Guangdong power grid limited liability company information center, Guangzhou, China

Keywords: multi-factor, node; network security; communication link

Abstract: To solve too complex problem of man-in-the-middle attack and the deployment existing in the Ethernet Media Access Control security (MACsec), the MACsec was analyzed in the paper, proving MACsec mechanism could not resist the man-in-the-middle attack. Based on TePA ternary equity identification architecture, a new identity authentication protocol of Ethernet data link layer TDLsec was put forward. The protocol could provide security service with higher strength, resist the man-in-the-middle attack, and ensure legal users access legal network. Results showed TePA-based data link layer security (TDLsec) mechanism could resist the man-in-the-middle attack and it eliminated the practice adopted by MACsec mechanism as erecting safety path between identification center and exchange device in davance. It was easy to deploy and had higher security and stronger superiority.

1. Introduction

With gradual publicity of 100Mbps, 1000Mbps and other Ethernet standards, corresponding products appear in succession. By virtue of efficiency, high speed and high performance, Ethernet has been widely used in finance, commerce, education, government, factories and mining enterprises, but the Ethernet network security problem doesn't attract enough attention [1]. Most Ethernet lack security technology support at the early development stage. Even if latest Ethernet standard IEEE802.3-2012[2] doesn't provide security access and data privacy method. As people's attention to information security increases, Ethernet administrator intensifies the security protection work gradually. However, the endlessly emerged hacker attack results in possibility of network security accident in WLN. According to attack source, WLN security accident can be divided into two types: one is security accident from network border. It refers to intrusion and attack outside network, such as malicious attack, remote invasion, virus worm, etc. The other is security accident from the internal network. It refers to security problem occurred in the internal network, such as the stolen information, access without authorization, financial fraud, etc. At present, a majority of network administrators pay additional attention to external protection, but ignore the internal management. The statistics from authority indicates that above 70% attach behavior threatening the network security comes form the internet users [3].

2. Model Introduction

Traditional authentication security proof is given using observation method. New attack means and attack ways emerge endlessly, so the analytic results obtained from security analysis in the attack type range with finite exhaustion are limited, while adopting formalized analysis can break through such limitation. Therefore, the security analysis of MACsec authentication protocol is made using formalized analysis method in the research.

The formalized analysis of security protocol is realized based on the calculation complexity. Polynomial reduction technology is adopted for valid formalization and conversion of security protocol and to reduce the valid attack of password system to an instance of known NP problem. Such analysis method is widely used. It is an important means of analyzing and designing security mechanism. Literature [8] points out, using polynomial time reduction method is equivalent to security analysis of different concepts of security mechanism. If a problem is difficult to solve

under one polynomial time reduction, it can be deemed that the security mechanism of such problem is safe.

Bellare-Rogaway formalized analysis model is a common formalized analysis method. The model is established on a hypothesis that the attacker controls the whole communication network, the protocol participants don't communicate directly, but take attacker as the communication medium [7]. Attacker can read, create, revise, delay and reset all the communication information in the protocol, sponsor a new round of identification conversation, and imitate the operation of state machine of any protocol participants. When the operation of security protocol comes an end, the communication entity of participating in security authentication could obtain a totally identical secret key, while attack can only participate in the protocol authentication process by means of transmitting the method of authentication information loyally (namely benign attacker). Then, it is deemed that the protocol is safe enough.

The formalized analysis of the model security can be divided into the following three steps:

Step 1: Model the participant's and attacker's behaviors of formalized protocol;

step 2: formalized security target;

Step 2: formalized proving of the reduction of a polynomial time, reducing the attack to a given target to an unsolvable difficulty.

Function $\Pi(1^k, i, j, a, \kappa, r)$ is used for formalized authentication of protocol participant. Hereinto, is security parameter, are k$\in$N and i$\in$I are the mark of sponsor, j$\in$I is the mark of responder, a$\in\{0,1\}$*is the security information, and $\kappa \in \{0,1\}$* is the information cascade interacted at present, and r$\in \{0,1\}^{\infty}$ is the random input of sender. I is a set, and the elements of the set are all the participants that can participate in these protocols. Attacker E doesn't belong to the participant ($\notin$I) of protocol, II function can execute end during polynomial time.

The reaction form of authentication protocol participant $\Pi(1^k, i, j, a, \kappa, r)$ is converted into (m, δ, t), where, m$\in\{0,1\}^* \cup \{*\}$is the information to be input, $\delta \in$ {Accept,Reject,No-Decide} is the decision made by the authentication protocol participant, and t$\in\{0,1\}^* \cup \{*\}$is the secret information obtained by the participatn.

Suppose protocol P has R rounds of message interaction (R is an odd number, and 2t-1=R), the time of the ith round mutual information is $\tau = \tau_i$. In each authentication protocol process, for all the i<j, $\tau_i < \tau_j$ is true (that is the ith round of information interaction occurs before the jth round of information interaction). If the conversation sequence κ and κ' conforms to the following requirement:

The prefix of κ is

$(\tau_0, \lambda, \text{m1}), (\tau_2, m1', \text{m2}), (\tau_4, m2', \text{m3}), ..., (\tau_{2t-2}, m'_{t-1}, \text{mt})$ (1)

The prefix of κ' is

$(\tau_1, \text{m1}, m1'), (\tau_3, \text{m2}, m2'), (\tau_5, \text{m3}, m3'), ..., (\tau_{2t-3}, m_{t-1}, m'_{t-1})$ (2)

Then, it is deemed that conversation sequence κ and κ' is a pair of matched conversation sequence.

If both parties of protocol participant own a pair of matched conversation sequence, then the state machine of two protocol participants will turn to the state of trusting the other party. If such two conversations exist, when one party's state machine turns to the state of trusting the other party, but the state machine of the other party doesn't turn to the state of trusting the other party, such two conversations are called abnormal conversion sequence [8] (that is, protocol design Bug results in the occurrence of such case).

When the possibility of a abnormal conversation sequence for a protocol is as small as to be ignorable and the both participants of protocol has matched conversation sequence, the state machines of both protocol participants will turn into the state of trusting the other party. Thus, the protocol is deemed to be safe.

3. Security Analysis of MACsec Mechanism

3.1 General analysis of MACsec

MACSec provides secret key management, identity authentication and access authorization according to IEEE 802.1X standard, while IEEE 802.1X protocol [9] adopts EAP approval standards. EAP doesn't define specific authentication protocol by itself, but uses the authentication interaction provided by the upper layer for identity authentication. Whereas MACSec doesn't provide secrete key management or identity authentication, IEEE 802.1 security panel updated the version of IEEE 802.1X in 2010 so as to support MACSec.

The protocol defined by IEEE 802.1X standard requires presetting a safe communication path between the switching equipment and identity authentication server so as to ensure the safe communication between switching equipment and identity authentication server. Whenever the switching equipment links the network, it requires network administrator to set up security channel, which increases the workload of network administrator and limits the application of MACsec.

In the research, the universal Bellare-Rogaway model was used for formalized analysis of EAP-TLS protocol.

3.2 Formalized analysis of MACsec identity authentication

In the research, the security analysis is made for EAP-TLS protocol used by MACsec.

The formalized EAP-TLS protocol is shown in Fig. 1.

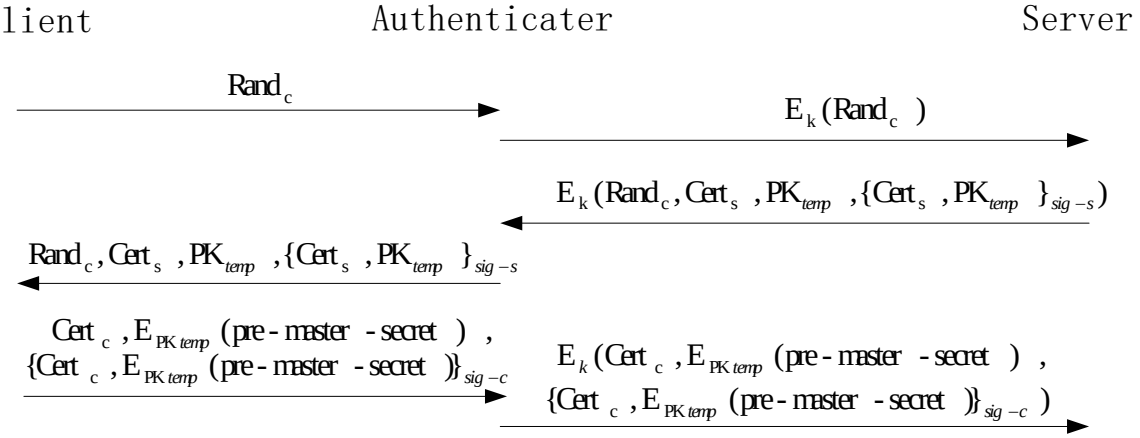

Fig. 1 EAP-TLS protocol information interaction diagram

In the protocol, $Rand_c$ is the random number transmitted for user Client at random, $E_k(m)$ is the ciphertext obtained using encryption message m of secret key k, $Cert_x$ refers to the digital certificate of participant x, PK_{temp} is temporary public key, $\{m\}_{sig-x}$ is the signature of participant for message m, and pre-master-secret is the same secret key owned by the client and AS authentication server before the running of protocol.

Secret key k is a secret key for communication between authenticator and authentication server, so it is used for ensuring the safe communication between them. That is, the authenticator has no essential identity, and it is only taken as a medium of encryption, decryption and transmission, while the identification information is only identified at client side and authentication server, so the three-party protocol should be formalized to the two-party security authentication protocol.

Inference 1-1: Suppose the attacker between Π_{cs} and Π_{sc} is benign attacker, then $\tau_0 < \tau_1 < \tau_2 < \tau_3 < \tau_4 < \tau_5$. When the authentication server Π_{sc} accepts the following conversation:

$$conv = (\tau_1, Rand_c, Rand_s \| Cert_s \| PK_{temp} \| \{Cert_s \| PK_{temp}\}_{sig-s}),$$

$$(\tau_3, Cert_c \| E_{PKtemp}(pre\_master\_secret) \| \{Cert_c \| E_{PKtemp}(pre\_master\_secret)\}_{sig-c}, \text{EAP-success})$$

Inference 1-2: Client side Π_{cs} will accept the following conversation:

$conv' = (\tau_0, "", Rand_c), (\tau_2, Rand_s \| Cert_s \| PK_{temp} \| \{Cert_s \| PK_{temp}\}_{sig-s},$

$Cert_c \| E_{PKtemp}(pre\_master\_\sec ret) \| \{Cert_c \|$

$E_{PKtemp}(pre\_master\_\sec ret)\}_{sig-c}), (\tau_4, \text{EAP-success}, ""), (\tau_5, \text{Disassociate}, "")$

Conclusion 1: Apparently, $conv''$ and $conv'''$ are a pair of abnormal conversation sequence. When the authentication server Π_{sc} has been in a state of trusting the other party, and the client side has been in the state of trusting the other party. At this time, attacker can pretend to be the client side so as to access WLN.

Inference 2-1: When the attacker is non-benign attacker, the next conversation sequence exists. When the attacker accepts the following conversation,

$conv'' = (\tau_1, Rand_c, Rand_E \| Cert_E \| PK_{temp} \| \{Cert_E \| PK_{temp}\}_{sig-s}),$

$(\tau_3, Cert_c \| E_{PKtemp}(pre\_master\_\sec ret) \| \{Cert_c \|$

$E_{PKtemp}(pre\_master\_\sec ret)\}_{sig-c}, \text{EAP-success})$

inference 2-2: the client side accepts the following conversation.

$conv''' = (\tau_0, "", Rand_c), (\tau_2, Rand_E \| Cert_E \| PK_{temp} \| \{Cert_E \| PK_{temp}\}_{sig-E},$

$Cert_c \| E_{PKtemp}(pre\_master\_\sec ret) \|$

$\{Cert_c \| E_{PKtemp}(pre\_master\_\sec ret)\}_{sig-c}), (\tau_4, \text{EAP-success}, "")$

Conclusion 2: Apparently, $conv''$ and $conv'''$ are a pair of matched conversation, but the client side finally communicates with the attacker. In other words, the attacker easily finds a chance to pretend to be authentication server so as to obtain the private information at client side.

4. Conclusion

The research solves the problem that switching equipment fails to perform identity legality verification. In the MACsec identity authentication process, the switching equipment doesn't have real identity actually, and the authentication depends on the preset security access between switching equipment and identity authentication server, but this limits the use scope of authentication server. The TDLsec mechanism proposed in the paper uses certificates to determine the identity of switching equipment. It doesn't need to preset security access between switching equipment and identity authentication server, but eliminates the binding relationship between switching equipment and identity authentication server, and expands the use scope of identity authentication server.

References

[1] Kurup, P.; Sullivan, C.; Hannagan, R.; Yu, S.; Azimi, H.; Robertson, S.; Ryan, D.; Nagarajan, R.; Ponrathnam, T.; Howe, G. A Review of Technologies for Characterization of Heavy Metal Contaminants [J]. Indian Geotech J, 2017, 47 (4):421–436.

[2] Dalia S. Abdelhamid, Yingyue Zhang, Daniel R. Lewis, Prabhas V. Moghe, William J. Welsh, and Kathryn E. Uhrich. Tartaric Acid-based Amphiphilic Macromolecules with Ether Linkages Exhibit Enhanced Repression of Oxidized Low Density Lipoprotein Uptake [J]. Biomaterials, 2015, 53:32-39.

[3] Ghebrebrhan, M.; Aranda, F.; Walsh, G.; Ziegler, D.; Giardini, S.; Carlson, J.; Kimball, B.; Steeves, D.; Xia, Z.; Yu, S.; et al. Textile Frequency Selective Surface[J]. IEEE Microwave and Wireless Components Letters 2017, 27 (11):989–991.

[4] Stephygraph, L.R., Arunkumar, N. Brain-actuated wireless mobile robot control through an adaptive human-machine interface [M]// Advances in Intelligent Systems and Computing, 2016,

397:537-549.

[5] Weisen Pan, Shizhan Chen, Zhiyong Feng. Automatic Clustering of Social Tag using Community Detection [J]. Applied Mathematics & Information Sciences, 2013, 7(2):675-681.

[6] Song Y, Li N, Gu J, Fu S, Peng Z, Zhao C, Zhang Y, Li X, Wang Z, Li X. β-Hydroxybutyrate induces bovine hepatocyte apoptosis via an ROS-p38 signaling pathway[J]. Journal of Dairy Science, 2016, 99(11):9184-9198.