ATLANTIS PRESS
Advances in Intelligent Systems Research (AISR), volume 151
2018 International Conference on Computer Modeling, Simulation and Algorithm (CMSA 2018)

Research on Trusted Authentication Method Based on Three Elements and Three Layers Architecture

Liwei Liu, Jianzhi Sun, Li Tan* and Bin Yang
School of Computer & Information Engineering, Beijing Technology & Business University, Beijing 100048, China
*Corresponding author

***Abstract*—The security problem of network devices and terminals has been attracted much attention. Many experts and scholars have done a lot of research on this. Based on the TNC three elements and three layers architecture, a new scheme about the network device and terminal connection and authentication is proposed, and the feasibility of the case is verified by experiments.**

Keywords—trusted network; device authentication; terminal authentication

I. RELATED WORK

In recent years, a lot of experts and scholars have invested a lot of energy in the research of network security. Paper [1] Propose an authentication scheme which can extend authentication capacity at the application boundary security device. It solves the problem such as passive attack. That is existed in the current password-based authentication schemes at the application boundary security devices like Socksv5 servers. Paper [2] analyses descriptors of USB mass storage device, proposes a concept of USB mass storage device identity key, performs authentication of the mass storage device identity key in database and accomplishes the method of control USB mass storage device to access to host computer. Based on security management requirement of classified storage media, paper [3] discusses the necessity to make use of unique identification on removable storage device. In order to achieve a more secure and reliable unique identification of removable storage device, the unique identification management technique of removable storage device is studied. Paper [4] proposes a credible certification model based on trusted computing. Though computing and evaluating security state of current network users, using the corresponding access control policy, we can identify the credibility of the network user, which ensure the security of user access. Paper [5] provides the idea which is recording and controlling of action. Besides conventional identity certification, certification and access control base on behavior creditability control the actions of entities by its action creditability. The action creditability is obtained by inspecting, scoring and recording the behaviors of entity. In paper [6], according to the standards of the trusted computing group, based on the analysis for the traditional identity authentication, a new identity authentication, called the Trusted Login Authentication Based on TPM (TLABT), has been put forward, which can be realized by the TPM which stores the users identities and the key, and guarantee the authenticity of the user identity.

II. TRUSTED AUTHENTICATION

A. *Trusted authentication protocol for network device and terminal*

Figure I shows the trusted authentication process for network device and terminal.

The trusted authentication process for network device is represented by a solid line

(1) Switch A sends EAPoL-Start packets to switch B.

(2) Switch B sends an EAP-Request/Identity message to switch A for the identity information.

(3) After receiving the message, switch A sends the user name and password to B according to the request of switch B.

(4) Switch B forwards the information sent from Switch A to the trusted authentication server.

(5) The trusted authentication server compares the user name and password sent from Switch B with the pre-stored reference values on the server. If they are consistent, it sends a Challenge value to switch B.

(6) Switch B passes the encrypted MD5 -Challenge value to switch A and requires switch A to provide more authentication information.

(7) After receiving the message from switch B, switch A provides the TCM EK value according to the requirements of the trusted authentication server, and sends the MD5-Challenge value to switch B.

(8) Switch B forwards the above information to the trusted authentication server. The server has responsibility to judge.

(9) During several times interaction, if the device meets the requirements of the trusted authentication server all the time, the trusted authentication server sends a Radius-Access -Accept message to the switch B.

(10) Switch B informs switch A and allows it to access the network.

The trusted authentication process for terminal is represented by a virtual line

(1) Switch B sends EAPoL-Start packets to PC.

(2) PC sends an EAP-Request/Identity message to switch B and requests to the authentication.

(3) After receiving the message, switch B sends the

EAP-Response to PC for the identity.

(4) Switch B forwards the information sent from PC to the trusted authentication server.

(5) The trusted authentication server compares the user name and password sent from Switch B with the pre-stored reference values on the server. If they are consistent, it sends a Challenge value to switch B.

(6) Switch B passes the encrypted MD5 -Challenge value to PC and requires PC to provide more authentication information.

(7) After receiving the message from switch B, PC provides the TCM EK value according to the requirements of the trusted authentication server, and sends the MD5-Challenge value to switch B.

(8) Switch B forwards the above information to the trusted authentication server. The server has responsibility to judge.

(9) During several times interaction, if the device meets the requirements of the trusted authentication server all the time, the trusted authentication server sends a Radius-Access -Accept message to the switch B.

(10) Switch B informs PC and allows it to access the network.

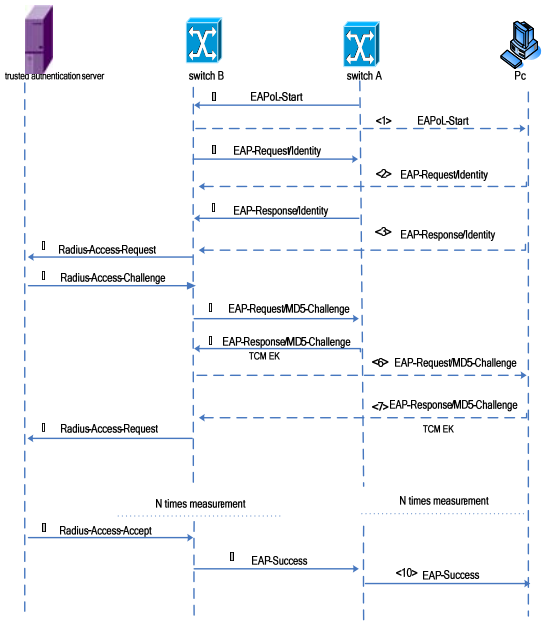

FIGURE I. AUTHENTICATION PROCESS

B. Trusted authentication process

Trusted networks should not only consider local authentication, but also cascading -security, and hierarchical relationship security. The way of traditional centralized authentication brings great pressure to main servers. The way of distributed authentication has no hierarchical relation between devices. In this paper, we design an authentication method to meet the authentication requirements of cross-domain devices. Figure II is the network topology diagram.

In cross-domain authentication, the entire network is divided into three levels .which is shown in Figure III. According to the domain' level, the top-level domains are located in the first-tier cities, the first-level domains are located in the second-tier cities and the second-level domains are located in the third-tier cities. They connect through the WAN. All the switches, except theses connecting to WAN, need to be creditable.

Trusted authentication server, located in the highest level network domain is regarded as the most credible one. This server is the trusted root of the entire network. Trusted authentication servers in other domains must register and authenticate from this trusted roots. After the authentication is completed, the server opens the corresponding cascade port so that it can connect to the devices and terminals in other domains. Every trusted authentication server saves the authentication information of all the devices and terminals in the network. The root trusted authentication server specifies the priority of every trusted authentication server. Usually every trusted authentication server is only responsible for authenticating the network devices under its jurisdiction. As the procedures ③ —>② —>① of second-level domain in following Figure. The unauthenticated switch provides its authentication messages to the trusted authentication server through the authenticated switch. If the server in the local domain is faulty, as shown in step (4), the switch requests authentication from the trusted authentication server in the upper-level domain.

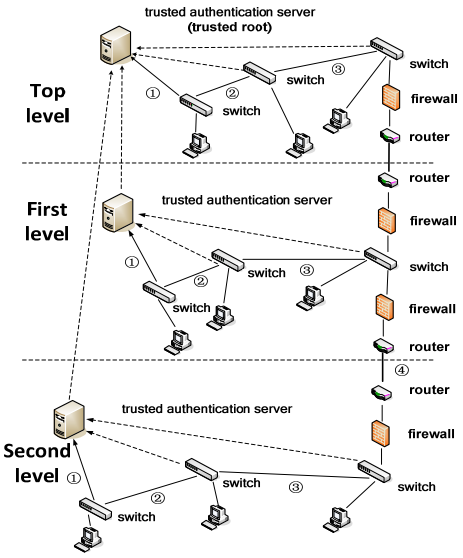

FIGURE II. NETWORK TOPOLOGY DIAGRAM

III. EXPERIMENTS AND EVALUATION

In order to evaluate the authentication method, considering the occupancy of system resources caused by trusted authentication on devices and terminals, the memory occupancy rate and CPU occupancy rate are compared and tested before and after performing network authentication. It is

shown as FIG.III and FIG. IV

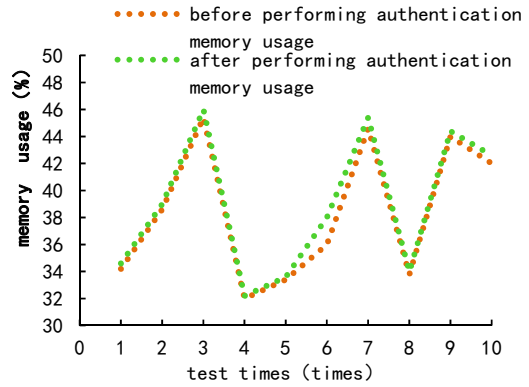

FIGURE III. MEMORY USAGE

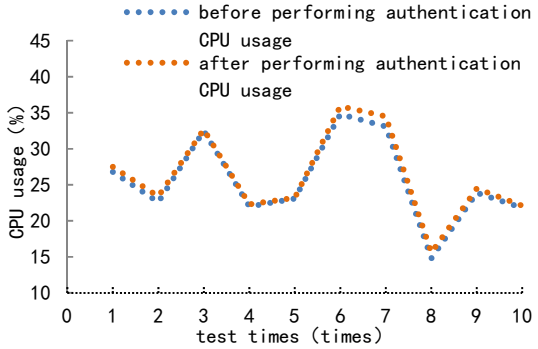

FIGURE IV. CPU USAGE

As shown in the picture, we test the usage rate of the CPU and memory. Taking the whole data into account, trusted authentication impacts little on consumption of system resource.

IV. Conclusion

With the increasing use of networks, it is becoming more and more important to guarantee the security of the network access. Based on traditional trusted networks, the design of trusted network construction under wide-area network environment is proposed and verified experimentally in this architecture. The impact on the performance of the computer is relatively small, and it can meet the needs of securely and efficiently connecting network devices and terminals to the network.

Acknowledgement

We are grateful for the supported by The National Natural Science Fund of China (61702020), Beijing Natural Science Foundation (4172013).

Reference

[1] Shuanghe Peng, Zhen Qin, Changxiang Shen. A Way to Extend the Authentication Capability of Application Boundary Security Device [J]. Journal of Beijing Jiao tong University, 2004, 28(5):6-10.

[2] Huabing Chen, Fusheng Zhang, Youjie Zhang. Implementation of Authentication Method to USB Mass Storage Device Identity [J]. Computer development and Application, 2008, 21(9):47-49.

[3] Hongqi Liao, Jie Ling, Yanjun Hao. Study on unique identification methods of USB removable storage device [J]. Computer Engineering and Design, 2010, 31(12): 2778-2780.

[4] Wei Li, Shibin Zhang, Yujun An. A Trusted Certification Model Based on Trusted Computing [J]. Computer Security, 2011(3): 29-31.

[5] Hongmei Liao,Qianping Wang, Guoxin Li. Certification and access control based on creditability in grid[J]. Computer Engineering and Design, 2007, 28(6): 1306-1308.

[6] Liang Tan, Mingtian Zhou. Design and implementation of a trusted login authentication project based on the trusted platform module [J]. Computer Applications, 2007, 27(5):1070-1072.