National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 453-457

Secure framework for administrator authentication in UTM system

[1] Pradeep Gupta, [2] Ravi Singh Pippal
[1] MITRC Alwar, Rajasthan, India
[2] VIT, RKDF University, Bhopal, Madhya Pradesh, India

Abstract
Unified Threat Management (UTM) solution has evolved from traditional firewall and VPN appliances to offer anti-virus capability, e-mail spam filtering, web content filtering and IDS/IPS in one pack. As it is accessible solely to the administrator, strong authentication mechanism is required to ensure the identity of administrator before performing any operation. Traditional single factor authentication depends on user's knowledge of some secret i.e. a password or a PIN. However, it is not secure enough. Two factor authentication is one which can be used as strong authentication scheme. This paper proposes secure framework using smart card to ensure UTM administrator's identity. It sorts out all the essential requirements that have to be achieved.

Keywords: cryptography, mutual authentication, password, smart card, UTM

Introduction

The concept behind mixing of multiple features into one system is that it is easier to set and maintain policy on a single system than on several systems that are deployed at a similar location. A typical unified threat management (UTM) [1] system encompasses a firewall, sensing and blocking of suspicious network probe, malware detection, etc.

- The main advantage of UTM is the undeniable fact that numerous necessary functions are combined into one box.
- Maintaining network security is usually become complicated. However when all the security features are pooled into a single system, it is simple to ascertain how all the functions are integrated and the way they work together. The basic network architecture without or with UTM system is shown in Fig. 1(a) and (b) respectively.

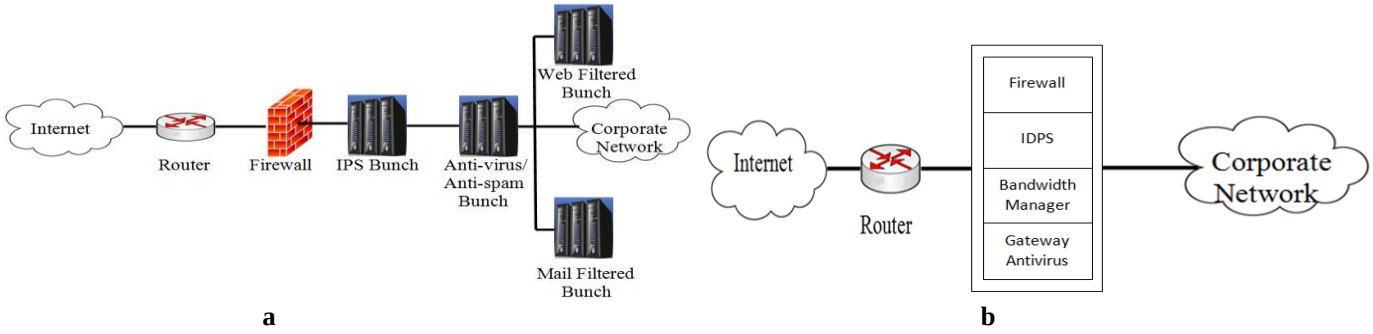

Fig 1: (a) Network without UTM (b) Network with UTM

The administrator accesses the UTM device within the LAN as well as WAN by entering the IP address of it in web browser and then credentials to prove the identity. Any remote access over untrusted networks to the UTM for administration ought to use strong authentication. Two-Factor authentication [2] is a better option using password as one and smart card as other factor. Smart card is a tamper resistant integrated circuit card with memory to store personal information and a processor capable of performing computations [3]. Considering the essential security necessities, this paper proposes secure framework to ensure UTM administrator's identity. The security of the proposed work relies on two factors; password as one and smart card as the other. It increases the security by providing two factor authentication as a replacement for simple password based authentication.

The remainder of this paper is organized as follows. Section 2 discusses the requirement for identification, authentication and authorization. Section 3 portrays authentication in current UTM appliances. The previous work related to UTM system is explored in section 4. Section 5 discusses the proposed smart card based secure framework to ensure UTM administrator's identity along with all the essential requirements (ER) that need to be fulfilled. Finally, section 6 concludes the paper.

Requirement for Identification, Authentication and Authorization

With the fast development of computer networks, several activities like online-shopping, online-banking, etc. are conducted over it. In a decentralized environment where a network is a heterogeneous collection of computing platforms, the primary issue is to provide access to services in such a way that only authenticated subjects (user, program, or process) having appropriate privileges can gain access to these services. It raises the problem of proper identification, authentication and authorization. Identification refers to the task of assigning a unique identifier to each and every subject. It is the prime step and might be provided with the utilization of a username or account number.

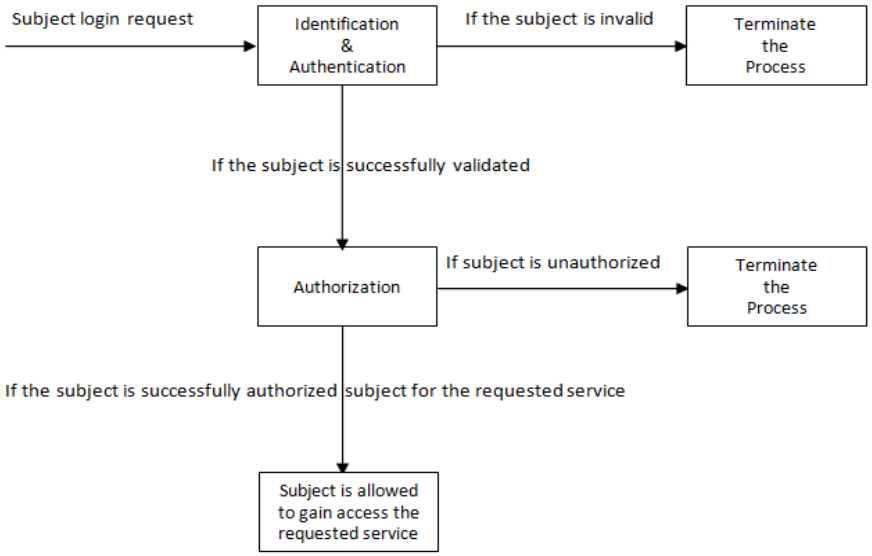

Fig 2: Identification, Authentication and Authorization

Authentication refers to the verification of the credentials (a password, a cryptographic key, personal identification number (PIN), etc.) presented by a subject through login request to the system. It is a way designed to prove the identity of one entity with another entity. The entity whose identity has to be proved is known as the claimant; the party that tries to prove the identity of the claimant is known as the verifier. The verification can be done in three ways; subject is aware of something, subject possesses something and subject inherits something. Strong authentication contains two out of these three ways (Two Factor Authentication). If identification and authentication credentials match the stored information in the system, the subject is authenticated.

After successful authentication, the system has to confirm whether the requested subject is permitted to access the particular resource. The decision of whether or not to allow subjects to access some resource relies on access criteria like role, group, location, time and transaction types. Access control assumes that the authentication of the subject has been successfully done before enforcement of access control. Read (R), Write (W) and Execute (X) are the three basic forms of access permissions.

As shown in Fig. 2, identification and authentication are initiated by a login request from a subject. The subject provides the credentials to pass the identification and authentication phase. If the subject is invalid then the entire process will be terminated otherwise the system checks the access privileges for the subject. If the subject is successfully authorized for the requested service then the subject will be permitted to gain access to the requested service. If not, the process will be terminated.

Authentication in UTM

Since emerged in 2004, UTM has gained popularity. Current UTM vendors include: Check Point, Cisco Systems, FortiNet, Juniper, Endian, Net Defend, Secure Computing, Sonic Wall, Symantec, Gaj Shield, ZyXEL, Cyberoam, Netgear and Netasq. Authentication is the act of confirming the identity of an individual or an entity. The standard way of user authentication in UTM is password based authentication. It relies on user accounts stored in a local user database but can also access credentials from external authentication servers like Lightweight Directory Access Protocol (LDAP) authentication server, Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control Service (TACACS, TACACS+), Microsoft Internet Authentication Service (MIAS), Microsoft Windows NT Domain authentication server and Microsoft Active Directory authentication server. UTM first checks the local user database for the user credentials. If the user account is not present, UTM connects to an external authentication server and communicate using any of Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAP v1) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication schemes.

Communications between UTM appliances and administration tools are primarily based on any of the two exchanges: Response only (PAP) and Challenge-Response (CHAP, MS-CHAP v1, MS-CHAP v2). In response only, user enters username and password at its terminal and sends it to UTM appliance for authentication. If the authentication succeeds

after verifying the credentials either from local user database or from external authentication servers, the user will receive a confirmation message. While in case of challenge-response, user enters username and password at its terminal to trigger the challenge code. UTM sends a challenge code to the user. Once the challenge code is received, user responds with a value calculated using a one-way hash function as a response code. UTM verifies the response code against its own calculated hash value. If the values match, the authentication is acknowledged; otherwise the connection must be terminated. There is a 3-way handshaking between user and the UTM appliance.

Nevertheless, these authentication schemes do not seem to be secure enough [4-6]. As a single layer of password protection merely is not enough, there is an alternative to increase security i.e. Two-Factor authentication. It is provided by the utilization of password and user's registered phone or email to receive the dynamic one-time password (OTP). OTP is a multiple digit authentication code that is valid for only one login session and sent to the user's mobile device or emailed. Now, suppose an unauthorized user has access to the user's computer, proper authentication cannot be achieved even though the correct password is supplied. After remote users or administrators enter their regular user name and password, they have to enter one-time password into the login interface. It provides further security.

However, sending a one-time password or authentication code by SMS text message is not secure enough because they are often sent in clear text. Mobile phones are simply lost and stolen and if another person has possession of the user's phone, the result could be more hazardous. SMS text messages can even be intercepted and forwarded to a different phone number, allowing an unauthorized user to receive the authentication code. As unauthorized users increasingly target mobile authentication methods and intercept SMS text messages, it will be crucial to use a more secure approach rather than sending an authentication code as a plain SMS text message.

Previous work related to UTM

UTM is a term coined by Charles Kolodgy of International Data Corporation. The desired requirements of UTM system include cost effectiveness, simple to use, scalability, interoperability, efficiency, consistency and obviously, security. However, most existing UTM systems operate by just combining together variety of security applications operating alone without system level optimization. In order to optimize the performance of UTM system at both algorithmic and architectural aspects, a generic framework has been proposed [7] by employing the concept of Integrated Protocol Processing (IPP). They claimed that their proposed scheme resolves the difficulty of redundant packet classification and unnecessary deep inspection. By combining trusted network connect (TNC) and UTM, Deng *et al*. [8] recommended TNC-UTM, a holistic solution to secure enterprise networks from gateway to endpoints and save the computing and communicating resources of UTM. In order to limit the unauthorized access to sensitive server resources, role based access control (RBAC) mechanism has been imposed. However, it fails to cover the whole resource access control process [9].

To beat this drawback, Liu *et al*. [9] proposed a unified network access control (UNAC) design which incorporates the network access control, network security mechanism and system access control through the trust degree. To attain high performance network processing, an extensible open-architecture services platform (OASis) has also been proposed which gives multiple network security services, together with stateful firewall, virus scanning and intrusion detection [10]. Chao *et al*. [11] gave an integrated protocol processing scheme by optimizing the security applications at the system level. To realize essential requirements like simple to use, scalability, interoperability, efficiency and consistency, Zhang *et al*. [12] proposed UTM control mechanism (UTM-CM).

Throughout the literature, administrator authentication in UTM systems is not properly mentioned. This paper proposes smart card based secure framework to ensure UTM administrator's identity. Authentication schemes based on smart card usually consist of three phases namely; registration phase, login phase and authentication phase. The registration phase is invoked whenever new user registers in the server. Upon receiving the registration request, server issues a smart card to the user by storing the necessary parameters into smart card memory. The login phase and authentication phase are invoked at the time when user login into the server. After receiving the login request, server checks the validity of the login request to authenticate the user. In this context, Chang and Wu [13] first proposed password based smart card authentication scheme without verification table in order to resist all the potential attacks on the verification tables. Subsequently, authentication based on smart card has been employed continuously in several applications like cloud computing [14], healthcare [15], key exchange in IPTV broadcasting [16], wireless networks [17], authentication in multi-server environment [18], wireless sensor networks [19] and many more.

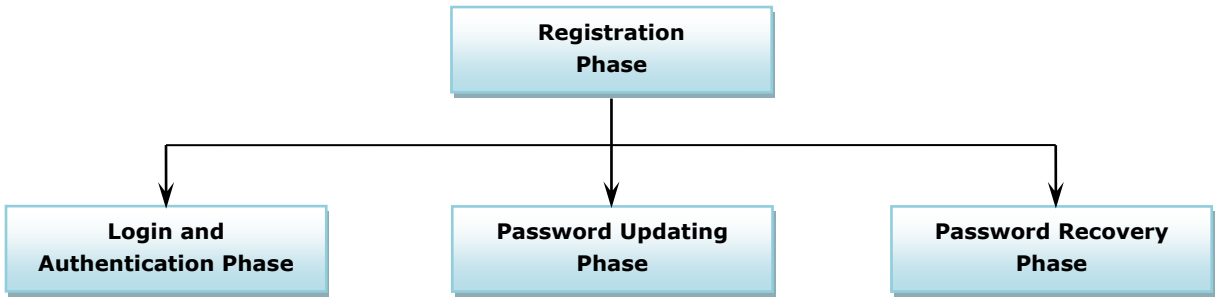

Fig 3: Different phases in the proposed framework to ensure UTM administrator's identity

Proposed Secure Framework using Smart Card to ensure UTM Administrator's Identity

This section discusses the proposed secure framework using smart card to ensure UTM administrator's identity. It consists of four phases: Registration phase, Login and Authentication phase, Password Updating phase and Password Recovery phase (as shown in Fig. 3).

Registration Phase

In the registration phase, administrator (UA) chooses its own identity and password. He or she then submits the credentials to the UTM device (UD) over a secure channel. Upon receiving the registration request, UD computes the necessary parameters and issues a smart card over secure channel to UA by storing these parameters into smart card memory.

ER1: It is difficult to memorize the system generated passwords. Hence, the scheme must provide the facility to choose the password.

Login and Authentication Phase

Fig. 4 gives you an idea about the activities and actions performed during login and authentication phase. In this phase, UA inserts the smart card and keys in its own credentials to the terminal. The terminal verifies the authenticity of the inputted credentials corresponding to the data stored inside the smart card memory. If it finds true, UA is the legitimate bearer of smart card; otherwise rejects the login request.

ER2: To check whether or not the requested entity is a legitimate bearer of smart card, entered identifier as well as the password must be verified at the terminal level prior to login request creation to avoid unnecessary burden on UD.

After verifying the authenticity of requested entity, the terminal prepares the login request, say M_1, using the entered credentials and data stored in the smart card memory. The terminal sends the login request M_1. Upon receiving, UD first checks the validity of UA's identity contained in M_1 to accept/reject the login request. If it holds, UD verifies the authenticity of M_1 using its own secret key rather than stored credential information about UA in the database.

ER3: Maintaining credential information about UA in the database must be avoided. UD has the ability to verify the authenticity of UA's login request using its own secret key.

Once succeeded, UD computes the session key (SK), creates the response message M_2 and sends it to the terminal. After getting M_2, terminal verifies SK received in M_2. If it holds, UD is authentic otherwise terminates the session. Subsequently, terminal uses SK, prepares the message M_3 and sends it to UD. Once received, UD verifies SK received in M_3. If it holds, mutual authentication is achieved between UA and UD.

ER4: It is necessary that not only UD verifies the authentic UA, but UA also need to verify the identity of the authentic UD in order to achieve mutual authentication.

Now, both the parties agree upon a common shared session key SK for further communication.

ER5: Session key is used to secure the entire communication between the communicating parties (UA and UD) and it must be changed from session to session. Moreover, it must support perfect forward secrecy (PFS) which tells that even though the current session key is revealed it does not facilitate the attacker to compromise the session keys of earlier sessions.

Password Updating Phase

This phase is invoked when UA wants to change the password. UA inserts the smart card and keys in its own credentials to the terminal. The terminal verifies the authenticity of the inputted credentials corresponding to the data stored inside the smart card memory. If it finds true, UA is the legitimate bearer of smart card; otherwise rejects the password update request.

ER6: Before updating the password, entered identifier as well as password must be verified at terminal level to check whether or not the requested entity is a legitimate bearer of smart card.

After verifying the authenticity of requested entity, the terminal prompts UA to enter a new password. UA enters new password and the terminal updates the data stored in the smart card memory without any assistance from UD.

ER7: To extend efficiency, password must be changed freely at any time without any interaction with UD, the server or the verifier.

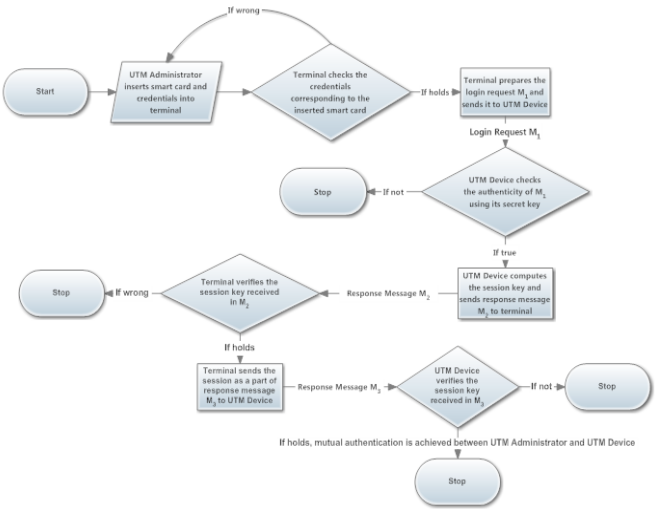

Fig 4: Flow diagram of proposed login and authentication phase

Password Recovery Phase

An ideal password based scheme must support easy and effective recovery or reset of forgotten passwords. If the password recovery procedure is easy and adequately safe, it provides a basis to select strong passwords without the headache to memorize them. Basically, the forgotten password is recovered in two ways; enable the existing password to be recovered or require a new one to be set. From a security perception, resetting the password is preferable rather than revealing the existing one.

This phase is invoked when UA wants to recover the forgotten

password. In this phase, UA inserts the smart card to the terminal and presents its identity. The terminal prepares password recovery request using UA's identity and stored data in the smart card memory and sends it to UD. Upon receiving, UD checks the authenticity of the request using its own secret key. If it holds, UA is the authorized owner of smart card. UD sends the response message to the terminal. Once the message is received, the terminal verifies the legitimacy of UD. If successful, UA is prompted to reset his/her old password by entering a new password. After getting the new password, the terminal updates the data stored in the smart card memory.

ER8: UA can reset the forgotten password by proving his/her identity to UD.

Conclusion

Unified Threat Management (UTM) is a complete solution that has recently come out in the network security industry and has gained widespread popularity. It allows the administrator to monitor the network and performance of the UTM device through a single management console. Hence, a strong authentication scheme is needed to ensure the UTM administrator's identity. Today, numerous advanced authentication measures like smartcards, biometrics and software based mechanisms are designed to defy the weaknesses of traditional password based authentication schemes. This paper proposes smart card based secure framework to ensure UTM administrator's identity. Moreover, it lists out all the essential requirements that need to be fulfilled. Through this framework, UTM device efficiently verifies administrator's identity prior to granting the privileges to manipulate any security policy or component of a UTM system. Further, it listed out eight essential requirements (ERs) that have to be achieved. These issues are definitely helpful for the researchers who are working in this direction or some other adjacent directions.

References

1. Stevens M. UTM: one-stop protection. Network Security. 2006; (2):12-14.
2. http://en.wikipedia.org/wiki/Two-factor_authentication.
3. http://en.wikipedia.org/wiki/Smart_card.
4. Krahmer S. Cheating CHAP. 2002, 1-7. http://dl.packetstormsecurity.net/groups/teso/chap.pdf.
5. Schneier B, Mudge. Cryptanalysis of microsoft's point-to-point tunneling protocol (PPTP). In Proceedings of the ACM Conference on Computer and Communications Security, San Francisco, CA, USA. 1998, pp. 132-141.
6. Schneier B, Mudge, Wagner D. Cryptanalysis of microsoft's PPTP authentication extensions (MS-CHAPv2). In Proceedings of the International Exhibition and Congress on Secure Networking, CQRE (Secure)'. 1999; 99:192-203.
7. Qi Y, Yang B, Xu B, Li J. Towards system-level optimization for high performance unified threat management. In Proceedings of the 3rd International Conference on Networking and Services. 2007, pp. 7-7.
8. Deng F, Luo A, Zhang Y, Chen Z, Peng X, Jiang X, Peng D. TNC-UTM: a holistic solution to secure enterprise networks. In Proceedings of the 9th International Conference for Young Computer Scientists. 2008, pp. 2240-2245.
9. Liu Y, Zhang H, Zhang L, Zhao B. Research on unified network access control architecture. 2009; I:295-299.
10. Qi Y, He F, Wang X, Chen X, Xue Y, Li J. OASis: towards extensible open-architecture services platforms. Symposium on Architecture for Networking and Communications Systems. 2009, pp. 66-67.
11. Chao Y, Bingyao C, Jiaying D, Wei G. The research and implementation of UTM. IET Conference Publications. 2009, pp. 389-392.
12. Zhang Y, Deng F, Chen Z, Xue Y, Lin C. UTM-CM: a practical control mechanism solution for UTM system. In Proceedings of the WRI International Conference on Communications and Mobile Computing. 2010, 86-90.
13. Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proceedings E: Computers and Digital Techniques. 1991, 138:165-168.
14. Pippal RS, Jaidhar CD, Tapaswi S. Enhanced time-bound ticket-based mutual authentication scheme for cloud computing. Informatica. 2013; 37(2):149-156.
15. Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards and Interfaces. 2010; 32(5-6):274-280.
16. Pippal RS, Jaidhar CD, Tapaswi S. Secure key exchange scheme for IPTV broadcasting. Informatica. 2012; 36(1):47-52.
17. He D, Ma M, Zhang Y, Chen C, Bu J. A strong user authentication scheme with smart cards for wireless communications. Computer Communications. 2011; 34(3):367-374.
18. Pippal RS, Jaidhar CD, Tapaswi S. Robust smart card authentication scheme for multi-server architecture. Wireless Personal Communications (Springer). 2013; 72(1):729-745.
19. Fan R, He DJ, Pan XZ, Ping LD. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. Journal of Zhejiang University-SCIENCE C (Computers and Electronics). 2011; 12(7):550-560.