Centralized Network Security Model Using Dynamic Vlan and Client Authentication

Liberios Vokorokos, Martin Chovanec, Ondrej Látka, Juraj Halász

Department of Computers and Informatics, Technical University of Košice
Letná 9, 042 00 Košice, Slovakia
Liberios.Vokorokos@tuke.sk, Martin.Chovanec@tuke.sk, Ondrej.Latka@tuke.sk

Abstract: Computer networks noticed the great progress and an application extension in the last decades. In the present the quantum of the data is transferred via computer networks. These data are critical from point of the confidentiality and the properly delivery only to the authorized clients. In terms of the security it is needed to refer on high security interaction in the computer networks from the lowest level, that means from the clients. Authorized client communicating in the network must possess essential authentication requirements represented by authentication conditions before connecting into the network. Intruder or client not connected in the computer network can not cause network problem or eventually obtain information, which are not assigned by him. Division network to the individual circuits provide logical users partition into groups, in which they can communicate. To provide clients mobility is needed to solve assigning dynamically and also ensure centralized service management. This article describes network models, security protocols providing primary protection and suggestion of their combination for network security model fulfilling mobility conditions (dynamic VLAN) and clients verification (protocol 802.1x). Security analysis provides information about protocol defections that are needed to consider and include their countermeasure in the real computer network model implementation.

Keywords: computer network security, dynamic virtual networks, VLAN, 802.1x, RADIUS, client authentication, access verification

1 Introduction

Computer security is a field of computer science concerned with the control of risks related to computer use. Rapidly evolving technological world is always more dependent on computer networks. In the present computer networks have key position in many communication services. Computer network security is necessary to understand not as stabilized state but as a continuous process which is necessary to improve. For this reason it is important constantly review the

security, reliability of computer networks and then reacts on identified problems. Computer network is possible to use as unauthorized and so cause for example destruction of the constructed computer systems or perform other violations towards persons' privacy. In the present information era is necessary to provide quick access to information and their availability from any place. For that purpose they are used different distributive channels giving possibility to spread information. Computer network is so secure as its the weakest part; therefore it is necessary to choose components and arrangements concerning on the restrictions of the particular network elements. Designed network model increases the stations mobility, virtual circuit security in local area networks forcefully on centralized management and authentication. Mentioned safety model is a part of the research executing on Department of Computers and Informatics in connection with the infrastructure created for electronic education and students network connectivity extension on the ground of the Technical University in Košice. This project is linked with the performing VEGA 1/1064/04 research project, which includes distributed and parallel systems research utilizing computer networks as transport medium. This communication is equally sensitive to secure data transmissions.

2 Characteristics of Used Model and Authentication Protocol

2.1 Dynamic Virtual LAN

ID	VLAN	MAC address
1	1	00:0A:CD:FA:DA:CA
2	4	00:01:AD:CA:AA:BC
3	4	01:0A:AC:A1:CC:BA
4	5	02:0B:CC:DA:0C:CA
5	5	00:11:AA:CA:DA:BA
6	1	01:0C:0A:AA:DA:BC

Figure 1
VLAN-to-MAC address mapping

Dynamic VLANs were introduced to grant the flexibility and complexity that Static VLANs did not provide. Dynamic VLANs are quite rare because of their requirements and initial administrative overhead. Therefore most administrators and network engineers tend to prefer Static VLANs. Dynamic VLANs, as opposed to Static VLANs, do not require the administrator to individually configure each port of network device. For this purpose is designed central server called the VMPS (VLAN Member Policy Server). VMPS is utilized for automatic configuration device port providing connection into participating on the VLAN network. The VMPS server contains a database of all workstation MAC addresses with the associated VLAN and this way occurs required VLAN-to-MAC address mapping (Figure 1). Following this statement is possible that server identified connected device and consequently

assign him access into desired virtual circuit. Basic restriction of present model is problem with connection several client at the same time on one device port in dynamic mode. In this case system can't divide clients into corresponding VLANs and therefore supports only one virtual network on one device port. Important attribute is possibility of "fallback" VLAN, which supports classification unregistered address for visitors, where retrieval and registration MAC address would be difficult. In case lower security dynamically assigned VLAN is required to deal with protocols for securing networks and authentication on client side [6], [3].

2.2 Protocols 802.1x and RADIUS

802.1x is standard for port-based Network Admission Control, part of the IEEE 802 (802.1) group of protocols. Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases which the authentication and authorization fails. It is based on the EAP, Extensible Authentication Protocol. The authentication is usually done by a third-party entity, such as a RADIUS server. This provides for client-only authentication, or more appropriately, strong mutual authentication using various protocols. EAP is an authentication framework, not a specific authentication mechanism. The EAP provides some common functions and a negotiation of the desired authentication mechanism. EAP did not provide single verification, but open transport mechanism for authorization systems. With EAP standardization was simplify compatibility various systems and producers. Advantage of protocol 802.1x is the possibility of integration into startup process, which allow to verify device identity, before active connection into computer network (Figure 2). Verification includes main encryption, where client and device communicating through cipher text protocols [9], [7].

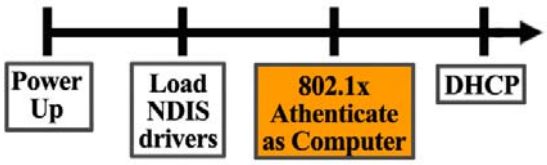

Figure 2
Integration 802.1x into OS

RADIUS (Remote Authentication Dial In User Service) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or computer mobility. When client connects into computer network, must enter your username and password. This information is passed to a Network Access Server (NAS) device over the EAP, then to a RADIUS server over the RADIUS protocol. Device supporting 802.1x authentication can be used

as NAS. The RADIUS server checks that the information is correct using authentication schemes. If accepted, the server will then authorize access. RADIUS is also distributed security system, which cover networks connection and network services towards unauthorized access. Include two component authentication server and client protocols. RADIUS is designed for simplification of security processes dividing their from communication technologies. All data about users and entry terms to network services are stored on authenticating RADIUS server. These data can be stored in various forms adjusting network requirements. Interaction protocol between client and server utilize UDP transport protocol. RADIUS packet structure in computer network is displayed on Figure 3 [5].

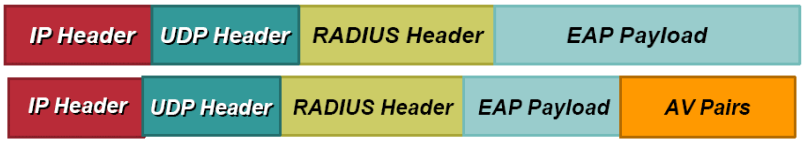

Figure 3

RADIUS packet structure, request and respond in computer network

Interaction principle begins from authenticator in our case device, which accepts request for connections into computer network from clients. Device creates "access-request" RADIUS packet, containing minimally user name and password. Packet identifier, generated also by client, is not defined by protocol and is implemented as single counter. Packet contains a 16 octet Request Authenticator in the authenticator field and this request is a randomly chosen 16 octet string. Outgoing packet is completely unprotected, except for the User-Password attribute. Password protection is based on following principle [4]:

$$
\begin{aligned}
c_1 &= p_1 \oplus MD5(S + RA) \\
c_2 &= p_2 \oplus MD5(S + c_1) \\
&\cdot \\
&\cdot \\
c_n &= p_n \oplus MD5(S + c_{n-1})
\end{aligned}
\qquad
\begin{aligned}
&\text{RA - request authentificator} \\
&c_1 \ldots\ldots c_n \text{ - ciphertext block} \\
&p_1 \ldots\ldots p_n \text{ - password broken into 16 - octet blocks}
\end{aligned}
\qquad (1)
$$

The client and server share a secret. That shared secret followed by the Request Authenticator is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the Request Authenticator. The User-password attribute contains $c_1+c_2+\ldots+c_n$, where + denotes concatenation. After the server receives the RADIUS access-request packet, authenticator device is verified thought address and secret password stored on server. If server does not possess a shared secret for the authenticator, the request is silently dropped. Because the server also possesses the shared secret, it can obtain the unprotected password through reverse

algorithm and using its authentication database validates the username and password. If the password is valid, the server creates an Access-Accept packet to send back to the authenticator. If the password is invalid, the server creates an Access-Reject packet. [3].

$$Auth = MD5(Code + ID + Lenght + \text{Re}questAuth + Atributes + Secret) \quad (2)$$

If authenticator received a response packet, it attempts to match it with an outstanding request using the identifier field. If the client received a verified packet, with correct login information, user computer is authenticated. [9], [1].

3 Security Model with Centralized Management

Standard use of dynamic VLAN model does not provide resistance towards disaffection MAC address of computer client. In local area networks operating on second layer OSI reference model this address is known from ARP (Address Resolution Protocol). This issue provides opportunity to attacker access into virtual LAN with higher priority or connecting in groups, that is not authorized communication. Resulting from definition of communication protocol it is possible to cipher MAC address because it is required for basic interaction and addressation of the clients in computer network. Choosing secure authentication form for clients it is needed for security assignation of dynamic VLANs. Authentication model using protocol 802.1x includes advanced authentication and encryption possibilities.

3.1 Proposal Model Using Dynamic VLANs and Protocols 802.1x, RADIUS

By using 802.1x, RADIUS server is able to send a series adjusting statements for authenticating component within AV response. According to IETF, RADIUS supports 92 basic and approximately 300 extensive attributes identified using key word or identification number. Besides User-Name" and "User-Password" concern us attributes like "Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id" for authentication process that supports dynamic VLAN configuration depending on user name and password. Important setting on authenticating device (in our case switch), is setting "guest VLAN" which present assignment unauthorized client for example into restricted network section. RADIUS protocol is possible simply append for additional attributes and variables then is needed only to provide their support by authorization devices. For authentication possibilities verification using RADIUS server and the 802.1x authorization for the network access within the research was chosen the following model situation.

Researched model include both main implementation methods in case of mobility dynamic VLAN and in case of security protocol 802.1x, but expects improvement

in centralized device management and security improvement at assigning dynamic circuits in computer network. Model suggest effective protocol combination to create model with higher security and mobility in computer networks.

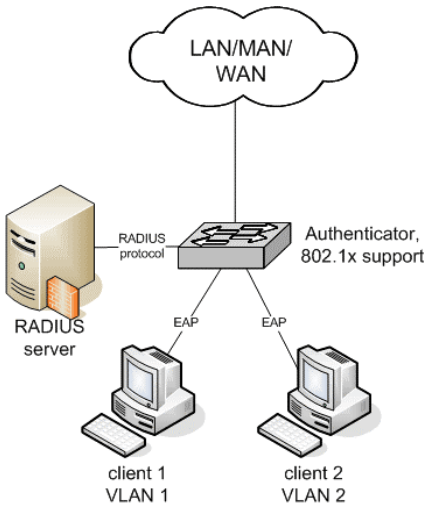

Figure 4
Experimental model situation

3.2 Security Analysis of Designed Model

The RADIUS protocol has a set of vulnerabilities that are either caused by the protocol or caused by poor client implementation and exacerbated by the protocol, on following theoretical protocol analyses is possible divide attacks into groups [2]:

- response authenticator based shared secret attack
- password attribute based shared secret attack
- password attribute cipher structure
- password based attack
- request authenticator based attacks
  - passive password compromise through repeated request authenticators
  - active password compromise through repeated request authenticators
  - replay of server responses through repeated request authenticators
  - DOS arising from the prediction of the request authenticator
- shared secret structure definition

Response Authenticator based Shared Secret Attack

The Response Authenticator is essentially an ad hoc MD5 based keyed hash. This primitive facilitates an attack on the shared secret. If an attacker observes a valid Access-Request packet and the associated Access-Accept or Access-Reject packet, they can launch an off-line exhaustive attack on the shared secret. The attacker can pre-compute the MD5 state for (Code+ID+Length+RequestAuth+Attributes) and then resume the hash once for each shared secret guess. The ability to pre-compute the leading sections of this keyed hash primitive reduces the computational requirements for a successful attack.

Password Attribute based Shared Secret Attack

Because of the selection of a stream cipher for protection of the User-Password attribute, an attacker can gain information about the Shared Secret if they can observe network traffic and attempt an authentication. The attacker attempts to authenticate to the client with a known password. The attacker then captures the resulting Access-Request packet and XORs the protected portion of the User-

$$c_n = p_n \oplus MD5(S + c_{n-1}) \quad (3)$$

Password attribute with the password they provided to the client. This results in the value of the MD5(Shared Secret + Request Authenticator) operation. The Request Authenticator is known (it is in the client's Access-Request packet), so the attacker can launch an off-line exhaustive attack on the shared secret. Note, though, that the attacker cannot pre-compute the MD5 state of the hash for the Request Authenticator, because the Request Authenticator is hashed second.

Password Attribute Cipher Structure

The User-Password protection scheme is a stream-cipher, where an MD5 hash is used as an ad hoc pseudorandom number generator (PRNG). The first 16 octets of the stream cipher display the same properties as a synchronous stream cipher. After the first 16 octets, the stream cipher state integrates the previous ciphertext, and becomes more accurately described as a self-synchronizing stream cipher. The security of the cipher rests on the strength of MD5 for this type of use and the selection of the shared secret. It is unclear what the requirements for this cipher are, so it is unclear if the MD5 function is appropriate for this use. MD5 is not designed to be a stream cipher primitive, it is designed to be a cryptographic hash. This sort of misuse of cryptographic primitives often leads to subtly flawed systems.

Password based Attack

The use of a stream cipher to protect the User-Password attributes results in a vulnerability that allows an attacker to circumvent any authentication rate limits imposed by the client. At first the attacker attempts to authenticate to the server using a valid username and a known (and likely incorrect) user password. The

attacker then captures the resulting Access-Request packet and determines the result of the MD5(Shared Secret + Request Authenticator) operation (in the same way as in the previous attack). The attacker can then replay modified Access-Request packets, using the same Request Authenticator and MD5(Shared Secret + Request Authenticator) value, changing the password (and the associated User-Password attribute) for each replay. If the server does not impose user based rate limits, this will allow the attacker to efficiently perform an exhaustive search for the correct user password.

Request Authenticator based Attacks

Passive Password Compromise through Repeated Request Authenticators

If the attacker can sniff the traffic between the RADIUS client and the RADIUS server, they can passively produce a dictionary of Request Authenticators, and the associated (protected) User-Password attributes. If the attacker observes a repeated Request Authenticator, they can remove any influence of the Shared Secret from the first 16 octets of the passwords by XORing the first 16 octets of the protected passwords together. This yields the first 16 octets of the two (now unprotected) user passwords XORed together.

The impact of this attack varies according to how good the user passwords are. If the users all chose random passwords of the same length, the attacker can gain nothing because no information about either password can be extracted. Unfortunately, this is a somewhat unlikely occurrence. In reality, users choose passwords of varying lengths (generally less than 16 characters) and of varying quality.

Active Password Compromise through Repeated Request Authenticators

The attacker can attempt to authenticate many times using known passwords and intercept the generated Access-Request packets, extracting the Request Authenticator and User-Password attributes. The Attacker can then XOR the known password with the User-Password attribute and be left with the MD5(Shared Secret + Request Authenticator) value. The attacker generates a dictionary of Request Authenticator values and associated MD5(Shared Secret + Request Authenticator) values.

When the attacker sees a valid Access-Request packet that has a Request Authenticator value that is in the attacker's dictionary, the attacker can recover the first 16 octets from the protected region of the User-Password field by looking up the associated MD5 (Shared Secret + Request Authenticator) value from the dictionary and XORing it with the intercepted protected portion of the User-Password attribute.

Shared Secret Structure Definition

The RADIUS standard specifically permits use of the same Shared Secret by many clients. This is a very bad idea, as it provides attackers with more data to

work from and allows any flawed client to compromise several machines. All RADIUS clients that possess the same shared secret can be viewed as a single RADIUS client for the purpose of all these attacks, because no RADIUS protection is applied to the client or server address. Most client and server implementations only allow shared secrets to be input as ASCII strings. There are only 94 different ASCII characters that can be entered from a standard US style keyboard (out of the 256 possible). Many implementations also restrict the total length of the shared secret to 16 characters or less. Both of these restrictions artificially reduce the size of the keyspace that an attacker must search in order to guess the shared secret.

3.3 Security Model Experimental Verification

On the base of this proposed model has been suggested topology for testing of computer network in laboratory condition of the Department of Computers and Informatics. Using experimental methods and presented attack methods were verified safety parameters of the designed model.

Verification of User Change Possibility after EAP Authentication

First situation represents connection of authorized client and its sequential authentication using login and password. This client is consequently authorized to communicate in computer network. Then situation is created when attacker disconnects authorized client and connects into his device port. In case of the physical clients changeover port is automatically switched into unauthorized state and communication is blocked. After this, request is transmitted for new client authentication.

Verification of User Change Possibility with Simultaneous Users Operation

In this experiment on device port with configured authentication 802.1x is connected other attacker device transparent to authentication protocol. In this device are connected both clients, where only one is authenticated (Figure 5).

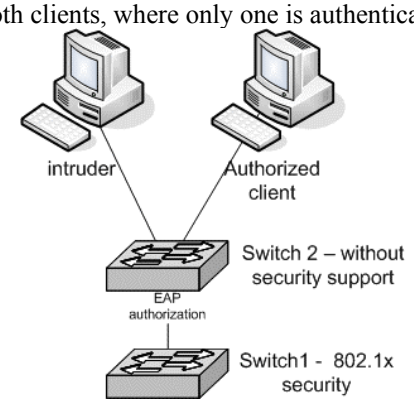

Figure 5
802.1x security verification against attacks

Authenticator device can be configured in two modes. Option hostmode multi allows attacker to access network if the authorized client is connected, when port is authorized supports several clients' communication. Option hostmode single is more secure and allows only one client to communicate on device port configured with authentication by 802.1x. In this experiment was attacker connected trough transparent device into authenticator followed with the network access attempt. Attacker connected into this network can not communicate, because one client is authenticated, only obtains data assigned to the authorized client. This data can be rerouted to intruder using ARP poisoning method. Intruder can communicate only in small segment of network created by transparent device.

Verification of User Change Possibility with Duplicate MAC Address Definition

Because authentication device is a network switch which operate on second layer OSI model, this experiment verify duplicate MAC address definition. This possibility is verified using previous network topology. Obtaining valid MAC address of authorized user is possible by monitoring network communication in segment. The prediction was confirmed and security device allowed intruder to communicate in computer network. Option "dot1x reauthetification" can be used for partial security improvement, which reauthenticates client in defined time intervals. If the authorized client switch's with the intruder, communication is restricted because it can't send login information.

Interaction Verification between Client and Authentication Device

In case of securing authentication is necessary to verify communication among the network devices during the authorization process. Using experimental methods are needed to obtain valid authentication information, which is transferred between clients. For this purpose is used classic method "man-in-the-middle" (Figure 6).

Collected data was using sniff software classified as protocol EAP.

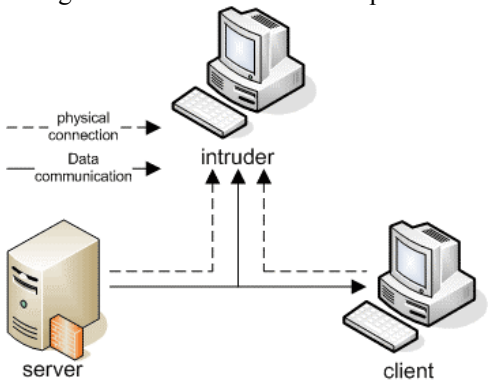

Figure 6

Man-in-the-middle attack

Communication process matches mentioned analyze and contains identification, verification, authorization and conclusion. During analyze of collected data security issue was discovered in authentication process. Communication between clients was unencrypted, exception is only the attribute containing user password. Intruder therefore can obtain useful information for authentication process. Password is not transferred via computer network only MD5 Challenge of this password is sent between client and authentication device. Low encryption of MD5 cipher is the reason why user password can be extracted from the challenge using brute force decrypting methods. Therefore is needed to choose stronger encryption method. Operating systems support stronger methods like PEAP and LEAP which encapsulate standard protocol.

Interaction Verification between Authentication Device and RADIUS Server

Authentication process security is similar like communication between client and authenticator. Identification and login information are transferred in plain form, which can be disaffected by potential attacker. Password is in base configuration transferred in MD5 challenge form (Figure 10).

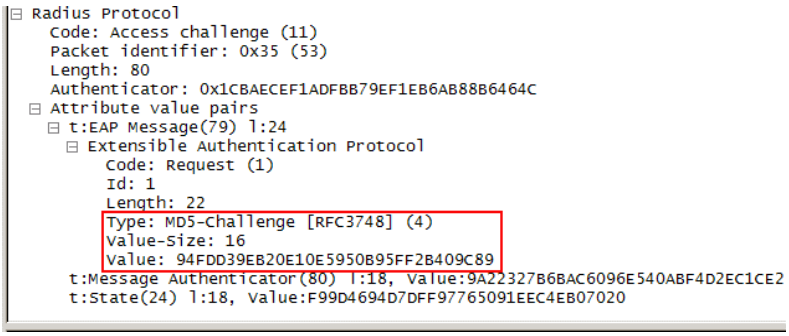

Figure 10
Password encryption in RADIUS protocol

Conclusions

Using experimental verification suggested security policy was revealed as adaptable for different computer networks. This security model includes high security level in case of connection of the client network. Suggested model, which is a part of research on Department of Computers and Informatics, is based on hardware network components. Hardware support makes model stable and high-performance. For implementation of protocol 802.1x authentication is needed support in hardware devices. Security of protocol 802.1x appeared to be resistant to disaffection of authenticating statements. Research expects one client connection on one device port, what eliminates possible security problems with MAC address authentication using base implementation of dynamic VLAN. Protocol is useful to implement on computer networks with requirement of clients mobility and for wireless networks. The RADIUS server has providing broad support for security devices as its centralized management.

The RADIUS protocol has several interesting issues that arise from its design. The design and policy characteristics, that seem to be principally responsible for the security problems, are needed to consider before its implementation. Because of these issues it is recommended to use separate segment for communication between authentication devices in implementation of the security model.

For extension of the implementation there can be applied additional authorization of RADIUS towards LDAP (Lightweight Directory Access Protocol) server, which provides superior password and access management. RADIUS protocol is in point of view less secure then evolving TACACS+ protocol, but provides wider device support and responses of parameters. Significant advance in this technology is possible to reach by modules creation, database connection improvement like LDAP for TACACS+ protocol. In case of possible client intrusion into authentication communication it is necessary to implement strong encrypting algorithms into communication protocols.

References

[1] Vokorokos, L.: Digital computers principles, Typotex Publish House, Budapest 2004, ISBN 9639548 09 X

[2] Prosise, C., Mandia, K.: Počítačový útok: Detekce, obrana a okamžitá náprava, Computer Press, Praha 2002, ISBN 80-7226-682-9

[3] Vokorokos, L., Jelšina, M.: Počítače základy technických prostriedkov, Mercury s.r.o., Košice 2004, ISBN 80-89061-90-7

[4] Wenstrom, M.: Zabezpečení sítí Cisco. Computer Press, Brno 2003, ISBN 80-7226-952-6

[5] Chapman, D., Fox, A.: Zabezpečení sítí pomocí Cisco PIX Firewall, Computer Press, Brno 2004, ISBN 80-722-6963-1

[6] Pružmanová, R.: TCP/IP v kostce, Computer Press, Brno 2004, ISBN 80-7232-236-2

[7] Kurz, G., McClure, S., Scambray, J.,: Hacking bez tajemství, 3. aktualizované vydanie, Computer Press, Brno 2004, ISBN 80-7226-948-8

[8] C. Rigney, Remote Authentication Dial In User Service (RADIUS), http://www.ietf.org/rfc/rfc2865.txt, Jún 2000

[9] B. Aboba, Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc3748.txt, June 2004

Supported by VEGA project No. 1/1064/04