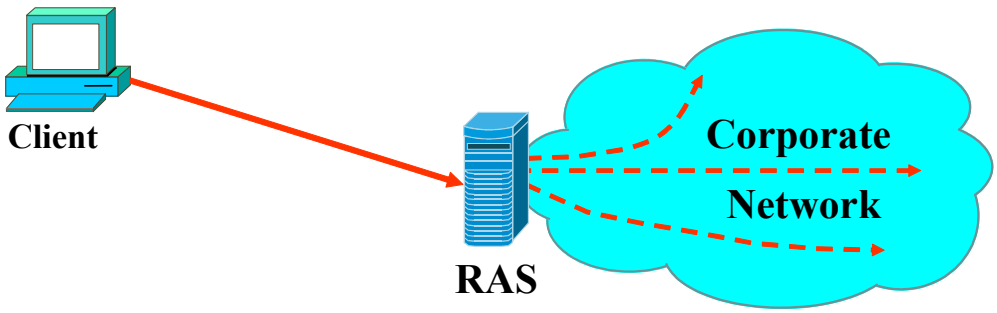
Bob's Authentication Overview

An overview of basic Network Authentication Concepts & Technology

Authentication – Objectives

- Describe the function of a Remote Access Server .
- Explain the role of authentication, authorization and accounting.
- List 3 popular methods for providing user authentication.
- Compare the use of PAP and CHAP as part of an authentication scheme.
- Identify 3 common authentication categories.

Remote Access Server (RAS)



- **Security is not just keeping the black hats out!**
- **Security is also about letting white hats in.**
- **RAS is used in dial-up networks.**
  - **Concepts also used to restrict access from Internet.**

Remote access servers (RAS)

Remote access servers (RAS) refers to the hardware and software used to connect dial up users to a LAN or the Internet. There are two main types of remote access servers: **File servers with dial in access** and **Dedicated dial in servers**.

A file server with dial in access uses the network operating system (NOS) of a PC or server. This feature is included in all modern operating systems and provides a very low cost way to implement a RAS. However, it is worth nothing that this capability can present a significant security risk on computers that have this feature enabled and are connected to a phone line and modem.

A dedicated dial in server has multiple modems, Network Interface Cards, and the software needed to dozens, hundreds, or even thousands of dial up calls.

RAS consists of a server and a client portion. The server authenticates the client and manages the connection. RAS provides mechanisms to protect a potentially insecure connection between server and client. To take full advantage of the RAS security functions, a RAS server must be used in conjunction with a RAS client. These mechanisms include authentication, encryption and dial-back functions.

Many of the concepts used in a RAS are in other authentication systems like RADIUS, TACACS+, and Kerberos.

Authentication, Authorization, Accounting (AAA)

- **Authentication:**
  - Who are you?
- **Authorization:**
  - Are you allowed to enter?
- **Accounting:**
  - What services did you use and for how long?

Authentication, Authorization, Accounting (AAA)

Authentication – In order to gain access to the network, users must prove that they are really who they say they are. Many systems use passwords and usernames authenticate to verify a users identity. Other authentication methods include biometrics and special keycards.

Authorization – Once access to the network has been gained, then "authorization" determines what the user is allowed to do, or what services the user has access to. For example: If a users dials into the network remotely and passes authentication, authorization could dictate what IP addresses the user has access to and what applications on those devices as well.

Accounting – In many networks it is important to keep track of what the user did, and when the services were used. Accounting uses start and stop messages to keep track of when a service was started and when it was terminated. Accounting records can can be used for billing, tracking individual/group usage, and for a security auditing purposes.

RADIUS

- **Remote Authentication Dial In User Service.**
- **Encrypts passwords:**
  - **Does not encrypt User ID, authorized services, or accounting info.**
- **Connectionless service (UDP).**
- **3 Components:**
  - **Radius Server**
  - **Client**
  - **Protocol**
- **RFC 2058.**

RADIUS

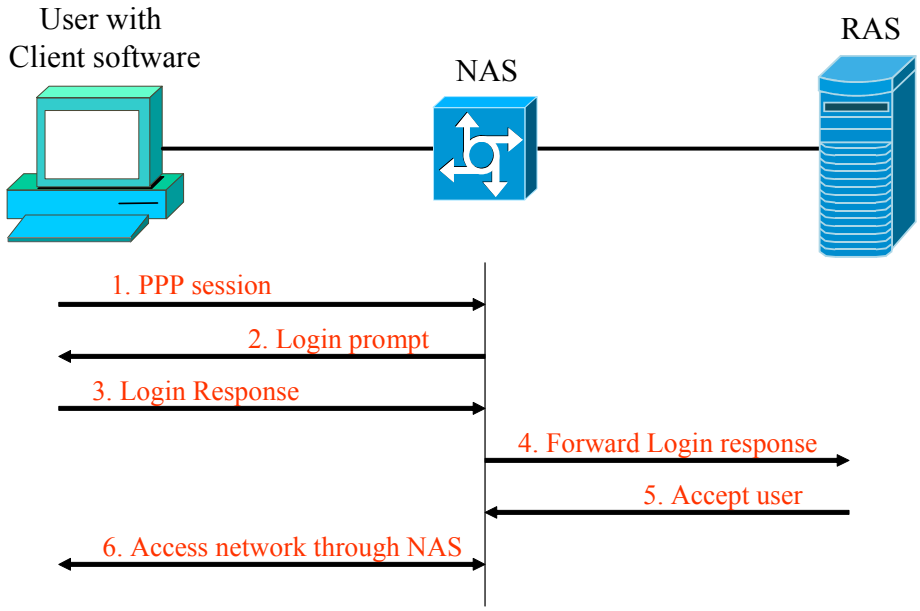
RADIUS (***R***emote ***A***uthentication ***D***ial-***I***n ***U***ser ***S***ervice) represents one mechanism for maintaining control over security for the large number of network access points.

RADIUS is a UDP-based protocol used to authenticate and authorization of users attaching to a network via remote access through Network Access Servers (NAS). It provides a standard mechanism for communications between the NAS and one or more centralized security servers responsible for authentication and authorization.

Livingston Enterprises (now part of Lucent Technologies) originally introduced RADIUS. It is now an Internet Engineering Task Force (IETF) standard (RFC 2058)

RADIUS is now a widely accepted protocol that has been adopted by a number of hardware and software vendors. RADIUS technology has likewise been extended to include a number of other functions in the "AAA services" (Authentication, Authorization, and Accounting) category.

RADIUS Process



RADIUS Process

A RADIUS system consists of a client with radius software, server responsible for authenticating users requesting network connection via a remote access device – typically this is a Network Access Server .

When the user connects through the Network Access Server (NAS), an authentication request is sent to the RADIUS server.

This authentication request message contains the name and password, as well as the identity of the access device sending the request and the port being used for the remote connection. If the client is using PAP then it is important for he password to be encrypted by the NAS before the authentication request is sent to minimize the chance for the password to be compromised.

Here is the process in six steps:

1. The user initiates a dial up PPP connection to the (Network Access Server).
2. The NAS prompts for username and password (if PAP) or challenge (if CHAP).
3. User replies with username and password (if PAP) or challenge (if CHAP).
4. The NAS sends username and encrypted password to the RADIUS server.
5 RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and and authorizes (or rejects) the users access to the network (through the NAS).

TACACS+

- **Connection-oriented.**
- **Created by Cisco.**
- **Encrypts entire packet (except header):**
  - **Password.**
  - **User ID.**
  - **Authorized services.**
  - **Accounting.**

TACACS+

Developed by Cisco, TACACS+ is a popular AAA system for remote network access. Although TACACS+ will support multivendor networks, additional options are available when implemented in a homogenous Cisco network.

How does it work? TACACS+ runs on either UNIX or Windows NT/200 and uses a client-server model. The client is not on the user's machine, but instead it is the device that is trying to determine if the user should be let through the network (typically a router or a firewall).

When a user wants to access the network, the server is questioned by the client and the server in turn replies by stating whether the user passed or failed the authentication. This is very similar to RADIUS. One difference is that TACACS+ uses TCP as the transport protocol (default port 49). One of the benefits of using TCP is that accounting logs are more reliable.

Both TACACS+ and RADIUS use a shared secret key to provide encryption for communication between the client and the server. Unlike RADIUS, TACACS+ encrypts the entire payload when communicating between the client and the server. This makes it more difficult to decipher information about the communication between the client and the server.

Kerberos

- **Uses a proprietary certificate model.**
- **Created at MIT in the 1970's.**
- **Provides mutual authentication.**
- **Defined in RFC 1510.**
- **Kerberos is:**
  - Secure.
  - Free.
  - Standard for Windows 2000 networks.

Kerberos

Kerberos was developed in the 1970's by the Massachusetts Institute of Technology. Since then it has evolved through several version (currently at version 5). Kerberos gets it's name from the three-headed dog that guards the entrance to Hades.

Kerberos uses an authentication server that stores user IDs and passwords. These item are used to generate a "ticket" for network users. In Kerberos, a ticket is roughly equivalent to a X.509 certificate and a Kerberos authentication server acts like a certificate authority. However, Kerberos uses symmetric (DES) cryptography – not public key cryptography.

A ticket is generated when the user first logs in for the day with a user name and password. Tickets have a short life time (no more than 23 hours in Version 5) but they authenticate the user for all services on a network. The short life time minimizes the potential for a "replay attack" or a "man-in-the-middle" attack.

Kerberos only authenticates – it does not authorize. Without an additional authorization mechanism, Kerberos assumes that a user has access to all services. Kerberos (version 5) is the standard authentication protocol for Windows 2000 networks.

PAP vs. CHAP

- **Password Admission Protocol (PAP).**
  - An older protocol.
  - Simple to implement.
  - Password/username are sent in the clear.
- **Challenge Handshake Admission Protocol (CHAP).**
- **Challenge sent by network to user.**
  - Challenge is hashed with users key.
  - Hash is sent back to network access device.
  - If the response is not valid then access is terminated.
  - Can be repeated periodically.

PAP vs. CHAP

In Password Authentication Protocol (PAP) the client authenticates itself by sending a user name and an plain text password to the server. The server compares to its password database. This technique is vulnerable to eavesdroppers who may try to obtain the password by listening in on the serial line, and to repeated trial and error attacks. Even if the password is encrypted, someone could capture the password and decrypt it, or simply replay the encrypted password.

CHAP is not vulnerable in this way. With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge'' string to the client, along with its hostname. The client uses the hostname to look up the appropriate password, combines it with the challenge, and encrypts the string using a one-way hashing function. As previously covered, a hash function produces a compressed, unique result for each key/day combination. The hash is sent to the challenging server along with the client's hostname. The server now performs the same computation, and acknowledges the client if it arrives at the same result. If the results do not match, the connection is terminated.

Another benefit of CHAP is that challenges can be sent at regular intervals to make sure the client hasn't been replaced by an intruder. In this way CHAP defeats both replay attacks and man-in-the-middle attacks.

3 Methods of authentication

- **Something you know:**
  - **Password.**
  - **Personal information.**
- **Something you have:**
  - **Token.**
  - **Smart card.**
- **Something you are:**
  - **Biometrics**

Choosing Effective Passwords

- **Passwords must be as long as is practical.**
- **Passwords must not be in any dictionary.**
- **Passwords must be a non-sequential mixture of letters, numbers and special characters.**
  - Passwords must never use:
    - Family-oriented names.
    - Fan names.
    - Ego names.

Choosing effective passwords

One of the most common way that hackers breach networks is through weak passwords. Exploiting weak passwords is often the first step towards obtaining unauthorized access to a system. Many users resist using “strong” passwords. Many users do not want to remember complex passwords. Therefore, many users choose simple passwords that are easy to remember. Examples include the passwords like “private" or "abc123", or the name of a family member.

Computer systems with weak passwords are susceptible to dictionary attacks. This type of attack uses automated login attempts to guess the password by using words from a dictionary.. Electronic dictionaries exist for a variety of languages, including English, Spanish, Arabic, Farsi, Chinese, Japanese, Russian, TV shows, movies, music, works of literature, sports and even Klingon. Password guessing programs such as the NetBIOS Auditing Tool (NAT), John the Ripper, and L0phtCrack can use these password dictionaries in attempt to determine weak passwords.

Effective password policy

- **Impose a lockout after a number login attempts.**
- **Enforce regular password changes.**
- **Forbid:**
  - Default passwords.
  - User ID passwords.
  - Improper password storage.
  - Any password sharing with anyone – ever!
- **Run a program like L0phtCrack to test for weak passwords.**

Effective password policy

Password policies protect the integrity of corporate networks by keeping unauthorized users out of computer systems. A policy that addresses passwords should include high-level statements that the entire company is expected to follow, regardless of departmental or operating system differences.

In addition to the information on the slides, a policy should address:

Administrative passwords must be changed whenever there is a security breach or if an employee with that administrator privileges leaves the company. Administrative passwords should be listed on paper in a sealed envelope in a lock-box for non-administrative access.

Helpdesk procedures for password changes are a tempting target for the social engineering techniques of hackers. All help desk personal should receive annual training on the social engineering issues associated with password changes and account lockouts. Users is should register a pass phrase that has no relationship with the user's login and password. The help desk should call back (and log time/number) any user before reissuing passwords – even with the users pass phrase. Passwords must not be reset, revealed or accounts unlocked without photo identification or a call back number and pass phrase.

Administrators should run programs regularly to test the network for weak passwords. Some programs (most notably L0phtCrack) enables administrators to test the strength of a password file with or without gaining visibility to the actual passwords.

Security Tokens

- **Physical possession of token required for network access.**
- **Overcomes the vulnerabilities of memorized passwords.**
- **Two main types:**
  - **Plug in tokens (i.e. USB)**
  - **Token Cards.**

Security Tokens

As we have seen, passwords can be compromised in a number of ways. To access a protected resource a user must insert the token, or manually enter the information generated by the token, along with a User ID. Security tokens can include users credentials, digital certificates, and PKI private keys. This information can be used to provide advanced authentication, confidentiality, and non-repudiation.

Smart Cards

- **Chip embedded in card.**
- **Microprocessor in card:**
  - **Typical 16 bit processor.**
  - **32 KB of storage.**
- **More sophisticated than tokens:**
  - **Access rights and privileges.**
  - **User profile and other data stored on card.**

Smart cards

Smart cards are tamper resistant, credit card size devices that include an integrated circuit chip to provide data storage and processing. Smart cards have an electronic circuit chip integrated into the card. These cards store all the relevant information needed for a transaction on the card. Therefore, they are not required to access a remote databases or service in order to complete transactions.

There are 3 basic types of smart cards:

Memory card: Memory cards are the oldest type of smart card. Memory cards simply store data and provide no processing power.

Microprocessor card: The typically includes 32KB of memory with a 16-bit microprocessor. This type of card may also includes security features like a Personal Identification Number (PIN) or other authenticating data.

Cryptographic card: These cards employ a more advanced microprocessor with specialized cryptographic programming for hashing, digital signatures, and private key capabilities.

Contact Smart Cards must have a physical connection to a reader in order to work. Contactless Smart Cards communicates with the reader and derives its power from RF energy.

Biometrics

- **Access method based on who you are.**
- **Common methods:**
  - **Voice recognition.**
  - **Fingerprint scanning.**
  - **Iris/retinal scan.**
  - **Facial/Hand geometry.**

Biometric Access laptop TransPort GX3

Biometrics

Biometrics uses "who you are" (physical or behavioral characteristics) to identify, or authenticate an individual's identity.

Voice, fingerprint, iris, retina, facial geometry and hand geometry are examples of physical characteristics. Behavioral characteristics, including signature or handwriting, might also be used. A recent product, the Transport GX3, uses fingerprint scanning to authenticate the user before allowing the computer to boot up.

One of the benefits of biometric is the prevention of against identity theft. Identity theft is one of the fastest growing crimes in the United States. Victims of identity theft know how difficult it is to prove a criminal has stolen their identity.. A biometrics system can prevent identity theft because it is based on the unique biology of an individual. This biology is unique and cannot be easily duplicated.

Password attacks

- **Redundancies in the password.**
- **Redundancies in the algorithm.**
- **Password compromise.**
- **Common passwords.**
- **Brute force.**

Password attacks

The issues of redundancies and key compromise have been explored in a previous chapter. A password has the same potential weaknesses as an encryption key. Because a key is relatively short, a brute force attack is quite effective. IN the context of passwords, a brute force attack is also known as a dictionary attack.

A dictionary attack can be made much more effective if the user has chosen a “common” key. A dictionary attack will. usually begin with a list likely (common) passwords and add numbers and symbols to that list.

Token and biometric attacks

This is just one web page (of many) on hacking smartcards!

- **No System is immune from hacking!**
- **Token and biometrics are less susceptible to social engineering.**
- **Biometrics may be vulnerable to coercion or even amputation.**
- **Many resources are available on the web.**

Token and biometric attacks

This web page gives the readers all they need to crack a smart card: The over view page lists five steps (links and specific information have been omitted):

1. Getting started

This page tells you how to get started with smart card hacking. First of all you will need to learn what smart card you have.

2. Hardware

Next, you will need a smart card reader. There is a lot of smart card equipment for sale.

3. Software

Once you have got your reader, you will need software. Most commercial readers come with their own proprietary software, that is not compatible with other readers, and most of it runs on Windoze machines only. A few hobbyists (including ourselves) are working on platform independent and reader independent software, so that everyone can play with smart cards. The ISI software works with multiple readers, but this software can only be used for one purpose…

4. Technical information

Before you start hacking your card, try to read some documentation for the card you want to hack. If that is not available, you should try to find things out yourself. More and more cards however are compliant to some standard. ….

5. Subscribe to the mailinglist

If you have a really nice smart card system you want to discuss or have questions about, have made interesting software or have found a nice way to crack a certain system? Share it with other interested people!

Summary

- A Remote Access Server acts as an authentication gateway providing AAA.
- AAA services are:
  - Authentication - who are you?
  - Authorization - what are you allowed to do?
  - Accounting - what services did you use?
- Popular methods of authentication:
  - Radius
  - TACACS+
  - Kerberos

Summary

- **Password Authentication Protocol**
  - PAP transmits the actual passwords
  - Often the password unencrypted.
- **Challenge Handshake Authentication Protocol**
  - CHAP never transmits the password.
  - Instead, transmits a hash of a shared password.
  - Can periodically repeat this challenge.
- **3 possession can be used for authentication:**
  - Something I know.
  - Something I have.
  - Something I am.