User Authentication Methods

by Sophia

WHAT'S COVERED

In this lesson, you will learn more about authentication systems.

Specifically, this lesson will cover the following:

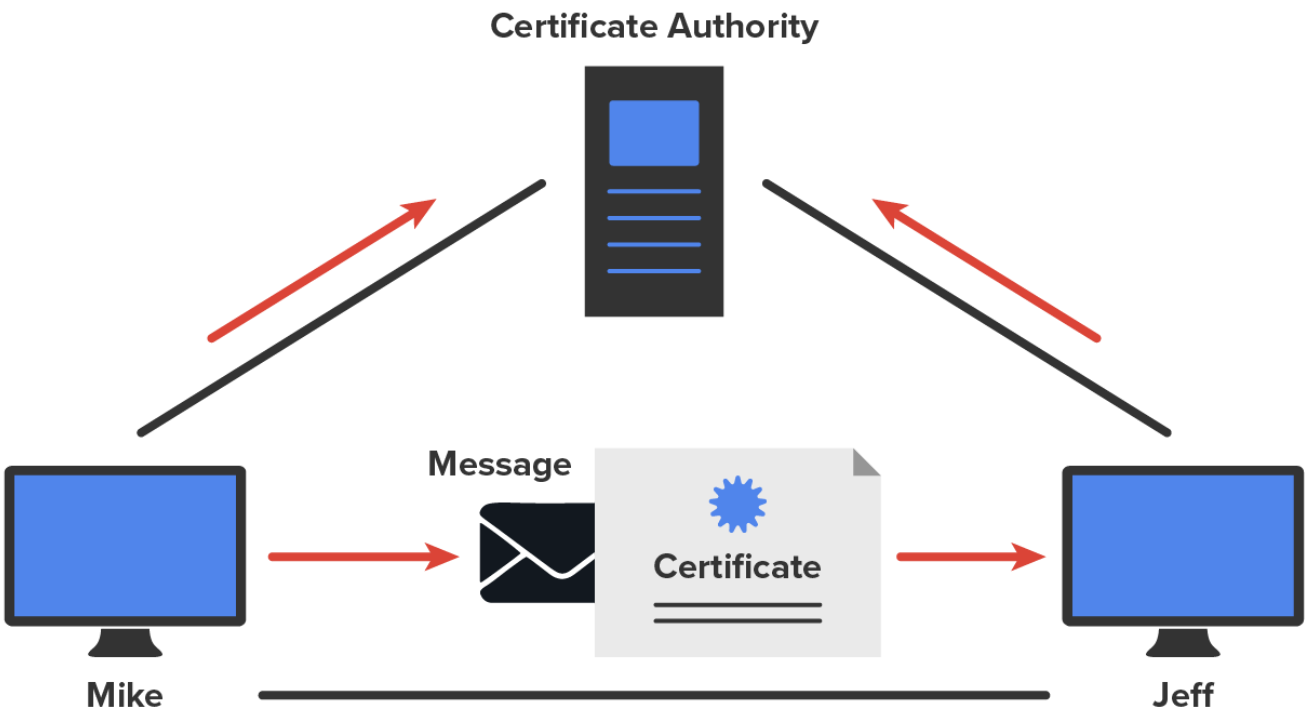
1. Authentication Systems

There are a number of authentication systems in use today, and this lesson will focus on the ones you're most likely to work with in the networking field.

1a. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a system that links users to public keys and verifies a user's identity by using a **certificate authority (CA)**. Think of a CA as an online notary public, an organization that is responsible for validating user IDs and issuing unique identifiers to confirmed individuals to certify that their identity can really be trusted.

> EXAMPLE The diagram below shows how the CA process works in relation to two users. In the diagram below you see Mike sending a message to Jeff, using a certificate that Jeff uses to verify Mike is authorized to send Jeff data.



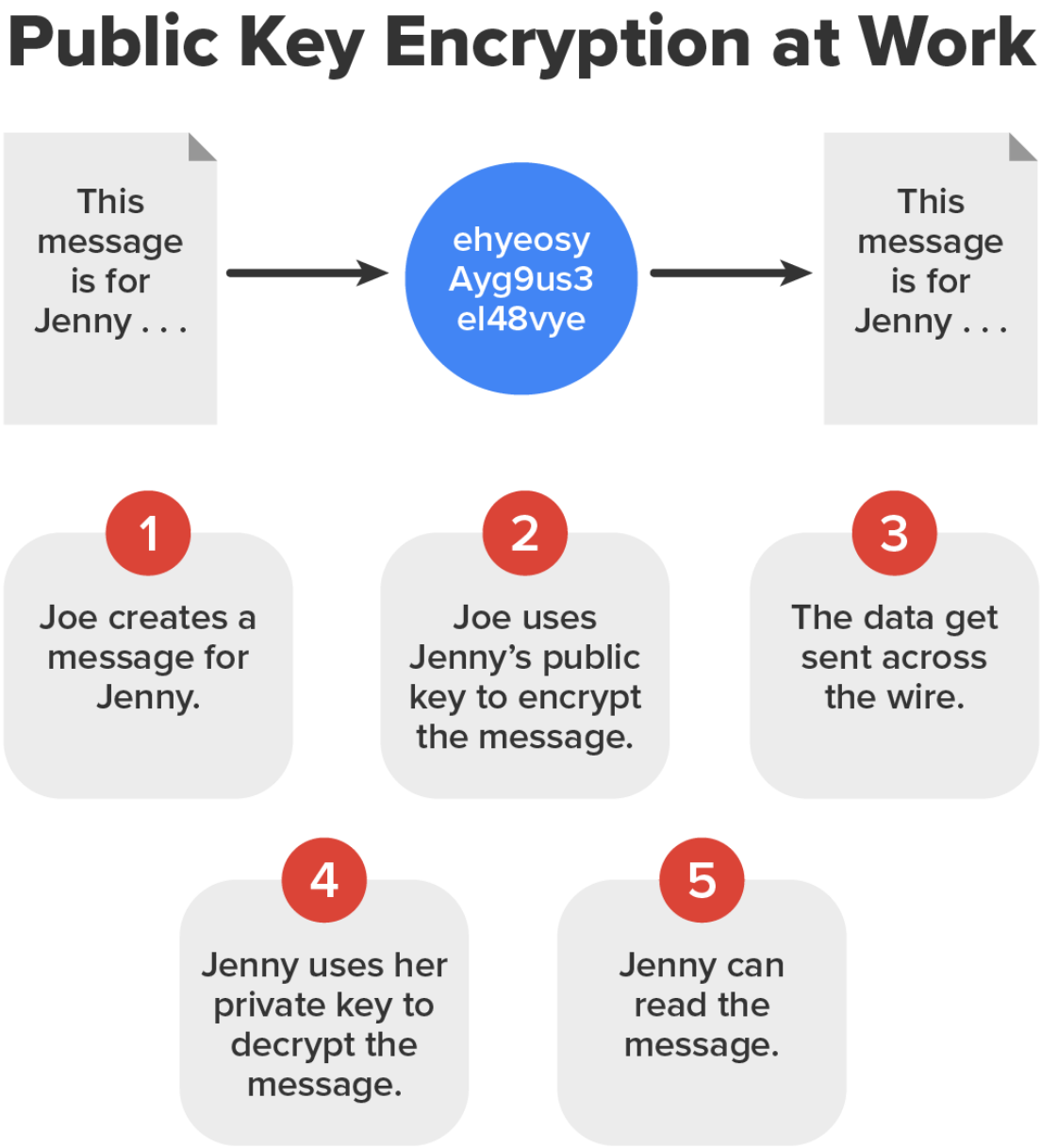
PKI allows people to communicate with each other with confidence that they are talking to whom they think they are talking to. It is used to establish confidentiality and to ensure message integrity without knowing anything about the other party prior to the conversation. It is also used to verify the digital signature of a private key's owner.

As you learned in the previous lesson, public-key encryption operates through asymmetric cryptography, meaning a different key is used to encrypt and decrypt the message respectively. In contrast, symmetric cryptography uses the same key to encrypt and decrypt, so it is a lot less secure.

KEY CONCEPT

Here is how public-key encryption works: When I send you a message using PKI, I use your public key to encrypt the message. When you receive the message, you use your private key, which is theoretically the only thing that can be used to decrypt the message back into something readable by humans. If a digital signature isrequired, you sign the document with your private key, and anyone with access to your public key would be able to verify that the signature was truly yours.

So clearly, you should be the only one who has access to your private key. The diagram below illustrates the process just described.



This type of authentication is used a lot in websites that perform transactions.

TERMS TO KNOW

Public Key Infrastructure (PKI)

A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Certificate authority (CA)

An organization that issues digital certificates for use by other parties.

1b. Kerberos

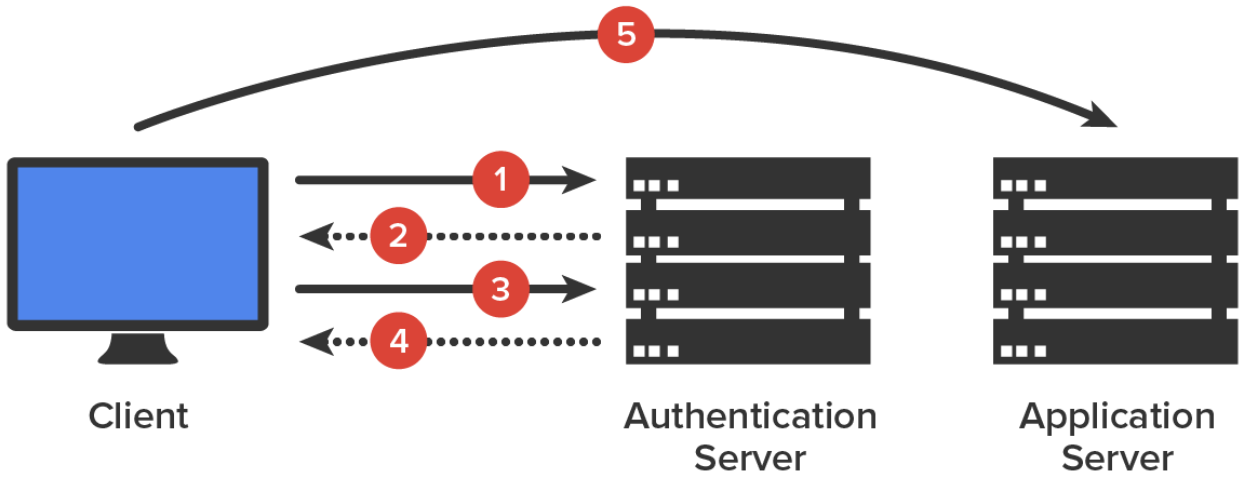
Kerberos is an entire security system that establishes a user's identity when they first log on to a system that is running it. It employs strong encryption for all transactions and communication, and it is readily available.

HINT

The source code for Kerberos can be freely downloaded from lots of places on the Internet. Kerberos works by issuing tickets to users who log in, kind of like going to an amusement park. As long as you have your ticket to ride, you are good to go. Even though the tickets expire quickly, they are automatically refreshed as long as you remain logged in. Because of this refresh feature, all systems participating in a Kerberos domain must have synchronized clocks.

If you have only one Kerberos authentication server and it goes down then no one can log in to the network. So when running Kerberos, having redundant servers is vital. You should also know that because all users' secret keys are stored in one centralized database, if that is compromised, you have a serious security incident on your hands. Luckily these keys are stored in an encrypted state.

The diagram below shows Kerberos in action.



1. Request for ticket granting ticket (TGT)
2. TGT returned by authentication
3. Request for application ticket (authentication with TGT)
4. Application ticket returned returned by ticket-granting
5. Request for service (authenticated with application ticket)

TERM TO KNOW

Kerberos

An authentication protocol using a central ticket server.

1c. Authentication, Authorization, and Accounting (AAA)

Authentication, authorization, and accounting (AAA) is a systematized conceptual model for managing network security through one central location. Two common implementations of AAA include RADIUS and TACACS+.

Although its name implies it, the **Remote Authentication Dial In User Service (RADIUS)** is not a dial-up server; it originated that way, but it has evolved into more of a verification service. Today, RADIUS is an authentication and accounting service that is used for verifying users over various types of links, including dial-up. Many ISPs use a RADIUS server to store the usernames and passwords of their clients in a central spot through which connections are configured to pass authentication requests. RADIUS servers are client-server-based authentication and encryption services maintaining user profiles in a central database.

KEY CONCEPT

RADIUS is also used in firewalls. Deployed this way, when a user wants to access a particular TCP/IP port, they must provide a username and a password. The firewall then contacts the RADIUS server to verify the credentials given. If the verification is successful, the user is granted access to that port.

BIG IDEA

RADIUS is an authentication server that allows for domain-level authentication on both wired and wireless networks.

The **Terminal Access Controller Access-Control System Plus (TACACS+)** protocol is also a AAA method and an alternative to RADIUS. Like RADIUS, it is capable of performing authentication on behalf of multiple wireless APs, RAS servers, or even LAN switches that are 802.1X capable. Based on its name, you would think it is an extension of the TACACS protocol (and in some ways it is), but the two definitely are not compatible.

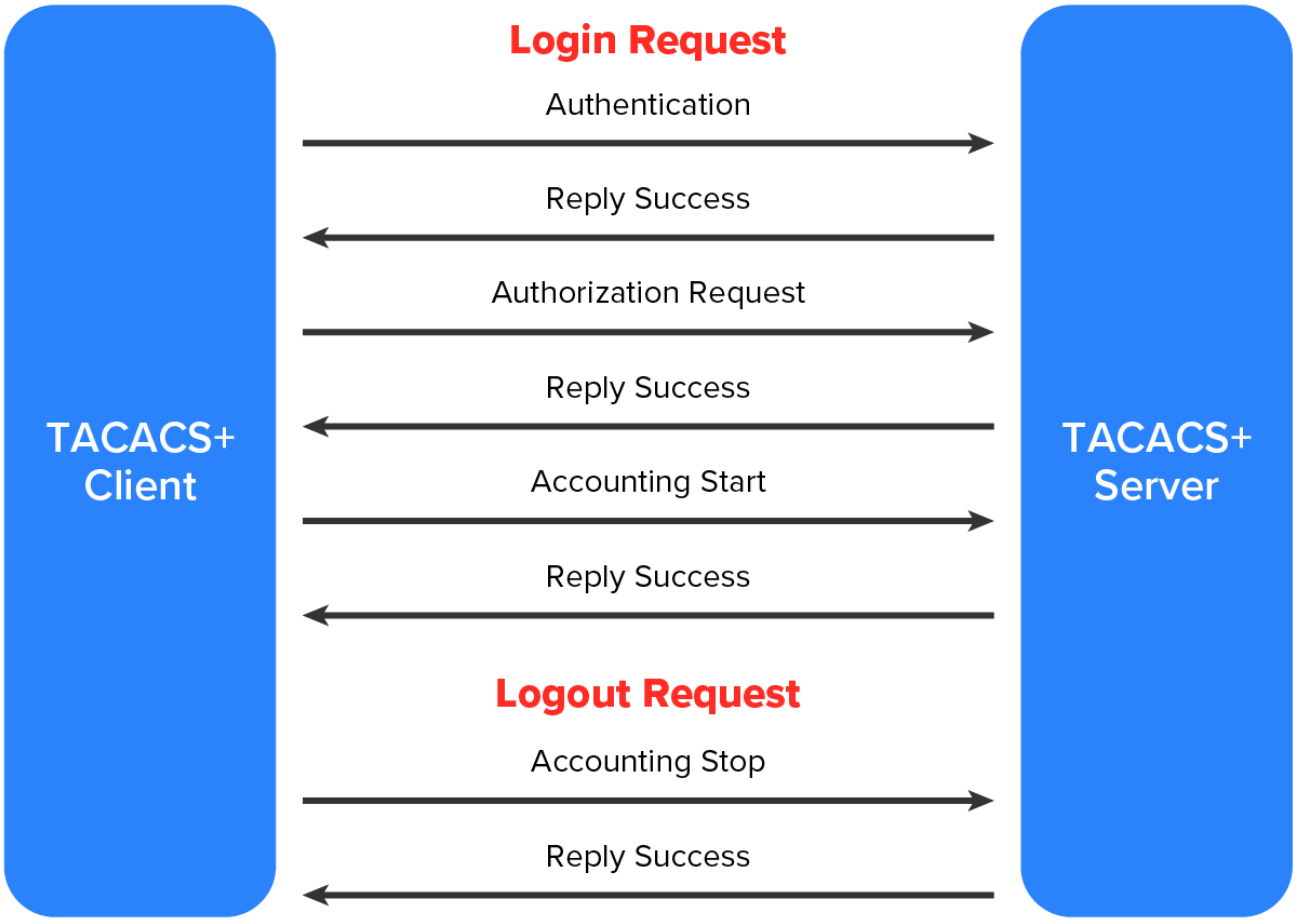
KEY CONCEPT

There are two major differences between TACACS+ and RADIUS:

- RADIUS combines user authentication and authorization into one profile, but TACACS+ separates the two.
- TACACS+ utilizes the connection-based TCP protocol, but RADIUS uses UDP instead.

Even though both are commonly used today, because of these two reasons TACACS+ is considered more stable and secure than RADIUS.

The diagram below shows how TACACS+ works.



Accounting is the logging of system use to monitor and measure the amount of system resources used during authorized access, for example counting the number of pages printed or measuring the bandwidth used. Just to clarify, in the IT world, accounting has little to do with money and everything to do with measuring and logging resource utilization.

KEY CONCEPT

When a TACACS+ session is closed, the information in the following list is logged, or accounted for. This is not a complete list; it is just meant to give you an idea of the type of accounting information that TACACS+ gathers:

- Connection start time and stop time
- The number of bytes sent and received by the user
- The number of packets sent and received by the user
- The reason for the disconnection

The only time the accounting feature has anything to do with money is if your service provider is charging you based on the amount of time you have spent logged in or for the amount of data sent and received.

TERMS TO KNOW

Authentication, authorization, and accounting (AAA)

A systematized conceptual model for managing network security through one central location.

Remote Authentication Dial In User Service (RADIUS)
An authentication and accounting service that is used for verifying users over various types of links.

Terminal Access Controller Access-Control System Plus (TACACS+)
An authentication protocol used for remote communication with any server housed in a UNIX network. TACACS provides an easy method of determining user network access via remote authentication server communication. The TACACS protocol uses port 49 by default.

Accounting
The logging of system use to monitor and measure the amount of system resources used during authorized access.

1d. Network Access Control (NAC)

Network Access Control (NAC) is a method of securing network hosts before they are allowed to access the network. The most common implications for NAC are in wireless networking, where nodes are often added to and removed from the network freely. One of the most common forms of NAC is IEEE 802.1X.

> **IN CONTEXT**
>
> Even the Institute of Electrical and Electronics Engineers (IEEE) recognizes the potential security holes in wireless networking, so it came up with the **IEEE 802.1X** standard as a way to authenticate wireless users. 802.1X is an open framework that is designed to support multiple authentication schemes. Before a client, called a supplicant in 802.1X-speak, can communicate on a wireless network, it asks the access point, or authenticator, for permission to join and then provides its credentials. The access point passes those credentials to a centralized authentication server that sends back an accept message to the access point if the authentication is accepted. Only then will the access point allow a user to connect to the wireless network.

Network Access Control systems that control access to devices based on their security settings include Cisco's Network Admission Control (NAC) and Microsoft's Network Policy and Access Services (NPAS). These systems examine the state of a computer's operating system updates and anti-malware updates before allowing access, and in some cases they can even remediate the devices prior to permitting access. The following sections cover key components of network access control systems.

When devices attempt to access the network, the devices are examined closely by the network, which is called a Posture Assessment. The following items can be checked:

- Anti-malware updates
- Operating system updates
- Windows Registry settings

When the assessment is complete and is positive, admission is granted. If problems are found, admission may be denied and the user notified that action must be taken, or the device may be directed to a remediation server that can install missing updates or quarantine the device if necessary.

Guest Network

When a device is attempting to connect to a network using a form of network access control, the device is first placed in a guest network until a posture assessment is performed. Until it is either approved or remediated, it will remain in the guest network.

HINT

The guest network will not allow access to the balance of the network to prevent the device from introducing issues to the network.

Persistent vs. Nonpersistent Agents

Network access control systems can be deployed using either persistent or nonpersistent agents on the devices. A **persistent agent** is one that is installed on a NAC client and starts when the operating system loads. This agent provides functionality that may not be present in the **nonpersistent agent**, such as system-wide notifications and alerts and auto and manual remediation.

TERMS TO KNOW

Network Access Control (NAC)

A method of securing network hosts before they are allowed to access the network IEEE 802.1X standard as a way to authenticate wireless users.

802.1X

An open framework that is designed to support multiple authentication schemes.

Persistent agent

A software agent that is installed on a NAC client and starts when the operating system loads.

Nonpersistent agent

A software agent that is installed on a NAC client that starts when the operating system loads and then terminates itself after running.

SUMMARY

In this lesson, you learned more about **authentication systems**, including Public Key Infrastructure (PKI), Kerberos, Authentication, Authorization, and Accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

802.1X
An open framework that is designed to support multiple authentication schemes.

Accounting
The logging of system use to monitor and measure the amount of system resources used during authorized access.

Authentication, authorization, and accounting (AAA)
A systematized conceptual model for managing network security through one central location.

Certificate authority (CA)
An organization that issues digital certificates for use by other parties.

Kerberos
An authentication protocol using a central ticket server.

Network Access Control (NAC)
A method of securing network hosts before they are allowed to access the network IEEE 802.1X standard as a way to authenticate wireless users.

Nonpersistent agent
A software agent that is installed on a NAC client that starts when the operating system loads and then terminates itself after running.

Persistent agent
A software agent that is installed on a NAC client and starts when the operating system loads.

Public Key Infrastructure (PKI)
A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Remote Authentication Dial In User Service (RADIUS)
An authentication and accounting service that is used for verifying users over various types of links.

Terminal Access Controller Access-Control System Plus (TACACS+)
An authentication protocol used for remote communication with any server housed in a UNIX network. TACACS provides an easy method of determining user network access via remote authentication server communication. The TACACS protocol uses port 49 by default.