Network Security system

Chapter - 3

Prepared by

Afifa Hoque

Jr. Instructor

DIIT, CTG.

Tacacs+

- The TACACS+ protocol **provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process**. ... TACACS+ uses Transmission Control Protocol (TCP) for its transport. TACACS+ provides security by encrypting all traffic between the NAS and the process.

Radius

- Remote Authentication Dial-In User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises in 1991 as an access server authentication and accounting protocol.

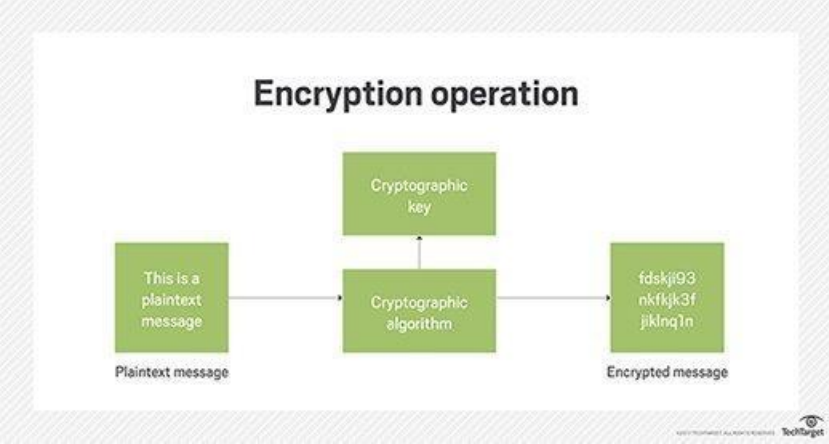
Difference between TACACS+ and RADIUS

- RADIUS was designed to **authenticate** and log remote network users, while TACACS+ is most commonly used for administrator access to network devices like routers and switches

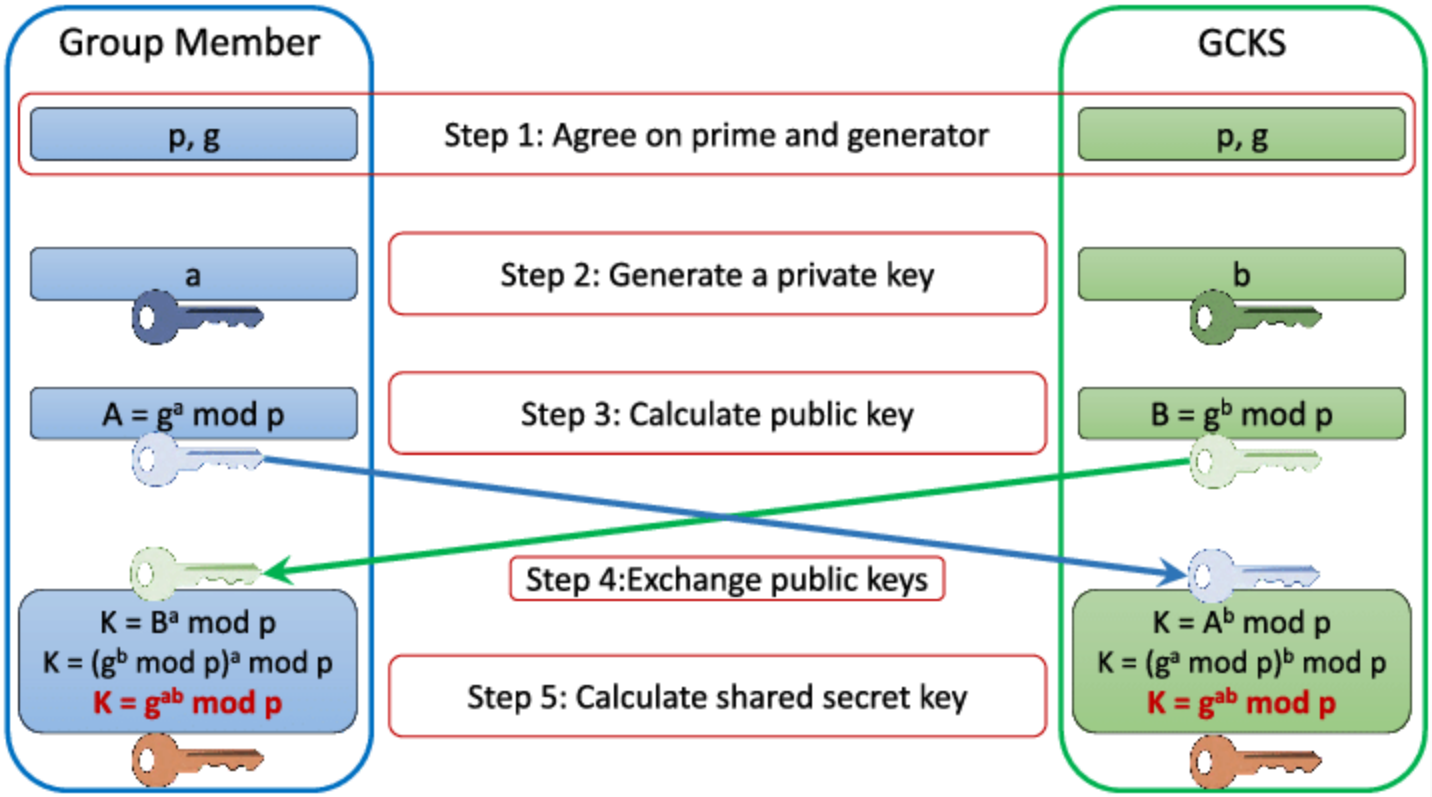
- Traditionally authorized users provide a username and password to verify their identity for both RADIUS and TACACS+.

Encryption Technology

- Encryption is the **process of taking plain text**, like a text message or email, and scrambling it into an unreadable format — called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.



Diffie-Hellman Technique



(cont.)

- The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to **jointly establish a shared secret key over an insecure channel**. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Encrypt and decrypt a number

- Select the shared numbers. select a large prime number P. ...
- Select the private key and share the public key. Let's look at two users, Alice and Bob. ...
- Compute the super key for encoding and decoding. Alice computes her super key as X = B^a mod P. ...
- Use the super key to encrypt and decrypt.