CSEC-600 - Operating Systems and Applications Security

Assignment 1

(Define PGP & GPG and Summary of Chapter 2)

Yuvraj Singh Gill

000560556

gill0680@saskpolytech.ca

Task 1: Define PGP?

Definition:

PGP stands for Pretty Good Privacy. It was developed by Phil Zimmermann in 1991, It is an encryption tool that provides cryptographic privacy and authentication for data communication. PGP is proprietary software, requiring a paid license for commercial use. It is used for securing emails, files and messages. PGP can be used for symmetric and asymmetric encryption to protect data and ensure confidentiality. (Villanueva, 2024)

PGP Encryption Algorithms:

1. **Symmetric Encryption Algorithms:** Symmetric encryption uses one key to encrypt and decrypt.
    - AES (Advanced Encryption Standard)
    - Triple DES (3DES)
    - Blowfish
    - Twofish
    - CAST-128
    - IDEA

2. **Asymmetric Encryption Algorithms:** Asymmetric encryption encrypts using a key pair consisting of a public key and a private key.
    - RSA (Rivest-Shamir-Adleman)
    - DSA (Digital Signature Algorithm)
    - ElGamal

Task 2: Define GPG?

Definition:

GPG stands for GNU Privacy Guard. It is a free and open-source alternative tool to PGP, developed as part of the GNU Project. It was built on OpenPGP standards, which was originally derived from the PGP software, created by Phil Zimmermann in other words, GPG is an open-source implementation of PGP and follows the OpenPGP standard. Like PGP, it uses both symmetric and asymmetric encryption to secure data. It is a cli-based utility that allows users to encrypt and sign data, ensuring confidentiality in communications. It supports the majority of modern encryption algorithms. (Villanueva, 2024)

GPG Encryption Algorithms:

1. **Symmetric Encryption Algorithms:** Symmetric encryption uses one key to encrypt and decrypt.
    - AES (Advanced Encryption Standard) – 128, 192, 256-bit
    - Camellia – 128, 192, 256-bit (Alternative to AES)
    - 3DES
    - Blowfish
    - Twofish
    - CAST5

2. **Asymmetric Encryption Algorithms:** Asymmetric encryption encrypts using a key pair consisting of a public key and a private key.
    - RSA (Rivest-Shamir-Adleman)
    - DSA (Digital Signature Algorithm)
    - ElGamal

How Symmetric Encryption and Decryption Works?

1. Before sending a file, both the sender and recipient must have the same secret key. This key must be shared securely.
2. The sender encrypts the file using the secret key. This converts the plaintext into unreadable ciphertext.
3. The sender sends the encrypted file to the recipient.
4. The recipient decrypts the file using the same secret key and reads it.

How Asymmetric Encryption and Decryption Works?

1. Before sending a file, both people must exchange their public keys while keeping their private keys secret.
2. The sender then encrypts the secret key using the recipient's public key. This ensures only the recipient can unlock the file.
3. The sender sends the encrypted file.
4. The recipient decrypts the file using their private key and reads it.

Task 3: Relationship between PGP and GPG?

PGP and GPG share many similarities. GPG's encryption and decryption process is similar to PGP's as both were developed based OpenPGP Standard. OpenPGP is a set of rules and guidelines that define how to securely encrypt and sign emails, files, and messages. While using these rules or standards PGP was built as proprietary software and using same rules or standards GPG was built as GNU project which is a free, open-source alternative to proprietary PGP. GPG is compliant with RFC 4880. Meaning it adheres to the OpenPGP standard and hence possesses the core functionality of PGP. (Villanueva, 2024)

Key Differences Between PGP & GPG:

PGP	GPG
Proprietary Software	Open-source software
Uses its own or proprietary encryption methods	Follows the OpenPGP standard
Code not available freely	Code available freely
Proprietary support	Community support

Task 4: Read Chapter 2 of Mastering Linux Security Hardening, 3rd Edition. by Donald A. Tevault. Summarize Chapter 2 (Securing Administrative User Account)

This chapter highlights the importance of user management in Linux and how to protect systems from unauthorized access. Since Linux is a multi-user operating system, each user must have specific privileges to prevent security risks.

The root account is the super user, with full administrative access to modify or delete files, change configurations, and manage the system. Misuse of the root account can lead to security vulnerabilities. Logging in as root is dangerous because accidental mistakes or security breaches can damage the entire system. If an attacker gains access to a root user, they have full control over the system.

Example: Imagine an attacker finds a remote code execution vulnerability on a web server and if the web server is running as root, the attacker can take full control of the system.

Instead of using the root account, use sudo utility. Sudo allows users to run specific admin commands without logging in as root. This improves security and prevents accidental or unauthorized changes. It also provides accountability. If multiple admins share the root password, it is impossible to track who made specific changes. It also prevents someone from abusing super user privileges.

In Linux, sudoers group is a special pre-defined user group that controls who can use the sudo command. Users in this group can execute administrative commands without needing the root password. Instead, they use their own password to gain temporary admin privileges.

The sudoers file is the main configuration file that controls which users or groups have sudo privileges and what commands they can run. We can apply different sudo policies which help in maintaining security by controlling who can run privileged commands and how they use them. It ensures that users only have the necessary permissions while logging all administrative actions for auditing and security purposes.

References

- Villanueva, J. C. (2024, May 29). PGP vs GPG: The Key Differences Explained. JSCAPE. https://www.jscape.com/blog/pgp-vs-gpg-the-key-differences-explained
- How To Linux. (2021, October 31). 148 What is The Difference Between PGP, OpenPGP, and GPG [Video]. YouTube. https://www.youtube.com/watch?v=M0vC_WMh-Fo
- Tevault, D. A. (2023). Mastering Linux Security and Hardening - Third edition. Packt Publishing.