Seminar Impact Considerations

Casper Kristiansson

February 17, 2024

Technology: Identity verification using GPG

1 Before Seminar

1.1 What is it

GPG is a free and open-source library used to encrypt and sign data [1]. The goal is to ensure privacy and authenticity. The tools enable users to encrypt messages and files and create digital signatures.

1.2 What it is used for

In the context of identity verification, GPG is used to prove the ownership of an email address or digital identity securely. A user can prove their identity by signing a message or a document with their private key. It can be proven using the public key to decrypt and verify the signature. This process is often used for secure email communication and code signing.

1.3 How it works

First, a user generates a pair of keys, a private key and a public key. For a user to verify its identity the user signs a message or a document with their private key. The sender's public key can then decrypt the signature to verify that the signature is valid.

2 After Seminar

I chose to pick the two cards; Inside Knowledge and Personal Data. Both of these cards were chosen because their relevance is directly connected to the functionality of GPG. Addressing these two cards' concerns can help in providing insight into how to mitigate risk and enhance user trust in GPG.

2.1 Inside Knowledge (Adversary's Resources)

When developing a technology such as GPG it is important to understand what type of inside knowledge a adversary might have or gain access to and how that information can be used to perform attacks on the technology. If an attack would access a person's keys it could lead to the attacker utilizing the keys to impersonate the original owner of the keys. This could for example be:

1. **Understanding GPG's Mechanics:** An attacker might have a good understanding of how GPG's encryption, decryption, and signing verification work and possibly could exploit vulnerabilities in the implementation.
2. **Good knowledge in Key management Practices:** A big issue often with encryption technologies that utilize keys is the poor management of the key. This for example could be reusing keys across multiple platforms, not updating or rotating keys. If not applying the recommended practices it could lead to unauthorized access to the keys.
3. **Social Engineering:** Another big thing is social engineering. If an attacker has a good understanding of social dynamics it could lead to phishing attacks where the attack might trick users into revealing their private keys.

2.2 Personal Data (Human Impact)

The usage of GPG for identity verification involves a unique set of regards to the collection, storage, and sharing of personal data [2]. GPG is fundamentally designed to enhance privacy and security with digital communication. But even so, GPG could potentially compromise and corrupt the collected for example via:

1. **Email Addresses:** GPG is commonly used for securing email communication. This means that a user's email address with be involved in the process where it will work as an identifier and an endpoint for the encrypted communication.
2. **Signatures and Encrypted Messages:** GPG allows users to sign documents, messages, and code commits. By doing this, it means that the signed piece of information will directly be linked with an individual's identity.
3. **Unauthorized access:** If an attacker gains a user's private key it means that they can impersonate the user and can sign documents or messages to further access restricted resources of the original user.

References

[1] *The gnu privacy guard*, https://www.gnupg.org/, (Accessed on 02/17/2024).

[2] *What is gpg encryption and do you need it?* https://www.liquidweb.com/kb/is-gpg-still-useful-in-todays-insecure-world, (Accessed on 02/17/2024).