ELEC-C7420 - Basic principles in networking

PART-II Security

Assignment IV – PGP

What is PGP?

PGP (Pretty Good Privacy) encryption has become a mainstay of internet privacy and security for one main reason: it allows you to send a coded message to someone without having to share the code beforehand. There's a lot more to it, but this is the fundamental aspect that has made it so useful.

Let's say you needed to send a sensitive message to a friend without anyone else discovering its contents. One of the best solutions would be to alter it with a secret code that only you and the friend know, so that if anyone intercepts the message, they can't read the contents.

Systems like this work fine in many different types of encryption, but there is one major flaw: **How can you send a coded message to someone if you haven't already had a chance to share the code with them?**

If you haven't shared the code beforehand and use it to encrypt your message, then your friend will have no way to decipher the coded message when they receive it. If you send the code alongside the coded message, then anyone that intercepts the message can access the contents just as easily as the recipient.

It's a conundrum that PGP has managed to solve with **public-key encryption** that you all are familiar with.

What else does PGP encryption do?

PGP's core function is to enable its users to send secure messages without needing a prior introduction, but that's not all it does. It also allows recipients to verify whether a message is authentic or if it has been tampered with. It does this by using something called **digital signatures**

On top of this, PGP can be used to encrypt other things besides email. You can use it to encrypt your hard drive, instant messages, files and more. While these are all important features, this assignment will mainly focus on using PGP encryption for email, PGP's most widespread use.

Why is PGP important?

You may not be aware, but **email isn't a very secure way to communicate**. When your email leaves your account and gets sent across the internet, it transits through networks that are beyond your control. It can be intercepted and tampered with, all without you or the recipient's knowledge.

If you need to send something valuable or sensitive, normal email just isn't suitable. Your personal messages can be snatched by hackers who might use it to commit identity fraud, while important government messages can fall into the hands of spies. A person's stalker could even be reading everything that goes through their inbox.

These dangers are part of why PGP was invented–to bring some semblance of privacy and security to the Wild West that is email communication. It stands for **Pretty Good Privacy**, which may not inspire a whole lot of confidence for something that people rely on to keep their communications secure.

How does PGP encryption work?

First, let's cover the key concepts, then we'll go into an example to give you a more concrete understanding. PGP encryption relies on several major elements that you will need to get your head around in order to understand how it works. The most important ones are **symmetric-key cryptography, public-key cryptography**, **digital signatures** and the **web of trust**.

- **Symmetric-key cryptography**

Symmetric-key cryptography involves using the same key to both encrypt and decrypt data. In PGP, a random, one-off key is generated, which is known as the **session key**. The **session key encrypts the message**, which is the bulk of the data that needs to be sent.

This type of encryption is relatively efficient, but it has a problem. How do you share the session key with your recipient? If you send it alongside your email, then anyone who intercepts the message can access the contents just as easily as your recipient. Without the key, your recipient will only see the ciphertext.

- **Public-key cryptography**

PGP solves this problem with public-key cryptography, also known as asymmetric cryptography. In this kind of encryption there are two keys: a **public key** and a **private one**.

Each user has one of each. The public key of your potential correspondent can be found by searching through key servers or by asking the person directly. **Public keys** are used by the sender to encrypt data, but they cannot decrypt it.

Once data has been encrypted with the recipient's public key, it can only be decrypted by their **private key**. This is why public keys are freely handed out, but private keys need to be guarded carefully. If your private key is compromised by an attacker, it enables them to access all of your PGP encrypted emails.

In PGP, public-key encryption isn't used to encrypt the message, just the one-off **session key** that was generated to encrypt it. Why? Because public-key encryption is simply too inefficient. It would take too long and use a larger amount of computational resources.

Since the body of the message usually contains the bulk of the data, PGP uses the more economical symmetric-key encryption for this. It reserves the lumbering public-key encryption for the session key, making the whole process more efficient.

In this way, the message gets encrypted through more practical means, while public-key encryption is used to securely deliver the session key to your recipient. **Since only their private key can decrypt the session key, and the session key is needed to decrypt the message, the contents are secure from attackers**.

➢ Digital signatures

Our written signatures are frequently used to verify that we are who we say we are. They are far from foolproof, but they are still a useful way of preventing fraud. **Digital signatures** are similar, using public-key cryptography to authenticate that the data comes from the source it claims to and that it has not been tampered with.

The process makes digital signatures essentially impossible to forge unless the private key has been compromised. **Digital signatures can be used alongside PGP's message encryption or separately**. It all depends on what you are sending and why.

If the message is sensitive and shouldn't be read by anyone but the recipient, you need to use encryption. If the message must be delivered intact and without alteration, then a digital signature will need to be used. If both are important, you should use them together.

Digital signatures work by using an algorithm to combine the sender's private key with the data that they are authenticating. The plaintext of your message is fed through a **hash function**, which is an algorithm that transforms inputs into a fixed-size block of data, called a **message digest**.

The message digest is then encrypted with the sender's private key. This encrypted message digest is what is known as the **digital signature**. In PGP encryption, the digital signature is sent alongside the message body (which can either be encrypted or in plaintext).

➢ The web of trust

How do you know that a public key actually belongs to the person who says it does? Couldn't someone just post up their own public key and claim that they're the Pope in an attempt to access all of his incoming PGP-encrypted emails (assuming he's tech savvy enough to use PGP)?

Thankfully, this was all thought of ahead of time and solutions were put in place. Otherwise, something so simple would completely undermine the whole system. To prevent this kind of activity, the **web of trust** was developed.

The web of trust grew as a way of vetting that each PGP public key and user ID are really connected to the person or organization that they are said to represent. The web of a trust connects the real life entity with the public key by using a third party to sign the user's **PGP digital certificate**. The best part? It does it all without a central authority that can collapse or be corrupted.

A digital certificate contains the user's identifying information, their public key and one or more digital signatures. If you know a PGP user personally, you can confirm that their public key is linked to their actual identity. You can put your trust in them and digitally sign their certificate, which shows that at least one person vouches for their identity. They can also do the same for you.

If both of you meet one new PGP user each and digitally sign their certificates to verify their identities, you start to build a small network, where the four of you can trust the links between the public keys and identities, based on the trust each person has in others that they are linked to.

Over time, **this builds an interconnected web of trust**, with lots of people vouching for each other with digital signatures that verify their ownership of a public key.

PGP encryption in action

Let's put all of this together in an example to show how these elements work in relation to each other. To make things more interesting, let's say you're a whistleblower from a totalitarian country who has uncovered an extreme case of corruption.

You want to get the message out to journalists, but you are terrified for your own safety. What if the government finds out that you were the one who leaked the information and they send people after you?

You eventually decide that releasing the information to the public is the right thing to do, but you want to do it in a way that protects you as much as possible. You search online and find a journalist who is renowned for this kind of work and always protects their sources.

You don't want to just call them or email them normally, it's too risky. You've heard about PGP before and decide to try using it to protect your message. You download a program like Gpg4win and configure it with an OpenPGP-compliant email.

Once everything is in order, you seek out the journalist's **public key**. You find it on their website or by searching a key-server. Their public key has numerous **full-trust signatures** on the digital certificate, so you know it's legitimate.

You import the journalist's public key, then use your OpenPGP-compliant email to begin. You type out the message:

Dear Susan Peterson,

I have some information about a huge corruption scandal in The United States of Mozambabwe. Let me know if you are interested and I will send you more details.

➢ **Adding your digital signature**

If you are worried about the email being tampered with, you can add your **digital signature**. A **hash function** turns the plaintext into a **message digest**, which is encrypted with your private key. The digital signature will be sent to the journalist alongside the message.

➢ **Encrypting the message**

When this is finished, PGP compresses the plaintext. Not only does this make the process more efficient, but it also helps to make it more resistant to cryptanalysis.

Once the file is compressed, PGP creates the one-off **session key**. This session key is used to efficiently encrypt the plaintext with **symmetric-key cryptography**, turning the body of the message into ciphertext. The session key is then encrypted using the journalist's public key. This **public-key encryption** is more resource-hungry, but it allows you to securely send the session key to the journalist.

The ciphertext, the encrypted session-key and the digital signature are then sent to the journalist. When the journalist receives the message, it will look something like this:

```
wcBMA97wCTWE/j6yAQf9EIv17btMUCL8BwIn4bAf/gE3GVdPmpfIQLSpOa1yN9d8

KI9K8xs9MAEF7fgl94/nXg0h9e1KcTjgi81ULMRMkDjIoYd33TQTMqXnRQu4b5mU
```

```
hOKn+BGJ2LNeWI/tLLCXHfN27x3RkDHZR7q8UupnukVlArCt+1ck+Fph0xE9G3UG
JF5KmQWm9n+1fWMzynj9vy4CBERtOgc5ktVNJOek4Mr+14vz9NykbBwgJthpDaFK
HtRgVimokTCxVckIc3aLK9dXPUBCh9D3GpUw6ruEn17/PWvveAnLDmbsfpGxizlF
uC8OWRgaKSdgZhZBqyFS0Wb6B39gWgoK9xh4/Ma90dLADAEbDAN6eRqvhYhADWW+
fLkFU3q8If0CYZY1tIeXLa46IxqiQaBPQfOQ7MfG5gAWAV5AHdd6ehWMKfy1Yoye
K3ikc18BZMRCLMmEilI+pDrIpcii5LJSTxpzjkX4eGaq1/gyJIEbpkXRLr5OSKmN
m/pS1ylm5XvapQCpDo7DAAFZ13QpLmGf54gMZOTFYGZzg7EMcShL5nZ4y16GJ2DK
qlpLCcVluNzJDEBnlYaVEGzrHJNgpNldNDjYn2NN780iJuronSwzyMP7NPTm0A==
=iO3p
```

➢ **Decrypting the message**

The journalist uses their private key to decrypt the session key. The session key then decrypts the body of the message, returning it back to its original form:

Dear Susan Peterson,

I have some information about a huge corruption scandal in The United States of Mozambabwe. Let me know if you are interested and I will send you more details.

➢ **Verifying the digital signature**

If the journalist is skeptical about the integrity of the message or believes that it may not have been sent by you, they can verify the digital signature. They run the message they received through a **hash function**, which gives them the **message digest** of the email they received.

The journalist then uses your **public key** and your **digital signature** to give them the **message digest** as it was when you sent the message. If the two message digests are identical, then they know that the message is authentic. From this point, you and the journalist will be able to communicate backwards and forwards with PGP to discuss the details of the corruption scandal.

Reference

JOSH LAKE. (2018) *What is PGP encryption and how does it work?* Available from: https://www.comparitech.com/blog/information-security/pgp-encryption/ (Accessed 15th March, 2019)

kraken. (n.d.) *What is PGP/GPG encryption?* Available from: https://support.kraken.com/hc/en-us/articles/201648223-What-is-PGP-encryption- (Accessed 15th March, 2019)

Radu Raicea. (2017) *How Pretty Good Privacy works, and how you can use it for secure communication.* Available from: https://medium.freecodecamp.org/how-does-pretty-good-privacy-work-3f5f75ecea97 (Accessed 15th March, 2019)

CHIRS BROOK. (n.d.) *What is PGP Encryption? Defining and Outlining the Uses of PGP Encryption.* Available from: https://digitalguardian.com/blog/what-pgp-encryption-defining-and-outlining-uses-pgp-encryption (Accessed 15th March, 2019)

Assignment

Create a secure mail communication with some particular privacy layers. You can use any OS platform you want (Windows, Linux/Unix, MACOS) and any mail client you like (Outlook, Gmail). Look for some available tools to perform tasks like Gpg4win (for Outlook), Secure Compose (for Gmail). There are lots of tutorial available for both such as 'PGP encryption using Outlook' & 'Encryption using Gmail'.

Implement the following privacy layers-

- Digital Signature from sender & receiver (Hint: You can use Kleopatra).
- Encrypt & decrypt the plaintext (Sender & Receiver end).
- Encrypt & decrypt the attachment (Sender & Receiver end).

*****Please, remember, you have to demonstrate the assignment in the exercise session (27th March, 2019) where both the group member will participate during demonstration.**

Assessment Criteria (Total 8 Points):

- Successful Plaintext Encryption (2 points)
- Successful Plaintext Decryption (2 Points)
- Successful attachment Encryption (2 Points)
- Successful attachment Decryption (2 Points)
- **Implement Digital Signature (Bonus: 2 Points)**