Pretty good privacy

Law, Security

Information security is a significant issue which attract people’s a lot attention in current society. The email security is highlighted problem in this area. According to Email Statistics Report 2012-2016 (Radicati Group), there are 3. 3 billion worldwide email accounts in 2012, and are expected to increase to 4. 3 billion accounts in 2016. In general, transfer of email has many protocols; the SMTP is a main one. In this protocol, the content is required to be plaintext for transfer. So, the detail of email is actual send as plaintext.

Any attempted individual or group can intercept emails. For example, companies or websites reply a notice mail to you for confirming you register information. This kind of mail usually contains some sensitive information (account ID, password). The leaking of this information will produce many security problems. The email providers only offer security methods in physics layers or servers, while the practical content of mails always is plaintext in the email environment. Therefore, people consider a method which is able to encrypt the contents of emails to achieve the security requirement.

Pretty Good Privacy (PGP) is system which is widely used in the email environment and digital signature. This system employs few encryptions to ensure the information security and integrity during network transmission. In this project, we are going to analyze many aspects of PGP, such as standards, protocols and implementations. Also, we will use SVO logic to proof the authentication of PGP. Description: In this project, firstly, we will collect some general information to review the background and history PGP.

Then we will focus on the details of mechanism of its different aspects, like what algorithm does it use to achieve authentication, and how does it

encrypt the emails, etc. In this step, We are going to read some papers and books to get good understanding of the encryption system it utilizes, and the mechanism of how does it implement these encryption systems. For example, how does it generate the public and private key pair and how does it use the web of trust to manage the public keys and private keys, etc.

After the paper review above, we should know PGP pretty well. The next step, we will do some analysis about the encryption systems and their implementation in PGP. At the beginning, we will do some basic comparison of the encryption system used, like AES, 3DES, Twofish, etc, to see which one is faster and which one is safer. Then we are going to use SVO logic proof to analysis PGP authentication to prove its effectiveness. At the end we will analysis the mechanism generally to find the potential weaknesses and probable successful attacks.