JSS Academy of Technical Education
Kengeri-Uttarahalli Main Road, Bangalore-560060

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Subject: Information and Network Security Assignment 3

Topic: Email Security

Academic Term: Aug-Dec 2020

Name: Ritwik Gupta

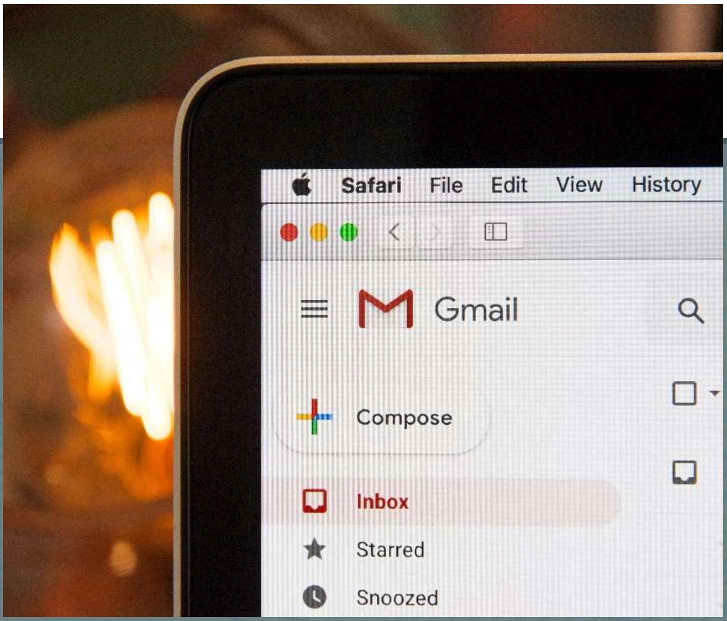
USN: 1JS17CS081

Class: 7B

What is Email Security?

Email security explains diverse procedures for storing delicate information in email communication and accounts protected against unauthorized path, loss or settlement. An Email is usually prepared to increase malware, spam and phishing attacks. Attackers use ambiguous reports to attract recipients. For sharing reports with delicate information, free attachments or click on hyperlinks. These install malware on the victim's machine. It is also a common entry point for attackers scanning to gain a space in an enterprise network and important company data.

Email encryption involves encrypting, or changing, the content of email messages to preserve possibly sensitive knowledge from being read by anyone other than expected recipients. Additionally, it often includes authentication.



EMAIL SECURITY REQUIREMENTS

There are two potential concerns about the security of email:

Confidentiality. By default, email messages are unprotected during their transfer from the email sender's device to the email receiver's device. During that transfer the email message resides on several email servers and internet routers, as well as passing through various potentially unprotected networks. There are many points at which, at least in theory, the contents of an email message could be viewed by someone other than the intended recipient.

Data origin authentication. Email messages are structured using a simple protocol that facilitates their transfer. This protocol includes fields for specifying the sender, recipient and subject, as well as the message itself. An informed attacker can fairly easily generate forged emails. In addition, at most of the points at which an attacker can read a genuine email, the attacker could intercept and make changes to the email message before forwarding it on to the recipient.

APPLICATION CONSTRAINTS THAT INFLUENCE DECISION MAKING

Because of its ubiquity and inherent vulnerabilities, email is a popular vector for cyber-attacks. These attacks can include:

- Malware, such as viruses, worms, Trojan horses, and spyware. When attacks using these vectors succeed, an attacker can take control of workstations or servers. This access can then be exploited to compromise otherwise secure information.
- Spam, which can be disruptive to worker productivity, and can also serve as a transportation method for malware.
- Phishing, which entails the use of computer or social engineering tricks to convince victims to disclose sensitive information, or to provide access to sensitive systems.

Email security is the set of methods used for keeping email correspondence and accounts safe from these attacks

Cryptographic Primitives

There are two well-known standards for protection of email, each of which are implemented by a wide range of email security applications.

Both ***Open Pretty Good Privacy (OpenPGP)*** and ***Secure/Multipurpose Internet Mail Extensions (S/MIME)*** broadly work in the same way, although precise implementations may have minor differences. They both provide confidentiality and data origin authentication (non-repudiation) through support for encryption and digital signatures. They are either supported by default in certain email clients or can be installed through plug-ins.

There are three ways in which email messages can be protected using these applications:
Confidentiality only. This is provided by hybrid encryption. The symmetric encryption key is either generated using a deterministic generator or a software based non-deterministic generator. The body of the email message is then encrypted using this symmetric key, and the symmetric key is encrypted using the public key of the recipient.
Data origin authentication only. This is provided by a digital signature scheme with appendix. The email message is first hashed and then signed using the signature key of the sender. The receiver will need to obtain the corresponding verification key in order to verify the resulting digital signature.
Confidentiality and data origin authentication. This is typically provided by following the MAC-then-encrypt construction. In other words, a symmetric encryption key is generated and the email message is digitally signed, as described above. The email message and the resulting signature are then both encrypted using the symmetric encryption key. Finally, the symmetric encryption key is itself encrypted using the public encryption key of the recipient.

Cryptographic Algorithms

There are various types of email encryption, but some of the most common encryption protocols are:

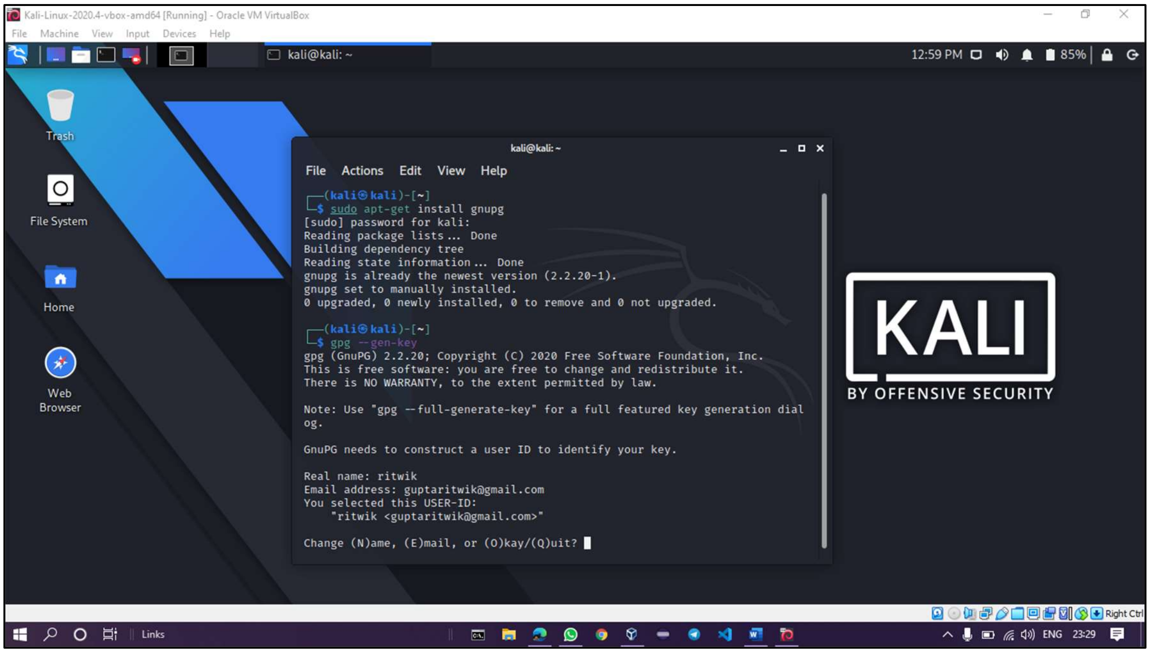
- **OpenPGP** - a type of PGP encryption that utilizes a decentralized, distributed trust model and integrates well with modern web email clients. OpenPGP is the most widely used email encryption standard. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a Proposed Standard in RFC 4880. OpenPGP was originally derived from the PGP software, created by Phil Zimmermann.

- **S/MIME** - a type of encryption that is built into most Apple devices and utilizes a centralized authority to pick the encryption algorithm and key size. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most

Key Management

OpenPGP is more flexible and can be supported by almost any form of public-key management system. The default public key management model for OpenPGP is to use a web of trust, although more formal public-key management can also be supported. On the other hand, S/MIME is based on the use of X.509 Version 3 certificates supported by a structured public-key management system relying on Certificate Authorities.

Let’s have a look at HOW IT WORKS?



Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
12:59 PM
85%
Trash
File System
Home
Web Browser
kali@kali: ~
File Actions Edit View Help
KALI
BY OFFENSIVE SECURITY
Right Ctrl
Links
ENG
23:29

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install gnupg
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
gnupg is already the newest version (2.2.20-1).
gnupg set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[~]
└─$ gpg --gen-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dial
og.

GnuPG needs to construct a user ID to identify your key.

Real name: ritwik
Email address: guptaritwik@gmail.com
You selected this USER-ID:
    "ritwik <guptaritwik@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? █
```