Email Security

Information Security Term Project

Prepared By:

Tahreem Jamal	30604
Saad Imran	29818
Muhammad Waqas	29567
Usama Hayat	
Usama Ali	29348

Prepared For:

Dr. Muhammad Aihab Khan

Introduction

Email security describes the process and procedures used to secure email accounts, information, and communication against unauthorized access, loss, or compromise. Malware, spam, and phishing attacks are frequently transmitted over email. Attackers employ fake message to persuade users to provide personal information, open attachments, or click on hyperlinks that download malware to the victim's device. Attackers attempting to get a foothold in an enterprise network and obtain valuable company data frequently use email as an entry point. Email encryption encrypts or disguises the content of emails to prevent sensitive information from being read by anybody other than the intended receivers. Authentication is frequently included in email encryption. Email encryption often includes authentication.

How Secure Is Email

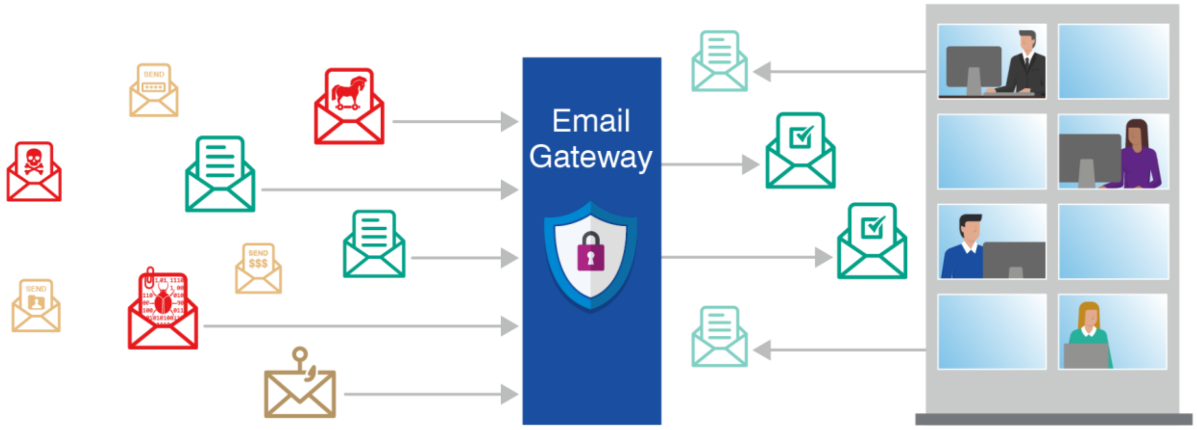
Email was created with the goal of being as open and accessible as possible. It enables employees in one organization to communicate with employees in other organizations. The issue is that email is not a secure medium. As a result, attackers can utilize email to cause issues in order to profit. Spam campaigns, malware and phishing attempts, sophisticated targeted attacks, and business email compromise (BEC) are just some of the ways attackers try to take advantage of email's lack of security. Because most businesses rely on email to do business, attackers use it to try to steal important information. Because email is an open format, anyone who can intercept it can read it, posing a security risk. As businesses began sending confidential or sensitive information via email, this created a problem. By intercepting an email, an attacker might readily access its contents. Organizations have increased email security measures throughout time to make it more difficult for attackers to access critical or confidential information.

Email Security Policies

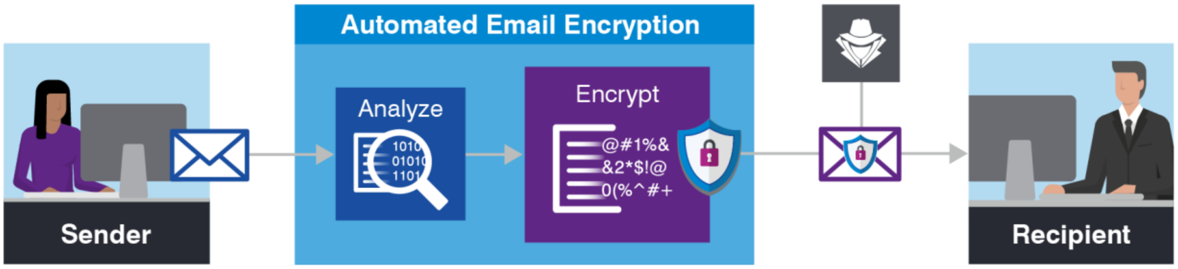
Organizations have formed policies surrounding how to handle email because it is so important in today's business world. Viewing the contents of emails travelling through email servers is one of the first practices most firms set. It's critical to comprehend the entirety of the email in order to behave effectively. Following the implementation of these baseline principles, an organization can enact various security measures on those emails. These policies can range from simple measures like deleting all executable content from emails to more in-depth activities like forwarding questionable content to a sandboxing tool for full investigation. If these procedures detect security issues, the organization must have actionable intelligence about the attack's extent. This will aid in determining the extent of the attack's harm. Once a company has insight into all emails sent, it may enact email encryption policies to keep sensitive email information out of the wrong hands.

Email Security Best Practices

Implementing a secure email gateway is one of the first best practices that enterprises should employ. All incoming and outgoing email is scanned and processed by an email gateway, ensuring that no threats are allowed in. Standard security methods, such as preventing known dangerous file attachments, are no longer effective due to the sophistication of assaults. Deploying a secure email gateway with a multi-layered strategy is a superior choice.



As a best practice, you should also implement an automated email encryption system. This solution should be able to examine every outbound email traffic to see if it contains sensitive information. If the information is confidential, it must be encrypted before being sent to the designated recipient. Even if attackers intercept emails, this will prevent them from being viewed.



Employee training on proper email usage and understanding what constitutes a good and bad email is another crucial best practice for email security. Users may get a malicious email that gets past the secure email gateway, therefore knowing what to check for is crucial. Phishing assaults, which include unmistakable indicators, are most commonly used against them. Employees who have received training are better able to recognize and report these types of emails.

Email Security Tools

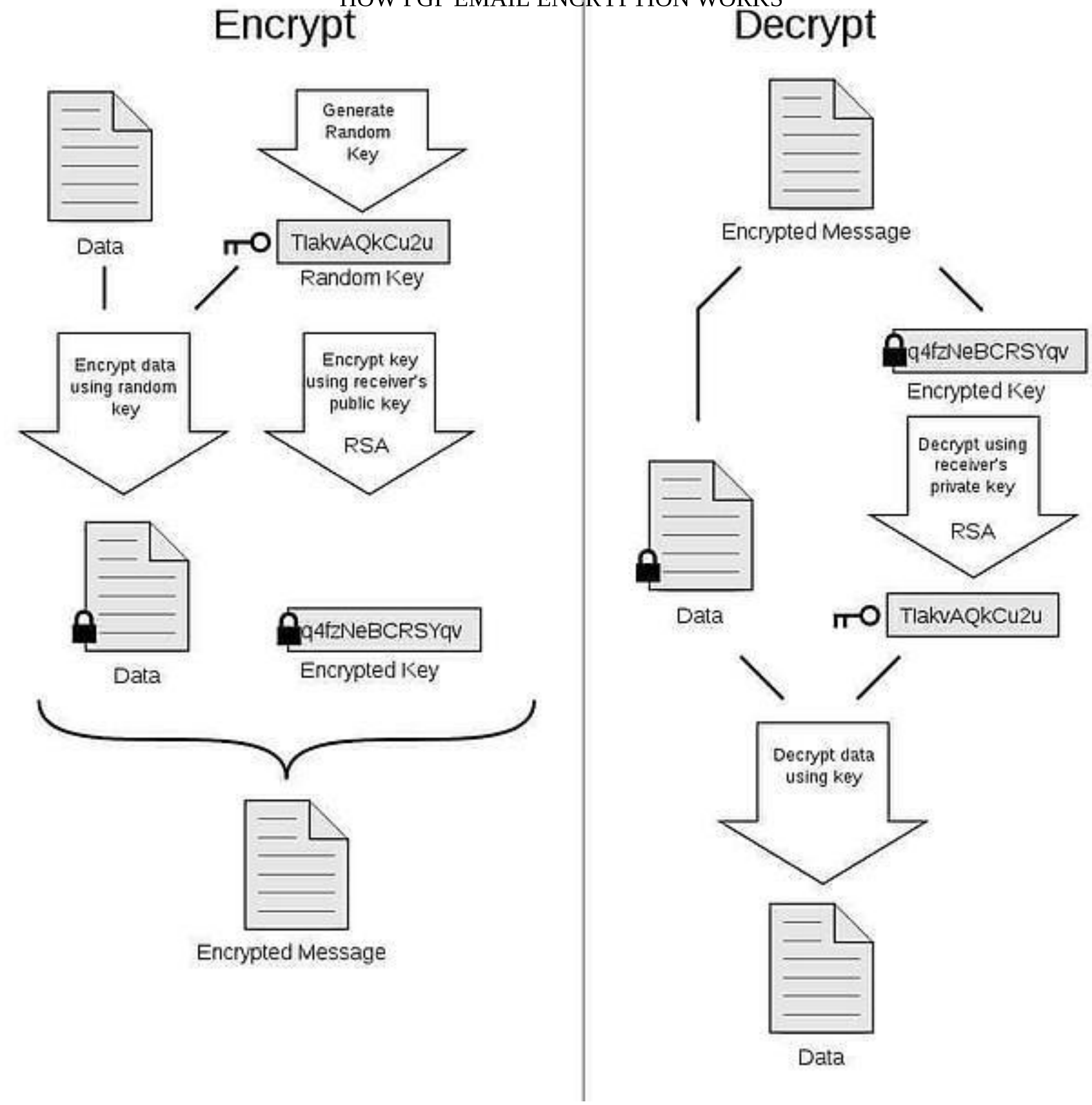
- A Secure Email Gateway, deployed either on-premises or in the cloud, should offer multi-layered protection from unwanted, malicious and BEC email; granular visibility; and business continuity for organizations of all sizes. These controls give security teams confidence that they can protect users from email threats while also keeping email communications running in the event of a system failure.

- An Email Encryption Solution, reduces the risks associated with regulatory violations, data loss and corporate policy violations while enabling essential business communications. The email security solution should work for any organization that needs to protect sensitive data, while still making it readily available to affiliates, business partners and users—on both desktops and mobile devices. An email encryption solution is especially important for organizations required to follow compliance regulations, like GDPR, HIPAA or SOX, or abide by security standards like PCI-DSS.

Encryption Keys for Email Encryption

A main characteristic of a cyphering code, or algorithm, is to make sure that the email message is unreadable by a third party, even if it falls into the wrong hands. A best-in-class encryption algorithm encrypts your email messages at a level of cyphering that requires many years for a bad actor to decrypt even the simplest message.

HOW PGP EMAIL ENCRYPTION WORKS



Why is Email Encryption Important?

Email encryption is important because it protects you from a data breach. If the hacker can’t read your message because it’s encrypted, they can’t do anything with the information. Since 2013, over 13 billion data records have been lost or stolen. The average cost of a data breach in 2018 is $3.86 million. This number has grown by 6.4% since 2017. Data breaches can be costly because they take a while to identify. In 2018, the mean time to identify a breach was 197 days and the mean time to contain it was 69 days. Email encryption is a preventative measure you can take to avoid being part of a cybersecurity statistic.

Email Encryption Source Code

```
#include "stdafx.h"
#include <tchar.h>
#include <Windows.h>

#include "EASendMailObj.tlh"
using namespace EASendMailObjLib;

const int ConnectNormal = 0;
const int ConnectSSLAuto = 1;
const int ConnectSTARTTLS = 2;
const int ConnectDirectSSL = 3;
const int ConnectTryTLS = 4;

int _tmain(int argc, _TCHAR* argv[])
{
    ::CoInitialize(NULL);

    IMailPtr oSmtp = NULL;
    oSmtp.CreateInstance(__uuidof(EASendMailObjLib::Mail));
    oSmtp->LicenseCode = _T("TryIt");

    // Set your sender email address
    oSmtp->FromAddr = _T("test@emailarchitect.net");
    // Add recipient email address
    oSmtp->AddRecipientEx(_T("support@emailarchitect.net"), 0);

    // Set email subject
    oSmtp->Subject = _T("Encrypted email from Visual C++ (S/MIME)");
    // Set email body
    oSmtp->BodyText = _T("this is a test encrypted email sent from Visual C++");

    // Your SMTP server address
    oSmtp->ServerAddr = _T("smtp.emailarchitect.net");

    // User and password for ESMTP authentication, if your server doesn't
    // require User authentication, please remove the following codes.
    oSmtp->UserName = _T("test@emailarchitect.net");
    oSmtp->Password = _T("testpassword");

    // Most mordern SMTP servers require SSL/TLS connection now.
    // ConnectTryTLS means if server supports SSL/TLS, SSL/TLS will be used automatically.
    oSmtp->ConnectType = ConnectTryTLS;

    // If your SMTP server uses 587 port
    // oSmtp->ServerPort = 587;
    // If your SMTP server requires SSL/TLS connection on 25/587/465 port
    // oSmtp->ServerPort = 25; // 25 or 587 or 465
    // oSmtp->ConnectType = ConnectSSLAuto;

    //add signer digital signature
    if(oSmtp->SignerCert->FindSubject(_T("test@emailarchitect.net"),
        CERT_SYSTEM_STORE_CURRENT_USER , _T("my")) == VARIANT_FALSE)
    {
        _tprintf(_T("Error with signer certificate; %s\r\n"),
            (const TCHAR*)oSmtp->SignerCert->GetLastError());
        return 0;
    }
    if(oSmtp->SignerCert->HasPrivateKey == VARIANT_FALSE)
    {
        _tprintf(_T("certificate does not have a private key, it can not sign email.\r\n"));
        return 0;
    }

    // Find the encrypting certificate for every recipients
    ICertificatePtr oCert = NULL;
    oCert.CreateInstance("EASendMailObj.Certificate");
    if(oCert->FindSubject(_T("support@emailarchitect.net"),
            CERT_SYSTEM_STORE_CURRENT_USER, _T("AddressBook")) == VARIANT_FALSE)
    {
        if(oCert->FindSubject(_T("support@emailarchitect.net"),
                CERT_SYSTEM_STORE_CURRENT_USER, _T("my")) == VARIANT_FALSE)
        {
            _tprintf(_T("Encrypting certificate not found; %s\r\n"),
                    (const TCHAR*)oCert->GetLastError());
            oCert.Release();
            return 0;
        }
    }

    // Add encrypting certificate
    oSmtp->RecipientsCerts->Add(oCert);
    oCert.Release();

    _tprintf(_T("Start to send email ...\r\n"));

    if(oSmtp->SendMail() == 0)
    {
        _tprintf(_T("email was sent successfully!\r\n"));
    }
    else
    {
        _tprintf(_T("failed to send email with the following error: %s\r\n"),
            (const TCHAR*)oSmtp->GetLastErrDescription());
    }

    return 0;
}
```