CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

E-mail Encryption
IoT Privacy
Compliance & Security
Security Automation

Halting Hackers for the Holidays

12 Tips Before Christmas

November 2015

MORE INSIDE!

End-to-End Encryption for Emails. An Organizational Approach

by Dr Burkhard Wiegel, Founder and CEO, Zertificon Solutions

The threat to electronic enterprise communication used to be beyond the firewall. With the increased use of mobile devices for business email, the need to secure communication from sender to recipient and within the corporate network has raised the awareness for industrial scale end-to-end encryption.

There are risks and pitfalls associated with the existing concepts of end-to-end encryption. Many solutions are available which deliver personal simple client-side encryption or just transport layer encryption which are not suitable for organizations. This paper will introduce an alternative organizational approach for secure end-to-end communication.

Secure Channel versus Content Encryption

When discussing email encryption the topic of Transport Layer Encryption (TLS) always arises. TLS has become a popular and established technology but it is often mistaken for a full-blown end-to-end encryption solution. TLS however, only secures the communication between two mail relay servers and not the actual message content. Not only is the message content unencrypted during transport but also whenever it is stored. This includes temporary storage on mail relay servers as well as mid-term to permanent storage in users' server-side mailboxes and archives.

Any hackers who can make it through the firewall can simply help themselves to whatever they find. In case of sync, pop or push services emails are also unprotected on the client device. TLS gives the appearance of being secure, but does not deliver enterprise level security. Even VPN and other secure channel methods which secure the transport but not the content have the same security problems as TLS. It is always better to secure the message.

End-to-end encryption appears to be the only solution which provides real security and confidentiality. After the NSA scandal, security experts who were vocal in the media, called for the comprehensive adoption of end-to-end encryption but never came up with realistic day in, day out solutions which could be rolled-out throughout companies.

Enterprise Email Encryption Status Quo

Modern encryption is based upon asymmetric keys which commonly utilize a Public Key Infrastructure (PKI) such as S/MIME or OpenPGP. Not surprisingly, these two systems are incompatible. Although they both rely on the same cryptographic concepts their trust models are very different.

OpenPGP relies on a peer based “web of trust” in which users vouch for each other. S/MIME on the other hand relies on a hierarchical trust model where a higher entity vouches for a lower entity and states how this trust is established (e.g. identity checks).

Certification Authorities (CAs) sign the public keys and from that moment on a public key becomes a certificate. The CA publishes the certificate alongside up to date status information relating to the

Copyright © Cyber Defense Magazine, All rights reserved worldwide

validity of the certificate. Certificate servers such as www.globaltrustpoint.com collate and validate certificates from the CA servers.

S/MIME is supported by all popular email clients and has become the standard in the business world. Because obtaining an S/MIME certificate can involve cost, most private users utilize OpenPGP based encryption which requires usually free 3rd party software.

Both S/MIME and OpenPGP use a key pair which consists of an encryption and decryption key. The encryption key is public and must be made available to the message sender whereas the recipient keeps hold of the private decryption key.

Only the holder of the private key can decrypt messages encrypted with the public key. The public key also contains information which can be used to check the authenticity and validity of the key.

Certificate Management Challenge

It becomes clear that the real challenge for businesses is not the encryption itself, but the management of the private and public keys. Private keys for employees have to be protected, issued and revoked when staff join and leave the company whilst their public keys have to be made available to communication partners.

At the same time the public keys from communication partners have to be made available to employees.

Throw into the mix the fact that many communication partners may be using OpenPGP keys and the scalability of key management suddenly becomes a problem. Public keys from communication partners have to be searched for, saved, validated and checked against revocation lists in real time. The PKI challenge is to automate the full key management and make it fully transparent to employees.

Centrally applied encryption with Policies

Encryption and security is only guaranteed when it is applied every time it is required. Removing the encryption decision and the key management from employees and making the encryption process automated and invisible guarantees security and compliance.

The solution is “Secure Email Gateways”. These fully automate the key management and use configurable policies to ensure that encryption is applied when it is required.

Secure Email Gateways deliver a number of key advantages to businesses. Their centralized deployment removes the need for any end-user software and training. Emails are en-/decrypted automatically and all keys are managed centrally. Keys from 3rd parties are checked to ensure that they are valid and employee's keys are made available to communication partners.

But one of the key advantages delivered by Secure Email Gateways, is the ability to communicate securely with any partner regardless as to whether they are using S/MIME, OpenPGP or do not have any encryption software installed at all.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Communicating without PKI Keys – Secure email delivery

Password based encryption has become an established alternative to key based encryption. The message can be delivered directly to the recipient as an encrypted PDF file or a secure web mailer account can be created on the fly for each recipient.

Only instructional messages to the recipient are communicated using non-encrypted emails whilst the sensitive content is always protected. Secure PDF or web mail delivery enables businesses to communicate instantly and securely with any recipient.

Limits of Gateway Security

A Secure Email Gateway acts as an interface to the Internet at which emails are en-/decrypted. Within the company network however, the emails are transmitted in a plain state without any encryption.

This remains a secure method to protect against foreign intelligence services and industrial spying and has been used by companies, institutions and public authorities for years. At the same time however, there are situations in which end-to-end encryption is required.

When using mobile devices such as laptops, phones and tablets emails are transmitted outside the company network via WiFi or mobile network in plain text. It takes little investment and only basic skills to gain access to the message content.

Therefore the aim is to secure the content itself between the gateway and end users as well as between users. Securing the transport layer with TLS or VPN can add some level of protection and investment in Mobile Device Management Systems (MDM) should not be ignored.

But foolproof security can only be achieved when the content is secured in transit and of course when it is stored in an encrypted state on intermediate servers and end devices.

End-to-End Approach for Enterprises

End-to-end encryption usually means complete content encryption between end devices and also the encrypted storage of the message on the end device. Only the recipient who is in possession of the required key can decrypt and access the message and its content.

However, this highly secure communication method raises a number of problems for businesses. Employees work for the business and the information and communication they generate belongs to the company. In order to support audit compliance, archiving and business continuity, it is imperative that the company has control over its entire email traffic.

Companies also need be in control in order to protect themselves from spam, viruses, loss of data and even phishing attempts despite email encryption. The roll-out of distributed content filtering and scanning would be simply not scalable or practicable in a standard end-to-end encryption scenario.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Organizational Approach – Combining internal with external encryption

For everyday use within a business environment, even with end-to-end there needs to be a point of access to the actual mail content. The organizational approach sees this single point of access at the Secure Email Gateway if the Gateway is deployed together with an End2End encryption solution.

The task of the End2End solution is to manage an encapsulated internal PKI and enable the Gateway to bridge between the internal and external PKIs. Imagine this as encrypting in two different worlds with a passage from one world to the other. This passage is the access point that gives organizations control over their email traffic.

The internal world speaks only S/MIME. S/MIME is supported by all standard email clients out of the box which means low administration efforts. The Gateway translates S/MIME to and from other encryption languages. An internally S/MIME encrypted email can reach an external recipient as an OpenPGP encrypted mail or via secure Webmailer depending on the recipient's environment.

Emails are stored in an encrypted state on email servers and cannot be read by system administrators – especially important if the company email infrastructure is a third party hosted service. The email also remains encrypted on the end device and can only be decrypted as needed by the user.

The work flow proceeds as follows: Encrypted emails reach the gateway, they are decrypted at the Gateway from which they can be routed to content filters such as virus scanners or data loss prevention tools. Those tools process the emails following their own routines and send them back to the Gateway where they are re-encrypted for the next part of their journey. If the journey is internal the email will be re-encrypted using the keys of the internal S/MIME PKI.

Outbound emails will be received by the Gateway in an S/MIME encrypted state. In order to re-encrypt this email for the travel over the Internet the Gateway checks the possibilities for secure email delivery depending on the external recipient's data. This enables instant end-to-end encryption with virtually everyone.

And the original sender does not even need to know how things work. All the sender needs to know is that the email was securely encrypted without worrying about the actual technical details. This scenario is ideal for organizations and is referred to as “Organizational End-to-End”.

Organizational End-to-End can work in parallel with the so called “Personal” method. Messages are fully encrypted from sender to recipient. This is analogue to the classic form of End-to-End encryption and is targeted at users with high security needs such as a board of directors.

Encryption takes place on the client devices and no content filtering can take place. In fact, not even the gateway administrator can access the message content.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Spicing up the internal world

As we learned standard email clients support S/MIME and therefore make end to end encryption possible without any extra software. However without any additional plug-ins, the end-user is responsible for encrypting emails and must be trained accordingly.

Any risks can be eliminated through the deployment of email client plug-ins which take over the responsibility for activating encryption and for selecting the appropriate encryption method according to centrally configured security policies.

Even with state of the art technology, security is only good when it is accepted and used correctly by employees.

Summary

Public key infrastructures provide the corner stone of secure email communication. It does not matter what encryption technologies the communication partners use or even if they have a method of decrypting messages.

Secure Email Gateways can ensure that emails are delivered securely from the employee's computer right to the recipient. For organizations, companies and public agencies that do not use use mobile end devices and do not have any secrets to hide from their mail server admins, a Secure Email Gateway is all they need.

For all others Organizational End-to-End combined with Personal End-to-End delivers a universal solution for secure email communication that protects emails in transit and in rest.

About The Author

Dr. Burkhard Wiegel is the founder and CEO of Zertificon Solutions. He graduated in computer science and obtained his doctorate at the Technical University in Berlin. He has published many papers on secure email and was a pioneer in the IT security market, long before email security became a mainstream topic.

His research and insights led to the development of Zertificon's Z1 SecureMail Gateway – one of Europe's leading email encryption solutions.

Burkhard can be reached online at LinkedIn and our company website https://www.zertificon.com/ He will be available for meetings at the German Pavilion on next years RSA® February 29 – March 4, 2016 in San Francisco. Zertificon is looking for resellers in the USA.

Copyright © Cyber Defense Magazine, All rights reserved worldwide