Thoughts on E-Mail Transport Security

Uwe B. Meding
uwe@uwemeding.com

Encryption and signatures enable a confidential and secure email communication. This revelation is not new, however, a lot of companies shy away from implementing and deploying these technologies. In particular small- and mid-sized companies have little investment in this area.

Background

Almost every business process today uses email as a communication tool, all the way from a simple exchange of information to the completion of legal transactions. For these reasons it is paramount that

- the email systems are available around the clock
- the communication partner can be uniquely identified (*authenticity*)
- the content of an email is not changed during transport (*integrity*)
- the content does not end up in somebody else's in-box (*confidentiality*)

Anyone of these information security goals can be systemically undermined in a number of ways: malware (viruses and trojans), spam, phishing, illegal access, or human error. The threats have a great impact on availability, integrity, authenticity, and confidentiality of the data being sent. Encryption and signatures are protective measures that can help mitigate these issues.

Analysis

Before implementing any protective measures we need to go through a needs analysis to determine the parameters for a solution that will address the security requirements of a company and also determine budget and effort. First off, the security goals: These is mainly developed by interviewing the subject experts in each of the business areas of a company. The aim is to identify the role and influence of email communication in their particular operational areas.

We also need to determine the level of protection for the data and the required availability of the email system. Any technical planing details need to be defined with the IT management. Regulatory rules have to be added to the plan as well as company internal guidelines with respect to data security. A more or less complete analysis is a major factor for the acceptance for a particular solution. This should be followed by a gap analysis to determine what aspects of the desired plan have already been realized.

During the initial implementation phase we need

to evaluate how to meet the professional, technical, and administrative needs:

- create the appropriate architectural concepts
- design the corresponding processes (business or technical)
- define the accompanying roles

This forms the basis for the evaluation of suitable products. A proof of concept implementation phase validates that all the professional and technical needs have been met. Following this, the company-wide implementation and deployment should begin.

Technical Solutions

The goals for integrity and confidentiality for email communication can really only be met with encryption and signatures. There are two established standards available for this: Pretty-Good-Privacy (PGP) and Secure Multipurpose Internet Mail Service (S/MIME).

Both implementation are based on asynchronous methods in which each participant has a key-pair, one public and the other private. The private key is only known to the owner and needs to be protected accordingly, for example, storing it on a smart card, or local key store (sometimes called "wallet").

The public key on the other hand has to be accessible by all communication partners. The public key should be stored in a convenient place: a public web server or a directory service. Sending an encrypted e-mail requires the public key of the recipient. The corresponding private key is used the recipient to decrypt the email content. This process guarantees the confidentiality of an email message. The authenticity of the email sender and integrity of the email content can be verified with the aid of a signature. The signature has no impact on the readability of the email message; it only guarantees that the email was not manipulated or changed during transport.

E-mail signing process

1. create a hash key digest of the entire email
2. use the sender private key to encrypt the hash key
3. send the email along with the *encrypted* hash key

E-mail signature verification process

1. create a hash key digest of the entire email
2. decrypt the senders hash key digest using the senders public key
3. compare both hash keys

The integrity and authenticity of the email is guaranteed when both hash keys are the same.

Caveats

Strictly speaking, the S/MIME and Open PGP methods are using the same cryptographic processes, however, their implementations are not compatible with each other. Hence users of either method cannot exchange signed or encrypted messages. The issues arises mainly from the different transfer formats for the email content.

Another difference is the validation test of the public key portion. S/MIME uses certificates are following the X.509 standard. In particular, it calls for only *one* signature for the public key - in general this a certificate authority (CA).

Whereas S/MIME uses a strict hierarchy of issuing certificate authorities, OpenPGP allows many signatures and is additionally signed by itself. OpenPGP uses decentralized servers and the so called *web of trust*, where the authenticity of a public key is validated through a net of mutual confirmations.

E-Mail Encryption

There are two solutions for the implementation of email message encryption: the *end-to-end* approach which is a complete encryption between the communication partners or the *gateway* approach which is an encryption of the communication paths between the partners.

End-to-end Encryption

The end-to-end method uses encryption applications on the local computer of the sender. Modern email client applications typically integrate the encryption and signature processes.

The encryption is an action initiated by the user. He alone decides if and for whom an email is encrypted.

The decryption takes place on the target computer of recipient of the email communication.

This variant leaves the email encrypted for the entirety of the transport. Unauthorized access to the email content during transport is therefore not possible. Only the owners of the private keys can view the content that has been encrypted with their respective public keys.

The advantage of this method is that the content is not only protected throughout transport, but also within a company's network. The drawback of this method is that it requires the user to be knowledgeable about which data needs to be encrypted and which one doesn't.

Initially, processes and an infrastructures need to be implemented that

- assign and comprehensively manage the private keys for every user
- make the corresponding public keys accessible to all communication partners

Great care needs to be taken during design and implementation of these processes to preserve the integrity of the unique user assignment. Access to the system must be revocable if the need arises.

Apart from the obvious security enhancement, there are a several disadvantages:

- any anti-spam or anti-virus measures at the exchange gateways are ineffective because encrypted emails cannot be introspected.
- any content protection measures are also ineffective and it opens up the possibility that critical intellectual property ends up with a competitor.

Gateway encryption

The gateway encryption method leaves the email communication unencrypted within the networks of the company and only uses encryption to communication partners outside. For this it makes to choose products that can handle both, the S/MIME and OpenPGP standards as well as email access through the web (via HTTPS) for communication partners that do not have a corresponding email encryption infrastructure.

Gateways can also work with so called *corporate keys* (all emails are signed and encrypted using the same corporate key) or with user specific keys (transparent implementation of the end-to-end method). The advantage is that all outgoing email is encrypted through centrally managed rules and systems (and transparent to the user). Alternatively, this process could be guided by the user by adding special keywords to the email, for example, be adding the word "secret" into the subject line. The gateway encryption process will then automatically encrypt the message to the recipient.

Conclusions

Which of these method makes sense depends very much on the needs of the company for security and functionality. Therefore we will always need a comprehensive and detailed needs analysis prior to implementation and deployment.

Encrypting the transport channel is a quick way to secure the transfer of the email communication. However, this is only really useful for companies that work together directly and need to secure the communications between them. For example geographically dispersed companies, or different companies that participate in a supply chain.

If the communication partners change frequently, the end-to-end encryption or a central gateway based on S/MIME or OpenPGP are the only solutions. This usually a higher effort with respect to designing and implementing the required processes and infrastructure.

Do not underestimate the human factor!

Access to corporate information has been dramatically increased via the rapid deployment of laptops/notebooks and by the mobile computing devices (tablets and smart phones). Access to information has become unlimited by time, location, or distance. Structuring a program for identifying and safeguarding essential information against the wide array of threats at this level of complexity is substantially more difficult than protecting information safely inside a fixed location.

"Business: Anywhere, Anytime, Anyway" seems to be the implicit mission of many organizations. The most important fact to emphasize in considering the new risks arising from global operations and associated global networks information systems infrastruc-

ture is that the organization truly is “only as strong as the weakest link” whether that is an unlocked file cabinet in the head office, an unsecured desktop workstation logged on to a corporate system half-way around the world, or a laptop computer forgotten at an airport.

Technology alone does not provide complete security from all threats. Users need to be trained and sensitized to the ways confidential data is must be treated. The key to an acceptable security level is the combination of responsible users and appropriate technologies.