White paper

E-mail encryption:

What it is and why you need it

Introduction

This white paper provides useful background information on encryption, an essential e-mail security feature. It will help you examine the risks involved in sending unsecured corporate and personal e-mail messages, and explains how encryption eliminates such hazards.

The following topics are covered:

The information contained in this document represents the current view of GFI FAX & VOICE on the issues discussed as of the date of publication. Because GFI FAX & VOICE must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI FAX & VOICE, and GFI FAX & VOICE cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. GFI FAX & VOICE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Corporate e-mail messaging

By 2001, 35 percent of business documents will move across the Internet, according to Darcy Fowkes, an analyst at Boston-based Aberdeen Group, as quoted by *The Industry Standard* of August 9, 1999. That would amount to a stunning 21 million missives a day.

Business executives tend to select e-mail as their preferred form of communication because it proves cheaper, faster and more reliable, a choice set to become increasingly popular as e-commerce gains more ground. As suggested in the same *The Industry Standard* article, e-mail is the likeliest contender as “the killer e-commerce app”.

E-mail reaches the recipient’s desktop with immediacy, enabling prompt feedback and, with the right tools, automatic confirmation of receipt upon arrival. Unless the recipient uses a fax server with inbound routing that distributes faxes to each user’s desktop as though they were e-mails, this level of precision is not provided when documents are faxed.

However, without the right security tools, e-mail messaging is vulnerable to being read by unauthorized people because of the way a message is routed to reach its destination.

How e-mail travels from sender to recipient

On its journey from the sender to the addressee, an e-mail message travels across the Internet through various computer systems before reaching its final destination. The path followed is unpredictable, dictated by network traffic at the time and the routers encountered along the way. This means that a message from New York to North Carolina can be routed via Singapore and Australia, if this proves faster and more accessible at that moment.

The problem is that, although reliable in delivery, the Internet e-mail system is not innately secure. Message transmittal can take anything from a few seconds to a couple of hours, but no matter how fast transmission is, data privacy cannot be presumed.

Unless security technology is used, there is no way of preventing an e-mail message from being read by unintended prying eyes as it wends its way to the recipient – with potentially detrimental consequences.

The perils of sending unsecured mail

Although countless press stories depict the sorry repercussions of not using e-mail security systems, in April 1999, the ZDNet Help Channel reported that 99 percent of all e-mail traffic travels over the Internet unsecured.

The risks incurred by sending unsecured mail are several.

“E-mail is notoriously unsafe. It is truly mind-boggling that millions of people use e-mail without realizing or caring about this simple fact,” writes André Bacard in

The Computer Privacy Handbook, where he alarmingly describes e-mail as “an ideal invention for mass surveillance”.

Unsecured e-mail can fall prey to malicious software tools such as sniffers, which automatically lie in wait for interesting information relayed through their system as e-mails are transferred from sender to recipient.

Unknown to e-mail senders, sniffers are placed in the path of all e-mail messages going through a computer. The individual who has planted this device receives copies of all the messages passing through and is then in a position to read – and store – those deemed interesting or profitable. The person in question might look out for credit card numbers, e-mail addresses, passwords, personalities or competitors.

Some indulge in this pastime simply for the voyeuristic thrill of accessing messages addressed to others. The situation is more worrying when the intentions behind sniffers are injurious, stemming from a desire to spy on competitors, enemies, the wealthy, or whatever.

Apart from scanning and intercepting mail traffic, it is also possible for unauthorized people to tamper with e-mails so that the message reaching the recipient is not the one originally sent by its author.

Besides, on being discovered through scanning, the sender’s name and address can be used to send false e-mail messages. The results of such practices could be damaging, embarrassing and expensive.

Yet, *The Industry Standard* of August 9, 1999 expresses confidence that “secure e-mail could be a good medium for a number of heavy-hitting business communications, such as prospectuses, medical records, shareholder communications, accounting forms, statements, proxies and confidential reports”. The accent here is on the word “secure”.

E-mail encryption

With point-to-point e-mail encryption, messaging across the Internet becomes a valid business option that guarantees safe transmission, confidentiality and data privacy.

The Information and Privacy Commissioner/Ontario web site stresses that “if you e-mail sensitive, personal or business information, then encryption is likely a necessity”. The site describes e-mail encryption as “a powerful tool in helping to protect an individual’s privacy”.

An encryption package consists of data-scrambling technology that allows users to e-mail information across the Internet without misgivings. Through encryption, a message is encoded so that only its intended recipient can decrypt it. This way, if a message is scanned or intercepted, it cannot be read.

The two main forms of e-mail encryption are PGP (short for Pretty Good Privacy) and S/MIME (short for Secure Multipurpose Internet Mail Extensions).

How PGP works

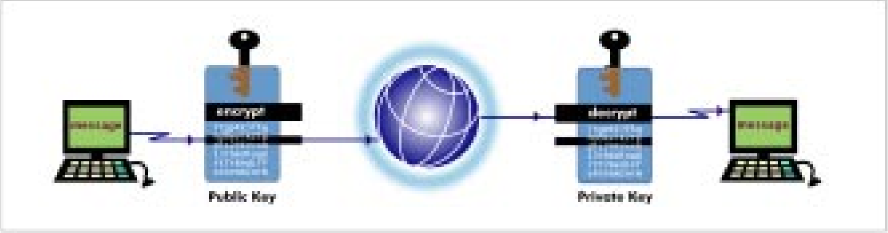
Programmer Philip Zimmermann released PGP in 1991 to encrypt ordinary e-mail using 128-bit encoding keys. Zimmermann's point of departure was the concern that unsecured e-mail could easily be read, and even changed, by anyone with privileged access to any of the computers along the route followed by the mail.

His solution was to develop a standard public key encryption program for secure e-mail and file encryption on the Internet, allowing people to secure e-mail messages against unauthorized reading.

PGP encryption technology is based on cyptographic keys that consist of a binary sequence of 1s and 0s. In simple terms, the longer the sequence, the greater the security afforded. An eight-bit computer key has 256 possible combinations, for example, whereas a 56-bit key creates 72 quadrillion possible values.

The PGP standard is 128-bit cryptology, a code emerging as the new digital standard that is considered "uncrackable", according to a *Washington Post* article dated May 1998. The article explains that "if a key is 128 bits long, or the equivalent of a 16-character message on a personal computer, a brute-force attack would be 4.7 sextillion (4,700,000,000,000,000,000,000) times more difficult than cracking a 56-bit key".

Public and private keys



Encryption packages such as PGP generate a pair of keys per user that can be used to encrypt and decrypt an e-mail message. The system is based on algorithms that encrypt messages with one key (the public key) and permit decryption with a different key to which it is paired – the private key. Users can freely make known and publish their public key so that anyone wishing to contact them securely by e-mail can use it to encrypt their message.

The public key transforms the message into a string of garbled, undecipherable text that can only be decoded with the user's private key. The reader's private key then decrypts the information that was sent after being encoded by the public key. The user alone can access his/her private key by means of a password.

In short, anyone who knows your public key can send you an encrypted message, safe in the knowledge that only you can decrypt it and read it using your secret (or private) key.

How S/MIME works

The S/MIME specification was developed by a private consortium of software vendors who joined forces in 1995 to counter the problem of e-mail interception and forgery.

At the moment, PGP is the more widely known and used e-mail encryption protocol as it is decentralized in nature. S/MIME requires a greater administrative input and some view it as being more US-centric, which international companies see as a disadvantage.

S/MIME installs on top of the standard Internet mail protocol, MIME, and the different S/MIME products are usually interoperable – although S/MIME and PGP are incompatible.

As with PGP, public key technology (described above) lies at the core of S/MIME.

S/MIME encompasses encryption and digital signature capabilities to guarantee confidentiality, message integrity and authenticity. This system works on the basis of hierarchies that specify and formalize the role of user and certifier.

In implementing S/MIME, users access a Certificate Authority which issues a signed certificate that contains the user’s public key. The Authority therefore serves as a point of reference to third parties wishing to enjoy secure messaging with the user.

Because of US legal restrictions as to the export of 128-bit e-mail encryption products, most S/MIME vendors offer products supporting 56-bit encryption coupled with a digital signature function for the secure exchange of public keys.

Ensuring e-mails are “For your eyes only”

To quote Robert Morris Sr., former senior scientist at the American National Security Agency: “Never underestimate the time, expense and effort someone will expend to break a code.” The encryption standards described above help ensure that such efforts are futile.

It is thanks to e-mail encryption technology that we can send credit card numbers, order forms, confidential contracts and other absolutely private messages by e-mail without needing to worry that the information is somehow being intercepted, read or altered.

Use of encryption gives rise to e-mails that are demonstrably authentic and unaltered, private and non-reputable (i.e., the sender cannot deny being their originator).

Resistance towards e-mail encryption

The current trend as regards e-mail encryption is characterized by a general resistance towards adopting such protocols, despite the great benefits they offer.

Users tend to find secure e-mail systems cumbersome to apply, because to date most must be installed at the client level, involving high technical input.

Implementing the software at client level also implies the need for end-user training – as well as being costly because an encryption package is needed per machine.

The client-based encryption process is usually viewed as being complex, as it requires users to give out their public key to each sender whose message is to be encoded, and also handle the decoding of each message received.

A server-based solution

A server-based security solution puts an end to such complaints, of course, because it eliminates the need for client action, saving time while proving far more cost-effective.

With a server-based solution, the laborious process of installing software on each machine in the corporate network is bypassed.

Similarly, each end-user is not obliged to become acquainted with encryption software. All e-mail messages reaching the corporate server are automatically decrypted, meaning that each user receives a legible text message right away. Likewise, the server automatically encrypts all outgoing mail, without any effort on the part of the sender!

This way, encrypted corporate messaging is ensured, as it is handled by the server, requiring no commitment on the part of employees.

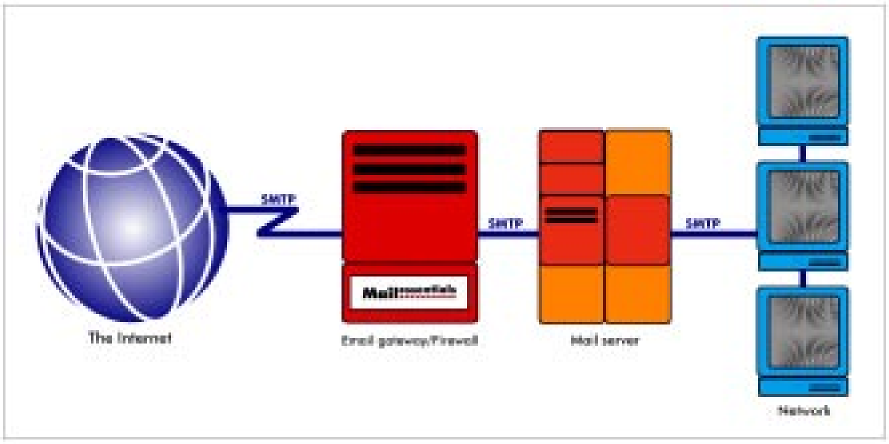
A server-based solution with a disclaimer feature also saves time and effort – because it allows the public key to be shared through a company-wide message automatically added to all outgoing mail. This enables all senders to encrypt messages to the company and helps cater for the legal liability connected to the unprotected transmission of confidential or sensitive data.

One of the first software packages to offer server-based PGP encryption is a leading solution that also includes the facility to add disclaimers and a host of other prime e-mail security features: Mail essentials for Exchange/SMTP. A future version of Mail essentials will also support S/MIME.

A powerful solution that arms your mail server

Mail essentials for Exchange/SMTP

Mail essentials for Exchange/SMTP is the ideal solution for those seeking to enhance their corporate mail security.



Mail essentials adds powerful e-mail security and management features to existing mail servers, such as:

- Encryption – Guarantees secure incoming e-mail by encoding it through PGP, while automatically informing senders of the public key through its disclaimer function.
- Disclaimers - Automatically includes a company-wide message to each e-mail sent.
- Content checking for offensive or confidential information - Blocks undesirable e-mail before it is sent or received.
- Quarantining of e-mail - Allows managers to approve the sending or receiving of e-mails with certain content or attachments.
- Virus checking of all incoming and outbound mail, using technology by anti-virus leaders such as Norton, McAfee and F-PROT.
- E-mail management - Allows companies to track e-mail usage and communications (for example, to know when an e-mail was sent and received by another party). In addition, it facilitates the compiling of reports on e-mail usage.
- Automatic compression of all outbound mail to save on bandwidth.
- Personalized auto-replies with tracking numbers - Enables companies to automatically confirm to customers that their e-mail was received. Tracking numbers give customers and employees an easy point of reference.

- Advanced anti-spam measures - Picks up on typical spam practices such as incorrect From headers and addresses in the e-mail body, and prevents spammers from using a company's mail server to relay their mail.
- POP3 downloader with built-in dial-up and support for multiple POP3 servers.
- Archiving of e-mail to any ODBC database - Allows companies to keep a complete record of all e-mail communications and provides the possibility to periodically check e-mail content.
- Transparent operation for user and administrator.

Mail essentials operates as a gateway between the mail server and the Internet. Therefore its implementation is completely transparent to the user. For the administrator, there is little or no additional user administration.

An evaluation version can be downloaded from: **http://www.gficomms.com**.

The Small Business version of this package means that it is well suited to small enterprises as well as larger organizations. Pricing of Mail essentials starts at $149 for the Small Business Version. An added bonus is the fact that GFI has issued the Mail essentials anti-spam feature as freeware.

For more information on e-mail security, see GFI's white paper on the topic. GFI is shortly issuing a white paper on managing a corporate e-mail system.

GFI FAX & VOICE

GFI FAX & VOICE is the leading supplier of Windows NT based communications software. Founded in 1992, GFI FAX & VOICE is a global company with offices in the US, Germany, France, Australia, Malta and the UK.

Leading the way through innovation and engineering excellence

In 1995, GFI FAX & VOICE was one of the first companies to launch a Windows NT based fax server: FAXmaker. Soon after, in 1996, GFI FAX & VOICE again proved its cutting edge status by developing one of the first Exchange fax connectors, FAXmaker for Exchange. During this year, GFI FAX & VOICE partnered with Microsoft Asia to allow Microsoft to penetrate a market that required fax as part of the Exchange server solution. In 1997 alone, GFI FAX & VOICE shipped 20,000 fax servers, proving FAXmaker to be one of the most popular fax server platforms for Windows NT.

GFI FAX & VOICE is also leading the way in e-mail management and automation. Launched in 1997, Emailrobot for Exchange/SMTP was one of the first applications designed to help companies handle the fast increasing e-mail overload. Emailflow develops on this product’s strengths, adding more winning features to this corporate tool.

Corporate clients

GFI FAX & VOICE's customer list includes: Microsoft, Digital, Honeywell, Siemens, Matshushita, Ericsson, OKI, Olivetti, Triumph Adler, Berliner Investment Bank, Bayersdorff A.G., PTT Telecom, Norwegian Telecom, Swiss Telecom, Cumbria Police Force, London Fire Brigade, UK Police departments, German financial institutions, Giorgio Armani, Benetton and many more.

GFI FAX & VOICE is a privately held company, and employs 55 people. The company has been named one of 1999’s fastest growing software companies for Windows by Microsoft Corp. and CMP Media.

USA & Canada
GFI FAX & VOICE USA
105 Towerview Ct.
Cary, NC 27513
Tel:1 (888) 2-GFIFAX:
Tel: (919) 388-3373; Fax: (919) 388-5621
Email: sales@gfifax.com

United Kingdom
GFI FAX & VOICE
5 Princeton Mews
167/169 London Road
Kingston-Upon-Thames
Surrey KT2 6PT
Tel: (020) 85460640; Fax: (020) 85460741
info@gfifax.co.uk

Central Europe
(Germany, Austria & Switzerland)
GFI FAX & VOICE Gmbh.
Palmaille 59, 22767 Hamburg, Germany
Tel: 040-306810-0; Fax: 040-306810-10
Email: info@gfigmbh.de

France
GFI FAX & VOICE France S.A.R.L.
30, avenue Charles Flahault,
34090 Montpellier
Tel: +33 (4) 99.61.40.17
Fax: +33 (4) 99.61.40.18
E-mail: ventes@gfifrance.com

Australia
GFI Australia (Fax & Communications) P/L
26 Stirling Street
Thebarton, SA 5031
Sales FreeCall: 1800-CALL-GFI
Tel:+61-8-8351-9780; Fax:+61-8-8351-7997
Email: sales@gficomms.com.au

GFI FAX & VOICE Ltd.
‘Communications House’
Mediterranean Street, SGN 07
St Julians, Malta
Tel: +356-382 418; Fax: +356-382 419
Email: sales@gfifax.com