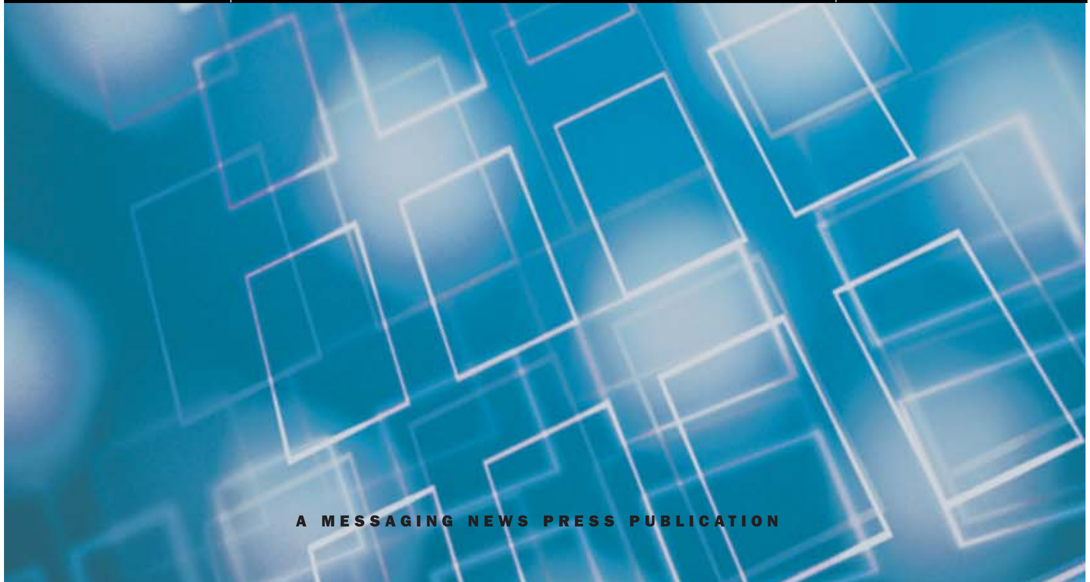
Email Security

GLOSSARY OF TERMS

*Defining Industry Acronyms, Abbreviations,
and Buzz Words.*

CO-AUTHORED BY
JOHN DICKINSON AND WILLIAM LEIBZON



A MESSAGING NEWS PRESS PUBLICATION

DISCLAIMER: The lexicon of any technology grows right along with the technology's progress, and email is no exception to that rule. Progress will inevitably add new terms and acronyms, but it will also change the meaning of terms already in use, some at a gross level, others through minor nuances caused by new uses of the term. Neither the authors nor sponsors make any guarantees or warranties regarding the outcome of the uses to which this material is put. This paper is provided with the understanding that the authors and sponsors are not engaged in rendering technical or professional services to the reader.

Introduction

The Email Security Glossary of Terms is designed to inform you of the often arcane and cryptic terminology behind the technologies of email as well as the forces that do them harm. By using it, you will better understand the value of email and how it works, the problems you face in implementing and using it, and what you are dealing with as you seek to fix those problems. Of overall importance, is our objective of giving you a quick reference guide that is easy to use and understand.

The Internet email system we use today started out as a simple way to communicate research information within a community of colleagues. At its core, it is the same system but today but it runs at a vastly higher message traffic volume, and creates a much greater security risk than was ever anticipated by its designers. This security risk is the larger problem and today's email has become seriously damaged by the work of nefarious people who use email as a weapon or as a transport system for their weapons.

Today's email traffic contains as much or more bad information as good, including spam, virus attacks, denial of service attacks, and phishing attacks. In addition, email privacy can be invaded–violating the confidentiality of the information messages contain.

Email is the oldest medium for computer messaging and widely considered to be the arterial system of Internet-based communications, carrying the lifeblood of worldwide business. That makes it critical for you to keep this glossary close at hand as you explore, defend and manage this vital medium.

Spam will cost the world $50 billion in lost productivity and other expenses in 2005. More than a third of that, or $17 billion, will be wasted by U.S. companies.

SOURCE: FERRIS RESEARCH
The Global Economic Impact of Spam, 2005

A

Accreditation: Procedure in which an email sender may be certified by an accrediting agency. Such an agency will certify that a sender meets certain criteria, and then publishes a list of accredited senders or sending entities with accreditation information.

AES (Advanced Encryption Standard): A cryptographic standard algorithm known in cryptography circles as Rijndael because it uses an algorithm of that name. It was chosen by National Institute of Standards & Technology (NIST) in November, 2000.

Algorithm: A sequence of steps whose order and process will solve a particular problem. Examples are mathematical formulae or a group of computer programming instructions. This is not the same as a computer program, which is comprised of a larger set of steps that involves many individual algorithms.

ARPA or DARPA (Defense Advanced Research Projects Agency): The organization that sponsored the development of a research-oriented network in the 1960's that was originally called ARPANET. The network has more recently evolved into what is now called the Internet.

ASCII (American Standard Code for Information Interchange): The 7-bit encoding format consisting of 128 characters which is the de facto worldwide alphanumeric standard used by computers to represent all the upper and lower-case Latin letters, numbers, and punctuation.

ASRG (Anti-Spam Research Group): Part of the Internet Research Task Force (IRTF) that focuses on junk email, more commonly known as spam.
See asrg.sp.am

ASTA (Anti-Spam Technical Alliance): A group of the largest ISPs, including AOL, Earthlink, Microsoft, and Yahoo!, which coordinate their actions to combat spam email.

AsyncOS™: A software architecture created by IronPort Systems to address concurrency-based communications bottlenecks and the limitations of file-based queuing. The system uses a high-concurrency threading model that addresses allocation of system resources and AsyncFS™, an Asynchronous File System optimized for message queuing.

Authentication: Verification of a computer user's identity See Sender Authentication.

Autoresponse: A message generated automatically by a program, usually an MUA, acting on behalf of an email recipient. Such responses inform senders of an email address change; the fact that the recipient is away and cannot receive the message; a receipt that acknowledges that an email was received; or a message rejection notice.

B

Bayesian Filter: A filtering system used by some anti-spam tools that analyzes an email message mathematically in order to develop a probability that it is spam. It uses a Bayesian Logic-based method of inference that compares the message content to known spam messages, thereby rating its probability of also being a spam message.

Blacklist: A list of domains, hosts, IP addresses, and email addresses, from which email is blocked. Such lists can be maintained locally by each recipient or by an external organization. A blacklist is an early version of an email reputation system.

> **RBL** (Real Time Blacklist): Blacklist with immediate access available to parties using it through the Internet.
>
> **DNSBL** (DNS Blacklist): IP-addresses in a blacklist that is maintained centrally and can be checked by the DNS protocol which returns an address within 127.0.0.x if an entry is in the list (where "x" is a code representing the reason the domain is blacklisted).

Bogon IP: Derived from "bogus number" as that term applies to IP addresses, it is used to identify an IP address that should not be used on the public Internet because the address is reserved in special-purpose IP address blocks or is unallocated. Use of these IPs on the public Internet is most often for malicious purposes or in order to make it more difficult to find the entity responsible for their use. There is no Whois data for the such IPs. See www.completewhois.com/bogons/

Bonded Sender™: The leading third-party email certification organization used by companies to validate a sender's email address so that their email isn't mistaken as spam and inadvertently deleted before reaching its intended recipient. See www.bondedsender.com

Bot: **1.** An abbreviation of the word robot that is used to describe an automated computer system that visits websites or desktops and does tasks on its own. The term is commonly used in reference to Web spiders (for example "Google Bot") which are systems that visit websites to be able to index them and reference them in search engines. It is also used to describe desktop applications that act as agents for the user or for a network administrator (for example, AIMBots). **2.** A hacked or otherwise compromised computer being remotely controlled by someone other than its owner. Bots are most often created by virus attacks, and are frequently used by spammers to distribute spam or for DDoS attacks. Synonymous with Zombie PC, Hijacked PC and Drone.

Botnet: A large number of Bot PCs controlled by single entity. Spammers and their associates create large Botnets to send emails and for other purposes. Botnets are bought and sold on a black market. Also known as Drone Army or Zombie Army.

Bounce: A Bounce occurs when a message is not delivered and is returned to the original sender or to an agent designated by the sender to receive returned mail. The process of creating a bounce is called bouncing.

Bounce Address: The email address transmitted during the SMTP session when the MAIL FROM command is issued and is the email address to return the message to in the case of delivery failure. The return is usually handled by an MTA or an MDA. Bounce Address is also known as "Return-Path", "Envelope From" and "SMTP2821 MAIL FROM".

C

CAN-SPAM (CAN-SPAM Act of 2003): A law passed by the US Congress that makes it unlawful to send unsolicited commercial email (spam email) with a purpose to deceive or with false source data. The law sets out rules regarding how to legally handle pornographic and other types of spam, but is generally regarded as having been ineffective in stopping or even stemming spam email. See www.spamlaws.com/federal/108s877.html

Caller ID (CID): A Microsoft-designed email sender authentication proposal that was used on RFC2822 headers Sender, From, Resent-Sender, and Resent-From. The proposal used DNS XML records, but was superseded by combining it with the SPF sender authentication proposal to create Sender ID. Sender ID was for a time adopted and promoted by ASTA.

CAUCE (Coalition Against Unsolicited Commercial Email): An ad hoc volunteer organization that was created by Netizens to advocate for a legislative solution to the problem of UCE, better known as spam. See www.cauce.org

CBV (Call-Back Verification): A technique used by some email systems to verify sender email addresses. The receiving email server connects back to the MTA of the sending domain (as identified by MX records) to verify that the sending address exists before accepting the message.

CMS (Cryptographic Message Syntax): A general syntax standard for cryptographic email message data.

Collision: Term used in cryptography to describe the situation in which two distinct data sets produce an identical hash digest. A good cryptographic hash function is one that would make it computationally very difficult to purposely create a collision. Encrypted messages are more difficult for an unauthorized agent to decipher or counterfeit.

Companion Virus: A companion virus will rename either itself or its target file in an attempt to trick the user into running the virus rather than the target program. For example, a companion virus attacking a file named GAME.EXE may rename the target file to GAME.EX and create a copy of itself called GAME.EXE.

Compliance: Messaging and email compliance – email and messaging regulatory requirements mandated by governing entities. These include: the Health Information Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLB), and Sarbanes-Oxley Act (SOX) Act as well as others.

Challenge/Response (C/R): A technique used by some spam and fraud prevention systems to distinguish good email senders from bad ones. The assumption is that all senders are bad until they have responded to a challenge email sent by the receiving system. Senders who have properly responded are placed on local whitelist and their email is then allowed through to the recipient.

Cryptography: A process by which a piece of data is transformed into another seemingly unrecognizable piece of data by means of a special function. The result can be transformed back into the original only by a user who possesses the correct decryption key.

CSV (Certified Server Validation): A verification of SMTP session HELO/HELO identity which checks to see if the incoming SMTP server's IP address is listed as a valid SMTP client based on the DNS SRV record of the domain in HELO. CSV was formerly called Client SMTP Validation.

D

Directory Harvest Attack (DHA): An attack in which a Bot is set loose in an organization's network to sniff out and "harvest" email addresses and other information that can be used for spam and other malicious attacks.

Digest: **1.** A collection of messages on a discussion forum, mail list, or newsgroup, for a certain period of time. Messages collected for one-day constitute a daily digest, for one-week constitute a weekly digest, for one-month a monthly digest, and so on. **2.** A cryptography digest, often referred to as a cryptographic message digest or digital fingerprint, is a hash of message data, that is used when cryptographic signature is created. The encrypted message digest is in fact the signature.

Digital Fingerprint: A term often used to describe a cryptographic hash of an email message. Also known as the Digest of an email message.

DomainKeys (DK): A proposal by Yahoo! in which sending MTAs would include a special header containing an RSA signature which can be verified by retrieving a public key from the sender's DNS TXT record. See http://antispam.yahoo.com/domainkeys

DMP (Designated Mailers Protocol): A proposal for identifying computer systems authorized to act as SMTP clients for an email domain. It is one of the earlier proposals that grew into SPF. See www.pan-am.ca/dmp/

Domain Name Accreditation (DNA): One of the proposals aimed at identifying domain accreditation services.

DNS (Domain Name System): A distributed data lookup system used on the Internet to identify network end-points or hosts by name, usually referred to as domains. DNS also finds domain attributes, usually referred to as Resource Records (RRs). Domain IP Addresses and MX Records are the most well-known attributes. See www.dns.net/dnsrd/

DNS Host: The final end-point naming identifier in the DNS system which would refer to the actual physical Host system. Note that the same Host can have more than one hostname. Synonymous with Hostname.

DNS RR (DNS Resource Record): The DNS record type, which includes "A" (IP), "MX", "SRV", "PTR", "TXT" and others.

DNS Zone: A collection of related DNS records, usually referring to all DNS records for same domain, although zones can have records that spawn multiple domains.

DNSSEC (DNS Security): A set of extensions to DNS designed to prevent attacks that would direct users to an erroneous website. DNSSec uses a digital signature to ensure that the correct IP address is used.

Domain (Domain Name): An entity's unique name on the Internet, sometimes called an Internet end-point. Typically names are hierarchical, with the various levels separated by periods or decimal places, (e.g., www.anyname.com). The TLD or top-level domain (typically .com or .org or .net) is generic and, within that level, name delegation is done by various domain registrars. The Internet Corporation for Assigned Names and Numbers (ICANN) is the current manager of Internet addresses and domain names.

DoS (Denial of Service Attack): An attack against a system that typically involves sending a large number of identical queries in order to overload the server capacity of the target system, thus denying service to legitimate users. While DoS attacks often use identical messages, it is the number of messages (not their content) that makes them problematic.

DDoS (Distributed Denial of Service): A very common form of DoS that employs multiple attacking computers, often thousands of them, controlled by a single individual. Such attacks originate either from directly hacked computers or computers that have become zombies and are now part of a Botnet.

DRIP (Designated Relays Inquiry Protocol): A sender authentication proposal similar to DMP, but which uses a different DNS syntax.

Drone (Robot Drone): A hacked or otherwise compromised computer being remotely controlled by someone other than its owner. Drones are most often created by virus attacks, and are frequently used by spammers to distribute spam or for DDoS attacks. Synonymous with Hijacked PC, Zombie PC and Bot.

Drone Army: A large number of Drone PCs controlled by single entity. Spammers and their associates create large Drone Armies to send emails and for other purposes. Drone networks are bought and sold on a black market. Also known as BotNet or Zombie Army.

Dropper: An executable file that "drops" a virus or Trojan onto the target computer when the program is run. A Dropper file's intention is to create a virus or trojan and then execute it on the user's system, possibly at a later date or time.

Designated Sender: A generic term for systems like RMX, DMP, SPF and Caller-ID, in which domain owners can designate which hosts can send email using their domain names. Also known as Designated Sender Scheme.

Digital Signature: A generic term for any kind of cryptographic signature. Also known as Digital Signature Standard.

DSA (Digital Signature Algorithm): General term for algorithms used to create digital signatures. Such algorithms include RSA, Deffie-Hellman, ECDSA, HMAC, and others.

DSN (Delivery Status Notification): The email delivery status message sent by an MTA to the message sender. It most often is used for notice of a failure to deliver.

E

ECC (Elliptic Curve Cryptography): A public key cryptography method that uses points on an elliptic curve to derive a public key. The public key is created by agreeing on a standard generator point in an elliptic curve group and multiplying that point by a random number, which is the private key.

ECDSA (Elliptic Curve Digital Signature Algorithm): The cryptography algorithm used in ECC.

EES (Escrowed Encryption Standard): A standard used by some branches of the U.S. Government to encrypt telecommunications data which have been intercepted for law enforcement purposes. It is based on the SkipJack symmetric-key encryption/decryption algorithm.

EDI (Electronic Data Interchange): Communication of business transactions such as orders, confirmations, invoices, and exchanges, between different organizations. Used mostly in supply chain and inventory management, it is usually automatically run on a computer-to-computer basis, although some interaction is possible. EDI service companies provide systems through which transacting entities with incompatible systems can communicate.

EHLO (Extended HELO): An extended format of the HELO command given by the initiator of an ESMTP session.

Email (email, Electronic Mail): A generic term describing store-and-forward messaging systems on the Internet that use domain-based sender and recipient addresses.

Email Filter: A process that sorts emails based on certain criteria, typically as an attempt to sort out unwanted and bad email such as spam, viruses, and phishing attacks. A filter may also be used to sort email relevant to a particular subject or project.

Email Header: The header placed in front of the message containing the "to" address, "from" address, subject, and "cc" and "bcc" addresses. It is normally created by the email client when sending the message and modified by all email servers between the source and the destination in order to enable tracing the path of the message.

Encoding: 1. The process of transforming data, most often to enable arbitrary binary data to be represented as ASCII text so it can be safely included in email. MIME format of email data may require encoding and 8-bit data block or Base64 encoding is often used for this purpose. **2.** The format and algorithm of the encoding system used for the data in an encoding applications. Some examples of such systems are: MIME w/Base64, UUencode, and BinHex.

Encryption: A change made to data, code or a file so that it can no longer be read or accessed without being decrypted. Secure email systems encrypt messages so they cannot be read by someone without the key necessary for decryption. Viruses may use encryption in order to avoid detection by hiding their viral code. Viruses can also encrypt code or data on a system as part of their destructive payload.

ESMTP (Extended Simple Mail Transfer Protocol): A system that extends the original SMTP protocol with syntax that allows additional features. ESMTP is what virtually every SMTP server now supports.

F

Fingerprint: A cryptographic fingerprint is a hash of a public key, often used to verify that a public key is correct.

Forwarder: 1. Any Mail Redirection Agent that redirects an email such that the sender appears to be different from the original source of the message. Email marketing services use forwarders to make it appear that an email message originated from the marketing company rather than from the service that actually sent it. **2.** Any Mail User Agent that redirects that user's email to a different email address. These are often embedded in email client software to allow users to receive email at a different location when traveling.

FQDN (Fully Qualified Domain Name): The complete domain name for a host on the Internet. It provides enough information to be converted into a physical IP address.

FTC (Federal Trade Commission): The branch of United States Government responsible for promoting fair trade and ensuring that consumers are not hurt by bad business practices. The CAN-SPAM Act, regulating spam email, is administered by the FTC.

FTP (File Transfer Protocol): A common file exchange protocol used on the Internet. It is one of the oldest TCP/IP protocols.

G

Gateway: A device or system that manages and translates traffic coming and going between two different networks which are not directly connected or compatible.

Greylisting: A technique in which some or all SMTP connections are temporarily refused by an MTA by using a failure error that requires delivery to be retried at a later time. Normally this is used so that delivery attempts from a previously unknown source can be examined to decide if the new source is likely to be good or bad. See www.greylisting.org/

H

Harvesting: A covert act in which email addresses are collected for compilation of email databases to be used for unsolicited mailings.

Header: A temporary data record added to the beginning of the transmitted text in order to transfer a message over a network. Typically a header contains source and destination locations as well as data that describe the content of the message.

HELO: The command that initiates an SMTP conversation. The new extended version of this command used in ESMTP is EHLO.

Heuristic: A method of scanning which looks for patterns of activities that are behaving as a virus. Most leading anti-virus packages have a heuristic scanning method to detect new or previously undetected viruses. Heuristic scans can however lead to false virus alarms.

Hijacking: When a computer resource or the control of a computer resource is taken by someone not its owner, and without the permission of its owner, it is said to have been hijacked. This may be done simply to control the resource, but as often it is done in order to for the perpetrator to be able to pretend to be the resource owner.

Hijacked PC (Hijacked Personal Computer): A hacked or otherwise compromised computer being remotely controlled by someone other than its owner. Hijacked PCs are most often created by virus attacks, and are frequently used by spammers to distribute spam or for DDoS attacks. Synonymous with Zombie PC, Drone and Bot.

Hijacked IPs: A group of IP addresses, known as an IP block, that is controlled and used by someone who is not the person or entity to whom the block was allocated, without permission of that person or entity. See www.completewhois.com/hijacked/

Host: A computer attached to the Internet. A host may have one or more DNS names (Hostnames) and may have one or more IP addresses. Hosts with more than one interface and with IP addresses in different networks can function as a router or a gateway.

Hostname: Synonym for DNS Host.

HTTP (Hyper Text Transfer Protocol): The protocol used to connect clients to servers on the World Wide Web. It establishes a temporal request/response system that establishes the connection at the client's request, and maintains it only long enough to fulfill the request, at which point it is severed. See www.w3.org

I

IANA (Internet Assigned Numbers Authority): The body formerly responsible for managing Internet addresses, domain names and protocol parameters. It was superseded by ICANN in 1998. See www.iana.org

IBE (Identity-Based Encryption): An encryption scheme that uses some form of a user's identity, such as an email address, as the key in a public key system. First proposed by Shamir (co-founder of the widely-used RSA encryption algorithm) in 1984, its first practical implementation was derived in 2000 at Stanford University and UC Davis.

ICANN (Internet Corporation for Assigned Names and Numbers): The successor to IANA that manages Internet addresses, domain names and the parameters associated with Internet protocols, including such items as port numbers, router protocols, and multicast addresses. ICANN provides a list of accredited registrars that accept domain registrations. See www.icann.org

IEEE (Institute of Electrical and Electronics Engineers): An organization of electronics engineers and scientists involved in setting standards for computers and communications. The IEEE Computer Society is the largest of its member societies. See www.ieee.org

IETF (Internet Engineering Task Force): An organization, comprised mainly of engineers, that develops Internet protocols and standards. The organization identifies problems and opportunities in IP data networks and proposes technical solutions to the Internet community, typically through working groups that are chartered to explore specific tasks. See www.ietf.org

IIM (Identified Internet Mail): A signature-based sender authentication proposal by Cisco that requires sending MTAs to add a special header to the email message with an RSA signature and public key. The key can be verified by looking up its fingerprint in a special key registration server database. See www.identifiedmail.com

IM (Instant Messaging): A messaging service in which text messages can be sent directly from one person's computer to another. The messages are not stored as they are in email systems. Enhanced versions of these services provide large file transmission and point-to-point video and voice messaging. See www.jabber.org, www.icq.com, www.aim.com, http://messenger.yahoo.com and http://messenger.msn.com

IMAP (Internet Mail Access Protocol): Protocol used by the MUA to get access to an email box located at an ISP mail server where an MDA has delivered email. The current version of this protocol in general use is IMAP4.

Internet: The term comes from "Interconnected Network" and refers to a network that connects many other networks run by ISPs and end points to make one global network. Some now refer to the Internet as "International Network".

IP (Internet Protocol): The network protocol used by Internet end nodes to exchange data.

IP Address: Numeric identifiers of end point network nodes for systems connected to the Internet. There are two types of IP addresses - 32bit IP addresses used with IPv4 and 128bit IP addresses with IPv6.

IPSEC (IP Security): An effort to secure the core Internet infrastructure by means of public key cryptography.

IRC (Internet Relay Chat): A protocol used for real-time user chat computer networks. The networks are called IRC networks, and the largest of them have tens of thousands of users chatting via interconnection with a series of servers. See www.irchelp.org

IRTF (Internet Research Task Force): A sister organization to the IETF which does research in areas of Internet technologies and can often involve early work that is later picked up by an IETF working group. See www.irtf.org

ISO (International Organization for Standardization): An organization that sets international standards for weights and measures, and innumerable technical standards. Its membership is comprised of standards committees from 95 countries. The U.S. is represented in the ISO by ANSI. Electrical and electronic standards are governed by the International Electrotechnical Commission (IEC), which in cooperation with the ISO formed the Joint Technical Committee for information technology (JTC1) to create standards for computer technology. See www.iso.ch

ISP (Internet Service Provider): Term used to describe a company providing Internet access to the public. Each ISP runs its own network and when connected together with other organizations' networks they all make up what we call the Internet.

J

Joe-Job: The act of sending spam email using another party's email address as the sender. The spoofed user then receives bounces from failed delivery attempts. The user also gets angry complaints from people who did not want to receive those emails, as does the ISP who provided the account. The spammer's objective is for the ISP to shut the email account down.

K

Key: A term commonly used in cryptography to describe a piece of data necessary to create, verify, and/or decrypt encrypted data. For most cryptography systems, only one key is used to encrypt and decrypt the data. However, in public key cryptography one key is used to encrypt and another key can be used to decrypt.

Public Key: In public key cryptography, this is the data given out to the public so that anyone can encrypt a message. After the message is sent, the recipient can decrypt it only if he or she has the private key. An exception exists in message signing—where the roles of the keys are reversed with the private key used to digitally sign the message, while the public key can decrypt and open the message. See www.pgpi.org/doc/pgpintro/

Private Key: In public key cryptography, this is the piece of data necessary to decrypt a previously encrypted message. For message signing, this is the key that only the signer has and uses to create cryptographic message signatures. See www.pgpi.org/doc/pgpintro/

Asymmetric Key: Any encryption technique in which the encrypting and decrypting keys are different.

Symmetric Key: One key is one that can be used for both encryption and decryption of the same message. This is also sometimes called "single key" encryption. For message signing, it would be necessary for both sender and recipient to know this key, and to have kept it private from everyone else. A symmetric key is at times also called a "private key" but it is not the same as the Private Key used in public key cryptography.

PKI (Public/Private Key Infrastructure): Any network infrastructure that supports a Public Key or Private Key encryption system.

L

LDA (Local Delivery Agent): The email system component that delivers the message to the local message store. This can be used as a synonym for an MDA or to describe an actual mail delivery component of an MDA.

LDAP (Lightweight Directory Access Protocol): The industry-standard protocol used by email programs and Web browsers to access a directory listing. It is a version of the DAP protocol that is used to gain access to X.500 directories. See www.kingsmountain.com/ldapRoadmap.shtml

LMAP (Lightweight MTA Authentication Protocol): A working group within ASRG that met at the end of 2003 to attempt unification of the multiple proposals (RMX, DMP, SPF, DRIP, MTAMARK) that focused on per-hop authentication based on the SMTP client IP address. No unified protocol was agreed upon, however the result was a draft discussing this as an approach to email authentication.

M

MAAWG (Messaging Anti-Abuse Working Group): A group comprised of messaging service providers (primarily ISPs) and companies that provide them with services and software whose purpose is to address and create strategies to defeat several forms of messaging abuse including spam, virus attacks, denial-of-service attacks, and others. See www.maawg.org.

Mail Bomb: A special DoS attack in which a large number of email messages are sent to one email address or server, usually with a very large file attached. The objective is to overload the target server, make the target email box unusable, make good messages difficult to find, and generally annoy the target user.

Mail List: **1.** A list of email addresses, generally used for distribution purposes, such as sending an email newsletter or sending a marketing message via email. **2.** A discussion list of email addresses where each person on the mail list can send an email that will go to every other person on the list.

MAIL FROM: The first in a set of SMTP processing commands which creates the dialogue between the sending and receiving MTAs, and executes the email message transmission. The command contains the information necessary to determine where the email came from, including information contained in the Purported Responsible Address.

MAPS (Mail Anti-abuse Prevention System): One of the first Real-Time Blacklists was started by Pail Vixie. Later, it operated as an independent non-profit company providing a Reputation Service that could be used to judge the commercial legitimacy of an email sender. In 2004, MAPS was bought by Kelkea, and now operates as part of a commercial anti-spam service. See www.kelkea.com/

MARID (MTA Authorization Records In DNS): An IETF working group that was started in April, 2004 and disbanded in September, 2004. Its purpose was to discuss standardization of LMAP- and Designated Sender-related proposals for email sender authentication. It came close to standardizing SPF but later considered Sender ID (the amalgam of SPF and Microsoft's CallerID). MARID was disbanded because the group could not agree on how to address the intellectual property and technical issues raised by Sender ID.

MDA (Mail Delivery Agent): The end-point of an SMTP transmission, which then delivers an email message into a storage device where it can be picked up or directly accessed by an MUA.

MDN (Mail Disposition Notification): A type of DSN that, when sent, indicates successful delivery.

Messaging Gateway Appliance: A server-class computer that enhances MTA services by filtering incoming and outgoing mail for spam, viruses, and other malware. The device is often designed to also serve as the MTA.

Meta Tag: **1.** In HTML, meta tags are used in the header section of a page and provide references to, and short descriptions of, topics that are related to the content of the Web page to which the header belongs.
2: When referring to the subject of email messages, it is a reference to a topic of discussion which is usually put inside brackets "[...]" in the "Subject:" header. Mail Lists often add such tags automatically.

META (Message Enhancements for Transmission Authorization): A proposal that calls for automated email cryptographic signatures to be added by MTAs with flexible syntax in order to support signatures that can be verified after common email modifications, such as occurs in mail lists, and authorization support for DNS and HTTP verification of the public key.

MIME (Multipurpose Internet Mail Extensions): The IETF standard for email content that allows multiple types of objects to be included as part of text data messages. The SMTP protocol, by itself, only supports text in messages.

Miscreants: In general society, a villain. In messaging and other computer systems, the term refers to those who abuse vulnerabilities and bottlenecks of networks with the intent to harm others. Miscreants may hack systems or use Botnets to attack others. Some are employed by spammers to attack organizations and individuals who are engaged in anti-spam activities.

MRA (Mail Redirection Agent): An intermediate MTA or other SMTP participating entity that changes the destination or source of email message in transit. Forwarders and Mail Lists are two well known types of MRAs.

MSA (Mail Submission Agent): A program on the sender side of an email transaction that initiates the email transmission.

MTA (Mail Transfer Agent): Any server utilizing the SMTP protocol to send and receive email messages.

MTS (Message Tracking Server): A tracking server provides a history of a messages route from sender to receiver to a tracking client. It is a repository of the information about when a message passed through a particular MTA.

MUA (Mail User Agent): A program used by people to compose, read, and send, email. The same program is also usually an MSA.

MOSS (MIME Objects Security Services): The first standard for encoding non-text messages for email transmission. It is now obsolete and has been replaced by the MIME standard.

MTAMARK: A proposed standard that requires legitimate MTAs to identify themselves in DNS. Only mail servers would create the indication in their

DNS records. The receiving MTA could check for the indicator and be therefore assured that the sender was legitimate.

MX (Mail Exchange): A type of DNS RR that identifies MTAs that are supposed to receive email destined to addresses in a particular domain.

N

NANAE (News.Admin.Net-Abuse.Email): This USENET newsgroup discusses email abuse including spam. See www.nanae.org or http://groups.google.com/group/news.admin.net-abuse.email

NANOG (North American Network Operators Group): A membership organization consisting of network operators responsible for running the backbone infrastructure of the Internet. Founded in 1994, the group meets three times a year to provide a forum for the exchange of technical information, and promote discussion of implementation issues that require community cooperation. See www.nanog.org

NDN (Non-Delivery Notification): A type of DSN that is sent when email cannot be delivered.

Node: A network junction or connection point. Every terminal, server, computer, hub and switch in any network is a node.

> **End Node:** The ultimate physical destination of any data item on a network, which may be a desktop computer, a storage unit, an output device such as a printer, a database server, or any point at which the data transmission may end.

NSA (National Security Agency): This U.S. Government agency is the country's cryptologic organization. It coordinates, directs, and performs specialized activities designed to protect U.S. information systems and decrypt and produce foreign intelligence information.

O

Opt-In: A term used to indicate that a person has been asked to, and has agreed to, receive emails or other messages from some mail list or organization, such as a company or a discussion forum.

> **Confirmed Opt-In:** This status means that the user's opt-in subscription has been confirmed by that person. Most often that means that a verifying message was sent to the person, and that the person replied positively, either by email or by visiting a website and indicating approval.
>
> **Double Opt-In:** Same as Confirmed Opt-In.

OSI (Open Source Initiative): An industry-wide effort to promote the development and use of software with source code that is freely available to anyone, and which anyone has the right to modify and redistribute. See www.opensource.org

OSS (Open Source Software): Software with source code that is freely available to anyone. Anyone has the right to modify and redistribute this type of software. See www.fsf.org/philosophy/free-sw.html

P

Path: An email path is a list of systems that a message can pass through on the way from sender to recipient. Any number of MTAs and MRAs may be involved, but at least the sending and receiving agents have to be in the path.

Path Authentication: A generic term for email sender authentication schemes in which all systems on the email path authenticate the previous system on the path. SPF and Sender ID are path authentication schemes, as are RMX, DMP, and CID.

PGP (Pretty Good Privacy): This data encryption program was created by Phil Zimmerman of PGP Corporation and originally published as freeware in 1991. It is widely used for encrypting email messages and securing files. It is available from PGP for commercial use and as freeware for personal use.

> **OpenPGP** (An Open Specification for Pretty Good Privacy): The IETF standard for PGP that also extends the technology to encrypt MIME-encoded components of email messages.
>
> **PGP/MIME:** Same as OpenPGP.

Phishing: Spam-like emails are sent to users who are tricked into signing on to a spoofed website using their financial or other personal identification credentials. The phishing attack perpetrator gathers and keeps the credential information. Banks and other financial institutions are most often the targets of schemes, where users are sent an email urging them to update their account information by signing on with their bank identification and PIN or password.

PKI (Public Key Infrastructure): In a PKI environment, a unique digital certificate is used to generate personalized Public Keys or Private Keys used to encrypt messages. The issuer of the certificate also creates a means to carry out the encryption and to decrypt the message according to the Public Key or Private Key arrangement specified in the certificate.

Polymorphic Virus: A virus that changes some part of its binary pattern each time it infects a new file to keep it from being identified and profiled by anti-virus tools.

POP: 1. (Post Office Protocol): The protocol which enables an MUA to download an email from an ISP or other email server. POP3 is the current version. **2.** (Point of Presence): This term refers to a network node set up by an ISP or enterprise network to handle connections in a region. The size of the region is arbitrary and is determined by such issues as server capacity, density of users, and the quality of hardware connection services.

Postmaster: Email address of the mail service administrator, an address that all domains are required to have. Some mail systems route all email that is not accepted elsewhere in the domain to the Postmaster address.

PRA (Purported Responsible Address): The address of the MTA that has most recently transmitted the email message being analyzed. It is used by path authentication schemes, such as SPF. In the case where a message travels directly from a sending agent to a receiving agent, the PRA is always the sending agent's address. However, in cases where the message is handled by several MTAs en route from sender to receiver, the PRA is the last MTA to handle the message. If every MTA on the route checks the message's PRA and finds it legitimate, then the entire chain of PRA's will be legitimate.

R

Relay: Often called "third-party relay", this phenomenon occurs when an MTA allows an external mail client to forward mail for processing and delivery without any checks to ensure that the client is a legitimate user. This can be a legitimate service, however if the MTA allows third-party message relay, it can be abused by spammers who use the technique to send large amounts of spam email that appears to come from the original MTA.

Open Relay: This type of Relay does not use an authorization system to decide which messages can be retransmitted by the third party. This email architecture is no longer in wide use.

RCPT TO: An SMTP processing command that informs the receiving MTA of which email address the message is being sent to. The sending MTA waits for verification that the receiving MTA will authorize receipt of a message to that address. There may be an unlimited number of RCPT TO commands in any one SMTP message transmission dialogue.

Reputation: The most widely accepted type of email sender accreditation services are those that create a measure of senders' reputations. Usually administered externally, the reputation data is based on a collection of information about email senders. The database is made available to email recipients whose systems can use the reputation data to make informed decisions about acceptance or rejection of email messages.

Reputation Filters™: A technology created by IronPort Systems that utilizes email traffic data and email sender data to determine the reputation of an email sender. Senders with poor reputation scores are blocked, senders that look suspicious are throttled and senders with reputable scores are accepted.

RMX (Reverse MX): A modification of the MTA DNS record to include an RR that indicates the IP addresses of users authorized to send email from the MTA. It was proposed to, and is being considered by, the MARID working group of the IETF. See www.danisch.de/work/security/antispam.html

RSA (Rivest-Shamir-Adleman): Named for its inventors, this encryption scheme uses a two-part key. Data are encrypted by using the recipient's public key, and then decrypted by the recipient's private key. The private key is kept by the owner; the public key is published.

S

Sender Authentication: Verification of the source of an email message transmission. This technique has been proposed as a way of reducing or eliminating spam by requiring some type of sender authentication scheme that is communicated between sending and receiving email systems. See Caller ID, DRIP, IIM, Path Authentication, PRA, Sender ID, SES, SID, and SPF.

SenderBase™: SenderBase is an email traffic monitoring network created and managed by IronPort Systems. It is designed to help email administrators research senders, identify legitimate sources of email and stop threats such as spam and viruses. See www.senderbase.org

Sender ID: This sender authentication standard was developed as an integration of SPF and CallerID, originally proposed by Pobox, and Microsoft respectively. It was adopted by ASTA, and proposed to the IETF's MARID working group. Disagreements over its technical and intellectual property requirements led to its abandonment by the email industry and the disbandment of the MARIID working group.

SES (Signed Envelope Sender): This sender authentication proposal would have all messages include an encrypted signature in the MAIL FROM address. It requires the use of a special signature verification server to decrypt the signature and verify the sender.

SID (Sender ID): The proposal for sender authentication adopted in 2004 by ASTA and submitted to the IETF MARID working group by Microsoft. It uses features of Microsoft's CallerID technology and the SPF technology originally proposed by Pobox. MARID was disbanded because the group could not agree on how to address the intellectual property and technical issues raised by Sender ID.

Signature File: A file of virus patterns that can be compared with the content of existing files, as well as files downloaded or received in email messages, to determine if they are infected with a virus. Vendors of anti-virus software update these signatures frequently as new viruses are discovered and analyzed, and make them available to customers via the Web, usually through automatic update programs.

SkipJack: This secret key encryption algorithm was used by the U.S. government in the Clipper chip and the Fortezza PC card. Clipper was a cryptography chip used by the U.S. government for telephone security; Fortezza was a PC card used as an authentication token. Neither technology was adopted, and as a result SkipJack was declassified in 1998.

SMTP (Simple Mail Transfer Protocol): The widely-used standard protocol for transmitting email over the Internet.

SOA (Start Of Authority): This is the DNS record that contains the key information about a domain zone. It defines which server is the primary nameserver, contains the hostmaster contact information (email), and indicates the time-to-live (TTL) value for cached records.

Spam: The widely-used term that describes unwanted email communication sent in mass quantities. While the purpose is usually commercial advertising, more malicious types of spam, such as Phishing, are used for identity theft and monetary theft purposes. The recent very rapid growth of spam has led to a new breed of technology and technology companies, as well as laws, geared to suppress it, fight its origination, and penalize those who send spam. While the term was originally coined to describe unwanted legitimate marketing messages, it is now used to describe unwanted marketing messages that are generally considered illegitimate.

SpamCop™: A spam filtering database owned by IronPort Systems that captures reported spam and determines the origin of unwanted email. SpamCop provides a blocking list to help the Internet cut spam off at the source. See www.spamcop.net

Spamhaus: **1.** The term used to describe an organization or person responsible for sending spam as their primary business activity. Estimates vary widely, but many industry observers think that most spam emanates from only a few hundred sources. Not to be confused with www.spamhaus.org. **2.** (www.spamhaus.org): A website dedicated to tracking spammers, spam gangs and spam services. The site provides real-time anti-spam protection for Internet networks with its Spamhaus Block List, and works with law enforcement agencies to identify and pursue spammers worldwide.

Spam Trap: **1.** A list of nonexistent email addresses placed on a Web page or a discussion board that are likely to be harvested by spammers using Web crawlers to look for addresses. Spam sent to these addresses will be rejected, as they are fake. **2.** The term for a check box on a Web order form is defaulted to "yes" or "I agree," but positioned on the page so that it will most likely be overlooked. When it remains checked the user is placed on a spammer's target list.

SPEWS (Spam Prevention Early Warning System): An anonymous group comprised of system administrators, ISP postmasters, and other service providers that runs a service designed to expose and stop spammers, and the service providers who give them Internet access. SPEWS attempts to identify known spammers and spam operations as soon as they start spamming, and sometimes before they start. The private list is now available for the general public to read and/or use for email filtering, and can be seen at www.spews.org

SPF (Sender Policy Framework): This proposal for email sender authentication requires a modification to DNS records that enables a domain owner and an SMTP operator to specify policies that are followed by those using that domain in email messages. It also designates a list of MTA IP addresses that can be the source of email from the domain. SPF also requires an extension to SMTP to check for the modification in order to verify that a message is truly coming from the domain name indicated in the FROM field.

Spoofing: A spoof occurs when an email sender uses the sending address of a third party to entice the message's recipient to read the message. Spoofing is most often associated with spam email or phishing attacks.

Spyware: Software that gathers information about a user's Web surfing habits and sends that data to its home website. While it is usually intended to track habits in order to build marketing profiles, spyware is often used for nefarious purposes, and many consider it an invasion of privacy. Spyware is often included in free or commercial downloads, and may be downloaded to a user's computer merely as the result of visiting the site in what is known as a "drive-by download." Spyware is also called "parasite software," "scumware," "junkware" and "thiefware."

SRS (Sender Rewriting Scheme): This technique is required for SPF to work with forwarded email. In order to retain the original bounce address within each new bounce address added by an MRA, it creates one string including all bounce addresses that conforms to the definition of "Sender" for the purposes of an SMTP transaction. That list of addresses comprises the delivery route of the message so far, and one stage of the route is added for each server that re-originates the message.

SSL (Secure Socket Layer): This security protocol is designed to allow secure transmission within the HTTP used by the Web. SSL uses a public key based system that requires the browser to maintain a list of certificates of authority to determine the validity of the site, and a public key from the site to encrypt a random number that is sent back to the site. The random number is in turn used to create a session key. See http://wp.netscape.com/eng/ssl3/

Submitter: The person or other entity that submits mail to an MSA.

> **Responsible Submitter:** The most recent submitter of an email message into the message stream. The first submitter is considered the responsible submitter unless the message is forwarded or redirected, in which case the forwarding or redirecting agent is considered the responsible submitter.

T

Tarpit: A specially designed MTA, which responds to undesirable email it detects by purposely slowing things down. If the message is incoming, the MTA does not respond very quickly or close the connection in a timely way. A Tarpit may also be used as a way to cause spammer's servers to slow down so they are no longer able to send large amounts of email.

TCP (Transmission Control Protocol): The protocol that most Internet protocols use for communications. TCP contains a system for negotiating a data transmission channel between two network end-points, and ensures that the total number of bytes sent is received correctly at the other end by including error correction with retransmission upon failure.

TCP/IP (TCP over Internet Protocol): The IP part of this protocol provides the routing scheme, and the combination with TCP ensures correct transmission of a message to its desired destination. UDP is considered a part of TCP/IP, although it does not contain data correction features.

TLD (Top Level Domain): The TLD or top-level domain (typically .com, .org or .net) is generic and, within that level name, delegation is done by various domain registrars. The Internet Corporation for Assigned Names and Numbers (ICANN) is the current manager of Internet addresses and domain names.

TLS (Transport Layer Security): A security protocol based on SSL. TLS uses digital certificates to authenticate the user as well as the network. The TLS client uses the public key from the server to encrypt a random number and send it back to the server. The random number, combined with additional random numbers previously sent to each other, is used to generate a secret session key to encrypt the subsequent message exchange. HTTPS uses this protocol.

Trojan (Trojan Horse): A program that appears legitimate but performs an illicit activity, such as locating a password or other identity information, or making the system available for control by an outside unauthorized user. This latter use is how Zombie PCs are created in Bot networks. Trojans are often distributed through spam email, but sometimes are delivered within games. They resemble viruses, except that they do not replicate themselves. The name is derived from a major event in Homer's epic, The Odyssey.

TTL (Time To Live): This part of a DNS record sets the maximum amount of time a packet is allowed to propagate through the network or be cached before being discarded.

TUA (Tracking User Agent): An entity that initiates a message tracking request.

U

UBE (Unsolicited Bulk Email): See Spam.

UCE (Unsolicited Commercial Email): Same as Spam, but referring specifically to messages with commercial advertisements.

UDP (User Datagram Protocol): A protocol within TCP/IP that does not include any error correction processes. It is used when a reliable delivery is not required or when speed is more desirable than accuracy, such as in real-time video or audio transmissions.

UNIX: A multiuser, multitasking operating system widely used in workstations and servers, and as an underlying operating system for appliances such as MTAs. Variants are also used for embedded applications within consumer products such as cell phones and personal digital assistants. There are many variants, and variants of variants, on the market today. While it was originally developed by AT&T's Bell Laboratories in the 1960's, the trademark is now held by The Open Group.

URI (Uniform Resource Identifier, also Universal Resource Identifier): The addressing format used to identify resources on the Internet. A URI is defined by its purpose. The most ubiquitous URI is the HTTP URI, more commonly referred to as the URL, which is a Web page address typed into the Web browser address field or embedded in a Web page as a hyperlink. As widely used, is the MAILTO URI, which is embedded in a Web page to launch a user's email client.

URL (Uniform Resource Locator, also Universal Resource Locator): This subset of URI is used to address Web pages. The URL contains the protocol prefix (i.e., HTTP), port number, domain name, subdirectory names and file name. If a port number is not stated in the address, port 80 is used as the default for HTTP traffic; if the file name is not stated, "index.html" is used as the default.

Usenet (USEr NETwork): This public access network is a giant, dispersed bulletin board that is maintained by volunteers who provide news and email feeds to other nodes. All news that travels over Usenet is called "NetNews," and a running collection of messages about a particular subject is called a "newsgroup."

V

Variant (Virus Variant): A modified version of an original virus, which can be varied by simply changing text or just adding or deleting a few lines of code. Viruses are commonly changed, and sometimes damaged, by other virus authors over time. A variant often escapes detection when it is first released.

Virus: These self-replicating programs spread by inserting copies of themselves into other programs or documents, and sometimes completely replace other programs. Many email viruses are spread by adding themselves as attachments to emails that are then supposedly sent to the victim's address list with the appearance, to recipients, of coming from friends and/or associates. Recent virus programs contain Trojan Bot code that turns infected computers into remotely controlled Zombie PCs which then become part of Bot networks and are used by spammers for distributing unsolicited emails.

Virus Outbreak Filters™: A proactive security software created by IronPort Systems, which provides a first layer of defense to protect networks from viruses during the critical initial stages of a virus outbreak.

W

Whitelist: A list of email addresses from which an email server or email client program is configured to accept incoming messages. Email filtering that relies entirely on whitelists is severely restricted because only messages from addresses on the list are allowed, which creates a large array of situations in which legitimate messages are falsely identified as spam.

Whois: An Internet protocol that creates a query to find the person or entity responsible for a given Internet resource, usually a domain or IP address. A Whois query also returns the associated technical, administrative, abuse and other contacts. See www.completewhois.com

Worm: A self-replicating virus that spreads by sending copies of itself via email. Well known examples that have many variants are MyDoom, Nimda and Netsky. Other types of worms spread copies of themselves across an individual computer or network in a DoS-type attack.

X

XML (Extensible Markup Language): A SGML variant used for defining data elements on Web pages which require greater flexibility than HTML can offer. Like HTML, it uses a tag structure, however XML defines what elements contain rather than how they are to be displayed. XML also allows special tags to be defined by the developer of the page, enabling greater customization than is available with HTML alone.

X-Token: A general term for any non-standard site-specific header or its parameter. The convention generally used is that all such parameters should have a name that starts with "x-" or "X-".

Z

Zero-Day: An exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. A worm or virus attack uses email to deliver its destructive cargo. Blocking these threats requires more than the traditional approach to fighting viruses.

Zombie PC (or just Zombie): A hacked or otherwise compromised computer being remotely controlled by someone other than its owner. Zombie PCs are most often created by virus attacks, and are frequently used by spammers to distribute spam or for DDoS attacks. Synonymous with Hijacked PC, Drone and Bot.

ZombieNet (Zombie Network also Zombie Army): A large number of Zombie computers controlled by single entity. Spammers and their associates create large zombie networks to send emails and for other purposes. Zombie networks are bought and sold on a black market. Also known as BotNet or Drone Army.

Email Security Solutions

SPECIAL SECTION SPONSORED BY IRONPORT SYSTEMS AND POSTX

WE'VE SIZED UP THE EMAIL SECURITY PROBLEM.

IronPort C-Series
Email Security Appliance

THE CHOICE IS YOURS:

MULTI-LAYER DEFENSE.

BEST-OF-BREED OPTIONS.

IronPort C10™
For Companies with up to 1000 users

IronPort C30™
For Medium-Sized Corporations

IronPort C60™
For Large Enterprises and ISPs

The IronPort C-Series™ email security solutions combine market leading anti-spam, anti-virus, encryption, digital rights management, and archiving technology from Symantec, Sophos, Veritas, PGP Corporation, PostX, Sigaba, and Authentica — with the revolutionary IronPort MTA platform and preventive filters. This depth-in-defense solution is available in three models, sized for companies large and small. Industrial strength email security. For all. **www.ironport.com/leader**

IRONPORT™

Rebuilding the World's Email Infrastructure.

www.ironport.com/leader

Don’t worry.

You’ve secured your valuable email communications with PxMail from PostX. Now the world’s leading provider of secure email has created a solution that enables you to be up and running in minutes.

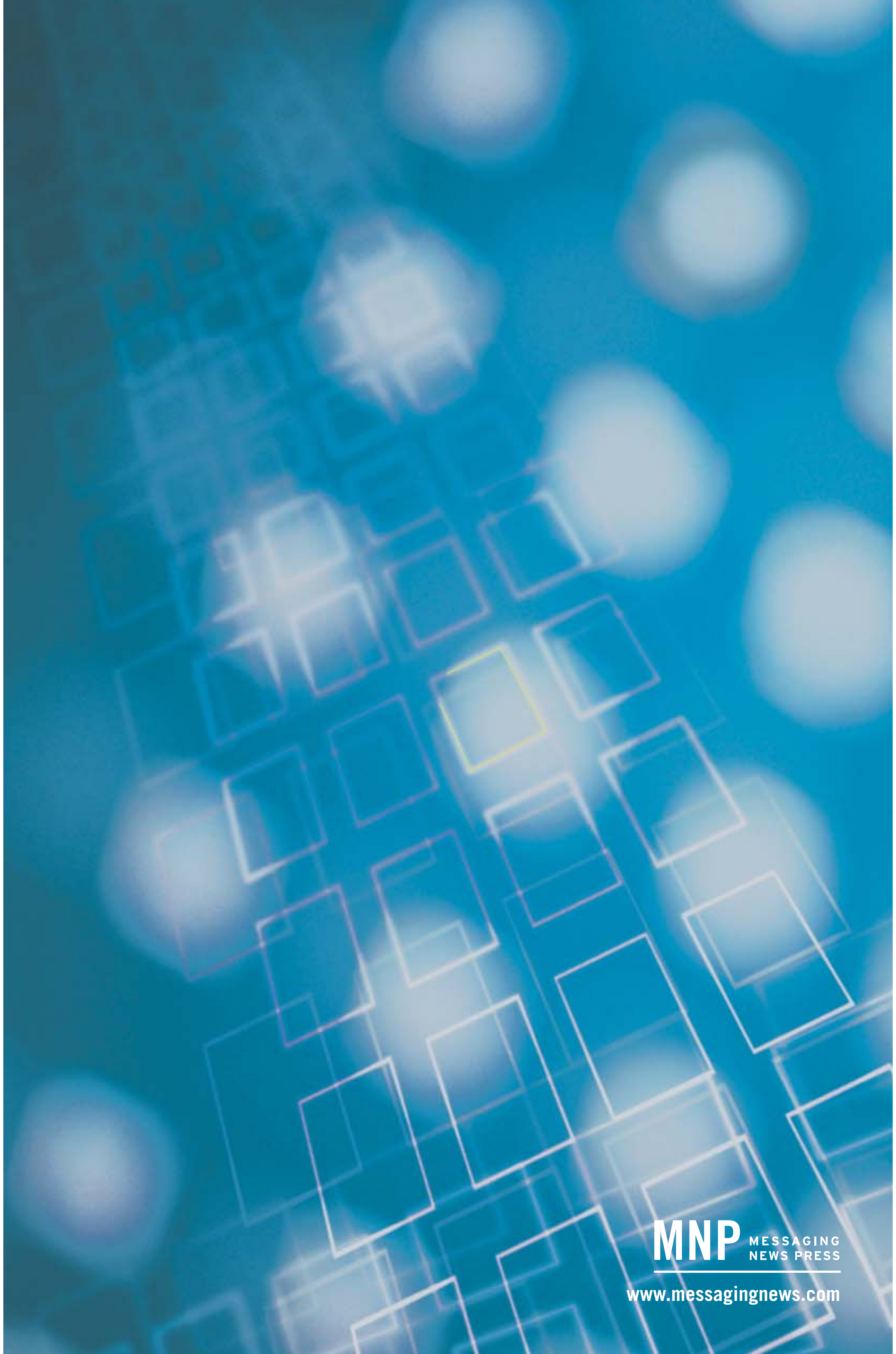
PxMail from PostX is the first secure messaging product that offers a blended deployment model; we host the complex key management and enrollment procedures while your critical customer data is safe within your enterprise.

Be up and running more quickly than ever before with PxMail.

1.888.44POSTX
WWW.POSTX.COM

POSTX

PXMAIL



MNP MESSAGING NEWS PRESS

www.messagingnews.com