Global Information Assurance Certification Paper

Encrypted E-mail: Close One Door, Open Another

[redacted]

It is common knowledge that virus detection should be a part of any corporation's security strategy. The threat of malicious code is an area of information security that is relatively well understood by the general population. However, with the introduction of more aggressive malicious code such as the Nimda virus, many corporations have realized that desktop virus scanning is necessary, but insufficient. With Nimda, the user does not even have to click on an infected attachment! Just opening the e-mail is enough to infect the computer in some cases. Detecting viruses before they enter the network, at the e-mail gateway for example, provides a much more proactive first line of defense. The use of server-based virus scanning techniques is part of an overall defense in depth strategy. One aspect of the virus threat that is not well understood is that server-based virus scanners cannot scan encrypted messages[1].

While e-mail encryption protects data against confidentiality and privacy attacks, encrypted e-mail messages open a new and relatively unexplored security vulnerability. Today, most popular virus scanners use a variety of techniques for detecting malicious code, but perhaps the most prevalent technique is scanning for telltale "signatures" of known malicious code. This presents an immediate problem: the malicious code is encrypted along with the message thus the scanner will not detect malicious code if it is present. The purpose of this paper is to propose a solution that allows protection of e-mail through content encryption without compromising server-based virus scanning.

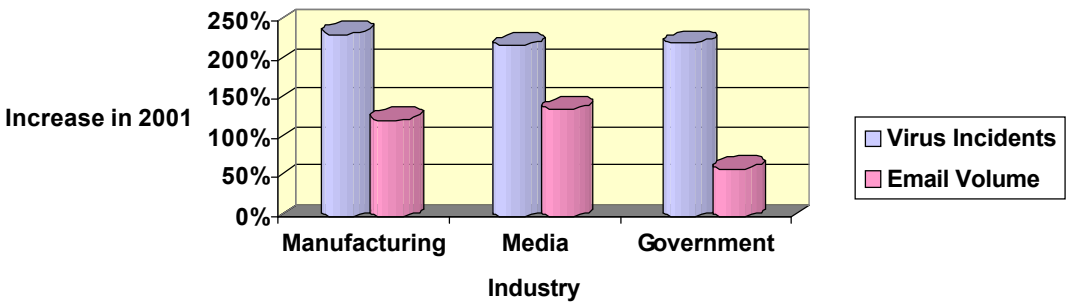
Maybe you are wondering, "Is this really important? How likely is a virus-infected encrypted e-mail anyway?" I have provided the following section entitled "Making the Case" for the cynics out there. Everyone else may skip to the section entitled "Solution for Virus Scanning of Encrypted E-mail Messages" to discover the solution.

[1] For clarification purposes, this vulnerability only applies to methods where e-mail remains encrypted until the recipient decrypts it at the desktop (most commonly uses public key technology) such as S/MIME and PGP. This does not apply to SSL or TLS technology because these technologies decrypt the data at the web server, not at the end user's desktop.

E-mail Use and Virus Incidents on the Rise

E-mail has rapidly become the preferred method of corporate communication. It's fast, easy to manage (for the user!) and provides a written record of communication. In the information age, it's hard to imagine corporate communication without it. But beware; e-mail circulation is not the only thing on the rise. MessageLabs states that "as many as one in ten e-mails circulating the globe would be infected by a virus by 2007."*(Legard)* In fact, virus propagation is outperforming e-mail growth in 2001 (see Figure 1). MessageLabs predicts that virus attacks may triple by the end of this year and that "government departments and companies will collapse under the weight of malicious e-mail attachments". *(Knight)*

Figure 1: Virus and Email Increases



Encryption: More Prevalent Than You Think

An InformationWeek survey of 500 sites found that 43% of the companies surveyed use encryption on stored and transmitted data. *(Boomer-Smith)* The number of products that support secure e-mail is rising as standards are developed and adopted by the industry. For example, RSA's S/MIME (see IETF RFC 2630 – 2633 for specification) Interoperability Center lists 32 S/MIME compatible e-mail clients. The growing importance of S/MIME is likely to be propelled by Microsoft's support of the standard beginning with the Outlook '98 e-mail client, which supports S/MIME out-of-the box. In fact, "Within enterprises in 2000, the probability that an S/MIME client is already on the desktop is about 30 percent."*(Graff)* Another example of the mass adoption of encrypted e-mail is the announcement from Yahoo in September of 2000. Yahoo announced that it would provide an encryption service for its account holders using ZixIt's SecureDelivery (which by the way performs content encryption, not just channel

encryption). *(Festa)* The use of encryption will continue rising as the technology becomes more manageable and affordable.

The Effects of September 11th

The terrorist acts have elevated the importance of cyber security to a national security objective. Analyses of the terrorist electronic communications made it apparent that, in many cases, the terrorists were using more sophisticated technology than our Federal Government (and most corporations). Furthermore, because of Anthrax fears, Gartner predicts that the compound annual growth rate of e-mail will increase to 45 percent through the fourth quarter of 2002. *(Graff2)* The new era that dawned the morning of September 11th will bring 1) an increased reliance on electronic messaging and communication 2) renewed urgency to protect out national security through technology such as data encryption.

By now you are probably getting the idea of what I am proving in this section; the use of e-mail is going up, the virus threat is increasing, the use of encryption is on the rise and security awareness has been fueled by September 11th. The logic follows that the occurrence of virus-infected e-mails that are encrypted will increase significantly in times to come. This introduce a new vector for malicious code introduction.

[redacted]

Comprehension of the proposed solution requires a basic knowledge of Public Key cryptography. If you do not know which key is used for encryption (public or private), I suggest you stop and read “Introduction to Public Key Infrastructure” available at:

http://www.iplanet.com/developer/docs/articles/security/pki.html.

Encrypted messages must be decrypted before any server-based virus scan can be performed. The only way to decrypt a PK encrypted message is with a private key that corresponds to the public key the message was encrypted with. Most PK encrypted messages are encrypted using the public key of an individual user, leaving two choices for a server-based virus scanning solution:

1) The virus-scanning server must have access to a copy of each users decryption private key to decrypt each message
2) Every e-mail message must be encrypted with the virus-scanning servers public key so that the server can decrypt the message with its own private key

Option 1: Virus-scanner has Access to End User Decryption Private Keys

With this option, the virus-scanning server must somehow have access to or store a copy of end users decryption private keys[2]. Technically, this is not a big problem since private keys should be backed up anyway to ensure that data can be recovered if something happens to a user's private key. However, from a trust and privacy perspective I can see eyebrows raising already.

This scenario could cause discomfort for users, implementers and integrators of public key technology because:

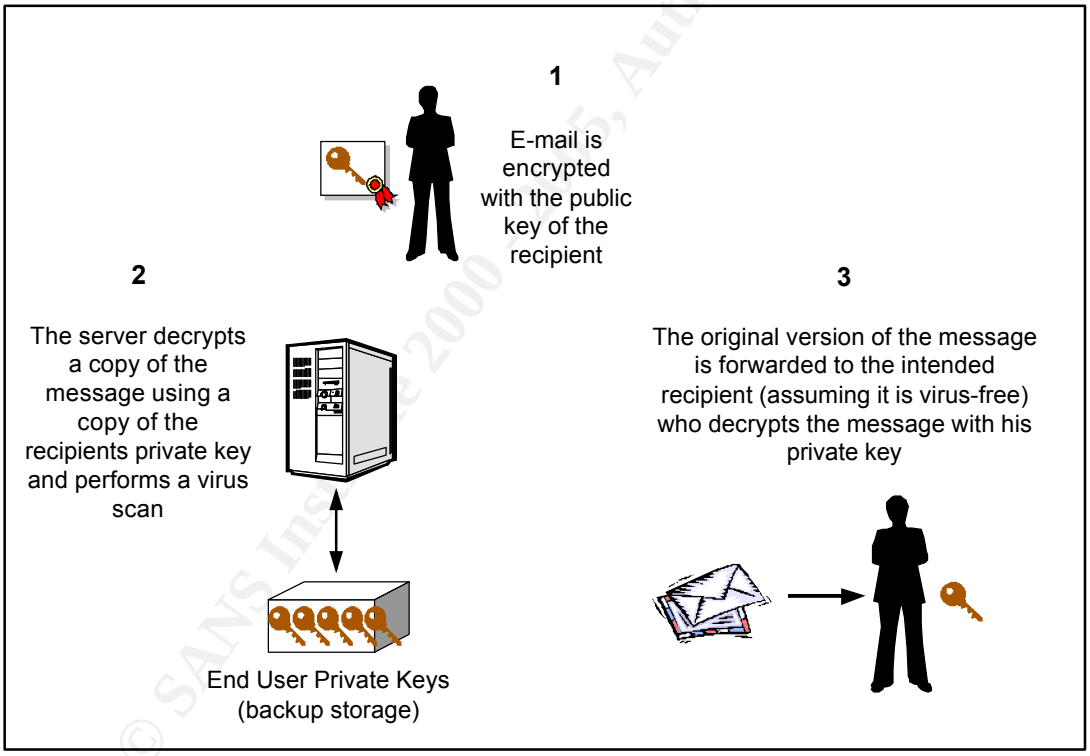
- PKI is supposed to provide end-to-end encryption. This means, in part, that only the sender and the recipient(s) should be able to decrypt and read the message (if the server decrypts it, the seal of confidentiality is broken).
- Private keys in PKI (as in symmetric cryptography) are sensitive.

Allowing any person or device other than the intended recipient to decrypt a message increases the risk of unauthorized disclosure. There will inevitably be questions about the possible compromise of the virus-scanning server, which would literally give away the keys to the kingdom, or at least access to them! Even without the total compromise of the virus-scanning server, users may be uncomfortable with the fact that their private keys are being accessed on a regular basis.

[2] From this point on, I will refer to the decryption private key as simply "private key". I am in no way referring to digital signature private keys as they should not be copied by anyone or accessed by anyone except the owner for any reason. Digital signatures are not addressed in this paper.

Based on my experience, although technically feasible, this solution introduces too much risk and uncertainty to be useful. The level of assurance that this solution would provide does not justify the cost of implementing PKI because the secrecy of private keys is a fundamental tenet of the infrastructure. Nevertheless, in case you are interested (and since I brought it up), here is how it works:

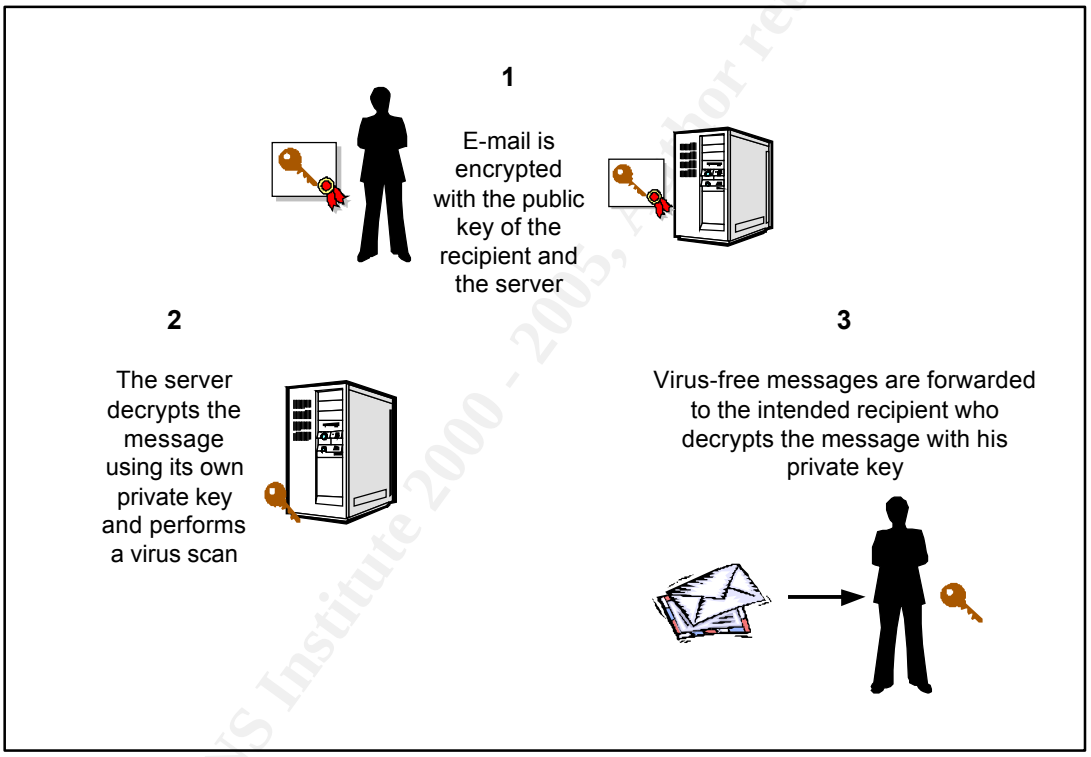
Figure 2: Virus-scanner Accesses End User Decryption Private Keys



Option 2: Messages are Encrypted for the Virus-Scanning Server

This method requires all e-mail to be encrypted using the public key of the e-mail filtering server in addition to the public key of the intended recipient(s). Encrypting the messages with the e-mail filtering server's public key will allow the virus scanner to open the message, scan it for viruses and send the "clean" messages along to the recipient (see Figure 3). Any messages that are found to be infected with a virus will be quarantined and will never reach the end user's desktop. This method allows safe end-to-end encryption of messages without a server having access to end users' decryption private keys.

Figure 3: Virus Scanning of Encrypted E-mail



The question is how does the sender know that messages must be encrypted for the virus-scanning server? There are several ways to achieve this.

In a closed PKI deployment[3], server based virus scanning can be implemented in a manner that is transparent to end-users. E-mail clients can be automatically configured to blind carbon copy (BCC:) the e-mail filtering server and encrypt the message using the server's public key. This will almost certainly require a small piece of software that enhances the e-mail client (a.k.a.

[3] "Closed", in this connotation, means an intra-domain deployment, such as within a corporation or agency.

an e-mail plug-in). The only effect on the end user will be performance since the message will be encrypted at least twice (using the public keys of the server and the recipient).

In an open PKI, where a user may be communicating with someone outside his domain, there are two possibilities.

1. The e-mail server can bounce back encrypted e-mails with a message to the sender that requires the sender to use the virus filtering servers key in addition to the recipients key, or else resend the message in plaintext. Most users will probably comply with this if they need to send the e-mail badly enough. However, this would make me a little suspicious if I were the sender because I don't know what this virus-filtering server is, who has access to it and whom I will be allowing to read my confidential communications. How do I know this is not a complicated scheme designed by an attacker? This solution works, but is a little cumbersome.
2. All external users are directed to encrypt messages only for the virus-filtering server. The server then performs a scan, encrypts the message using the intended recipient's public key and sends it along[4]. This solution has the added advantage of providing a simple solution for the sender since one public key is good for any recipient within the corporation or agency.

[redacted]

Most virus-scanning servers are capable of more than virus scanning. In fact, the three products I found that provide the solutions described in this paper are marketed as content filtering servers; virus scanning is a small fraction of the their capabilities. The software can be configured to perform other e-mail filtering functions such as:

- **Content Filtering –** The server can look for words or content in the subject or body of outgoing messages and filter any messages that contain unauthorized content. This can provide additional assurances for an agency or corporation. For example, an investment banking company used a filtering policy that did not allow any outgoing e-mail with the term "guaranteed return." This protects the company from liability should a client lose money on an investment.
- **Automatic Policy-based Encryption –** The corporation or agency could configure the server to encrypt outgoing messages based on source, destination, subject, words in the body, attachments etc. For example, a policy could be written that says that any e-mail that will be transmitted

[4] Note: Access to public keys is not sensitive since they are not meant to be kept secret.

over public networks such as the Internet must be encrypted.

[redacted]

The introduction of new technology causes new and unanticipated vulnerabilities. Username and password authentication presented many new problems of policy, technology, behaviors of end-users etc. The issues of how password databases would be protected, how passwords would be enforced and what would be done if users forget their passwords had to be ironed out. Does this mean we should not use passwords at all? No, because the relative risk of using passwords is still much less than the risk of not using any authentication at all. The same logic applies to encrypted e-mail. Consider that in a survey conducted by NFO worldwide, "21 to 31 percent of the respondents admitted to sending, via e-mail, confidential information like financial or product data outside the company." *(1999 E-mail Abuse Study)* The new risk introduced by encrypted e-mail (such as the introduction of malicious code) is still far less damaging than the risk presented by allowing sensitive communications to be transmitted without confidentiality services. This does not mean we must accept the risk of viruses entering the network through encrypted e-mail. It does mean that security professionals must look for new and innovative ways to combat this new threat. I have presented some ideas and methods that mitigate the risk of introducing viruses through encrypted e-mail.

Knight, Will. “Dramatic Increase in Virus Attacks Predicted.” ZDNet News. 5 April 2001. URL: http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2705266,00.html (8 Nov. 2001)

Boomer-Smith, Lisa. “Encryption: How Prevalent Is It?” Infromationweek.com. 15 October 2001. URL: http://www.informationweek.com/story/IWK20011011S0015 (8 Nov. 2001)

Festa, Paul. “Yahoo to offer encrypted e-mail option.” CNET.com. 25 August 2000. URL: http://news.cnet.com/news/0-1005-200-2605437.html (18 Nov. 2001)

Graff, Joyce. “Implementing e-mail security: Where and how?” techrepublic.com. 10 Oct 2001. URL: http://www.techrepublic.com/article.jhtml?id=r00620011010ern01.htm&page=1 (18 Nov. 2001)

Graff, Joyce. “Prepare for Higher E-mail Traffic Because of Anthrax Threat.” www4.gartner.com. 30 Oct. 2001. URL: http://www4.gartner.com/resources/102000/102070/102070.pdf (18 Nov. 2001)

Knight, Will. “Researchers predict virus avalanche.” ZDNet News. 5 April 2001. URL: http://news.zdnet.co.uk/story/0,,t269-s2085508,00.html (18 Nov. 2001)

Legard, David. “Viruses are getting faster, tougher.” CNN.com. 20 Sept. 2001. URL: http://www.cnn.com/2001/TECH/internet/09/20/faster.virus.idg/

“1999 E-mail Abuse Study.” Internet Manager URL: http://www.elronsw.com/pdf/1999_E-mail_Study.pdf (18 Nov. 2001)

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event