

RE: Email Encryption Between Servers

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-04/0051.html>

From: Robinson, Sonja (SRobinson@HIPUSA.com)

Date: 04/03/03

From: "Robinson, Sonja" <SRobinson@HIPUSA.com>

To: security-basics@securityfocus.com

Date: Thu, 3 Apr 2003 12:36:34 -0500

There are some interesting ideas and solutions depending upon your specific situation. I really like some of the ideas that are being presented. Each one has pros and cons and needs to be evaluated based on your environment and your need. VPN is all well and good for your major business partners providing you take certain precautions and mitigate risks and admin overhead. Each environment and company is different but I don't think I would want too many VPN connections. Overhead could become cumbersome depending of course on a number of factors. Remember – each company is different and there are risks associated with each solution. Also, it's not just confidentiality you have to worry about, there's integrity and authentication you have to think about too. So, if the e-mail is decrypted at the other gateway, how can you ensure that no one else has read it and that only the intended recipient has received it? Also, can I send a secure e-mail to ANYONE or just selected people?

Here are some scenarios to think about when you are evaluating your solutions.

Scenario 1: You are a healthcare company and you need to send PHI, in an e-mail for arguments sake, to a business company (hospital in this case). How would you do it? VPN connection? Secure E-mail, PGP, secure web server, secure compatible hardware? What kind of overhead and support for them and us will I need? Who is exchanging keys? Is everything encrypted? Only stuff with PHI?

Scenario 2: Same as 1 but now you are just transferring a list of all your members and their coverage? VPN? Dial up? Secure Ftp? Secure web server? Is there a difference for e-mail versus non-e-mail? What about e-mail with a file attached that has a client list?

Scenario 3: You are a healthcare company and you need to send PHI to a number of your members/patients. They don't have VPN and don't have the slightest clue how to set one up nor would most want to. How do send them encrypted e-mail? PGP? Perhaps. But who is going to support PGP for those people. Who is going to buy it for them and/or install it? Remember a lot of people who need to receive these e-mails are not technically savvy and

SecurityFocus BASICS: RE: Email Encryption Between Servers

key exchange between 100's, 1000's and 1,000,000's of users can be a monumental task. Think about e-mailing them their Claims Statements and the potential # of users you may have to deal with. Great ROI can be achieved but it has to be secure. Your members may only have to deal with 2 or 3 entities who want to send them secure e-mail.

Scenario 4: Same as above but now you are contacting your member doctors. Are the doctors going to have separate keys for each provider, doctor, hospital, pharmacy, insurance company they deal with? Are you going to require them to install software on their PC's? Who will install and support this? Are you going to show their admin/nurses how to manage the keys? What if they forget their passphrase? Will I, as the provider, be able to manager all of THEIR keys myself since potentially I may have well over a million keys to deal with? Will my users be able to or will I have to train them on multiple packages myself since they will be receiving encrypted e-mail from external entitites as well?

Scenario 5: I'm a doctor. I provide healthcare to my patients. Here is my dilemma: I deal with 5 insurance companies all with different solutions. I deal with hospitals, pharmcies ,etc who also have different solutions. VPN, desktop e-mail encryption, enterprise e-mail encryption. How am I going to manage key exchange (if their solution requires it), staff training, software installations, etc.? Can they really impose their solution on me and my business processes? My staff is not trained for this type of thing. What is encryption and keys? Who do I call to get a key? Where is it stored? What if I can't get it to work? Who will support me? What if I lose the key? Do I have to a have a key for each of my employees?

I'm not trying to endorse any solution, any product or any vendor, just trying to get a dialog going on solutions for other than major business partners. These are some of the things my company has thought about during our solutions. Multiple solutions may also be necessary. These are issues that we all need to think about.

DISCLAIMER: This is not necessarily the opinion of my company, blah blah blah

Sonja Robinson, CISA
Network Security Analyst
HIP Health Plans
Office: 212-806-4125
Pager: 8884238615

-----Original Message-----

From: White-Tiger [mailto:white-tiger@rocketmail.com]
Sent: Wednesday, April 02, 2003 11:18 AM
To: mleigh@austin.rr.com
Cc: security-basics@securityfocus.com
Subject: RE: Email Encryption Between Servers

Just another .2\$

RE: Email Encryption Between Servers

SecurityFocus BASICS: RE: Email Encryption Between Servers

in the ports there is pgpsendmail. Havn't tried it yet,
but what that will do for you is automagicly pgp encrypt
and decrypt email for anyone that you have there public key
in your keyring.
that way the users do not have to worry about it.

also. look into sendmail's TLS
that might help also.

I was looking at pgpsendmail for the same reason, HIPAA
but didn't want to have to retrain the whole staff.

Please let me know what you find that works for you.

WT

--- Michael Leigh <mleigh@austin.rr.com> wrote:

- > *I think the easiest way to do this would be with IPSEC tunnels,*
- > *between either your firewalls, routers or mail servers*
- > *explicitly.*
- >
- > -----Original Message-----
- > *From: Al Cooper [mailto:alc@2wh.com]*
- > *Sent: Monday, March 31, 2003 9:44 AM*
- > *To: security-basics@securityfocus.com*
- > *Subject: Email Encryption Between Servers*
- >
- >
- > *We are attempting to set up secure e-mail with our*
- > *partner companies to*
- > *comply with the upcoming HIPAA requirements. I would*
- > *like to find a way to*
- > *encrypt all e-mail going between our mail server and our partners. We*
- > *are using Exchange. Some of our partners are also using*
- > *Exchange and some are*
- > *using other SMTP servers.*
- >
- > *Is there a way to automatically force all e-mail between*
- > *our two e-mail*
- > *servers (either Exchange to Exchange or Exchange to SMTP)*
- > *to be encrypted*
- > *then decrypted on arrival with no end user intervention?*
- > *If there are,*
- > *what affect, if any will these encryption methods have on*
- > *our overall*
- > *network security.*
- >
- > *Thanks for your help,*
- >
- >
- >
- >
- >

SecurityFocus BASICS: RE: Email Encryption Between Servers

> SurfControl E-mail Filter puts the brakes on spam,
> viruses and malicious code. Safeguard your business
> critical communications. Download a free 30-day trial:
> <http://www.securityfocus.com/SurfControl-security-basics>
>
>
>

> SurfControl E-mail Filter puts the brakes on spam,
> viruses and malicious code. Safeguard your business
> critical communications. Download a free 30-day trial:
> <http://www.securityfocus.com/SurfControl-security-basics>
>

Do you Yahoo!?
Yahoo! Tax Center – File online, calculators, forms, and more
<http://tax.yahoo.com>

SurfControl E-mail Filter puts the brakes on spam,
viruses and malicious code. Safeguard your business
critical communications. Download a free 30-day trial:
<http://www.securityfocus.com/SurfControl-security-basics>

This message is a PRIVILEGED AND CONFIDENTIAL communication, and is intended only for the individual(s) named herein or others specifically authorized to receive the communication. If you are not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender of the error immediately, do not read or use the communication in any manner, destroy all copies, and delete it from your system if the communication was sent via email.

SurfControl E-mail Filter puts the brakes on spam,
viruses and malicious code. Safeguard your business
critical communications. Download a free 30-day trial:
<http://www.securityfocus.com/SurfControl-security-basics>