

RE: questions on setting up a mail server

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2007-09/msg00380.html>

- *From:* "Ted Mittelstaedt" <tedm@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 5 Sep 2007 23:27:14 -0700
-

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

From: Jonathan McKeown [<mailto:jonathan+freebsd-questions@xxxxxxxxxx>]
Sent: Wednesday, September 05, 2007 5:12 AM
To: Ted Mittelstaedt
Cc: freebsd-questions@xxxxxxxxxx
Subject: Re: questions on setting up a mail server

I've edited ruthlessly to reduce the length of this message.

On Wednesday 05 September 2007 11:07, you wrote:

My main question is on authentication. I was looking at authentication types in kmail to get an idea of what I

can use, and I

found:

[list of SASL methods plus question what to use]

Much of this depends on the mail clients that your going to be hitting the server with.

The first group does encryption of the password only.

Not sure what's meant by ``the first group" here.

RE: questions on setting up a mail server

CRAM–MD5, Digest–MD5, NTLM, GSSAPI, and APOP are associated with password encryption on SMTP auth and POP3 as you well know, so please do not try to be deliberately stupid to make a point. Just make your point and get on with it. Most people won't understand anyway.

I wasn't trying to be stupid: I saw a single list of SASL authc methods and wasn't sure where you had drawn the line to divide them into two groups.

[...certificates]

There is a large amount of arcane magic to do this, and to get it accepted into Windows, so that an Outlook client will do SSL.

This isn't true, in my experience.

Your experience is limited then.

Yes, it is: but with Windows 2000/XP and Outlook 2003, it's not magic. In fact I was pleasantly surprised how easy it was.

Sure it is simple – when ALL clients are running the same version of Windows, IE, and Outlook. Perhaps true in a small network. Very not true in a large network.

I'll bow to your experience on that. All I can say is that my own view is that the bigger the network, the more important it is to get software standardised across the organisation to reduce your support costs, and the cheaper it is to do through volume licensing.

That sounds like a line from a MS sales rep. It really isn't true and I'll explain why in a moment.

RE: questions on setting up a mail server

We're a small, donor-funded, African NGO, and we have two versions of Windows (2000 and XP) and one version of Office (2003). We will use Microsoft's down-licensing provision to stick with what we have until we're ready to upgrade everyone.

I don't know what licensing your running but I can tell you that MS has a program called Open Charity – if your donor funded, you very likely qualify for this, and are on it. The costs for licensing on that program are –unbelievably– cheap. It completely changes the capital cost/support cost equation that yes, indeed, it almost always makes sense to upgrade across the board under that program.

For most for-profit corporations it is –very– expensive to upgrade across the board. It also causes costs to spike in some years – most corporations hate that. Most corporations when faced with a choice of spending \$50K a year, every year, from now until doomsday, or a choice of spending \$100K every 3 years, from now until doomsday, they will take the \$50K a year, even though over the long run it costs them more. The reason is due to cash flow. This is also why corporations will buy a photocopier for \$10K, and immediately stick it on a 5 year lease that will cost them \$3K a year in interest and principal.

Yes I know it is stupid and it used to drive me bananas when I worked as an accounting clerk a couple decades ago, but it is how businesses (at least in the US) do business.

Anyway, because of this most large corps follow a staggered upgrade plan. Every 4 years a quarter of their employees get brand new computers and a quarter of the computers they have in production get scrapped. Or, every 3 years a third get new stuff. Or every 5 years a 5th get new stuff. Whatever they decide to budget for.

This is why Microsoft has twice extended the End Of Life software support deadline for Windows XP. Corporations are nowadays treating their computing purchases the same way they treat other capital expenditures, by staggering the costs over time.

The days of across the board software upgrades are over and done with, except for government contracts where most governments are still clueless.

Everyone supports LOGIN and PLAIN. (at least I never met a mail program that didn't – perhaps there is one) But, you cannot get password encryption with Outlook Express unless you do NTLM. It supports nothing else, except for SSL which is encryption of the entire channel.

RE: questions on setting up a mail server

If you know of a way to get OE to support CRAM-MD5 then do tell.

No, Outlook 2003 doesn't support PLAIN – at least I couldn't get it to. That's why I enabled LOGIN. It's true that NTLM is the only encrypted password protocol supported by Microsoft – that's why I'm using an encryption layer with cleartext authentication.

I've never enabled just PLAIN without enabling LOGIN since it is rather pointless to only enable one, since both of them are unencrypted. So that is interesting to note. I don't know that there would be any advantage to disabling one over the other, though.

The honest to god truth of the matter is that encrypting your POP3 and SMTP auth passwords is difficult to do on a large scale

no matter

what road you pick to do it, so there is really not a lot

of point to

doing it unless your in a rather limited environment.

I'm not sure I would agree with this statement either.

I perhaps should have explained this more. Encryption of e-mail is absolutely pointless unless done from [end to end]

It is only useful for protecting passwords from wire sniffing.

True up to a point. It can also offer integrity – an assurance that the message is from the authenticated identity. Although that assurance is only valid at the first server (the MSA), that may be enough to

RE: questions on setting up a mail server

prevent injection
of a variety of kinds of junk with forged sender information.

That is true but only if you purchase certs from a 3rd party, if you self-sign you lose the integrity aspect. Unless, of course, you use an outside channel – such as reading the SHA thumbprint over the phone to the end user or some such, and making sure they check it when they accept the certificate – or forcing all of the road warriors to return home to the mothership at least once to have a tech load a root cert, or some other such method.

I am not convinced though that most people dealing with certs understand what an outside channel is and how it relates to the integrity aspect, including most users, so this is more of a philosophical than a practical discussion.

But in most cases, the wire isn't sniffable.

Given that, certainly in my case, the "wire" may be cellular, radio, satellite, wireless LAN, or a government, academic or hotel/airport network providing temporary connectivity, I can't say that with confidence.

password sniffing only becomes a concern when you have road warriors who are NOT connecting into the mailservr via a VPN

Again true – but now you're talking about another method of protecting passwords, and another technology to master. In practice, even though I run a VPN as well, I still use TLS at the individual service level to protect passwords "in flight".

Naturally, if you can do an encrypted channel without involving a VPN you would be daft to involve a VPN – but there are a lot of company networks out there where these are political, not technical, decisions.

Curse those in-flight magazines on the airlines – you wouldn't believe some of the daft ideas I've had to put up with that came spewing out of some CEO's mouth that came across some article in one of those.

And even if you have valid concerns on password sniffing well that's simple enough to address – don't be an idiot and use

RE: questions on setting up a mail server

the same user name and password for your e-mail clients as you use for your network and windows logins.

I would dispute that this is idiotic. You do need to protect the password much more carefully, but there are advantages to having a single password, easily changed by the user and easily cancelled when the user leaves.

Not at all – it depends on your ratio of road warriors to in-situ folks. In your case you have a lot of them, coming from a lot of weird places – so what your doing with SSL is the obvious choice – at first glance.

But, keep in mind you have no real mail security in your setup. Your corporate jewels are not the passwords, or even the data on the mailservier – as since your running POP, the data on the mailservier is transient.

Your real corporate jewels are the information assets contained in the hundreds if not thousands of saved e-mails in the countless folders that your road warriors have created over the years. And that data is hanging out there in space like a ripe plum for anyone to pick.

Your road warriors have ample time to access that information and coorelate it how they want. You have a sales rep. leave – he takes his last 4 years of contacts with him as all he needs to do is make a copy of his mailbox.pst file and take it with him when he leaves. And not just contacts – all the sales history of those contacts. All tied up in a nice, searchable package in that .pst file.

And, how about the day when your road warrior's laptop get stolen? He's saved his e-mail login ID and password in his mail client – no need for sniffing there.

Now anyway, none of this may apply to a NGO but I think you get the idea. It would apply to most corporations.

[certificate authority not hard]

I didn't say doing that was hard. The problem is that the entire SSL picture is hard for a newbie.

[...]

RE: questions on setting up a mail server

It's only after digging for a long while will they come across some pointers that will shed the light.

That's certainly true. The longest part of the design, implementation and rollout of our new mail system was finding all the bits and pieces and working out how to put them together.

[of SASL authc methods]

Of the passwd-based methods, PLAIN is the preferred protocol according to the docs and RFCs – LOGIN is the one Microsoft uses (go figure).

LOGIN and NTLM. PLAIN and LOGIN are identical, it's merely a naming convention.

No. There are small differences but they are there. PLAIN sends a single string containing the authorization identity, authentication identity, and password. LOGIN expects a prompt to which it replies with the authc identity, then a second prompt to which it replies with the password. The protocol specifies that the content of the two prompts is irrelevant, but Outlook expects specific strings.

[long discussion of config details]

The first time someone collects email with Outlook, they get a warning that the certificate isn't trusted, but also the option to install it. Half a dozen clicks later the certificate is in place.

That is only for Outlook 2003, and that Outlook only comes with MS Office. Your making several assumptions here – first that it's an environment with all Outlook (not Outlook Express) and second it's all current Outlook.

With Windows Product Activation the bad old days of a corporation buying a single copy of Microsoft Office and loading it on 50 or so machines are long gone. Why do you think that there's a giant fight now over the OpenXML standard? Corporations are done with standardizing on a –version– of MS Office, as they now know that they are going to have mixed networks with different versions of

RE: questions on setting up a mail server

MS Office on them since they cannot pirate software anymore. They now want to standardize on a document format, so they don't get pushed into updating –everyone– on the network when a new version of Office comes out.

Again, I wouldn't run a network like that because of the support problems it causes – this being one example. You can buy one copy of Microsoft Office and a volume licence, and Microsoft will allow you to downlicense so that you can standardise on an earlier version until you are ready to upgrade. This approach to licensing is one thing they get right, IMO.

Yes, but you have to pay the fee for every copy of what you downlicense. This isn't cheap. Once more, quotes straight out of the MS salesbook.

It's a lot cheaper to simply pay for what you're using. Year 1 you have 5 PC's you pay for 5 copies of Office 98. Year 2 you have 5 more PC's you pay for 5 copies of Office 2000. You DON'T pay for 10 copies of Office 2000 then downgrade half of them. And so on until you start scrapping systems.

As for support costs – you're going to have support costs either way, and a lot of it depends on what the employees are doing. In most companies the majority of employees are NOT sitting in cubicles shuffling paper around. They are actually out there doing work – talking to people, operating machinery, making things, fixing things, building stuff, yadda yadda yadda. Consider Intel Corp.'s payroll – they don't outsource their chip manufacturing, at least, not the stuff that makes them real money. If their payroll was mostly suits in cubicles they wouldn't be making any products at all and what would be paying those salaries?

Sure – there's so-called "new economy, information only" companies out there where everyone is shuffling paper on a computer screen. I can think of a few – law firms, CPA's etc. But not the majority of companies. In fact, there's a huge movement these days to –take away– the general purpose PC from a lot of employees and replace it with windows terminals, and suchlike. Companies have many employees out there who they do not want wasting time downloading the latest .mp3 or surfing the web – they want them inputting data into the customer service database, or shipping paper, or whatever the company does to make money. They are running apps that do not change from year to year and the machinery they are running these apps on does not need to change every year – just because MS comes out with some new operating system and wants to make some money.

RE: questions on setting up a mail server

I've been in this arena since 1990 and I have watched as the computer has come into businesses – and the height of the "slap a PC and an Office Suite on their desk" was sometime in year 2002. Since then a larger and larger number of companies are looking seriously at their office productivity and finding out that the new version of MS Office don't grind out the sales quotes any faster than the old did, or the cad drawings, or the whatever. And that's just general purpose office cube farmers. The factory floor people got their PC's taken away years ago, and replaced with toasters that may look like PC's but do only 1 thing.

The hottest software markets today are things where they are coming out with narrow-market software that addresses specific needs, for specific industries. You can't name a single industry anymore that doesn't have a couple of ISVs in it that make turnkey systems that lock the entire workflow down.

The single largest penetration of Windows Vista today is among the home users, I kid you not. That will certainly change eventually, but so far your just not reading those countless testimonials of large wholesale rollouts of Vista among the Fortune 500 like you used to read years ago in the trade rags when XP came out.

For older Outlook versions, you can't just do 6 clicks and install it. And, are you aware that MS has dumped Outlook Express entirely with Windows Vista and IE 7? One more wrinkle for the sites that are not all MS Office on every desktop.

Granted, if you have clients using older versions of Outlook
or dozens of

different email clients, you may have issues finding working combinations of TLS/STARTTLS/port numbers and authentication methods,

Bingo!

Yes, but in a business environment, almost the first problem you need to solve is controlling which clients are going to connect to the mail server. If you haven't managed to standardise on one or two clients across a large organisation, you're probably too busy doing support to worry about setting up a new email system.

RE: questions on setting up a mail server

In these large organizations it's not really possible to standardize across the organization. There's just too many bodies and systems. It is like painting the Golden Gate Bridge – you start at one side and by the time you get to the end of it, it's time to start at the beginning again. The norm is a rolling upgrade program where your tackling groups a chunk at a time.

but by and large it's just putting a few slightly scary-sounding pieces together on the server – all of which are either in the base system (sendmail: most of the objections to sendmail haven't had any basis in reality for several years.

I agree wholeheartedly, I use sendmail for all my mailservers anyway.

It's now as easy to configure as Postfix, IMHO, and hooking Mimedefang in as a milter gives you the ability to reject a lot of junk during the connection rather than after the fact) or easily added from ports.

greylist milter is also a good one to have.

I haven't tried putting any obstacles in the way of incoming mail over and above the difficulties many mail admins cause themselves. You would be astonished at what I see coming over the transom on my mailservers,

I very much doubt that.

especially the Mailman box (we host a number of lists). As it is, we take a few steps that end up rejecting over 80% of our incoming connections.

Well, greylisting isn't an obstacle but I understand the controversy

RE: questions on setting up a mail server

RE: questions on setting up a mail server

on it. And I will tell you that in running it for the last 2 years I have proof positive that it works, why? Because the spammers are adapting to it. Each month it's less and less effective – just as each month the other filters are less and less effective. As for obstacles, its no worse than any of the other filters.

Ted

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"