Comment #: 17

From: Nathan von Colditz
Sent: Wednesday, September 29, 2004 4:24 AM
To: Authentication Summit
Subject: Email Authentication Summit - Comments, (Matter Number P044411)

Excuse me for the crudeness of this proposal but I just got word of this conference and this has to be in within the next day. So this is done quickly and by one person, not by Microsoft's entire SecureEmail staff. However, the ideas and concepts are there and hopefully it will get someone to listen... I have solutions if people are willing to listen. I have a lot of research and real world experience here... that is why I am sending this in. I should be starting grad school soon to work on this exact topic and this is the solution I have been working on thus far.

The question being posed needs to change. How can we insure who an email comes from? Email right now is a broad and undefined term. There should be different types as well. There should be an invite email much like they have for email lists requesting communication. That is easy to do and also easy to standardize and provide encryption or Ids for. There should be an attachment form, limited to those you know or who provide authentication. There should be a list email for distribution lists. Then there should be communication email that is only allowed after a person has been cleared through an invitation or a 'request for communication' email. Right now it is all just one big mess that covers too many kinds of communication. This is in part why I would suggest the structure of email in the US should be redefined and upgraded as I will describe further.

I actually have a different proposal and a different orientation that I think should be considered and I have to explain it before answering the questions. I propose that a law should be passed requiring some sort of virus detection software to be installed with every email sending program or at least making an agreement with the big companies that all their software that does email will come equipped with virus scanning software. I would also propose that a national standard for virus scanning software in email to be set where the client software stamps every single email that passes through it with a digital stamp that verifies that it passed from a legitimate client sending real mail from a real person. Batch files through open relays would not have these stamps. The stamp would have to include some system information to insure where the email was coming from but nothing that would invade privacy. Most simply, originating IP and domain would be good enough (something would have to be done about NAT). Emails without an initiation stamp would just go strait to spam. You could actually, if you got companies to agree, make this integrated into mail clients and webmail based products. It would be a standard to be met to get on the new communication network.

The fact is ninety-nine percent of email you actually read you expect. If the way to stop that is by requiring an invitation email or 'request' email, spam is gone. You change the format to require that a request or invitation is so small that it lowers network traffic and also requires the digital stamp to start conversation. If not there, the email is logged to a server as spam and disappears. If a spammer can no longer get to the victim, the point of sending the spam goes away and the problem will go away as well.

The important understanding here is that every email is basically treated as spam unless the client, the sender gives something up to honestly say who they are and where the email came from. Everything

that comes batched, spoofed, or whatever without a valid stamp goes straight to spam and if someone is dumb enough to spam through a program that is stamping origin, that goes straight to the FTC and the person is nailed.
The only loophole in this is viruses that turn computers into drones. However, none of the proposed technologies do this. However, if you are providing a stamping software that digitally Ids everything that leaves it, you automatically have a way to kill the spread before it stops. Emails coming from an unstamped environment, a spammer trying to spam would go straight to spam and never even hit the receiver. System wide updates would also have to happen for those who have strictly webmail based systems like MSN, hotmail, etc, but they could provide the same sort of digital stamping, much like Yahoo's DomainKeys through a global virus solution much like Brightmail's email protection software. That software in itself would also be called on to stamp the emails when they left through webmail insuring they were real and authenticate that it came from the protected domain.
Webmail is not so much an issue. It is very hard to successfully attribute spam to a person emailing one individual after another using current technologies. The issue is people being able to email ten thousand people at once through drones or what have you.
I do believe that the most important answer to this entire problem is email has to change and evolve. I would consider this being a push to SecMail where every email sent is required to pass a sender security check, and then pass onto the network and to a recipient that would check for honest origins. Those who chose not to upgrade can stay as just regular email and be susceptible to spam. However, businesses, ISPs, and other organizations will move up to SecMail just because it provides authenticity. In this new environment I would also propose that attachments are handled differently. Specifically a restriction over what can be sent. There is no need for many types of files to be sent. DOC files can contain macros but if it is originated from another person and can be traced, you can solve the problem before it becomes an epidemic.
The only real problem with any solution is that viruses will always be able to attack through the operating system and break computers and turn them into drones. However, if they are IDed and can be tracked, you can at least head off the problem right there. The systems can then be patched and fixed. My only issue I have now is with server authentication. It should be required to be on the SecMail network. Otherwise, if people can still spoof, you get rid of the point of stamping; though you can still trace the stamp. However, if you also change emails structure to require invitations or requests, the email is killed anyway.
Yahoo has some very good ideas and if you actually made every email recipient carry a certificate from a CA as well as the domain, you could solve a lot of issues... at least until someone steals the encryption keys or computing power breaks the codes. I also think it creates too much bureaucracy. Mandating virus scanning email software boosts that industry but it should be a no brainer anyway. Plus, if you then mandate who can be a virus scanning software creator by requiring the digital stamp, you can track people.
My suggestion would be to pull together the best minds and have them sit down in a room and solve the problem. The best people from Microsoft, Yahoo, hackers, reformed spammers, whatever. We need Rand part 2 or another group of people like we had creating Arpanet. The people involved now are too busy making money to give a totally impartial judgment call. I personally have nothing to gain as I am just a to-be graduate student who has been studying this problem for ever. I would like to be involved in finding a solution but right now I can't even get the players to talk to me because all of my solutions

might cost them money or profit margins. I have many more ideas and frankly if you had the room full of very smart people that were not allowed to leave without a solution, you might get somewhere. I am very afraid the FCC commission will just be full of people pushing their ideas that could make them money. If I would back anyone now it would be Yahoo, but even their method has flaws.
The solution needs to be a cross-development solution and that might mean creating a team to find a solution and getting them away from their company for a while… unless you are like me and your loyalty is simply to fix the problem. I like puzzles and I actually planned on making this my graduate thesis but as this is happening now, I figured I would weigh in on the issue. Once again, this all boils down to we usually know what is coming, except for something like this email address. However, I could have very easily sent a request for communication first that could be answered by a BOT as this is an open address looking for replies. Same is true for email addresses posted on sites. However, since many of those also are personal addresses, the first email, in the form of a request for communication could be sent with the email only to have the real communication pass through if a person accepts the request. (You can send a request and an email at the same time)
It is all about structure and interaction. If we are able to understand the individual side to the email problem and solve it we will get a solution. If we are forced to always just look at the technology, we are dead in the water from the start.

1. Whether any of the proposed authentication standards (either alone or in conjunction with other existing technologies) would result in a significant decrease in the amount of spam received by consumers.
I personally would have to back Yahoo's DomainKeys but I also like my proposal above. I don't know if it would kill all spam though because you will still have international domains and hijacking servers in domains to propagate spam. You have to tag email to an individual to make it work and that is why I like my methodology.
2. Whether any of the proposed authentication standards would require modification of the current Internet protocols and whether any such modification would be technologically and practically feasible.
You might have to modify SMTP to only allow stamped or keyed emails to pass-through. However, that is very feasible. This is not the days of Arpanet anymore and it might not be necessary to have all the open pass-throughs anymore. It is already being done so it would not be a problem to fix. If anything, you would simply expand on the current protocols and use the encryption protocols or new protocols to create a more secure network form communication traffic.
3. Whether any of the proposed authentication standards would function with the software and hardware currently used by senders and recipients of email and operators of sending and receiving email servers. If not, what additional software or hardware would the sender and recipient need, how much it would cost, whether it would be required or optional, and where it would be obtained.
My method would require a combined upgrade of servers and end users depending on how far you took my solution. DomainKeys would just be server level. I still think the easiest way is by upgrading the whole system and changing the way we create email communication, hence my way. A global upgrade user side will be needed regardless if any attempt is going to be made to attaché a sender to emails being sent. Otherwise it will be left up the servers. Once you have hit the first relay, you are already in problem city.
4. How operators of receiving email servers are likely to handle unauthenticated messages.
Well, they will go away. So long as we keep an open method for users to handle the unauthenticated, spam will exist. We have to give

people a way to upgrade and a way to become digital in a way. If people refuse to do so, it goes away. Or you could put it is a spam folder, unauthenticated folder, delete attachments, give users the ability to reply back, but then you have defeated the purpose of standardization. If they can still do it, standardization has done nothing.

5. Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.

No matter what method is used, the next wave of viruses is going to be disabling these services so that an 'authentic' sender gets their authenticator turned off. So there has to be ways to prevent this or have the recipient recognize this. I still this SenderID will create many false results just because SPF does not work. I don't trust it and I don't know many people who do. DomainKeys is more able but still there will be issues. I still say, restructure email correctly and their will not be false hits because there is structure. If you go out of the structure, the fault is your own, not the software's problem.

6. Whether the authentication standards are mutually exclusive or interoperable. Whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server A is using standard X, will it accept email easily from Mail Server B that is using standard Y?

I would suggest a new global standard people can build off of and make more secure for some environments. That would mean allowing current cryptography and other standards to stay in place and work. It would be best to create a standard for the US and see if other countries will see the success and copy. Otherwise, if you have multiple standards, there are going to be issues with framework, authentication, and acceptability. This will mean more false hits. This is why I would suggest SecMail. It's a baseline standard to build off of where you create your secure environment with standards. People can also define their own standards above a baseline if they want security for message length; content requirements allow and reject lists, etc. Song as there is a baseline standard, many problems will be avoided.

7. Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

I would suggest half open. But I also don't think you will be able to keep this closed. The ACLU will be all over this one and the open source community will never agree unless parts are public. I do believe that the standard for a new baseline should be made public but if there is a stamp framework, that should be kept only with those who are licensed to build the stamping software. Otherwise, people will grab it and start working to beat it. I am hard pressed to give that information away but I do believe that as far as a need-to-know basis, people need to know the new framework but they don't need to be made aware of how emails are stamped by virus scanning software or by domain-keys. Though, be ready for people to figure it out. No matter what happens, as long as the digital representation of each person is unduplicatable through a key, a stamp, a virus-scan stamp, whatever, it does not matter public or not.

8. Whether any of the proposed authentication standards are proprietary and/or patented.

Microsoft is trying to patent theirs. This is why I suggest creating a think tank to solve this. If a company makes it, they will patent it and screw the competition. If the standard is made by a group an it is a conglomeration, the standard could be given away or at least patented by a private third party. However, if it is a global

standard, monopoly issues will come into play and the standard has to be open to all.
Biggest issue right now is open source knows that the Microsoft's will go the patent route, they will give it away and badly. There has to be a middle ground. That may be a patented third party that licenses for cheap or gives away most of the technology but licenses the authentication only to people okayed for CA.
9. Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.
Microsoft's would. Mine would not. Not sure about DomainKeys.
10. How any of the proposed authentication standards would treat email forwarding services.
They would have to be modified to look for stamps, keys, or whatever the standard is. However, this will have to be done no matter what the method used is. There has to be more standards in forwarding services or at least more security anyway.
11. Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain).
Hard to spam from a mobile phone… though that is changing. However using my method, the stamp would be right at the connect point when the message hits the telco it is being sent through. These can already be tracked easily. If they are not directly connected, they still would have to send through virus scanners, or through the mail system. If that is not the case as of now, that needs to change. If you can send through anything and relay, the point of standards and methods of authentication become mute.
12. Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third party submission service when unable to connect to their own submission service).
Can't solve all the problems. The more you keep things like this open, the more holes spammers will use. For some form of security you have to give up some rights. This would be a problem to be worked out with any solution. How to handle something foreign. It would be possible to provide pass-through to be authenticated so long as the sender identifies themselves correctly in a way that can be verified by a third party.
13. Whether any of the proposed authentication standards would affect the use of mailing lists.
Unclear at the moment. Because they rely on bulk emailing methods, I think DomainKeys would not affect it but SenderID would not as well. However, this might move spammers toward highjacking lists because they can be used this way. I like how lists have moved to almost what I have proposed. They ask for verification first, and then the ability to opt out. It will now take more time to send depending on the method used except for mine because the relationship between sender and recipient is already established.
14. Whether any of the proposed authentication standards would have any implications for outsourced email services.
Only overseas. These methods will affect email on some level no matter what; that is what we are trying to do. However, if the cost is to the ISP, raising costs. If the cost is to the consumer to prove they are real, like in my framework, the ISPs will just have to upgrade to handle the new style of traffic. It's going to cost everyone money… bottom line.
15. Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

Separation needs to be created. Part of the problem is we allow too much lack of structure now. If you want to send from one account over one ISP. You get stamped by the program who sends it and that passes to the ISP who sees it is stamped. If you allow for a person to send a passthrough to the SMTP on their ISP, they must provide passwords to do so. It has to be locked down.

16. Whether any of the proposed authentication standards would have an impact on web-generated email.

I think the impact will be quite simple. Servers will have to upgrade to handle a new framework. However, spam through web-generated is not really a huge problem. When it is locked down with whatever standard, it will all just be an system wide upgrade that handles the new framework. If people then chose to spam through web-generated email, that is very easy to track and trace, and that is good enough for me. That requires logging in and that can be logged.

17. Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

I think they are all scalable. In fact, I think they are all HAVE TO BE SCALED because they will fail on initial implementation. My issue with the Keys is that as computing power goes up, the keys will have to get bigger. That is going to take computing power. It's a fight between power and brute force. I want to use something that is simple and a new baseline. There is also a lot of fighting I think that will evolve from a standard that is a fight between super powers. I am waiting from a standard from someone else that does not have a huge agenda. This is part of the reason I have always thought of a think tank redoing the standard.

18. Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

All have upgrade costs that will be passed to the consumer. It will help the large ISP because they have the money to do it. Email marketers are spammers. For those that are allowed to market because their marketing ahs been requested, their cost will be the same as all other email senders. The cost will be whatever the technologies cost. If this means to have a domain you need to purchase a DomainKey, there is your cost. If it is to get the software with integrated SenderID, that is a cost as well. This is why, go with something we all need. Stamps in virus scanners... we all need it, and it is a cost that already exists. Then the cost is development which can be subsidized by government and then the cost is just passed to users by requiring the scanners to be secure. That is worthwhile to me.

19. Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services.

Depends on where the upgrade is placed. If it is a new framework, they will have to adapt and make changes. With every methodology they are going to have to get keys, get patches to handle a new framework, or upgrade to deal with a new level of email authenticating.

20. Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

No, completely impossible. Imagine setting a day for everything to be upgraded. We could not even do that for Y2K and people were scared out of their mind. You might be able to get the US to move forward in

the private sector just because of cost. It might cut the ability of personal users of AOL or Yahoo to send to big business until they got an upgraded account or moved to a more secure email address, but that is the cost of being secure. I think my methodology would create a slide toward standardization and more like a migration. It would be hard seeing DomainKeys to just go live without issues, a lot of false positives, etc. Same would be true for SenderID.
However, if you give people the need and desire to move to the more secure, I do believe the slide to secure would be fast. I don't see how you could implement DomainKeys or SenderID without a sliding scale allowing spam for a long time till people are upgraded. That will take a LONG time. At some point you have to block those who are lagging behind. With my method, the old way still works, just everything is upgraded a secure methodology that business, government, and those who chose use. At some point you kill the old way of doing things but you give people time to move and migrate.
21. Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers.
DomainKeys would just because it is encryption. My methodology would not because it just changes the structure. Microsoft's would hurt speed because there is more being done and authentication.
22. Whether any of the proposed authentication standards would impact the ability of consumers to engage in anonymous political speech.
There are still plenty of ways to engage in political speech. You cannot at the same time keep complete anonymity in email and at the same time make people accountable for what they send. The whole point is to find a way to attach sender to email so that we stop the flood of spam. There will always be message boards, web sites, NNTP, etc, where people can post anonymously. If anything, this will encourage people to use just and good forms of political speech. All this would do is prevent a person from sending out millions of emails to random unsolicited people calling for the legalization of pot, down with big medical companies, or something else; that is spam.
23. Whether any safeguards are necessary to ensure that the adoption of an industry-wide authentication standard does not run afoul of the antitrust laws.
I would actually propose that a government distribute licenses to produce sender-stampers that each recipient can verify the authenticity of. You could also create a third party much like the CA that could do this nationally and internationally. You cannot mandate this internationally but you could make it impossible to communicate with US companies with the new standards… however, that is slightly unfair. So you do want a way to make sure other countries can upgrade as well. If the standard were email scanners that stamped on send, they could buy it as well. Might even boost sales. If the standard was a CA type organization for email senders, that would just be a standard to be met by those who wish to not be spammed.
24. Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

25. Whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft.
Everything is always vulnerable to the individual. However, digitally, yes, it should be secure.
26. Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.
In my method, if you are talking a digital stamp for servers using

webmail services, you could provide a government program to help people get the upgrade if Brightmail or another developer sells for very expensive. However, the rest of the cost is passed to the individual with the client on their machine. So in a sense, the cost goes to the person with the email account, where it should go. For most people, the cost is already their if they already have Virus protection software.

27. Whether any of the proposed authentication standards would have cross-border implications.

Open Source will always take issue to anything Microsoft produces just because it is Microsoft. Their cross-border implications come from the fact that it is Microsoft. Creating a digital stamp would be easy to do on any platform so long as you secure it. There are virus scanners on every platform, now you would just have to standardize a way to stamp it and release that information to those who can make the digital stamp and make people implement it.

28. Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.

I think I already answered this but basically, if the US community comes up with a standard, people will adapt. DomainKeys would require some sort of international standard of encryption but that already exists. No matter what the decision is, some way of allowing everyone to come on board will be necessary.

29. Description of how the Email Authentication Summit can support industry or standard-setting efforts.

I think you need people like me there to get anything done and then I think you need to pull people away to a think tank and make it work. People are going to be pushing agendas, this is politics. Without innovations form those who don't stand to make billions off of one way working, you are just going to get business solutions made by people trying to turn a profit. I really do hope there are a lot of academics there as well that can open a lot of the known holes in the proposals. Standardization is needed but it also goes against free-market. If we standardize, people will claim it pulls away innovation. However, it is needed if you want to stop spam.

30. Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.

Spam's biggest problem might not be domain level security and there is no way to insure that we can secure up every domain. It is true that we can secure those things that belong in the United States but policy would also suggest that we need to find a way to globally solve the problem. I have always felt the easiest way to do this is by mandating that all email in the US must go through a virus scanner before sending and then also coming up with a secure method of having each sender

Conclusion:

I know what I have written is quite biased because I have my own ideas about things. However, I have tested most of this and I know it works. I have worked with ISPs, hackers, and even challenged some spammers and won. I want a chance to propose something that will work and I want to help with the solution. Hope to hear back from you and good luck with a standardization… it seems like it is going to be a mess anyway. Can't get much worse than it already is.

Sincerely,
Nathan von Colditz