Comment #: 43

From: Annalee Newitz
Sent: Monday, October 04, 2004 2:49 PM
To: Clark-Coleman, Sheila
Subject: text version of email authentication summit comments from EFF

Hi Sana. Just in case the attachment I just sent doesn't work, I'm also including the comments from the Electronic Frontier Foundation below, in text form. Thanks!

Annalee
--

Email Authentication Summit – Comments

The Electronic Frontier Foundation (EFF) has long been concerned about the unintended consequences caused by anti-spam mechanisms. In their understandable zeal to stop unwanted email, service providers sometimes deploy spam prevention methods that can hinder free speech and create unnecessary burdens for small network operators. The EFF believes that what the Commission is calling "email authentication" is one such spam prevention method. It has the potential to do more harm than good.

The Commission frames the spam problem as a false choice, asserting that we must decide between maintaining "the cloak of anonymity" or controlling spam. This framing is wrong on two fronts: Removing options for anonymous communication will not stem the tide of spam for very long; and it will certainly chill speech protected by the First Amendment. What the Commission calls "email authentication" will, ultimately, undermine the usefulness of email by hobbling its ability to deliver anonymous free speech and by creating a system where spam flourishes and legitimate email may never reach its destination.

Spammers will piggy-back on authenticated servers

Sender ID and DomainKeys do not create a significant hurdle for a typical spammer. There is no reason spammers can't authenticate their servers. In fact, they are already doing so, and this makes server authentication useless as a means of identifying spam.

Researchers from email service company CipherTrust write that "a spam message is three times more likely to pass an SPF check than it is to fail it. Therefore, organizations cannot rely on such techniques alone to fight the spam epidemic, but should include e-mail authentication as part of their fraud and spam prevention arsenal." (see http://www.infoworld.com/article/04/08/31/HNspammerstudy_1.html and http://www.infoworld.com/article/04/08/31/HNspammerstudy_1.html and

It is well-known that spammers have teamed up with authors of malicious software ("malware") and system crackers, in order to take over several hosts on the Internet and use them as "zombies" to relay their messages. If email server authentication becomes widespread, and messages from un-authenticated servers are refused or rated highly likely to be spam, spammers will simply piggy-back on the authentication credentials of legitimate servers, by cracking into and zombifying them. As a result, the Internet will simply be littered with fully-authenticated zombie machines.

This will result in massive collateral damage and nullify any putative good effects of server authentication, since mail recipients will have to implement a policy of rejecting or downgrading all mail from the compromised servers.

Sender ID is a non-starter: IETF and AOL nixed it

Due to the unreasonable patent licensing terms set by Microsoft, the Internet Engineering Task Force (IETF) has shelved the proposal to standardize Sender ID, one of the primary email authentication proposals. America Online, the nation's largest ISP, also refused to implement Sender ID. Sender ID is therefore effectively dead.

Any Internet standard, including any for email server authentication, will have to be compatible with open source software licenses and cannot be burdened by intellectual property claims such as patents. According to a study done by Dan Bernstein(http://cr.yp.to/surveys/smtpsoftware6.txt), open source software accounts for the majority of Simple Mail Transfer Protocol (SMTP) servers on the Internet.

According to Yakov Shafranovich, a co-founder and software architect with SolidMatrix Technologies, Inc., and former co-chair of the Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF):"It is well known that free and open source software collectively called 'FOSS' runs majority of the Internet architecture: Linux, Apache, BIND, sendmail, OpenSSL and others have significant if not most of the market share in their respective categories. On the other hand majority of the desktop market is dominated by commercial software, a major part of which is either made or sold by Microsoft. This is even more expressed in the email market than other categories: the biggest four software packages used for email servers today are qmail, sendmail, postfix and exim, all of which are FOSS (although some dispute that regarding qmail)."
(http://www.circleid.com/article/732_0_1_0_C/

Additional burden on network and systems administrators

Small businesses with limited resources, home users and other organizations which can't afford a professional networking staff and yet still want to run email servers will face an additional hurdle to deploying email service if additional authentication becomes necessary. While SPF is reasonably easy for a professional to deploy, it's likely that many small operators will not deploy it. Messages from these operators' systems will be discarded or quarantined, even if the messages themselves are legitimate. This means that mail from large ISPs that have the resources to install SPF will be privileged over ones from smaller shops.

While SPF is relatively simple to deploy, it is also a weak means of authentication. Yahoo!'s DomainKeys is stronger but more complicated to install and manage. This reduces the likelihood that it will be deployed, and thus reduces the utility of authentication. It will also create an uneven playing field where the smaller players may find their email turned away from other mail servers on a routine basis.

The importance of anonymous and unauthenticated communications

The Commission advocates "domain-level authentication," which will tie email addresses to the domains from which they are sent. If implemented, this authentication method would burden or eliminate an important avenue for anonymous or pseudonymous communication - communications in which the sender has purposely chosen not to authenticate his or her message or to link it to an offline identity.

Such unauthenticated communications have an important place in our political and social discourse. A domain level authentication requirement forces email senders into an unacceptable position where they must choose between identifying themselves directly, as owners of domain names identified in the WHOIS database, or resting their privacy and anonymity interests with the third party ISPs who control the domains through which they send email. Those choices are unacceptable burdens because they compromise a right to anonymous free speech that has been upheld by the Supreme Court as protected by the First Amendment.

Many speakers may not want their online speech connected with offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow. For all these individuals and the organizations that support them, secure anonymity is critical.

The tradition of anonymous speech is older than United States. Founders Hamilton, Madison, and Jay wrote the Federalist Papers under the pseudonym "Publius" and "the Federal Farmer" spoke up in rebuttal. The U.S. Supreme Court has repeatedly recognized rights to speak anonymously derived from the First Amendment. See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent"); Talley v. California, 362 U.S. 60 (1960).

As the Court said in Talley, "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes." Id. at 65.

In McIntyre, the Court said, "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society." McIntyre, 514 U.S. at 357 (citation omitted).

Fears that their identity may be uncovered, and that they may be persecuted on account of their speech, may prevent minority speakers from speaking at all.

The right to anonymous speech is protected well beyond the printed page. Thus the Supreme Court struck down a law requiring proselytizers to register before going door-to-door, even where the town had supported its law with an asserted interest in preventing physical crime. See Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton, 536 U.S. 150, 166 (2002). A requirement that email senders authenticate themselves to recipients or to their ISPs would raise similar First Amendment concerns.

These long-standing rights to anonymity and privacy are critically important to contemporary modes of communication like the Internet. As the Supreme Court has recognized, the Internet offers a new and powerful democratic forum in which anyone can become a "pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." Reno v. ACLU, 521 U.S. 844, 870 (1997) Expansion of the Internet has created countless new opportunities for discourse and self-expression, ranging from the private diary to the multi-million-reader broadcast. The medium hosts tens of millions of dialogues carried out among weblogs, newsletters, mailing lists, and websites, as individuals and associations use the Internet to convey their opinions and ideas whenever they want and to whomever cares to read them.

The Court noted that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium." Id. Nor is there any basis for limiting the anonymity and privacy with which people can engage in online free speech.

Domain-level authentication burdens anonymity

We benefit from being able to speak via unsigned notes tacked to real-world bulletin boards and pamphlets left at the town hall, as well as through signed, sealed declarations. Likewise, we are well served by an email environment that lets us send anonymous, un-authenticated communications or digitally signed mail. Forcing authentication on every email sender cuts off entire categories of speech.

A domain level-authentication requirement binds the sender of email to a domain name. If the sender owns the domain name through which he sends mail, he must identify himself (and often reveal a great deal of private information) in the WHOIS records for that domain.

The alternative of sending email through a third-party domain, such as that of an ISP or webmail provider, is not satisfactory. In that case, only the provider would likely be authenticated, but the sender will often be asked to identify herself to that provider (and perhaps to authenticate to the provider before sending mail). Then she must rely on that provider's privacy and security practices to protect her anonymity. Someone seeking to use a stable pseudonym should not be left to the changing business practices of a third-party provider. The fact that many individuals must rely upon intermediaries to speak online should not mean that online speech is automatically less free than its offline counterparts.

The First Amendment burden imposed by authentication rises dramatically if Congress enacts the proposed Fraudulent Online Identity Sanctions Act (HR 3754), which imposes civil and criminal penalty enhancements for the use of false information in the registration of a domain name. Unfortunately, so long as domain name registrars and ICANN require the collection and publication of personally identifying information (name, telephone number, address, and email address), using false information is the only way to preserve privacy or anonymity in this component of online speech. See also EFF's comments to the ICANN WHOIS Task Forces <http://www.eff.org/Infrastructure/DNS_control/icann_whois.php>.

SPF breaks email forwarding

For many users, the ability to "spoof" the from address in emails is a feature, not a bug. Email forwarding service (in which an address such as name@company-a.com is not a "real" mailbox, and mail sent to it is forwarded to another address, such as name@company-b.com) depends on people's ability to send and receive emails at domains to which their names are not tied. This is a simple convenience that many people rely on when, for example, they travel and must send and receive work emails from a webmail account.

SPF, however, is known to impede forwarding. This would seriously undermine the conveniences of email to which many people have grown accustomed. (http://spf.pobox.com/faq.html#forwarding)

There is a workaround for this problem, which requires additional software implementation in the mail server. This is another potential barrier to adoption, especially for smaller ISPs and individuals.

Consequences for those who don't deploy authentication: the uneven playing field

Both the SPF and DomainKeys websites advocate the use of authentication as a means of evaluating whether email should be rejected before the recipient gets a chance to evaluate the message. Both sites suggest that, over time, service providers should implement policies in which un-authenticated email is discarded and authenticated email is sent to its intended recipient.

The SPF website states that "SPF fights email address forgery and makes it easier to identify spams, worms, and viruses. Domain owners identify sending mail servers in DNS. SMTP receivers verify the envelope sender address against this information, and can distinguish legitimate mail from spam before any message data is transmitted." (http://spf.pobox.com/)

And the DomainKeys site claims that "Spammers don't want to be traced, so they will be forced to [use] only spam companies that aren't using verification solutions." (http://antispam.yahoo.com/domainkeys#a1)

The implication is clearly that un-authenticated mail will, in the future, be treated like spam. This creates the uneven playing field effect, where legitimate email sent from service providers or individuals who don't have the resources to implement email authentication is discarded or downgraded. Meanwhile, senders who use authenticated mail servers will have no trouble getting their email to recipients, even if that mail is unwanted or could be classified as spam.

Another disturbing implication here is that control over email will be taken away from users and placed entirely in the hands of their email service providers. Users who receive email through a third-party service – and this is the vast majority of email users – may wish to receive un-authenticated email but will be unable to do so. Because the emails will be discarded before the user herself is able to evaluate it, she will never know which emails she has missed.

Conclusion

Stopping spam is, understandably, a high priority for email service providers and consumers. Unwanted commercial email is at best a nuisance, and at worst makes it nearly impossible for people to weed through their inboxes to find legitimate correspondence.

But in our haste to rid the Internet of spam, we should not sacrifice one of this nation's most dearly-held rights: that of free, anonymous speech. This is the sort of expression that allowed three rebels to publish the Federalist Papers without sacrificing their lives; it is what protects the identities of whistleblowers, critics, and children.

In addition, email authentication systems such as DomainKeys and Sender ID threaten to turn the currently democratic Internet into a class-based society where some speakers' messages are prioritized over others.

The EFF thanks the Commission for allowing us to submit our comments, and hopes that it will decide in favor of protecting both the democratic nature of email and the right of speakers to express themselves anonymously.

References

Legal references cited in the text.

Background on email server authentication:
http://www.circleid.com/article/730_0_1_0_C/

DomainKeys: http://antispam.yahoo.com/domainkeys

SPF: http://spf.pobox.com

/ * * * * * *
* Annalee Newitz
* Media Coordinator/Policy Analyst
* Electronic Frontier Foundation

* www.eff.org
* * * * * * /