

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.yip.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

