

**From:** jadeters  
**Sent:** Tuesday, September 28, 2004 5:08 PM  
**To:** Authentication Summit  
**Subject:** Comments on E-mail authentication

Dear Commissioners,

I have a few comments regarding the proposed solutions.

First, let me state that I am a computer professional, and have been for over 20 years. I have some expertise in cryptography and computer protocols in general, having authored several (private) protocols through the course of my employment. I am also familiar with the problems of spam, and I'm aware of many of the current measures employed to fight it as well as some of the proposed solutions.

I do not believe there will be a successful technological solution to spam at this time. I think much of the spam today originates from unsecured PCs, meaning PCs attached to the internet that do not have current security patches applied. These PCs are controlled by black-hat hackers, who sell the illegitimate use of these computers on the internet. Spam operators hire the hackers to send spam. If a "secure" email authentication protocol were to be deployed then the attackers will simply continue to send spam from these compromised computers. Their spam would be fully authenticated per the standard, but in the name of the victim, not in the name of the spammer. It is naive in the extreme to believe they would be stopped regardless of the protocol employed.

Given the computer industry's exceedingly poor track record in providing secure computing environments, I do not believe that any solution can currently avoid this problem. Future promises of "secure platforms" are still what we in the industry derisively refer to as "vaporware" -- the sales brochures are little more than smoke and mirrors covering empty promises.

I think you already have the required tools, yet have not employed them. Current laws, flawed as they are, are still not being effectively enforced (if at all.) If spammers were quickly identified, relentlessly pursued, and forced to cease business, much of the spam that plagues my inbox would disappear. The spammers operate on a business model that will suffer greatly if they're constantly forced to move to find new network access. Increased, effective, quick enforcement with stiff fines, equipment confiscation and jail terms would go a lot further (and be effective quicker and more cheaply) than some new protocol. Given the number of spammers and the money involved, this enforcement could pay for itself.

Protocol-based solutions also offer another huge problem: after all the expense of developing and deploying a new protocol has been spent, what do you do when it's broken in some new, novel way, and the spam continues to roll in the inbox? You get only one try before you've used up your credibility.

Finally, I'd like to add that if you feel you "must do something" and proceed with a "secure" protocol, any technological methods proposed must be unencumbered by patents, or otherwise many email users will be disenfranchised. There must be an open source reference implementation freely available in order to provide for non-mainstream computer architectures and operating systems.

Sincerely,

John Deters  
Minnesota