Comment #: 29

From: crownoverb
Sent: Wednesday, September 29, 2004 11:59 PM
To: Authentication Summit
Subject: E-mail Authentication Summit-Comments

Three questions and simple answers, with a detailed followup.

The current specification fails to address three issues.

Q1. What incentive will companies have to participate?

Q2. How does the current specification prevent malicious use of an innocent party's subverted computer?

Q3. How does the end user protect his privacy?

A1. Companies will not participate in a timely manner if they do not stand to profit from participation. This can be addressed by allowing companies to charge a fee to customers wishing to send authenticated email. This fee can be offset by corporations who require authenticated email from customers wishing to do business with them. Such companies could offer authenticated email as a part of their own services and products marketing.

A2. In order to prevent malicious use of an innocent parties subverted computer system, a good specification must require regular interaction by a third party service capable of detecting suspicious behavior. The third party could be any company that is willing to provide the resources necessary and meet guidelines established by the standard. This type of company might be common with the option to charge a fee for the service.

A3. Individuals wishing to protect their privacy must be assured that the emails they send are authenticated only by companies they have chosen to trust with their personal information. This is possible if the company that provides Internet service is not necessarily the one that provides authentication.

A good specification would be one that:

A. Allows any party willing to meet regulatory criteria the option to provide authentication services.
B. Encourages adoption by allowing companies offering authentication the ability to charge directly or indirectly for the service they are offering.
C. Allows users of the service to choose who authenticates their email and send authenticated email from any location with any email capable service.
D. Offers businesses assurance that the authenticated email is from the specified sender and that the content is the intended content.

E. Allows companies to build any software capable of meeting the criteria established by regulatory bodies and use it to profit from the authentication of email.
F. Prevents actively using an innocent parties computer system for the purpose of sending email not actually from the innocent party.

The first and most important step to implementing an authentication protocol would be creating a standard that must be met for government approval. With a standard that can be used by any company, the possibility for rapid adoption begins to become possible. Specifying that email sent must meet a standard that does not belong to any specific company allows free market interaction. Software companies are then free to design and market software that meets the standard but are not restricted to any particular code, license or language.

The protocol must implement a unique sender identification standard. Email sent must be registered and that registration must be verifiable. Note that identifying the sender does not mean that the senders private information is disclosed. The authenticating party has only to provide means to report a sender sending unsolicited bulk email. The protocol must provide a means, however of uniquely identifying a sender so that a single sender cannot circumvent the system by changing authentication services. This can be done by using hashes to identify a senders personal information if the information must provided in a standardized format that cannot be easily forged or changed.

Some suggestions:
Establish a protocol that identifies a sender by physical address or unique government issued ID, such as a social security number. This information must be verifiable by companies wishing to provide authentication services. The information should then be hashed to prevent the disclosure of personal information, even in the event the sender is prevented from future authentication.

The protocol must incorporate a method of verifying the sender and uniquely identifying the received email. This means that each email must be identified but the cost of recording this information would be offset by the potential to charge for the authentication service.

The consumer must be able to choose who authenticates their email. This allows for protection of privacy and prevents any service provider from monopolizing their customer base. Consumers must not fear that their service provider will limit their service based on their refusal to trust that service provider with personal information they deem private.

Businesses must be able to authenticate senders and message content. Signature services already allow this but a government standard encourages them to feel confident they can use a system without loss of support for the protocol.

Each sender should be protected from having their computer subverted by having all email be authenticated and feedback instantly available. In the event that a senders computer is compromised, individual email feedback would allow an automated system to quickly respond to potential abuse and stop authenticating for an individual sender. This allows a sender an opportunity to correct the problem before they are inadvertently responsible for any large number of mailings. It also would allow a sender to confirm that all email being sent with the senders identification is actually originating from the sender.

I personally want my email to be verifiable as coming from someone who is not

responsible for sending bulk unsolicited email. I want to know that each message I receive is from someone I can trust or from someone that I cannot verify is someone that can be trusted. I want to do business by email and feel confident that the recipients of my email will not receive instructions that appear to be from me but are instead from a different party.

As a common prank, I send email to people in my department at work with a forged senders' email address and from different networks. Currently there is no way for them to automatically determine that the email is not from the person it appears to be from. (Except, of course that George Washington, President of the United States and Shakesphere, Famous Writer are probably not legitimate senders.) This type of thing is all to easily abused and abuse can be eliminated by giving companies incentive and freedom to use a common standard of authentication.

I applaud you for your part in making email useful to business and safer for the common man.

Sincerely:
Boyce Michael Crownover