Comment #: 6

From: Steven Armstrong
Sent: Monday, September 27, 2004 2:45 PM
To: Authentication Summit
Subject: E-mail authentication summit - considerations

E-mail authentication is a global problem. Any E-mail Authentication solution considered by the summit should be acceptable to the global internet community and be easy to adopt globally, and on all systems using or handling e-mail. It might best be handled with an RFC (Request For Comments) approach, leading to a standard defined by internet protocol experts, and then give all software authors free latitude to implement it. Establishing a global e-mail standards body may be goodstarting point, run like the W3C for the browser/web server protocols. Any protocol adopted should include a verification suite and certification process to ensure all candidate software meets the standards.

It is absolutely critical that all software vendors and authors set aside commercial interests on this matter and solve the problem cooperatively, all together. Human rights to privacy and security should supported by any authentication mechanism adopted, and there may be various national laws that impact authenticiation considerations. An international standard needs to be adopted on a rapidly revisable basis.

It may be desirable to implement staged or phased authentication levels, allowing e-mail software to be implemented and upgraded as levels are agreed upon, and still allow older approved levels to be still processed at the old level. This is important since the job of authentication will evolve as global sophistication increases.

There is an important opportunity to separate the problem in two solution sets. Software handling bulk E-mail exchanged server to server, ISP to ISP, exchanged across national boundaries, could be handled on separate tracks from middleware and client e-mail software.

Relying upon any single vendor or a national mandated approach will fail. The degree of global acceptance and adoption required to eliminate the 'spam' and viral infection problems is 99.99999%. No solution that only works on one type of operating system/platform version will adequately solve the problem. Solutions should easily work on all types of client and server computers running e-mail client and server software: Unix, Microsoft Windows, MacIntosh, Linux, PDAs, web-enabled phones, etc. The optimal solutions would likely come from the Free and Open Software community since they already write the software powering 70% of internet servers.

Unauthenticated E-mail is currently available around the world. Any email authentication technique deployed should be made available to the entire world, free (as in lawful) to use, unencumbered by IP issues:

free of patent claims, in order to facilitate widespread and rapid adoption, and prevent post-adoption lawsuits for royalties or license fees.

Any protocol solution adopted needs to be allow for transition time, time for conversion, and not break the existing e-mail traffic handling on which business and private citizens have come to depend. The effort needed by large organizations to roll out an orderly upgrade can require substantial expense, testing, and deployment time. This is where promoting many free solutions meeting the same protocol standards can be very desirable. Some may be far easier to implement in large scale enviroments. Some may be easier for small groups or by home users. A transition time of up to two or three years may be needed in order to provide adequate upgrade and transition time. Early adopters should be able to interoperate with late ones throughout the transition time. E-mail authentication protocols need to be transparent across nationalities while allowing for national differences in approaches employed.

If copyrights are to be held, it needs to come with a license to freely distribute, so preference for a copyright/license like the GPL license, LGPL or BSD license should be given. No single vendor should have ownership of the adopted protocol on client, middleware or server sides of the software. Programmers around the world should be free to implement the defined standards, provided authorization and identification standards are met and certification passed. Using a defined protocol that can be amended and easily updated as technology advances must be built into the process. Vendors providing insecure and faulty software need to be held accountable and all new releases must be certified.

A decertification process could be employed which allows vendor, client and server users to be immediately notified when their software is found insecure or faulty. Vendors should be given an opportunity to provide a patch within 3 days or have a mechanism to withdraw their software previously designated as certified, or to drop in level of authentication provided. Recertification of vendor software should be allowed when problems require a long term rewrite solution.

The solution isn't just new software and certification. With millions of PC's already crippled by viruses, spyware and working as e-mail zombies, possibly under foreign control, no single vendor can credibly claim to be able to solve the trusted computing need alone. Any solution offered must have rapid mass global dissemination and may require distribution via all commonly used methods: CDROM, secure download via FTP sites, HTTP sites, P2P, floppy disks, USB pen drives, etc. and always should be offered at cost of media or free, for widest adoption. Provision needs to be made to keep distributions free from compromise and keep the executable software secure. Greater efforts are urgently needed come up with free and easy ways to detect and remove the current crop of PC infesting software that is at already work on a global scale. No authentication scheme is going to be reliable when many millions of PCs are already infected to the core, and available to remote manipulation and exploitation.

Steven Armstrong

WI