Introduction to DDX

DDX: An initiative to promote better email service among the research and higher-education community and partners
RL "Bob" Morgan, University of Washington and Internet2

The ubiquity and importance of the Internet have created new requirements for many Internet protocols regarding security. Users of protocols supporting the domain name system, email, routing, instant messaging, telephony, the web, and more are faced with the fact that Internet participants have a wide variety of interests, some of them actively malicious or criminal. Security requirements have been developed and capabilities have been added to many widely-used protocols, but in many cases the new security features are not being deployed, leaving security problems to be solved by workarounds or not solved at all. The reasons for non-deployment are varied and hard to assess, but often have to do with the network effect, or its absence: there's little utility in deploying a particular security protocol until everyone else does too, so no one makes the initial effort. The Internet Society (via its Trust and Identity Initiative), the Internet2 Middleware Initiative, and the InCommon Federationare interested in promoting the adoption of standard technical methods and policy regimes that enable a safer and more trustworthy Internet, and are partners in efforts to lower deployment barriers for promising Internet security technologies.

Email is one of the most widely-used Internet technologies. Unfortunately, email abuse, in the form of spam, phishing, and other attacks, is equally widespread, and threatens to render email useless. Not only is email abuse a problem for individuals dealing with it, but the volume of bad messages and the methods email administrators must use to deal with them cause delays and delivery failures for legitimate messages. Many originally-useful email features, such as bounce replies when a message is misaddressed, must be turned off due to abuse. Making progress against email abuse is a vast, difficult, and multi-faceted effort. A recently-developed IETF technology, DKIM, shows promise as a positive step organizations can take against abuse.

DomainKeys Identified Mail (DKIM), specified in RFC 4871, is a product of the IETF DKIM Working Group. DKIM is an email security framework whose "ultimate goal ... is to permit a signing domain to assert responsibility for a message, thus protecting message signer identity and the integrity of the messages they convey." After verification, "an authenticated email creates a predictable identifier by which other decisions can reliably be managed, such as trust and reputation." The reputation and observed or stated practices of the signer can then serve as valuable input into further message processing, providing a positive basis for disposition in ways that heuristics on unauthenticated elements cannot. The DKIM.org advocacy site provides much more information.

For the general-purpose Internet, with millions of organizations sending email, sender reputation is very difficult to manage. This can also be the case with large consumer email services, which serve a wide variety of interests. A natural community of trust such as existing higher-education identity federations can play an essential role as a solid source of reputation. Federations, operating in the web access scenario, provide assurance of institutional involvement and accountability and permit participating entities to publish their practices for others to see. These features are exactly what is needed to build upon DKIM signed email to make real improvements in email reliability.

DKIM deployment is not "a solution to the spam problem" but may be one of many tools useful in reducing the negative effects of email abuse. The DKIM RFC was published in May 2007. DKIM builds on the older pre-standard DomainKeys specification which has been in use since about 2005. Some large email providers are promoting the use of DomainKeys and DKIM today. However, deployments are still very few, especially in the higher-education community which historically has been a leader in socializing new Internet technology.

We propose an activity to eatablish some trial deployments of DKIM and associated technologies at R&HE institutions and their partners to assess the utility of the technology and create materials to support further use. Interested participants include R&HE sites around the world, and potentially other organizations such as government agencies and commercial email operators.