DOI:10.1145/3014064

Vinton G. Cerf

When Email Isn't Private

The title of this column might just have well be “Is email ever private?” In the first place, email is usually sent to someone other than yourself, so its privacy is dependent on the path it took

from your desktop, laptop, tablet, or mobile to your email service provider, the service provider's security, the path to the destination email provider, and the path taken to reach the intended recipient. There are more paths for exposure when there are multiple recipients served by yet additional email providers. Some systems, such as Google's Gmail, try to keep messages encrypted while in transit from the user's originating device to the Google cloud server(s) and encrypted while stored in the Google cloud. But the path to the destination mail relay may not be protected unless the source and destination relay agents have an agreed cryptographic protocol for transport. Moreover, the recipient of the email may not have or use an encrypted channel to pick up the email from the destination relay agent. This means that the conscientious sender of email has little or no control over the practices of the recipient.

The originator and the recipient of an email message may use weak methods to secure access to their email services. The email service provider may only support simple user name and password access control. Many of the break-ins into email services are a consequence of password guessing, dictionary attacks against one-way hashed password lists, “lost my password” processing in which the answers to secret questions may be found with some searching of the World Wide Web, and exposure of passwords in unencrypted password files or on Post-Its™ attached to laptops.

Efforts to allow users to encrypt their email on an end-to-end basis have generally not fared well in part owing to the awkwardness of maintaining lists of cryptovari-ables (or certificates) in the first place, dealing with lost or compromised certificates, and dealing with multiparty recipients of encrypted email. One of the most popular technologies, PGP,^a has been in use for many years, but has seen deployment largely in the technical community.

By the time you read this column, the U.S. presidential election will have taken place (and, hopefully been decided). What is clear, however, is that email exposure has been in the recent news on a regular basis, ranging from Hillary Clinton's email messages while in service as Secretary of State, or the email of the Democratic National Committee or of high-ranking Russian officials and their correspondents, to say nothing of intelligence agency demands for access. To the extent that we care, collectively, to secure improved privacy in our communications by electronic means, it seems essential to adopt and deploy a variety of methods to protect access to our online email accounts and to protect their contents when in transit or at rest.

As awkward as two-factor authentication may be, it is still among the most effective mechanisms for protecting access to online accounts. Over time, biometrics may prove to be a useful substitute, but I do worry that the digi-

tized representation of a fingerprint or an eye scan may be captured or fabricated in such a way as to be injected into the authentication system at the right point to penetrate an account.

It seems clear that we need standards and agreements to protect email while in transit between mail transfer agents and between users and transfer agents. Encryption at rest and end-to-end encryption are also very useful practices. But there are other vulnerabilities such as phishing attacks at the application level that cause users to ingest malware. Source email identifiers (for example, “From” field) are not reliable and can be easily spoofed. Among the popular mechanisms for validating email sources is Domain Keys Identified Mail (DKIM)^b that allows a source or intermediary relay to validate its identity in the sequence from origin to destination email server. Composing these various mechanisms improves email security but they have to be widely implemented and used by all users and providers of the service. Anything less leaves traps in the system into which users (or their email at any rate) may fall.

Email is such a useful service, it is difficult to imagine abandoning it although there is a growing attachment to other mechanisms including mobile texting and messaging built into social network services. Even though some of them promise that messages evaporate after a time, reports have been made that they can be captured, saved, and re-injected into the Internet via other communication channels. Those of us who are in the computer science profession owe ourselves and the general public a much better experience and that's one of many challenges for this online 21st century. **C**

^b <http://www.dkim.org/>

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google. He served as ACM president from 2012–2014.

Copyright held by author.

^a “Pretty Good Privacy,” <http://openpgp.org/>