MIT
Technology
Review

Why E-mail Can’t Be Completely Private

The closure of two “ultra-private” e-mail services shows just how weak the system really is.

By David Talbot on August 14, 2013

When Lavabit—an e-mail service used by National Security Agency leaker Edward Snowden —suspended service last week amid hints that it had received a government demand for information, a competing service called Silent Circle made a draconian decision: to obliterate all of its customers’ stored e-mail.

The episode pointed out two fundamental weaknesses in e-mail. First, even if an e-mail service encrypts messages for secrecy, as Lavabit and Silent Circle did, the e-mail headers and routing protocols reveal who the senders and receivers are, and that information can be valuable in its own right. And second, the passcodes used as keys to decrypt messages can be requested by the government (if held by the e-mail company) or simply stolen by sophisticated malware.

When e-mail was created 40 years ago, security or anonymity wasn’t part of the design. The routing and labeling protocols plainly state what computer sent it or forwarded it, what computer received it, and what time all this happened. “There are far too many leaks of information and metadata intrinsically in the e-mail protocols themselves,” says Mike Janke, CEO of Silent Circle, whose customers include people in companies and government agencies with secrets to protect. “It doesn’t matter what you try to do with e-mail, there are these inherent weaknesses. So we got rid of Silent Mail [the company’s e-mail service]. We deleted all of it, burned it, and threw it in the ocean with locks and chains on it. People lost all their e-mail, but the response went from ‘Why would you do this?’ to ‘Thanks for doing this.’ “

Lavabit and Silent Circle and some other providers have offered a straightforward proposition: they will keep your e-mail encrypted at all times, except when you are reading and writing it on your own computer. This is in contrast to services like Gmail, which encrypts e-mail only for the trip over the network but stores the messages “in the clear” in its servers and mines that data to serve you ads.

Lavabit’s founder, Ladar Levinson, says he suspended operations rather than be “complicit in crimes against the American people.” Levinson could not be reached for comment but told the *New York Times* that he was under a gag order, implying that he received a National Security Letter, in which the FBI or NSA demands information for an investigation relevant to national security and requires the recipient to not reveal even having received the letter. In contrast to Silent Circle, the Lavabit data has not been deleted, he says.

Janke says that news triggered an emergency conversation with Phil Zimmermann, a Silent Circle founder who in 1991 created the e-mail encryption protocol known as PGP for "pretty good privacy" (see "An App Keeps Spies Away from Your iPhone"). "Once we saw what happened with Lavabit, we realized it wasn't days, it was hours that we had to make a decision," Janke says. But he adds that he never did receive a request.

The problem – besides the metadata that accompanies all e-mail – was that 98 percent of Silent Mail customers opted to let Silent Circle hold the encryption keys, which made using the service much easier. When users manage their own keys, they have to log into a special system to exchange cryptographic keys with each person they want to e-mail with. By possessing the keys to manage this process, the company could decrypt the messages if forced to. "If we got a legitimate request, we could in fact turn it over," Janke says (see "NSA Chief Says U.S. Phone and Web Surveillance Sets Standard for Other Countries").

Silent Circle remains in business, because fewer than 5 percent of its customers were using the now-deleted mail service. Most of them use other Silent Circle services that encrypt phone, text, and video content. This allows users to, for example, send an encrypted file via text message and even attach a time limit so that it will be deleted from both the sending and receiving devices after some period.

Yet these services also can be undermined by malware that can steal encryption keys stored on computers or grab data that has been decrypted by the user. "It is very difficult to be malware-protected," says Radu Sion, a computer scientist and security expert at Stony Brook University. "A highly determined adversary – I don't want to say the government here – will have access to any machine in the world."

Existing e-mail services could become a little more private by encrypting header information. The techniques are well understood, but there is limited demand for them, Sion says. "The public is not asking for it since people don't care about privacy, really," he says. "And the cloud e-mail providers make lots of money by mining your messages."

Meanwhile, Silent Circle is working on replacing its defunct e-mail service with a system that doesn't rely on traditional e-mail protocols and keeps no messages or metadata within the company's grasp. It is based on a protocol often used for instant messages and other applications. Janke says the goal is for this to not be e-mail, but "for all intents and purposes it looks, feels, and acts like e-mail."

Tagged: Computing, Communications, Web, security, privacy, e-mail, National Security Agency

Reprints and Permissions | Send feedback to the editor