Is universal end-to-end encrypted email possible (or even desirable)?

End-to-end email encryption is getting more attention as security and compliance concerns mount, but practical use cases are rapidly being eaten away by other technologies.

 By Maria Korolov

Contributing Writer, CSO | 29 September 2017 05:45 PT

People expect their email to be private between them and the recipient, but in reality, the contents of your email are exposed during transmission. Full end-to-end encryption would mean that only the receiver of the email can decrypt their messages, but sharing public keys and agreeing on a common encryption standard can be tricky for most users. Plus, if email communications are fully encrypted along the entire path, then there's no opportunity for a service in the middle, such as Gmail or Office 365, to check for spam, automatically sort emails into folders, or offer full-text searches.

Unless the platform is integrated with a company's email gateway, firewall, and data loss prevention system, end-to-end email encryption may also prevent enterprises from monitoring for suspicious traffic. "Right now, a large number of companies just don't have a solution dealing with encrypted email," says Tom Fuhrman, cyber security practice leader at Marsh Risk Consulting.

As a result, most enterprise uses of encrypted email today are either within an enterprise or for special purposes such as trips to China or Eastern Europe. When a message from an encrypted enterprise email platform is sent to external users, the recipient typically gets a link to a secure online service where they can read the message.

Usability issues are just part of the battle. Competing services have carved out particularly high-value niches that may have been served by end-to-end encrypted email, instead.

The downloadable infographic at the end of this article illustrates how an email message might be encrypted end-to-end. It also shows three other common encryption scenarios.

Non-email alternatives

One potentially useful purpose for end-to-end encrypted email is for doctors, banks, and lawyers to send sensitive documents to their customers. Sending these files through ordinary email is a security risk, but also a compliance violation in many regulated industries. Often, getting those users to sign up for an encrypted email service is a non-starter.

Instead, institutions typically used third-party file sharing solutions. One of the most popular services for documents that need signatures is DocuSign. The company claims more than 300,000 business customers, and over 200 million users in 188 countries. Recipients get an email with a link to the DocuSign website, where they authenticate themselves, and can then easily read and sign documents. DocuSign meets the legal requirements of the U.S. Esign Act, as well as similar laws in other countries, and the company claims that it's signatures have never been successfully repudiated or challenged in any court anywhere in the world.

When documents don't need legally binding signatures, there are many online document-sharing sites like Box that offer enterprise-grade security and authentication. As with DocuSign, recipients get a regular email that contains a link to the shared document or folder.

If the communications don't involve documents but simply require short, secure messages, a new crop of mobile-first messaging platforms like Whatsapp and Signal are built with end-to-end encryption right from the start.

For companies that are concerned about hackers listening in to messages in transit, most of the major email providers currently support SSL or TLS to ensure that the communications are encrypted while in transit. In addition, major services like Gmail and Office 365 also offer encryption for data at rest.

"When the actual transmission was clear text, it [end-to-end email encryption] made perfect sense," says aid Morey Haber, VP of technology BeyondTrust, Inc. "Now that most transmission is encrypted, you've eliminated a whole use case for [end-to-end] encryption."

For business users traveling abroad, or logging in from public wifi hotspots, secure VPNs are standard tools used to protect their communications.

Finally, users who just need to send a single encrypted file to someone can simply encrypt it on their desktop. On Windows, for example, they can just open the file's Properties and turn on encryption. Then they can send the file as an attachment to their friend, and tell them the password by phone or text message.

The encrypted email systems companies use

Some companies still use end-to-end email encryption for communicating sensitive information to customers or for internal communications. They either use encryption add-ons for their existing enterprise email platforms, or use new cloud-based services. Typically, the end-to-end encryption is used just for a subset of messages, often in combination with data loss prevention tools, or for particularly sensitive projects.

"I expect if you did a lot of communication with China or Eastern Europe, you'll be using ProtonMail a lot," says Rob Enderle, principal analyst at Enderle Group. "In any kind of environment were the government looks at communications, something like ProtonMail or an end-to-end scheme is going to be safer because the government can't get them to give up the keys."

In particular, it makes sense to go with a provider that doesn't have a big presence in that country, he says, because if it does, the government can lean on the provider and, in effect, hold the investment at ransom. In fact, both China and Russia have cracked down recently on VPN providers, and Apple was forced to remove VPN apps from its App Store in China this summer.

In other countries, courts may require email services providers to turn over customer data. For example, email provider Lavabit shut down its services in 2013 after the U.S. government ordered it to turn over its encryption keys to get access to Edward Snowden's email. This year, Lavabit relaunched with a new end-to-end encryption system, one in which only the customer, not the email vendor, has the keys.

The fear that an email provider can access messages is what's driving some corporate users to fully encrypted platforms, confirmed Andy Yen, founder and CEO at ProtonMail, which is headquartered in Geneva, Switzerland. ProtonMail is one of the largest end-to-end encrypted email providers. The company claims to have more than 20,000 paying customers, mostly small and medium-sized businesses, and more than 3 million users total.

It's a cloud-based service that can be accessed via a browser or a mobile app, but the actual encryption and decryption happens on the client device. That means that ProtonMail itself cannot read the emails, and won't be able to turn them over to anyone even if ordered by the courts.

Encryption is also part of GDPR compliance, the General Data Protection Regulation that goes into effect in Europe next year, and in the medical industry, it is required for HIPAA compliance. "Health care is our biggest segment on the enterprise side," Yen says.

As with other platforms, if the recipient is not a ProtonMail user, they'll get emailed a link instead, which they can use to access the secure online services. "The encryption is not automatic, and you have to exchange a password," Yen added. "Sometimes banks will send passwords in the post, or in-person, or in a separate email. We've seen all the different possibilities."

Since ProtonMail itself can't read the messages, the email platform doesn't offer all the bells and whistles of a full-featured cloud email client. For example, users can't search the body of the messages, just the subject line, sender, recipient, and time of the message.

Other enterprise platforms focus on desktop clients, which allow more flexibility. That includes Symantec Corp., which says it has "hundreds" of enterprise customers for its end-to-end email encryption product. Users can access the platform on mobile devices, via Web browser, and via an add-on for Outlook. "For people who have email encryption on their desktop clients, they can search through their emails on their own desktops," says Kathy Kriese, principal product manager at Symantec.

That's not the case for the externally-facing gateway email product, she added. “That does not really allow for people to do searching easily," she says. "They would have to look message by message. Yes, that can be challenging, but it tends to be lower-volume communications, anyway."

Another vendor that supports Outlook desktop clients is Zix Corp., which claims to have 19,000 customers and 3.3 million users. ZixMail offers full end-to-end encryption with both the recipient and sender using the same platform, or a cloud portal when the recipient is not a customer. In addition, Zix offers filters so that companies can automatically have some emails encrypted end-to-end and the rest sent normally.

"The vast majority of our business users are in the health care and finance verticals," says David Wagner, CEO at Zix. If an email contains a patient record, it would automatically go through the encrypted channel. "That provides a very important level of protection for sensitive personal information, which is our primary use case," he says.

No interoperability in sight

A number of standards exist for end-to-end email encryption, but so far, none have reached critical mass with vendors. Take Symantec. It supports both the S/MIME and PGP/MIME encryption, says Symantec's Kriese. That doesn't mean that the system easily interoperates with those of other vendors.

"It does get more challenging when you're talking about partners," she says. "You can have a one-to-one relationship. That can be done. We even provide for the global directory, for people to put their public keys into a repository so others can search for them. But getting keys back and forth is a challenge."

Different platforms use different methods for managing encryption keys, and there are other bookkeeping types of issues that need to be resolved for vendors to interoperate. "Even with the best will in the world, the standards break down, because the vendors implement them slightly differently," says Steve Wilson, VP and principal analyst at Constellation Research Inc.

"People have been talking about getting encryption into email for decades now, and it still hasn't taken off because of the compatibility issue," says Jason Hong, associate professor in the human computer interaction institute at Carnegie Mellon University. Plus, you've got the current installed base working against you. "With email, you have to convince lots of people to upgrade simultaneously," he says. "When email was invented in the 70s, a lot of the encryption techniques weren't known and the CPU powers weren't that great," he says.

Earlier this year, Google open-sourced its own approach to end-to-end email encryption, E2EMail. "By open sourcing the technology, they would make it easily accessible and hopefully create some demand and momentum around their encryption, providing an industry standard for people to adopt," says Charles King, principal analyst at Pund-IT, Inc. At least, that was the idea. "I have not seen any sign of broad adoption of Google encryption," King says.

Even Google itself isn't using it. Three years ago, the company says that it was going to use E2EMail to in a Chrome extension that would seamlessly encrypt and decrypt Gmail messages in the browser, but that hasn't materialized.

Google does encrypt email in transit, and while the emails are saved on its servers, but it needs to be able to read the mail in order to filter our spam and phishing attacks, filter and search the emails, and, of course, mine it for marketing data.

"We're never really going to have widespread end-to-end encrypted email," says Kenneth White, director of the Open Crypto Audit Project. Purely internal email encryption systems can have as many protections and as much oversight built in as the company wants. "But as soon as you're interacting with a third-party system, you just have an email address," he says. "You have to think about whether everyone on the list has the same system, and that's just a non-starter for the vast majority of organizations."

Defaulting to a link inside the email that takes external recipients to a secure website works, he says. "But then it's a web application, it's a website. It's not email. I for one, and the others in the security field, don't see that there's ever going to be any kind of [general use] encrypted email."