Lawson Kurtz, Former Senior Developer

Posted on April 26, 2016

Trust your email? Don't. At least not until you've read this.

When was the last time your boss asked you to do something important via email? How about the last time you reset a password via email? The last time you emailed your tax attorney or HR rep a tax document?

Email contains our most personal and confidential information. Our email accounts hold all the digital keys to our lives. It's therefore no surprise why so many people are shocked when they learn that Simple Mail Transfer Protocol (SMTP), the internet standard that governs email transmission, contains no security mechanisms whatsoever. Yep, you read that correctly.

Email is completely insecure by default.

The security afforded to email today is provided by a complex system of optional add-ons. But most of these add-ons aren't in place automatically. It's up to you and your company's IT team to make sure that your email is secure.

Common Insecurities

Sender Verification

When most people receive a request from their boss via email, they typically trust that it was actually sent from their boss. However SMTP has no built-in mechanism for verifying that an email was sent from the person it claims to be sent from. Whoops.

In fact, the "From" field of an email doesn't really have anything to do with who actually sent it. Anybody can send emails "From" anybody else (widely known as email spoofing). Spammers and scammers use this technique *all*

the time. So how can we prevent people from sending emails claiming to be us?

Get this: **you can't**. There is no way to definitively prevent the transmission of spoofed email, however you can take a number of steps to limit its impact. DKIM, SPF, and DMARC are pretty effective tools designed to mitigate the impact of spoofed emails.

Message Disclosure & Modification

In Transit

By default, email is sent in clear text across the internet. SMTP does not include any mechanism for hiding or protecting your messages' content from others with access to the routers and networks through which your email travels. This means that it's possible for untrusted third parties not only to read your email, but also to *change it*. (It's worth noting that even networks you trust may already be secretly compromised. These days it's safe only to assume that the network isn't safe.)

Cryptography is the only way to ensure the integrity and confidentiality of emails sent over untrusted networks (like the internet). Applying cryptographic signatures to emails via DKIM allows us to verify the integrity of a message's content (i.e. we can prove mathematically that it has not been tampered with). Encrypting the entirety of a message's contents in-transit using StartTLS, or end-to-end via the tools listed below goes a step further and ensures that nobody on the wire can access your message's content.

(Ironically, even as the FBI itself warns of an oncoming tidal wave of expensive email fraud, they continue to fight the cryptographic technologies that are the only practical means of preventing it.)

At Rest

Even if you take the steps to properly protect your email in transit, transit security alone cannot ensure that your messages will not be read or tampered with before they are sent or after they are delivered. At these times, anyone with sufficient access to the email server storing the messages could compromise your messages. (Keep in mind that this is very far from a theoretical possibility. Governments now routinely—and secretly—access emails without their owners' consent from many common email service providers.)

The only way to ensure the confidentiality of the contents of an email is to use some form of end-to-end encryption. But keep in mind, even end-to-end encryption cannot hide your email's metadata. Encryption can protect the contents of your message, but cannot provide anonymity.

Dealing With the Insecurity

Okay, let's review. So by default, you can't be sure that the person who claims to have sent you an email actually sent it, that the content of the email you received is actually what the sender originally intended to send you, or that the content of the email hasn't been read by somebody else. Yikes.

Fortunately for all of us, an ecosystem of security add-ons allows us to use email relatively safely... but only if they're put to use.

DKIM

DomainKeys Identified Mail (DKIM for short) is a mechanism for applying cryptographic signatures to messages that allow recipients to verify their authenticity. In addition to verifying that the message was sent from an approved system, DKIM also allows the recipient to know that the message was not tampered with in transit, ensuring message integrity.

Every business should sign their outgoing email with DKIM signatures. Some email service providers/mail server setups don't support DKIM signing of outgoing messages or DKIM signature validation for

incoming messages. If yours doesn't, it's time to find a new one. Seriously, it's that important.

Setting up DKIM is a provider-specific process. Consult with your email service providers about how to enable DKIM signing.

Note that it's up to your email's recipient's email service provider to perform the validation of the message's DKIM signature. If your recipient's provider doesn't perform the check, they won't be able to tell your authentic emails apart from spammers claiming to be you. Unfortunately there's nothing you can do about this (except to point them to this post and kindly suggest that they find a new email provider) .

SPF & Sender ID

The Sender Policy Framework (SPF for short) and its newer cousin Sender ID are mechanisms that help verify that a particular email was sent from an approved email server. Sender ID offers more comprehensive protection than SPF, but its use is not nearly as widespread.

Configuring SPF for your domain is easy, and does not depend on your email service provider/mail server setup. You simply add a TXT record to your sending domain's DNS recordset that defines which IP addresses are allowed to send mail on your domain's behalf. You can choose to allow other services (like MailChimp) to send on your domain's behalf by simply including their SPF records into yours.

Viget's SPF record looks like this: `v=spf1 mx include:_spf.google.com include:mail.zendesk.com ~all`

This tells recipient email servers to validate that the message came from either a server indicated in viget.com's MX recordset, an authorized server for google.com, or an authorized server for zendesk.com. The `~all` bit at the end instructs the recipient email server to soft-fail (i.e. mark as spam) mail that originated anywhere else.

Note that like with DKIM, performing SPF checks is entirely up to the recipient's email service provider. Using an email setup that does not

perform these checks, or one that mishandles failures greatly increases your susceptibility to email fraud.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC for short) is a mechanism that allows domain administrators to establish a policy around what to do with fishy emails that fail SPF or DKIM validations.

This policy is a critically important security control for businesses. If a scammer sends an email claiming to be your CEO that lacks a valid DKIM signature, your domain's DMARC policy will help dictate what happens to that email. DMARC is what allows your business to dictate that these kinds of fraudulent email shouldn't even be allowed onto your company mail server.

DMARC policies are expressed as a simple TXT DNS record. Viget's DMARC policy looks like `v=DMARC1; p=quarantine;`
`rua=mailto:re+s3lxllhpvf6@dmarc.postmarkapp.com;`
`ruf=mailto:dmarcreports@viget.com; adkim=s; fo=1;`

This policy tells recipient email service providers to quarantine mail that fails authenticity checks. Data about messages that are quarantined will be sent to the email addresses listed. It also sets DKIM signature validation into strict alignment mode.

Since a DMARC policy has the potential for greatly affecting how your company's emails are delivered, great caution should be exercised in establishing the policy. The DMARC specification allows for monitoring-only policies (mail is treated as usual, but you receive notifications for emails that would have been rejected or quarantined once the real policy was in place. You can also define what percentage of mail should have the policy applied, allowing for a gradual ramp up.

The same disclaimer included for DKIM and SPF applies here as well: it's up to the email recipient's email service provider to perform all authenticity checks and apply the DMARC policy appropriately. (Although you can and

should make sure that your own company's email service provider supports and conforms to the DMARC specification.)

StartTLS

StartTLS is an extension of SMTP that allows for encrypted communication between email servers. It's also referred to as opportunistic TLS because in most implementations it will encrypt transmission if supported by the recipient email server, falling back to transmitting without any encryption if it's not supported.

But how can you ensure that your message is encrypted in-transit? It is possible to configure your mail server to only send if TLS is supported by the recipient's email server and the transmission can be encrypted. However since not all email servers support encrypted connections (e.g. email.downjones.com), and because universal compatibility is pretty much the only reason why people use email, this is not a common practice.

If you need to be sure that your message is not entering an untrusted network unencrypted, it's wise not to rely on transit security. Instead, reach for end-to-end encryption.

End-to-End Encryption

End-to-end encryption is a method by which the only parties that can read a communication are the parties communicating. Messages are neither stored nor transferred in an unencrypted state. End-to-end encryption has become incredibly popular in messaging (e.g. iMessage, FaceTime, WhatsApp), but has yet to see popular adoption with email due to its difficulty of use.

End-to-End Chrome Extension

End-to-end encryption tools traditionally have been rather difficult to use. Google is promising to change this with its forthcoming Chrome extension, End-to-End. Due to the importance of getting a tool like this right, Google has moved understandably slow on its public release of the

extension. It hasn't been released yet, but stay tuned. (And if you're a developer, you can follow its development on GitHub.)

Other end-to-end extensions exist (example: Mailvelope), but may have questionable implementations or be difficult to use. Do your research before choosing.

GPG/PGP

Gnu Privacy Guard (GPG) is open source end-to-end encryption software based on the now-proprietary Pretty Good Privacy (PGP) software. GPG plugins exist for most major desktop email clients. The Electronic Frontier Foundation maintains the best instructions for using GPG on your Mac, Linux, or Windows computer.

Commercial products (like Symantec Desktop Email Encryption) are also available. (The discussion around merits of open-source vs closed-source security products is outside the scope of this article.)

Specialty Email Service Providers

Certain security-focused, specialty email service providers (like ProtonMail) have easier-to-use end-to-end encryption built into their product offerings. But be warned that government action has resulted in the shuttering of several of these providers already (RIP Lavabit), however modern providers now choose hosting locations specifically to prevent government interference.

In Conclusion

Email is insecure by default, but a good setup can help ensure your safety. Here are some things you can do to keep yourself (and your company) safe.

- Learn more and educate others about email security. Security is everybody's responsibility.

- When in doubt, manually verify important, odd, or urgent requests made by email with a phone call or text (but not to any number listed in the email).
- Consider alternative tools for sending important or sensitive messages. (I'd wager that your teenage kid's chat app is way more secure than your email. Oh what a world we live in.)
- When you're done with a sensitive email, delete it. A hacker (or foreign government) can't compromise that which no longer exists.
- Choose a unique password for your email account. (All of the discussed security features are irrelevant if an attacker can simply walk in the front door.)
- Use a highly reputable third-party email service provider (e.g. Google Apps) for your company email. (Unless your business has a dedicated, well-paid information security team, you're probably better off not maintaining your own internal mail servers.
- Select an email service provider or internal email IT team you trust completely. Choosing a good provider or setup is important. We recommend using Google Apps if you can.
- Don't make assumptions about your email provider's security practices. Contact them to ensure they're keeping you safe by implementing the security features mentioned above. And double check that your specific configuration uses all available security mechanisms.
- Contract with a security expert to ensure your email setup is appropriate for your business, especially if you are in a high-stakes industry. Many large scale security breaches (costing businesses millions of dollars each to repair) start via a simple email.