ITL BULLETIN

ITL BULLETIN AUGUST 2020

Security Considerations for Exchanging Files Over the Internet

Karen Scarfone[1], Matt Scholl, and Murugiah Souppaya
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

For decades, employees have exchanged files over the Internet with coworkers, business partners, and others. This is often done through email—simply attach a file to an email message and send it to the person or people who need it. Some people enclose their files in a password-protected zip file in order to protect them, then email the zip file. And some people use free services where they can share their files with others, especially files too large to send in an email message. With work-from-home suddenly becoming the new normal for so many people, there's an even greater demand for exchanging files over the Internet. You can't hand your business partner a printout of a document or a USB drive with a set of spreadsheets, and you obviously can't ask your coworker to look over your shoulder at something. Doing your job means getting people the information they need no matter where you are or they are and in a timely manner.

This Information Technology Laboratory (ITL) Bulletin provides recommendations from the National Institute of Standards and Technology (NIST) for securely exchanging files over the Internet. It also explores several of the technologies currently available for doing so to educate readers on options they have.

Security Considerations for Improving File Exchange Security

Many of the file exchange methods being used today have major security deficiencies. Some don't provide any encryption or only support weak encryption implementations that aren't Federal Information Processing Standards (FIPS) validated[2], even though files are traversing untrusted networks. Files exchanged using those methods are at greater risk of eavesdropping and man-in-the-middle attacks. Other methods involve storing files on untrusted servers controlled by third parties, who may be able to access the stored files and might retain copies of them. On these servers, even files without sensitive information can be a security concern because the files could be tampered with.

---

1 Karen Scarfone is a NIST Associate from Scarfone Cybersecurity.

2 See https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules for more information on the Cryptographic Module Validation Program (CMVP) for FIPS 140 validations.

There are file exchange methods that can provide the needed security, but these methods are often difficult for users to set up and utilize. For example, a user who wants to send a file to someone might need to install software on their computer and have the recipient install the same software too, plus they might need to exchange cryptographic keys or share a password. Now imagine having to do that every time you need to share a file with a different coworker, partner, vendor, or customer. It's only natural to look for easier solutions, and that's how many people end up using their own ad hoc file exchange methods and unknowingly put organizations' data at increased risk of compromise.

NIST proposes that organizations consider these basic actions for improving the security of their file exchanges:

- Organizations should identify their users' needs to exchange files. This includes both sending and receiving files inside the organization and with other organizations. Identifying needs should include who the senders and recipients are and what the nature of the data being exchanged is (e.g., public information, personally identifiable information, protected health information).
- Organizations should provide solutions to address the identified file exchange needs. The solutions should take into consideration both security and usability, and users should be given adequate training on the solution(s) that are appropriate for their needs. Otherwise users are likely to circumvent organization-sanctioned solutions and use whatever ad hoc means they choose. Most organizations will need more than one solution to meet their file exchange needs. Additional information on possible secure file exchange solutions is provided below.
- When using cryptography to protect the confidentiality and integrity of files and file exchanges, organizations should only use implementations of NIST-approved cryptographic algorithms that are specified in FIPS or Special Publications (SPs) and are contained in FIPS-validated cryptographic modules.
- Organizations should conduct monitoring to ensure approved solutions are being used when needed to protect file exchanges. When an inadequately protected file exchange is detected, organizations should identify the root cause, such as a lack of awareness of approved solutions, shortcomings with usability, or a new file exchange need, and address that root cause for all applicable users. Near the end of this bulletin, there is more information about possible solutions for detecting file exchanges with inadequate protection.
- Organizations should be prepared to respond if sensitive data is leaked, such as a user inadvertently emailing an unprotected file containing personally identifiable information.

Possible Solutions for Secure File Exchanges

There are many possible solutions for securely exchanging files over the Internet. The items listed below describe several of these solutions, grouped by transmission method (for example, email). They are by no means comprehensive, and many organizations might prefer using other solutions instead of or in addition to those listed below. The primary reason for listing examples of solutions is to indicate the variety of options and the need to carefully evaluate the security and usability advantages and disadvantages of any solution before adopting it.

All of these solutions should safeguard the confidentiality and integrity of files in transit from sender to recipient. If files are stored with a third party en route from sender to recipient, the solution should also safeguard the confidentiality and integrity of those stored files. Note that while many products and services use encryption for file storage or transmission, many of these products and services do not use FIPS-validated cryptographic implementations, and thus should not be relied upon for protection.

Email has been used for ad hoc file exchanges for decades because it is convenient, fast, and ubiquitous. If you need to send someone a file, just ask for their email address, attach the file to the email, and send it. In a few minutes or less, the recipient should have the file. But there's no security built into that. Here are some of the options for protecting files sent by email:

- **Compress and encrypt the file**, such as by using a zip utility. That utility can encrypt the file, with the sender assigning a password to the zipped file that the recipient must use to decrypt it. This method is only acceptable if the password is not easily guessable and the sender uses a secure method to get the password to the recipient. Also, the compressed file must be small enough to be sent as an email attachment; many servers limit emails to 20 or 25 megabytes each.
- **Use an email encryption feature built into your existing email solution.** Some email clients and servers can already encrypt emails your organization's users are sending. They typically support any recipient, whether they are part of the organization or not. The external recipient of an encrypted email can decrypt it by visiting a portal; recipient authentication may not be needed. Recipients within the same organization would typically be authenticated. So this method may be most suitable for protecting files exchanged between an organization's users, and for protecting ad hoc file exchanges with external recipients where the files do not contain highly sensitive content.
- **Use a public key encryption email standard** like Secure/Multipurpose Internet Mail Extensions (S/MIME). This requires the sender's and recipients' email clients to all support the same standard, and generally it won't work with browser-based webmail clients. Furthermore, key management can be a major challenge, especially when attempting to send email from one organization to another. It is most feasible for securely exchanging files within a single organization where all users already utilize public key encryption. Also, this option has the same email size limitations as the compressed/encrypted file option above.
- **Use a third-party email encryption service or product**. The functionality these provide varies, but generally they can automatically encrypt email attachments to enforce the organization's policies, like protecting data that is sensitive or is being sent to certain recipients. Some services can host encrypted files that are too large to send through email; instead, they email the recipient with simple instructions on how to download and decrypt the file from the vendor's server.

File sharing services encompass a variety of server environments that store files and allow them to be shared with others. These environments are usually cloud-based, which means the cloud service provider and the file sharing service provider might be able to access the stored files—so the trustworthiness of the providers should be taken into account before using such a service. Many of these services offer additional features, like online collaboration workspaces where users can also create files and have multiple users revising the same file simultaneously.

Managed file transfer (MFT) solutions are specifically designed to perform secure file exchanges. They offer a variety of features for managing, automating, monitoring, and logging file transfers throughout an organization. Security capabilities include encryption, integrity checking, authentication, and auditing. The latter can be particularly helpful in demonstrating compliance with security and privacy requirements. MFT solutions typically have a centralized repository. When someone or an automated process sends a file, it's actually sent to the repository, where it's stored until the recipient retrieves it.

Custom web and mobile applications can be developed to meet particular secure file exchange needs. Unlike all the other options mentioned above, which are general purpose, a custom web or mobile

application would be used to send or receive files for a single purpose. The files would typically be encrypted in transit using HTTPS.

Possible Solutions for Detecting Inadequately Protected File Exchanges

Organizations have many ways of detecting file exchanges that aren't properly protected. Examples of detection methods include the following:

- Data loss prevention (DLP) solutions, which can monitor networks, client devices, or particular applications for attempts to transfer files containing sensitive data
- Network intrusion detection and prevention systems, firewalls, and other network security controls that can monitor network traffic and identify the use of application protocols that can exchange files but don't adequately protect them
- The organization's email servers and any other services used for file exchanges, which should already be logging data about which files passing through them are protected and which aren't
- Cloud access security broker (CASB) solutions, which monitor cloud-based file exchanges to provide visibility into cloud applications and associated risks.

It's unlikely that using only one method will be sufficiently broad to monitor most file exchanges. For examples, users who are teleworking might be using organization-issued laptops to interact directly with external third parties, so none of their network traffic would be visible to enterprise network security controls. Monitoring on client devices only would miss file exchanges between servers. Monitoring email activity only would miss all the file exchanges happening through other means. Most organizations will need to leverage a combination of solutions in order to identify inadequately protected file exchanges so they can address their root causes and reduce the likelihood of data exposure.

Conclusion

There are many possible solutions for secure file exchanges. Organizations should utilize these solutions in order to avoid sending files over untrusted networks without adequate protection, which exposes the contents of those files to eavesdropping and manipulation. Organizations should balance security and usability when selecting solutions, and they should also ensure users are aware of the solutions and are trained on how to use them. These steps should reduce the frequency of data breaches and other unintended exposure of sensitive information.

NIST Cybersecurity and Privacy Program
Information Technology Laboratory
National Institute of Standards and Technology
itl-bulletin@nist.gov