Encryption in the Hands of End Users

Также на русском
www.isaca.org/currentissue

As part of a defense-in-depth strategy, many organizations are expanding their usage of encryption. While encryption can provide protection from unauthorized access and reduce the likelihood of data theft, it is very difficult to implement systems and processes that can provide reasonable assurance of confidentiality in real-world implementations. In recent years, many software products have begun offering built-in encryption capabilities that are more user-friendly and manageable. When it comes to purpose-built encrypted communication tools or standards-based system-to-system encryption, the level of maturity is usually quite high. But many organizations are not prepared for the risk and pitfalls of end-user-managed (user-to-user) encryption.

The Call for Encryption

Industrial espionage, nation-state hackers and organized crime are concerns for even the smallest organization. This has not, however, slowed the rate of data capture and sharing among partners, regulators and customers. Organizations now regularly share large quantities of proprietary data and employees' or customers' personally identifiable information. Heightened awareness by the board and increased regulatory pressure are leading to increased focus on and funding for data protection.[1]

Most organizations today are comfortable deploying in-transit encryption. Security teams can easily sell the need for transport layer security (TLS)-secured web applications or push for secure protocols, such as Secure File Transfer Protocol (SFTP) and Secure Shell (SSH). Unfortunately, there are many data transfer workflows outside of IT's control or that must meet externally imposed requirements. As a result, critical and high-risk data still travel through email and attachments. More and more, users are also making use of both authorized and unauthorized cloud storage and file-sharing services. Because it is impossible to identify and control all of these scenarios, many organizations respond by deploying end-user-managed encryption tools, hoping that users will be responsible enough to integrate encryption into the existing processes (e.g., an IT request to encrypt before sending an email). However, this approach essentially delegates the security responsibility to uninterested end users who are looking for the path of least resistance.[2]

Welcome to the Jungle

In theory, encryption is just a matter of applying some math on bits of data before and after sending a file or message. However, there is a vast ecosystem of encryption technologies, algorithms, configurations, tools and file formats. Complicating matters, end-user encryption tools are notoriously unfriendly from the end user's perspective.[3] Management and transfer of encryption keys and/or passwords and ensuring secure storage are daunting requirements to place on end users.

Even if the best, most seamless tools and training are implemented, there is still the issue of compatibility with partners. If one partner is on a different platform, deploying that platform requires additional investment and implementation efforts. Given that organizations have multiple partners, the overhead from purchasing and supporting multiple tools can quickly escalate. Failure to support the tools that internal users need to make their business partners happy will result in end users seeking creative solutions and workarounds.

> **"End-user encryption tools are notoriously unfriendly from the end user's perspective."**

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Eric H. Goldman, CISA, Security+
Is an information security professional with experience in financial services and manufacturing. He focuses on human factors and human-computer interaction in the realm of information security. He can be reached at *Eric.Goldman@owasp.org.*

In addition to providing the "right" tools, it is also important to block unauthorized encryption solutions. Whitelisting is part of the solution, but today's user is likely to go searching for solutions in the cloud, and users may end up at some fly-by-night web site. This is problematic because a site's usage cannot be monitored or controlled. Furthermore, the services may not be properly secured or may be outright malicious. For example, that tool may offer to encrypt uploaded files, but may, unintentionally or purposefully, retain the original unencrypted copy. The user's attempt to improve security, could, unfortunately, result in a data exposure.

Even within an approved application list, there are many tools that can provide some form of encryption as a side feature. For example, many compression tools allow a widely accepted, but woefully outdated and weak form of .zip file-extension encryption (see sidebar). Allowing or encouraging users to use such tools is ill advised. Using weak or outdated encryption provides no real security value, and employing such tools could negatively impact an organization's reputation because partners may perceive a lack of knowledge or willingness to invest in security.

Even When It Works...

While an organization may be able to deploy tools that meet its needs and are compatible with partners, it is still not in the clear. Most tools are not end-to-end solutions, which increases opportunities for human error in the process. Other tools may not be enterprise ready and may not allow enterprises to disable inappropriate encryption parameters. When an organization deploys tools, it should ensure that the security team will be able to maintain oversight and control over algorithms, key length and any other variables. For example, if Office Open XML (OOXML) files (Microsoft Office 2007+ format) are being used, it is possible to control password length, complexity and algorithms centrally through the Group Policy/Office Customization Tool.[4] Standardizing using OOXML can be done, but, unfortunately, the defaults are not secure straight out of the box. There is no guarantee that partner organizations' configurations will adequately meet an enterprise's standards, and auditing partners' environments may not be practical. Furthermore, an enterprise cannot be sure that filters or other tools will not block the files along the way, since Office macro malware is a well-known threat.

Even if the technical deployment and compatibility issues have been addressed, it is important to also consider operational processes. For example, in the case of OOXML files, the user may save an encrypted copy in a directory with the original and then accidentally attach the unsecured version (users are notoriously bad at naming files, and neither the file extension nor the icon change when an OOXML file is encrypted). Crafty users may also circumvent Group Policy by emailing the original file for use at home and using a personal copy of Office without the restrictions, which results in an undesired, unencrypted external transmission.
In most cases, for end-user-managed encryption, password-based symmetric encryption is preferred since it avoids the complexity of managing keys/certificates. However, the challenge of

The Case of the Zip File

A first attempt in many organizations to provide encryption facilities is to leverage the .zip format. Most common operating systems support opening password-protected .zip files, but this support is typically limited to an outdated and weak form of encryption. Some third-party tools can encrypt .zip files with robust encryption, but compatibility on the receiving end is no longer guaranteed. Even if both partners can use the more robust encryption configuration, there is no assurance users will choose the correct settings or set a strong password since most compression tools are single-user-focused and they lack the ability to administratively enforce which configurations are possible.

securely communicating that password still remains. It may be possible to implement a tool or service for such sharing, but, again, there is the issue of support and compatibility. As a result, users must be relied upon to securely communicate the shared password over another channel (e.g., call to provide passwords for email attachment). However, this becomes difficult to manage (which password goes with which email?), and a complex, long or random password will be hard to dictate verbally from user to user.

A key goal of encryption is to protect the file even when direct access is possible or the transfer is intercepted, so users must be educated on the risk of insufficient segregation of encrypted content and password. It is never acceptable to simply send the password in another email. Also, Short Message Service (SMS) should not be considered a separate channel since many users have email on their phones, and phone malware can just as easily access emails as SMS messages. Malware could detect encrypted attachments and then scan all emails to build a dictionary based on unique words or combination of phrases to test as likely passwords. The attack can be optimized by searching for nondictionary words or key phrases (e.g., "The password is").

Unintended Consequences

There are potential downsides to consider when deploying end-user-managed encryption. Content inspection is required to detect and prevent attacks (e.g., antivirus, spam filters) and prevent data theft (data loss prevention [DLP]). Generally, tools do not provide centralized management or monitoring, key/password escrow, or any type of pipeline into security analysis tools. If a DLP system has no way to learn the password/key, it cannot decrypt and read the file. Will the DLP tool default to block an encrypted file from leaving? On the receiving side, email filters cannot inspect an attachment for macro viruses if they cannot decrypt the file. As a result, end users now have to make more difficult decisions, of which they may not understand all of the consequences.

Encryption Is Not a Substitute for Access Control

Both encryption and system access control provide confidentiality. Two key differences are that access control enables the access rights to change over time and the authorization is separate from the data themselves. An encrypted file, in essence, embeds the authentication and authorization within itself. Without some additional system, there is no way to later revoke access once someone else has the password or key; it is not possible to take back a digital file. Further, unlike access control, there is no way to implement rate-limiting (e.g., denying requests for short periods of time) on brute-force password guessing.

Mistakenly, sometimes encryption is used in lieu of access control. In such cases, the proper solution is likely some form of digital rights management (DRM) or information rights management (IRM). With IRM, there is the possibility to add a call back to the server that can discontinue access even if the proper password is provided, enabling centrally managed access control even outside an organization's boundaries.

In addition, in the case of extra-organizational file sharing, encryption on its own does not limit reuse or further sharing because the receiver can simply decrypt and discard the encrypted file or share the decryption password. For highly confidential information, secure virtual data rooms may be appropriate.[5] In any case, encryption and DRM are not replacements for other usage and handling controls such as legal agreements (e.g., nondisclosure agreements) or visible and digital watermarking. Providing an encrypted document on its own usually does not legally bind another party to handle data in any particular way.

Another unexpected consequence of empowering users to use encryption is the risk of self-inflicted denial of service (DoS). DoS is traditionally discussed in the context of servers, but a file that cannot be decrypted is another form of denial attack—consider criminals using CryptoLocker and variants.[6] A user overzealous with security spirit may encrypt all files. That will result in a lot of passwords to remember. The user may utilize a secure password manager, but those tools also tend to lack escrow features. If that user leaves the company, no one else will have access to those encrypted documents.

There are also consequences stemming from permitting end-user-managed encryption, which may not be evident immediately. For example, how does the usage of encryption factor in with legal email retention requirements or other similar archiving processes? How will this impact content management and the ability to perform searches on data? Encryption also impacts file compression, which may be a problem for attachments, given size restrictions. Special considerations may need to be made for backup and replication procedures when there is a lot of encryption being used at the file level.

The Advantages of Centralization

Traditionally, IT departments have either attempted to find encryption features in tools already deployed, or they have deployed one or two specific end-user encryption tools common among key partners. In recent years, however, encryption gateway/proxy solutions have become a viable option. Similar to the shift from desktop clients to web applications, the encryption gateway centralizes the encryption process and allows for enhanced monitoring and control by IT. Much like any other proxy, traffic travels in-line and the encryption/decryption can be applied transparently and automated.

> **“Decision making on protocols is no longer left to the users.”**

With a centralized deployment, it becomes much easier to set up connections with other partners who deploy centralized solutions, even from different vendors. The exchange of keys and certificates can be left to specialists and transmissions can use standards-based protocols. Decision making on protocols is no longer left to the users, allowing IT departments to work together on acceptable configurations or to employ machine-to-machine negotiations to ensure that only compliant encryption settings are permitted. Even if the recipient is not on the same platform, it may be possible to intelligently onboard the user/organization, leverage an IRM platform or utilize a secure file hosting service (at least access control).

The user's workload can be reduced to clicking a button or inserting a keyword (e.g., “Encrypt”) into the subject line of an email. Organizations could also deploy a web portal or drag-and-drop tool to prepare the file and escrow the key/password. DLP or mail filters may be able to intelligently detect when encryption should be provided in case the user forgets or can redirect users when blocking the transmission.[7] For the receiver, the file can be decrypted in a centralized manner automatically or held for release by the user, thus allowing inspection and sandboxing to happen between decryption and access by the end user.

Limit to Authorized Encryption

Once a centralized or user-managed solution has been deployed, it is necessary to take steps to block unauthorized encryption and encrypted file egressing over unauthorized channels. This helps block outdated encryption algorithms and prevent malicious insiders or hackers from using encryption to exfiltrate data. This is similar to the type of inspection and blocking already common for secured web transactions.[8] DLP system rules should be configured to block any encryption that cannot be inspected and/or is traveling over an unapproved service, port or destination.

In addition, it is advisable to monitor software and processes on end-user systems to ensure that

Who Is the Data Owner?

Encryption is typically thought of as securing communication between two or more individuals, and only those people involved with the transfer. However, in a business scenario, it is more likely that two organizations, rather than the individual users, should be considered the owners. Many message-encryption protocols and stand-alone file encryption tools are fundamentally designed for personal use scenarios. However, in a corporate environment it is often necessary to have some form of key escrow or ability to view the unencrypted version of data by others outside of the transaction, such as legal or security teams (or at least their automated tools).

When one is evaluating encryption software and systems, it is important to consider how the tools will impact the organization's legitimate access to data. If the tools are enterprise ready, they will integrate with the DLP and IDS somehow, such as by communicating the plaintext, transferring the keys or coordinating with local software agents before encryption. Such systems must also securely manage all of the keys/passwords to prevent misuse and targeting by hackers, and should also include approval workflows and logging as appropriate.

Personal communications can and should still rely on robust, backdoor-free encryption technologies to prevent eavesdropping. In enterprises, the fundamental ownership issue means that users must understand and accept that communication is being secured between enterprises, not people.

no unauthorized encryption software is installed or being used. If such software is found, an investigation can determine if there is a legitimate business need and see if it is possible to convert that workflow to a different, authorized encryption tool. Because of the growing usage of the cloud, web traffic should be reviewed to block unauthorized web sites and services that users have used, or may attempt to use, to encrypt or decrypt data.

Ensure User Understanding and Awareness

Even with a transparent solution, proper education on encryption responsibilities and capabilities is crucial. Users must understand that encryption is more than password protection, and not all encryption is equal. DLP and artificial intelligence (AI) will never catch all cases where encryption is needed so it is best to train users to manually initiate encryption; this will provide users with peace of mind. Also, reinforcement and reeducation must be provided periodically.

Policy is also important for ensuring clarity. The enterprise must clearly define the approved configuration tools, procedures and consequences so that there is no ambiguity among users. For example, users should be prohibited from sending encrypted data home (e.g., no personal encrypted backups). The security policy should make it clear that management reserves the right, where permitted by law, to inspect and decrypt all communications and files for security, legal and other applicable reasons.

> “Encryption is more than password protection, and not all encryption is equal.”

Conclusion

Organizations must be aware of the challenges and risk associated with putting encryption into the hands of users. Beyond finding and configuring the right technology, enterprises must ensure processes are well defined and there is sufficient user training. A centralized solution can reduce costs and support effort, while streamlining processes and enabling better integration with DLP. In any case, encryption must be controlled and limited or it will create a security blind spot.

Endnotes

1 NYSE Governance Services and Veracode, *A 2015 Survey: Cybersecurity In The Boardroom*, 2015, *https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf*

2 Besnard, D.; B. Arief; "Computer Security Impaired by Legitimate Users," *Computers & Security*, vol. 23, iss. 3, 2004, p. 253-264

3 Whitten, A.; J. D. Tygar; "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," USENIX Security Symposium, 1999, p. 169-184, *https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/*

4 Microsoft Technet, "Group Policy and Office Customization Tool Settings in Office 2010 for OpenDocument and Office Open XML Formats," 2016, *https://technet.microsoft.com/pt-br/library/dd723552(v=office.14).aspx*

5 Pang, A.; D. Stanton; T. Nagle; "Managing Cyber-Security Risks in M&A," *Financier Worldwide*, July 2014, *www.financierworldwide.com/managing-cyber-security-risks-in-ma*

6 US Federal Bureau of Investigation, "Criminals Continue to Defraud and Extort Funds From Victims Using Cryptowall Ransomware Schemes," Internet Crime Complaint Center (IC3), 23 June 2015, *www.ic3.gov/media/2015/150623.aspx*

7 Microsoft, "Conditions and Exceptions for Transport Rules," Microsoft Developer Network, 2010, *https://msdn.microsoft.com/en-us/library/ff628740(v=exchsrvcs.149).aspx#Attachments*

8 Lyngaas, S.; "Decrypting Outbound Data: A Key to Security," *FCW*, 11 August 2015, *https://fcw.com/articles/2015/08/11/ssl-encryption.aspx*