Managing Access to Confidential Documents

Subjects: Computer Science, Information Systems

Contributor: Elham Al Qahtani , Yousra Javed , Sarah Tabassum , Lipsarani Sahoo , Mohamed Shehab

User adoption and usage of end-to-end encryption tools is an ongoing research topic. A subset of such tools allows users to encrypt confidential emails, as well as manage their access control using features such as the expiration time, disabling forwarding, persistent protection, and watermarking.

access control confidential emails email security tool

1. Introduction

Sharing of confidential information via email and text has become an ingrained aspect of day-to-day life due to the ease of access and availability of high-speed internet, computers, and smartphones. A recent survey demonstrated that 70% of emails contain sensitive information [1]. However, although standard email, by default, is not end-to-end encrypted with tools such as PGP and S/MIME, people still use it to share their personal information without any extra protections. This was shown by a recent study that analyzed 81 million sent email messages and found that only about 0.06% of them were encrypted [2]. People are more concerned about data leaks from recipients' devices rather than data during transit [3][4].

2. Virtru

Virtru is an end-to-end encryption platform that encrypts Gmail messages, attachments, and files stored on Google Drive, including Google Docs, Google Sheets, and Google Slides [5]. Virtru's simple Chrome extension keeps emails and files secure in Google Workspace, preventing Google and unauthorized parties from accessing information. Recipients can read a Virtru encrypted email without Virtru installed. Virtru uses a secure reader platform that allows users to access it right in their web browser by clicking on the Unlock Message button in their Virtru secure email. Upon verifying that they are an authorized recipient of that email or file, they can read and reply to the secure email directly from their browser.

In addition to encrypting messages and attachments, the security options of Virtru (see **Figure 1**) allow users to perform the following tasks:

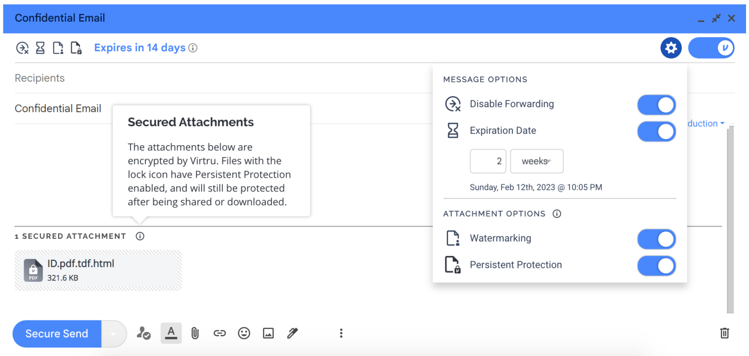
- Add persistent file protection (PFP) to the encrypted file: This feature restricts access to only authorized users, even if it is shared or downloaded. New (unauthorized) users are allowed to request access to a file, and they will be forced to authenticate in their web browser prior to seeing the secure file in Virtru's Secure Reader. If someone requests access to a file that a user owns, then the recipient will receive an email notification from Virtru. Unauthorized users will not be granted access.

- Set an expiration date for an encrypted email or file: Users can restrict access after a particular point in time. If a recipient tries to access the content after its expiration, then they will receive a prompt indicating their access has expired. Expiration can also be managed after an email has been sent.

- Disable forwarding: This ensures that the recipients can access the encrypted content but will stop any additional users from gaining access to the message. If the original recipient sends the email to a new party, then the new user will not be added as an authorized user and will not be able to unlock the message.

- Add watermarking to a secure file: Recipients will only have access to content inside the Secure Reader, and their email addresses will be watermarked across the document. This feature prevents the recipient from downloading the file and keeping a local copy.

- Revoke (or reauthorize) access: Virtru even allows the sender to revoke access to specific recipients granularly at any time. If recipient access is revoked, then users will receive a prompt indicating their access has been removed.



Secured Attachments

The attachments below are encrypted by Virtru. Files with the lock icon have Persistent Protection enabled, and will still be protected after being shared or downloaded.

1 SECURED ATTACHMENT

ID.pdf.tdf.html
321.6 KB

MESSAGE OPTIONS

Disable Forwarding

Expiration Date

2 weeks

Sunday, Feb 12th, 2023 @ 10:05 PM

ATTACHMENT OPTIONS

Watermarking

Persistent Protection

Figure 1. Virtru's email composition window along with its message security options.

Various universities and companies in the US utilize Virtru [6][7], allowing them to add an extra layer of security to their email messages. While Virtru works for a few email providers, it does not work with all web applications [8]. Furthermore, Virtru's private keys are associated with each device, and thus they cannot be used across devices. It also relies on a centralized server to verify that users own their respective email addresses and deliver private keys [9]. However, it uses a distributed architecture for unique symmetric key generation for each email [10]. By keeping content and encryption keys separate, only authorized parties are able to access unencrypted content, making it impossible for Virtru to decrypt user content [10]. In this way, data are kept private, even from Google or unauthorized parties. Although Virtru provides email transmission security, it does not protect against email accounts becoming compromised [11]. Therefore, Virtru offers secure encryption alternatives to portal-based encryption technologies. With these technologies, data can be encrypted, but this necessitates the use of separate systems by the recipient and the user [12]. This set-up may grant vendors access to their data, potentially introducing the risk of data breaches.

3. Comparison of Popular Email Security Tools

This section contrasts 6 popular email security tools, namely Private WebMail (Pwm), Tutanota, PGP (Mailvelope), ProtonMail, Gmail Confidential Mode (GCM), and Virtru. These tools can either be integrated with the major email service providers (Gmail, Outlook, Yahoo, etc.) or need a separate website or tool from where the encrypted email should be composed, sent, and received. Most of these tools provide end-to-end email encryption or other forms of access control. Virtru provides both integration with email service providers and end-to-end encryption, as well as additional forms of access control such as setting an email expiration date and time. **Table 1** summarizes this comparison.

Table 1. Comparison of popular existing email security tools.

Email Security Tool	Integration with Email Service Provider	Security Features	Threats
Private WebMail (Pwm) [13]	Yes, with Gmail via a browser extension	Automatic key management, end-to-end encryption	(1) An attacker that compromises the extension software (2) A malicious email service provider that impersonates the user or uses social engineering to obtain sensitive data
Tutanota [14]	No, needs a separate website	Key pair generation, end-to-end encryption, digital signature	(1) A malicious email service provider that provides software to access the user's data or to have their secure email account password guessed or stolen
PGP (Mailvelope) [15]	Yes, with many providers via a browser extension	Key pair generation, end-to-end encryption, digital signature	(1) An attacker who gains access to the user's email account could attempt to convince the user's contacts to encrypt messages with the attacker's public key instead of the user's true public key
ProtonMail [16]	Yes, with many providers	Key pair generation, end-to-end encryption, digital signature	(1) An attacker that compromises the software (2) A malicious email service provider that impersonates

Email Security Tool	Integration with Email Service Provider	Security Features	Threats
			the user or uses social engineering to obtain sensitive data
Gmail Confidential Mode (GCM) [17]	Yes, with Gmail	Email expiration time, revoke access, disable forwarding, recipient authentication	(1) Lack of end-to-end encryption (2) Screenshots and screen recording to save a copy of the document
Virtru [5]	Yes, with Gmail via a browser extension	Automatic key management, end-to-end encryption, email expiration time, revoke access, recipient authentication, persistent file protection, disable forwarding, watermarking	(1) An attacker that compromises the extension software (2) A malicious email service provider that impersonates the user or uses social engineering to obtain sensitive data (3) Screenshots and screen recording to save a copy of the document

3. Sharing Confidential Information

Users often need to share sensitive pieces of information, such as their social security number (SSN) and medical history, with trusted entities or possibly unknown recipients. Even though secure communication mediums are available, when privacy and security are considered minor factors, information will be shared without a formal security process [18][19]. To investigate sensitive data-sharing practices, Dell [20] commissioned a global survey of 2608 professionals handling sensitive data at companies. The survey results showed that 72% of employees were willing to share sensitive, confidential, or regulated company information without proper data security protocols in place. Also, Warford et al. [3] explored users' experiences with sending sensitive information via standard (unencrypted) email, which was the most common transmission method users used when they sent their sensitive documents, such as their financial information, health information, and information related to their children. Users could share sensitive health information on social media (Facebook), which can negatively affect users' privacy [21][22].

Recently, users have been using end-to-end encrypted messaging applications (e.g., Whatsapp or Signal) to communicate privately. However, many users believe that SMS is more secure than WhatsApp and that they are not targeted by government and special service surveillance [23]. Users' decisions are affected more by peer influence than secure messaging apps' security features [19]. Similarly, even though WhatsApp users were informed that their messages were end-to-end encrypted, the participants noticed it but failed to understand the implications correctly.

4. Adoption of Encryption Tools

Despite existing efforts toward raising user awareness about the security and privacy of their information and disseminating knowledge of how to utilize security and privacy tools, the adoption of encryption tools remains low. Taking this issue into account, Das et al. and De Luca et al. [19][24] investigated the social processes influencing people's decisions to adopt a new security tool or practice. They found that social processes played a significant role in adopting new security tools and were effective at boosting security sensitivity. Two studies evaluated the differences in motivations for (not) following computer security practices [25] and smartphone security measures [26] based on the rational decision model. They found there were differences in users' perceptions regarding the benefits, risks, and costs associated with their decisions.

In other studies [27][28], researchers explored the reasons why secure email tools are not widely used by users. Several barriers have been identified within the workplace that prevent the adoption of encrypted email [27]. As a result of technical issues, usability issues, and social considerations, the participants did not consider using them frequently. In another study [29], the researchers found that average users were more likely to adopt secure email tools (e.g., Virtru) when integrated with webmail, such as Gmail. Ruoti et al. [30] evaluated three secure email systems, with Virtru being one of them. As a result of users' interactions with Virtru, fewer mistakes were made, and its perceived usability score was higher.

5. Mental Models of Encryption

The cybersecurity research community has endorsed using secure communication methods to protect confidential information. Abu-Salma et al. [18] explored users' knowledge, experience, and perception of different communication tools. They found that many participants did not understand the fundamental concept of end-to-end encryption, which decreased their motivation to adopt secure tools. They identified several inaccurate mental models that underpinned participants' reasoning and decision making. Gaw et al. [27] conducted a study by interviewing a sample of users from an activist organization whose tasks required secrecy. The participants had different levels of technical sophistication and involvement with confidential information. They explored users' decisions about whether and when to encrypt emails and hypothesized that the organization's employees would have a strong motivation to encrypt emails. They found that the participants perceived only "paranoid people" or "people up to no good" would use encryption. Furthermore, a group of researchers [31] identified four mental models of encryption as a problem that illustrated how users perceived encryption.

Whitten and Tygar [32] found that non-adoption of secure encryption tools is due to usability issues, such as users having great difficulty using email encryption software. On the contrary, Renaud et al. [28] found that the non-adoption of secure encryption tools might not be entirely due to usability issues. Their results showed several fundamental issues, such as misaligned incentives, incomplete threat models, and insufficient understanding of encryption. They also mentioned that just expanding the availability and usability of encryption functionality will not be enough to increase the adoption of end-to-end encryption. They suggested that creating comprehensive end user mental models related to email protection could increase adoption. Krombholz et al. [33] explored users' mental models of the "HTTPS" protocol. They found that end users often mistake encryption for authentication, significantly undervalue the security advantages of HTTPS, and neglect security indicators. Recently, users began using Gmail's Confidential Mode (GCM) to share confidential emails, believing it encrypts them [34]. While GCM does not encrypt email content, it does ensure confidentiality by using built-in access controls.

References

1. How Much Sensitive Data Is Your Organization Sharing?—Virtru—virtru.com. Available online: https://www.virtru.com/blog/data-sharing-risk-calculator (accessed on 6 February 2023).
2. Stokel-Walker, C. Almost No One Encrypts Their Emails Because It Is Too Much of a Hassle. Available online: https://www.newscientist.com/article/2289747-almost-no-one-encrypts-their-emails-because-it-is-too-much-of-a-hassle/ (accessed on 6 February 2023).
3. Warford, N.; Munyendo, C.W.; Mediratta, A.; Aviv, A.J.; Mazurek, M.L. Strategies and perceived risks of sending sensitive documents. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Virtual, 11–13 August 2021; pp. 1217–1234.
4. Sjouwerman, S. 91 blog.knowbe4.com. Available online: https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email (accessed on 6 February 2023).
5. Virtru. Available online: https://www.virtru.com/data-protection-platform/email-encryption/gmail#:~:text=End%2Dto%2DEnd%20Encryption%2C%20Simplified&text=Virtru%20equips%20you%20to%20secure,Set%2 (accessed on 27 January 2023).
6. UM, T.S. Virtru: Added Security for Your U-M GMail. 2023. Available online: https://safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/virtru (accessed on 29 September 2023).
7. CRUZ, U.S. Virtru for Sharing Sensitive Data on and off Campus. 2023. Available online: https://its.ucsc.edu/virtru/ (accessed on 29 September 2023).
8. He, W.; Akhawe, D.; Jain, S.; Shi, E.; Song, D. Shadowcrypt: Encrypted web applications for everyone. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1028–1039.
9. Vaziripour, E.; O'Neill, M.; Wu, J.; Heidbrink, S.; Seamons, K.; Zappala, D. Social Authentication for Encryption. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016.
10. Virtru Encryption Key Management. Available online: https://www.virtru.com/encryption-key-management/?utm_campaign=2022_US_DataBreach_General&gclid=Cj0KCQiAw8OeBhCeARIsAGxWtUyk2j-CDf10x84XKRWd4XkaGCthgOfzZlVKe6CZiUgQzhgbOex9m7YaAiSiEALw_wcB (accessed on 27 January 2023).
11. Ferreira, L.; Anacleto, J. Usability in Solutions of Secure Email—A Tools Review. In Proceedings of the Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, 9–14 July 2017; Proceedings 5. Springer: Berlin/Heidelberg, Germany, 2017; pp. 57–73.
12. Hogan, B. Virtru Review: Easily Protect Data Wherever It's Created or Shared. Available online: https://www.softwarepundit.com/virtru-review (accessed on 29 September 2023).

13. Ruoti, S.; Andersen, J.; Hendershot, T.; Zappala, D.; Seamons, K. Private webmail 2.0: Simple and easy-to-use secure email. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology, Tokyo, Japan, 16–19 October 2016; pp. 461–472.
14. Tutanota. 2023. Available online: https://tutanota.com (accessed on 29 September 2023).
15. PGP (Mailvelope). 2023. Available online: https://mailvelope.com/en (accessed on 29 September 2023).
16. Proton Mail. 2023. Available online: https://proton.me/mail (accessed on 29 September 2023).
17. Gmail Confidential Mode. 2023. Available online: https://support.google.com/mail/answer/7674059?sjid=16859918329907772900-NA (accessed on 29 September 2023).
18. Abu-Salma, R.; Sasse, M.A.; Bonneau, J.; Danilova, A.; Naiakshina, A.; Smith, M. Obstacles to the adoption of secure communication tools. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–24 May 2017; pp. 137–153.
19. De Luca, A.; Das, S.; Ortlieb, M.; Ion, I.; Laurie, B. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016; pp. 147–157.
20. Brady, S. Survey Shows Sharing Confidential Data in the Workplace is Common. 2017. Available online: https://totalsecurityadvisor.blr.com/cybersecurity/survey-shows-sharing-confidential-data-workplace-common/ (accessed on 29 September 2023).
21. Asiri, E.; Khalifa, M.; Shabir, S.A.; Hossain, M.N.; Iqbal, U.; Househ, M. Sharing sensitive health information through social media in the Arab world. Int. J. Qual. Health Care 2017, 29, 68–74.
22. Househ, M. Sharing sensitive personal health information through Facebook: The unintended consequences. In User Centred Networked Health Care; IOS Press: Clifton, VA, USA, 2011; pp. 616–620.
23. Dechand, S.; Naiakshina, A.; Danilova, A.; Smith, M. In encryption we don’t trust: The effect of end-to-end encryption to the masses on user perception. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 401–415.
24. Das, S.; Kim, T.H.J.; Dabbish, L.A.; Hong, J.I. The effect of social influence on security sensitivity. In Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 143–157.
25. Fagan, M.; Khan, M.M.H. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In Proceedings of the Twelfth symposium on usable privacy and security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016; pp. 59–75.
26. Al Qahtani, E.; Javed, Y.; Lipford, H.; Shehab, M. Do women in conservative societies (not) follow smartphone security advice? a case study of saudi arabia and pakistan. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genova, Italy, 7–11 September 2020; pp. 150–159.
27. Gaw, S.; Felten, E.W.; Fernandez-Kelly, P. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 22–27 April 2006; pp. 591–600.
28. Renaud, K.; Volkamer, M.; Renkema-Padmos, A. Why doesn’t Jane protect her privacy? In International Symposium on Privacy Enhancing Technologies Symposium; Springer: Berlin/Heidelberg, Germany, 2014; pp. 244–262.
29. Ruoti, S.; Andersen, J.; Heidbrink, S.; O’Neill, M.; Vaziripour, E.; Wu, J.; Zappala, D.; Seamons, K. “We’re on the Same Page” A Usability Study of Secure Email Using Pairs of Novice Users. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; pp. 4298–4308.
30. Ruoti, S.; Andersen, J.; Dickinson, L.; Heidbrink, S.; Monson, T.; O’neill, M.; Reese, K.; Spendlove, B.; Vaziripour, E.; Wu, J.; et al. A usability study of four secure email tools using paired participants. ACM Trans. Priv. Secur. (TOPS) 2019, 22, 1–33.
31. Wu, J.; Zappala, D. When is a tree really a truck? exploring mental models of encryption. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 395–409.

32. Whitten, A.; Tygar, J.D. Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0. USENIX Secur. Symp. 1999, 348, 169–184.

33. Krombholz, K.; Busse, K.; Pfeffer, K.; Smith, M.; Von Zezschwitz, E. “If HTTPS Were Secure, I Wouldn’t Need 2FA”—End User and Administrator Mental Models of HTTPS. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 246–263.

34. Al Qahtani, E.; Javed, Y.; Shehab, M. User Perceptions of Gmail’s Confidential Mode. Proc. Priv. Enhanc. Technol. 2022, 2022, 187–206.

Retrieved from https://encyclopedia.pub/entry/history/show/116667