1 Le projet

Aujourd'hui, l'e-mail est indissociable de notre usage d'internet, professionnel comme récréatif : que ce soit pour créer un compte en ligne, recevoir une notification, s'abonner à une infolettre, planifier une réunion, partager un document, interagir avec les services publics, ou simplement écrire à une personne ou une organisation. L'entreprise Radicati Group [9] estime que 4.1 milliards de personnes possédaient au moins une adresse e-mail en 2021, que chaque jour plus de 319 milliards d'e-mails étaient échangés, et que cette tendance se maintiendra dans les années à venir.

Du fait de son hégémonie, l'e-mail se trouve donc au centre des questions de protection des données personnelles [23], d'espionnage industriel [3] et d'ingérence géopolitique [5]. Ces problèmes sont amplifiés par deux caractéristiques techniques : 1) une forte concentration des fournisseurs de services [16] liée à la difficulté de fournir un service hautement disponible qui passe à l'échelle et 2) le faible recourt aux techniques de cryptographies [21] qui expose les données confidentielles des utilisateurs au fournisseur de services et aux attaquants.

Afin qu'un plus grand nombre d'acteurs puisse gérer de manière autonome et souveraine leur service d'e-mail (data sovereignty), ce projet a pour but de concevoir un système de gestion de boite e-mail (Mail Delivery Agent, MDA) open source qui soit facilement opérable (haute disponibilité et passage à l'échelle) et protecteur des données (chiffrement des boites de réception), tout en restant compatible avec les protocoles et applications e-mail actuelles (via le protocole IMAP).

2 État de l'art

Dans cet état de l'art, nous passons en revue les logiciels de gestion de boite e-mail (MDA) existants, qu'ils soient industrialisés, à l'état de prototype ou en cours de spécification.

Services Gmail [6] et Outlook [20] sont les deux services de gestion de boite e-mail dominants. Les boites e-mails ne sont pas stockées chiffrées, les entreprises parentes (Google et Microsoft) ont accès aux e-mail de leurs utilisateurs. ProtonMail et Tutanota [22, 12] fournissent également un service e-mail, cette fois-ci en chiffrant la boite de réception de leurs utilisateurs. Cependant, le chiffrement des données étant une solution imparfaite (fuite de métadonnées, les mails en transit ne sont pas chiffrés, etc.), il est tout de même nécessaire de faire confiance à ces prestataires de service. La compatibilité IMAP a également souffert de bugs pouvant mener à la perte de données par le passé [17]. Qui plus est, rien n'assure de la pérennité de ces services dans le temps, à l'image de Lavabit, premier prestataire à chiffrer les e-mails qui a fermé ses portes en 2013 [1].

Logiciels sur le marché Dovecot [8], Cyrus IMAP [27], et Microsoft Exchange [24] sont les logiciels les plus utilisés pour créer un système d'e-mail souverain mais ne sont pas hautement disponibles ni chiffrés. Dovecot OBOX [18] et Cyrus Murder [7] sont deux extensions qui

ajoutent un système haute disponibilité à Dovecot et Cyrus respectivement. Dovecot TREES [15] est une autre extension, incompatible avec Dovecot OBOX, qui permet de stocker les boites e-mail chiffrées à l'aide du mot de passe de l'utilisateur. Aucun de ces logiciels n'a été nativement conçu pour la haute disponibilité ni le chiffrement des boites e-mail, ce qui rend les intégrations imparfaites et incompatibles entre elles. Apache James [2] supporte nativement Cassandra [13], qui permet la haute disponibilité et le passage à l'échelle, mais ne propose aucune solution pour la confidentialité des e-mails.

PGP et S/MIME PGP [4] et S/MIME [10] sont deux techniques de chiffrement des e-mails de bout en bout indépendantes du MDA, existant depuis 1996 et 1999 respectivement, avec de nombreuses implémentations. Cependant ces solutions n'ont jamais été largement adoptées, car elles nécessitent une intégration dans le client e-mail (MUA) de l'utilisateur ainsi qu'une configuration spécifique, d'autant plus complexe que l'utilisateur a plusieurs terminaux. PGP met également à la charge de l'utilisateur la gestion de sa propre toile de confiance. Enfin, ces deux protocoles ne chiffrent que le contenu des e-mails, et non leurs en-têtes (sujet, destinataire, heure de réception, etc.), et encore moins les informations du dossier qui contient ces e-mails (nom, nombre d'e-mails, drapeaux lu/non lu/important/etc.).

Prototypes, Recherche & Document de conception StalwartLabs propose un serveur e-mail [26] dont la haute disponibilité est gérée nativement via le protocole Raft [19], mais qui ne passe pas à l'échelle car le serveur leader doit gérer toutes les écritures. Il n'est pas non plus géo-distribuable à cause des contraintes de latence imposées par ce même protocole. De plus, il ne propose aucune solution de chiffrement des boites de réception.

Pluto [11] est un projet de recherche pour concevoir un serveur IMAP géo-distribué basé sur les CRDT [25]. Cependant il n'implémente qu'une partie de la norme IMAP en ignorant la partie sur les UID qu'il n'est pas possible d'implémenter à partir des résultats publiés, ce qui rend donc incompatible ce logiciel avec l'écosystème existant. Pluto ne propose aucun mécanisme de chiffrement.

Enfin, un projet nommé Dark Mail Alliance [14] avait pour objectif de spécifier un ensemble de protocoles pour mettre en place un système d'e-mail chiffré de bout en bout. Ce projet n'a mené à aucune réalisation ou implémentation à ce jour, n'est pas compatible avec l'existant, et ne précise pas comment les contraintes de disponibilité sont gérées.

Le Tableau 1 récapitule, pour chacun des projets étudiés, son positionnement par rapport aux fonctionnalités et caractéristiques que souhaite proposer le projet Aerogramme.

Roadmap Nous développons un prototype qui permet de valider l'intégration et la cohérence en pratique des différents composants décrits et conçus précédemment. 5 phases pour ce prototype sont déjà prévues :

- version 0.1 : version initiale validant l'intégration des modèles de données et des protocoles réseaux
- version 0.2 : support complet de IMAP4rev1
- version 0.3 : support partiel de IMAP4rev2

	Gmail, Outlook	Tutanota, ProtonMail	Dovecot OBOX, Cyrus Murder	Dovecot TREES	Apache James	S/MIME, PGP	StalwartLabs	Pluto	Dark Mail Alliance	Aerogramme
Souveraineté	×	×	✓	✓	✓	✓	✓	✓	✓	✓
Chiffrement	×	✓	×	✓	×	~	×	×	✓	✓
Disponibilité	✓	✓	~	×	~	N/A	✓	✓	N/A	✓
Géo-distribuable	N/A	N/A	~	×	~	N/A	×	✓	N/A	✓
Mise à l'échelle	✓	✓	~	×	~	N/A	×	✓	N/A	✓
Implémentation	✓	✓	✓	✓	✓	✓	✓	~	×	✓
Compatible IMAP	✓	~	✓	✓	✓	~	✓	×	×	✓

TABLE 1 – Comparatif des caractéristiques des différents projets e-mail

— version 0.4 : support préliminaire de CalDAV
— version 0.5 : support préliminaire de CardDAV

Références

[1] Spencer ACKERMAN. « Lavabit email service abruptly shut down citing government interference ». In : *The Guardian* (9 août 2013). ISSN : 0261-3077. URL : https://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden (visité le 14/08/2023).

[2] *Apache James*. URL : https://james.apache.org/ (visité le 14/08/2023).

[3] Lucian ARMASU. « 'Cloud Act' Creates Threat of U.S. Espionage, Say EU Lawmakers ». In : *Tom's Hardware* (25 fév. 2019). URL : https://www.tomshardware.com/news/cloud-act-us-espionage-threat,38688.html (visité le 14/08/2023).

[4] Derek ATKINS, William STALLINGS et Philip ZIMMERMANN. *PGP Message Exchange Formats*. RFC 1991. Backup Publisher : RFC Editor ISSN : 2070-1721 Published : Internet Requests for Comments. RFC Editor, août 1996. URL : http://www.rfc-editor.org/rfc/rfc1991.txt.

[5] Julian E. BARNES. « Hacking of Government Email Was Traditional Espionage, Official Says ». In : *The New York Times* (20 juill. 2023). ISSN : 0362-4331. URL : https://www.nytimes.com/2023/07/20/us/politics/china-hacking-official-email.html (visité le 14/08/2023).

[6] Adam de BOOR. « Gmail : Past, Present, and Future ». In : USENIX Association, juin 2010.

[7] *Cyrus Murder : Concepts — Cyrus IMAP 3.8.0 documentation*. URL : https://www.cyrusimap.org/imap/reference/admin/murder/murder-concepts.html#architecture (visité le 14/08/2023).

[8] *Dovecot | The Secure IMAP server*. URL : https://www.dovecot.org/ (visité le 14/08/2023).

[9] *Email Market, 2021-2025*. The Radicati Group, Inc., 2021. URL : https://www.radicati.com/wp/wp-content/uploads/2021/Email_Market,_2021-2025_Executive_Summary.pdf.

[10] Paul HOFFMAN. *Enhanced Security Services for S/MIME*. RFC 2634. Backup Publisher : RFC Editor ISSN : 2070-1721 Published : Internet Requests for Comments. RFC Editor, juin 1999. URL : http://www.rfc-editor.org/rfc/rfc2634.txt.

[11] Tim JUNGNICKEL et Lennart OLDENBURG. « pluto : The CRDT-Driven IMAP Server ». In : *Proceedings of the 3rd International Workshop on Principles and Practice of Consistency for Distributed Data*. PaPoC '17. New York, NY, USA : Association for Computing Machinery, 23 avr. 2017, p. 1-5. ISBN : 978-1-4503-4933-8. DOI : 10.1145/3064889.3064891. URL : https://doi.org/10.1145/3064889.3064891 (visité le 14/08/2023).

[12] Nadim KOBEISSI. *An Analysis of the ProtonMail Cryptographic Architecture*. Published : Cryptology ePrint Archive, Paper 2018/1121. 2018. URL : https://eprint.iacr.org/2018/1121.

[13] Avinash LAKSHMAN et Prashant MALIK. « Cassandra : a decentralized structured storage system ». In : *ACM SIGOPS Operating Systems Review* 44.2 (14 avr. 2010), p. 35-40. ISSN : 0163-5980. DOI : 10.1145/1773912.1773922. URL : https://dl.acm.org/doi/10.1145/1773912.1773922 (visité le 14/08/2023).

[14] Ladar LEVISON. *Dark Internet Mail Environment*. Juin 2018. URL : https://darkmail.info/downloads/dark-internet-mail-environment-june-2018.pdf.

[15] *liberate / trees · GitLab*. GitLab. 10 août 2018. URL : https://0xacab.org/liberate/trees (visité le 14/08/2023).

[16] Enze LIU et al. « Who's got your mail ? : characterizing mail service provider usage ». In : *Proceedings of the 21st ACM Internet Measurement Conference*. IMC '21 : ACM Internet Measurement Conference. Virtual Event : ACM, 2 nov. 2021, p. 122-136. ISBN : 978-1-4503-9129-0. DOI : 10.1145/3487552.3487820. URL : https://dl.acm.org/doi/10.1145/3487552.3487820 (visité le 14/08/2023).

[17] *Message UIDs are not stable / possible data loss (deletion of wrong messages) · Issue #220 · ProtonMail/proton-bridge*. GitHub. URL : https://github.com/ProtonMail/proton-bridge/issues/220 (visité le 14/08/2023).

[18] *obox format design — Dovecot documentation*. URL : https://doc.dovecot.org/admin_manual/obox/design/ (visité le 14/08/2023).

[19] Diego ONGARO et John OUSTERHOUT. « In search of an understandable consensus algorithm ». In : *Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference*. USENIX ATC'14. USA : USENIX Association, 19 juin 2014, p. 305-320. ISBN : 978-1-931971-10-2. (Visité le 14/08/2023).

[20] *Passez à Outlook avec Microsoft 365 | Microsoft 365*. URL : https://www.microsoft.com/fr-fr/microsoft-365/outlook/outlook-personal-email-plans (visité le 14/08/2023).

[21] Scott RUOTI et Kent SEAMONS. « Johnny's Journey Toward Usable Secure Email ». In : *IEEE Security & Privacy* 17.6 (nov. 2019), p. 72-76. ISSN : 1540-7993, 1558-4046. DOI : 10.1109/MSEC.2019.2933683. URL : https://ieeexplore.ieee.org/document/8886906/ (visité le 14/08/2023).

[22] Scott RUOTI et al. « A Usability Study of Four Secure Email Tools Using Paired Participants ». In : *ACM Transactions on Privacy and Security* 22.2 (31 mai 2019), p. 1-33. ISSN : 2471-2566, 2471-2574. DOI : 10.1145/3313761. URL : https://dl.acm.org/doi/10.1145/3313761 (visité le 14/08/2023).

[23] Jack SCHOFIELD. « What's the best email service that doesn't scan emails for ad-targeting ? » In : *The Guardian* (19 avr. 2018). ISSN : 0261-3077. URL : https://www.theguardian.com/technology/askjack/2018/apr/19/whats-the-best-email-service-that-doesnt-scan-emails-for-ad-targeting (visité le 14/08/2023).

[24] *Service d'hébergement de courrier professionnel pour les entreprises – Courrier Microsoft Exchange*. URL : https://www.microsoft.com/fr-fr/microsoft-365/exchange/email (visité le 14/08/2023).

[25] Marc SHAPIRO et al. « Conflict-free replicated data types ». In : *Proceedings of the 13th international conference on Stabilization, safety, and security of distributed systems*. SSS'11. Berlin, Heidelberg : Springer-Verlag, 10 oct. 2011, p. 386-400. ISBN : 978-3-642-24549-7. (Visité le 14/08/2023).

[26] *Stalwart IMAP Server | Stalwart Labs Ltd.* URL : https://stalw.art/imap/ (visité le 14/08/2023).

[27] *What is Cyrus IMAP ? — Cyrus IMAP 3.8.0 documentation*. URL : https://www.cyrusimap.org/ (visité le 14/08/2023).