Informatics & Technology

Dr Csaba Andras Moritz,
Dr Santosh Khasanvis & Kristopher Carver

Sender-controlled private email

Electronic privacy with EPRIVO

Dr Csaba Andras Moritz, Founder and Chairman of BlueRISC Inc. and Professor of Electrical and Computer Engineering at University of Massachusetts Amherst, together with Senior Research Scientist Dr Santosh Khasanvis, Technical Director Kristopher Carver, and research staff, are addressing digital privacy issues. In particular, the team are exploring the vulnerability of communication to privacy violations, and enabling private collaborations with the development of EPRIVO, the Electronic Privacy Circle. In its first phase, EPRIVO is a unique private-email service enabling users to continue using their existing email addresses whilst adding innovative privacy controls, authentication, and encryption to their messages. Users also have the ability to recall sent private emails anytime, making them vanish.

Omelchenko/Shutterstock.com

Digital privacy, including the vulnerability of emails to privacy violations, is a growing concern for consumers and organisations alike. Private emails are susceptible to threats from both socio-economic and technological aspects. Unauthorised access can occur during the transit of an email to its recipient as well as during storage on a device, at a recipient, email server or in the cloud. The research and development team at cyber-security firm BlueRISC Inc. are addressing broad privacy solutions including enabling private collaborations. A current effort relates to email privacy issues and the broader question of private collaborations. The team is led by Dr Csaba Andras Moritz, Founder and Chairman of BlueRISC Inc. and Professor of Electrical and Computer Engineering at University of Massachusetts Amherst.

EMAIL VULNERABILITY

Users can accumulate numerous emails that are regularly archived for many years and spread across multiple vendors in the cloud. These emails are exposed to privacy violations throughout their lifetime. Together with factors relating to the sender and associated providers, as soon as an email is sent its privacy will also depend on the recipient's security habits, their devices and their providers in the cloud. Throughout the development of EPRIVO, the researchers have taken these multi-faceted threats to privacy into account. They encompass both socio-economic and technical factors that lead to most people's emails being compromised at some point.

SOCIO-ECONOMIC THREATS

Socio-economic threats can be underpinned by societal factors such as money, politics, power, culture and religions. While these factors can be considered part of everyday life, they can also be described in the terms and conditions that form agreements between parties or in terms of privacy. Prime examples of this are the free services that require users to agree to their terms and then use the users' information to target advertisements as part of a monetization scheme.

Considering this socio-economical context, email privacy can be vulnerable to data mining by both service providers and storing companies for financial benefit. There is also the possibility of future changes in their terms and conditions that can potentially compromise the consumer's information. Furthermore, such email privacy violations can happen without the user's knowledge.

TECHNOLOGICAL THREATS

The technology employed by users, their service providers and their storing companies to maintain information security can provide gateways for email privacy to be exploited. In addition to the risks arising from weak user passwords, all three parties are susceptible to attacks from hackers, phishing and social engineering together with implementation vulnerabilities. There is also the possibility of security breaches involving service provider insiders.

The research team at BlueRISC Inc. have solved a number of critical issues in order to address email privacy. They also recognise that a conflict of interest associated with privacy promised by organisations that directly benefit from users' information exists, and they note that even with government regulation, this privacy is unlikely to materialise.

ROLE SEPARATION

The researchers stress that in order to manage privacy, the roles of those who store our information and those who provide security, or privacy for it, have to be separated from one another in order to remove the existing conflict of interest.

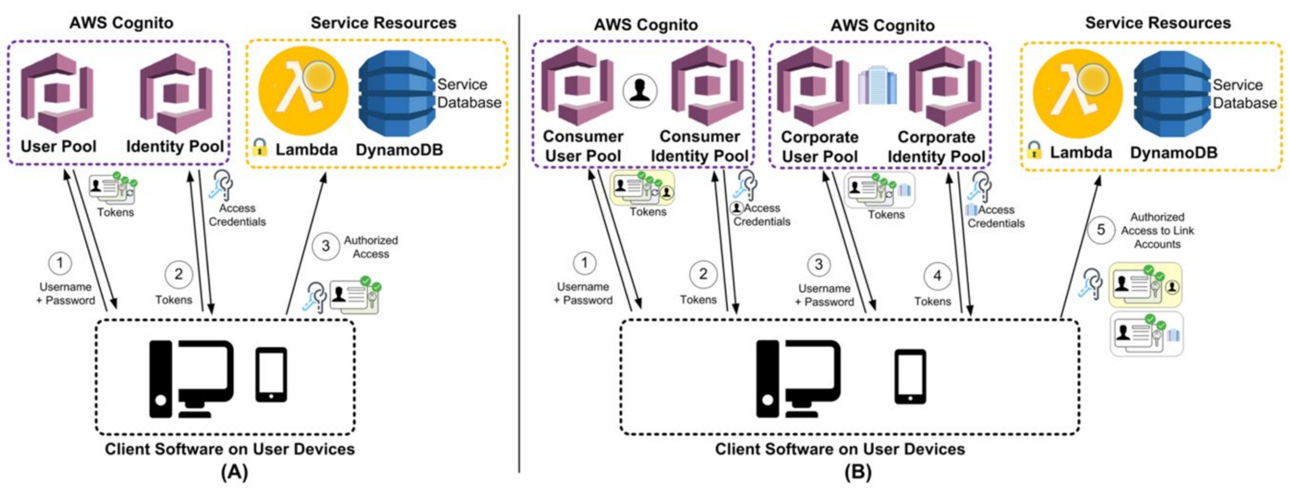

Figure 1. (A) Cloud architecture for consumer user authentication and authorised access to services resources. **(B)** Envisioned architecture for supporting corporate and consumer accounts in the same application with role separation, enforcing corporate policies for data access.

FUTURE PRIVACY

It only takes a single compromise at any time for our email privacy to be violated. Given the constantly changing threat models, together with the regular discoveries of new digital security vulnerabilities, the future privacy of secure emails in cloud models will still have to be guaranteed for users.

TRUE OWNER OF A COMMUNICATION?

Furthermore, senders require privacy controls in order to protect their email privacy long-term, both on recipients' devices and in the cloud.

Moreover, the team is facing the challenge of solving the trade-off between legal access and yet still maintaining privacy without opening backdoors (ways of bypassing normal authentication or encryption) into systems.

ELECTRONIC PRIVACY CIRCLE (EPRIVO)

BlueRISC Inc.'s team is addressing these challenges with the development of the concept of Electronic Privacy Circle, which is where the EPRIVO name is derived from. They are creating and supporting privacy collaborations and access to information with cryptographically enforced privacy controls. EPRIVO is available to both individual consumers and organisations and it operates on both mobile and desktop platforms. With its initial focus on private messaging through emails, in the form of both voice and text, the researchers are aiming to enable a private data collaboration system that performs private information management and sharing together with associated communication. The researchers believe that "within one's Privacy Circle, one should be able to maintain privacy and control access to information anytime in the future and independent if information is in the cloud or recipients' devices."

> **Within one's Electronic Privacy Circle, one should be able to maintain privacy and control access to information anytime in the future.**

Moreover, the EPRIVO approach is unique in that offers its users' security for their existing email accounts as well. There is no requirement to create a new email address as EPRIVO supports existing emails. The vision is that everything we use today as communication will be possible to turn into private.

OWNERSHIP DILEMMA: SENDER-CONTROLLED EMAIL PRIVACY

Through a combination of cloud-based authentication and cryptographically enforced access, the EPRIVO team introduced a new pioneering approach that allows senders to forever maintain control of sent content, including in the cloud and recipients' devices. Senders are enabled to maintain full

fizkes/Shutterstock.com

It only takes a single compromise at any time for our email privacy to be violated.

control of each private email for the entire lifetime of that message, even after the email has been sent. The sender can take back the email at any time, or erase it from both the recipients' devices and the cloud if they want to. The sender can also prevent the recipient from forwarding the email and set an expiration time for the message. In addition, EPRIVO allows its users to privatise old emails by enabling the archiving and encrypting of any old email message from any email account. EPRIVO was initiated by Dr Moritz and is primarily funded by BlueRISC. DHS-funded research aspects deal with exploring roots of trust in a cloud-based environment, and especially in a corporate setting.

SECURING EMAILS AGAINST THREATS

EPRIVO offers a patented email-privacy approach that is not susceptible to the socio-technological issues mentioned above. It combines government-grade digital security together with physical security, in the form of physical separation that is implemented in the cloud. This physical security means that no carrier or provider will have access to the complete message, even encrypted emails. Furthermore, EPRIVO does not store emails or content. Instead, it employs algorithms to shuffle emails through the users' own email carriers with the result that it never needs to store them. This means that EPRIVO can manage service and access throughout the world without having to maintain or fund the worldwide data centres. This is also a healthy separation of roles between content-storing providers and companies that provide security, avoiding any conflict of interest.

EPRIVO does not store emails. Instead, it employs algorithms to shuffle emails through the users' own email carriers.

Whilst the security is managed by EPRIVO, the email messages are kept fully encrypted in the users' email accounts. Users select the privacy features that will define how their messages are stored, retrieved, or destroyed. Users can also send a secure, confidential, encrypted email to non-EPRIVO users.

Societal threats are avoided as a provider cannot exploit an email's content as it is encrypted. Access to the complete email is impossible, even if digital security is compromised due to EPRIVO's physical separation. Similarly, technological threats are prevented as a security breach of a service provider or storing companies cannot endanger email privacy. To a certain degree EPRIVO can also provide security cover for the users' carelessness in terms of their security habits. If a user's email password is compromised, or if someone hacks into one of the carriers, the emails' privacy remains untouched.

A solution pioneered and patented relates to how access to information on the internet can be allowed. An approach requiring a multi-party agreement, across multiple providers, that uses cryptography creates a new fair mechanism to potentially support legal access.

EPRIVO'S VERSATILITY

EPRIVO can be integrated with all platforms and devices. It supports email-client software and web-based email access. It can be used for existing email addresses from any provider. It can be used for private text, attachment, as well as, voice responses or voice emails. Undoubtedly it moves usability to the fore and removes the burden of managing security management from its consumers.

Professor Moritz encapsulates EPRIVO as "the first Private Email Service enabling users to add innovative privacy controls, authentication, and encryption while using their existing email addresses. Sent private emails can be recalled anytime to make them vanish everywhere. A new form of collaboration that has privacy at its forefront is made possible."

Behind the Research

Dr Csaba Andras Moritz

Dr Santosh Khasanvis

Kristopher Carver

E: andras@bluerisc.com **T:** +1 413-320-7669 **W:** www.eprivo.com

Research Objectives

BlueRISC Inc. develops tools and systems to tackle issues as wide-ranging as vulnerability analysis/avoidance to exploit detection and software self-healing in the field, and post cyber-attack forensic analysis. It has completed advanced cyber-security R&D and been sponsored by several research organisations in the US including NSF, DARPA, and DHS. BlueRISC Inc. has customers in 19 countries.

Detail

BlueRISC Inc.,
400 Amity Street,
Suites 0-1-3-4,
Amherst, 01002 MA

Bio

Dr Csaba Andras Moritz is the founder and Chairman of the cyber-security firm BlueRISC Inc., the main organisation behind EPRIVO. He is the inventor and architect of BlueRISC's R&D directions, including EPRIVO for digital privacy. His vision is enabling future-proof private collaborations with privacy controls, across information shared on the Internet. He is also a Professor of Electrical and Computer Engineering at University of Massachusetts Amherst.

Dr Santosh Khasanvis, Senior Research Scientist at BlueRISC Inc., leads the ongoing implementation efforts for the electronic privacy circle initiative across multiple device platforms and cloud. He has published extensively on multiple topics related to cognitive systems, A.I., and contributed to theoretical foundations for cyber-security directions at BlueRISC.

Kristopher Carver is the Technical Director at BlueRISC Inc. and PI of many cyber-security R&D projects with both DoD and DHS. He has talked in leading cyber-security conferences and heads the R&D of several system-assurance and embedded security products developed at BlueRISC.

Funding

- BlueRISC Inc., internal funding.
- Department of Homeland Security Contract # DHS HSHQDC-16-C-00092.
- Department of Homeland Security Contract # DHS 70RSAT18C00000003.

Collaborators

Vincent Sritapan - Homeland Security Advanced Research Projects Agency - DHS, vincent.sritapan@hq.dhs.gov

References

Moritz, C.A. (2019). Sender-Controlled Private Email – Privacy Controls for Protection in the Cloud and Recipient's Devices. [online] Eprivo. Available at: https://www.eprivo.com/best-practices-sender-controlled-privacy/ [Accessed 19th September 2019].

Michael O. (2019). Comparing EPRIVO and ProtonMail. [online] Eprivo. Available at: https://www.eprivo.com/comparing-eprivo-and-protonmail/ [Accessed 19th September 2019].

Moritz, C.A. (2018). Threats to Email Privacy are Socio-Technological. [online] Eprivo. Available at: https://www.eprivo.com/threats-to-privacy-are-socio-technological/ [Accessed 19th September 2019].

Moritz, C.A. (2018). Physical & Digital Security. [online] Eprivo. Available at: https://www.eprivo.com/physical-digital-security-2/ [Accessed 19th September 2019].

US patent US10225075 by C Andras Moritz: Encrypting content and facilitating legal access to the encrypted content.

US granted patent 9940445 by C Andras Moritz: Transmitting content to promote privacy.

Personal Response

How did you develop the privacy architecture supporting EPRIVO?

" Privacy is a core human right and our team has always been keen to enable solutions that bring it to the forefront. Years ago, I kickstarted the privacy initiative at BlueRISC with a vision to facilitate information sharing on the Internet. Owners of information will be able to maintain control forever and communications shall remain private whether in the cloud or devices. After more than 16 years of cyber-security innovations at BlueRISC targeting government and industry, I established EPRIVO to address consumers' privacy concerns, bringing a new dimension to BlueRISC and creating its first consumer-focused direction. "