New app can secure all your saved emails

March 26 2019

This illustration depicts what users see E3 as their insecure email + their devices = secure encrypted email. The app--Easy Email Encryption--encrypts all saved emails to prevent hacks and leaks, is easy to install and use, and works with popular email services such as Gmail, Yahoo, etc. Credit: John S. Koh/Columbia Engineering

While an empty email inbox is something many people strive for, most of us are not successful. And that means that we probably have stored away hundreds, even thousands, of emails that contain all kinds of personal information we would prefer to keep private.

Current defenses, such as Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME), rely on public key cryptography that uses pairs of public and private keys generated by cryptographic algorithms. Because these systems are too technical and

difficult for the average user, most people don't use them. As a result, many email accounts have been hacked, including such high profile cases as the phishing attack on Hillary Clinton's top campaign advisor John Podesta and the 2016 email hack of one of Vladimir Putin's top aides.

In response to these kinds of widespread attacks, computer scientists at Columbia Engineering have built Easy Email Encryption (E3), an application for secure, encrypted email that is easy to manage even for non-technical users. Now in beta test mode, E3 automatically and invisibly encrypts email as soon as it is received on any trusted device, including smartphones, laptops, and tablets. It works on a variety of platforms including Android, Windows, Linux, and Google Chrome, and with popular mail services such as Gmail, Yahoo, AOL, and more.

The team—Professors Jason Nieh and Steve Bellovin and their Ph.D. student John S. Koh—presented its study today at EuroSys '19 in Dresden, Germany, one of the world's top forums focused on computer systems software research and development.

"Email privacy grows ever more critical as our email inboxes increase in size," notes Koh, the paper's lead author. "Thanks to free and widely popular mail services like Gmail, users are keeping more and more emails, thus providing a one-stop shop for hackers who can compromise all of a user's emails with a single successful attack."

Ever since 1999, when the seminal "Why Johnny Can't Encrypt" paper showed how extraordinarily hard it was for people to send encrypted email, researchers have been trying to design encryption systems that are easier for the average user to manage. The problem is that they have stayed focused on end-to-end encryption solutions, where only the original sender and recipient can read the messages. Third-parties, including telecommunications and Internet providers, cannot eavesdrop

as they cannot access the cryptographic keys to decrypt the conversation. While these solutions certainly work and offer the most security, PGP and S/MIME, the encryption solutions most favored by experts, are so complex that they are impractical, almost unusable, for a non-technical user.

"The field of email security is just begging for improvement," Koh notes. "For 20 years, the research community was fixated on end-to-end security. We took a different tack, positing that end-to-end encryption for email is not needed in the 21st century. Internet connections are increasingly protected by default using encryption. Our insight is that email needs to be protected when it's stored in our inboxes, not when it's being sent over the Internet, because hackers are mainly just trying to log into your email account. We thus apply an 'encrypt on receipt' model that provides excellent real-world security while being far more usable than end-to-end encryption."

Over the past three years, the Columbia Engineering team refined E3, trying many different approaches before finding a method that checked all the boxes they needed. They have been testing the app with a couple dozen study participants, many of whom were not particularly tech-savvy. All agreed that E3 is significantly easier to use than the state-of-the-art systems for secure email, to the point where E3 is almost as easy to use as a regular email client.

The team's new approach simplifies email encryption and improves its usability by implementing receiver-controlled encryption. Newly received messages are transparently downloaded and encrypted to a locally generated key and the original message is then replaced. A major problem was how to handle multiple devices, especially important these days as most people read email on several devices. Rather than moving private keys around, which is hard to do securely and puts great demands on the user, the researchers used per-device key pairs. With this

approach, only public keys need to be synchronized via a simple verification step. Hackers who successfully attack an email account or server can only gain access to encrypted emails. All emails encrypted prior to a breach are protected.

In E3, public keys are never shared with other people. They are self-generated and self-signed, and require no public key infrastructure for the user to understand. Previous work has shown that users find it confusing to correctly obtain and use public keys. In contrast, an E3 user needs only self-signed keys, and any public key exchanges among the user's devices are automated.

The researchers note that they do not intend E3 to be an end-to-end, maximum security solution, but rather a major improvement over the norm that is easy to deploy and use. Says Koh, "We traded perfection—end-to-end, sender-controlled encryption—for a significant increase in usability and the ability to protect what we now know is the real problem for most people."

The team is refining E3 and making its implementations—the actual applications—even easier to use by trying new approaches applicable to the modern user. They plan to make it available in the near future for Android users as an app freely available in the Google Play Store. An iOS version is also in the works.

More information: John S. Koh et al, Why Joanie Can Encrypt, *Proceedings of the Fourteenth EuroSys Conference 2019 CD-ROM on ZZZ - EuroSys '19* (2019). DOI: 10.1145/3302424.3303980

Provided by Columbia University School of Engineering and Applied Science