Perfecting email security

September 10 2012

Millions of us send billions of emails back and forth each day without much concern for their security. On the whole, security is not a primary concern for most day-to-day emails, but some emails do contain personal, proprietary and sensitive information, documents, media, photos, videos and sound files. Unfortunately, the open nature of email means that they can be intercepted and if not encrypted easily read by malicious third parties. Even with the PGP - pretty good privacy - encryption scheme first used in 1995, if a sender's private "key" is compromised all their previous emails encrypted with that key can be exposed.

Writing in the *International Journal of Security and Networks*, computer scientists Duncan Wong and Xiaojian Tian of City University of Hong Kong, explain how previous researchers had attempted to define perfect email privacy that utilizes PGP by developing a technique that would preclude the decryption of other emails should a private key be compromised. Unfortunately, say Wong and Tian this definition fails if one allows the possibility that the email server itself may be compromised, by hackers or other malicious users.

The team has now defined perfect forward secrecy for email as follows and suggested a technical solution to enable email security to be independent of the server used to send the message:

"An e-mail system provides perfect forward secrecy if any third party, including the e-mail server, cannot recover previous session keys between the sender and the recipient even if the long-term secret keys of

the sender and the recipient are compromised."

By building a new email protocol on this principle, the team suggests that it is now possible to exchange emails with almost zero risk of interference from third parties. "Our protocol provides both confidentiality and message authentication in addition to perfect forward secrecy," they explain.

The team's protocol involves Alice sending Bob an encrypted email with the hope that Charles will not be able to intercept and decrypt the message. Before the email is encrypted and sent the protocol suggested by Wong and Tian has Alice's computer send an identification code to the email server. The server creates a random session "hash" that is then used to encrypt the actual encryption key for the email Alice is about to send. Meanwhile, Bob as putative recipient receives the key used to create the hash and bounces back an identification tag. This allows Alice and Bob to verify each other's identity.

These preliminary steps are all automatically and without Alice or Bob needing to do anything in advance. Now, Alice writes her email, encrypts it using PGP and then "hashes" it using the random key from the server. When Bob receives the encrypted message he uses his version of the hash to unlock the container within which the PGP-encrypted email sits. Bob then uses Alice's public PGP key to decrypt the message itself. No snoopers on the internet between Alice and Bob, not even the email server ever have access to the PGP encrypted email in the open. Moreover, because a different key is used to lock up the PGP encrypted email with a second one-time layer, even if the PGP security is compromised past emails created with the same key cannot be unlocked.

More information: "E-mail protocols with perfect forward secrecy" in *Int. J. Security and Networks*, 2012, 7, 1-5

Provided by Inderscience Publishers