Email encryption standards hacked

May 14 2018

Credit: CC0 Public Domain

A research team from the University of Applied Sciences (FH) in Münster, Horst Görtz Institute for IT Security at Ruhr-Universität Bochum (RUB), and Katholieke Universiteit Leuven has demonstrated that the two most common email encryption standards are vulnerable to attacks. Their attack, referred to as Efail, proved successful in 25 out of

35 tested email programs using the S/MIME encryption standard and in 10 out of 28 tested programs using OpenPGP. The program developers have been informed and have fixed the security gaps. The experts urgently recommend updating the underlying cryptographic algorithms in order to withstand any potential attacks in future.

Detailed information on their attack has been published on their website efail.de .

Realistic attack scenario

Emails are encrypted in order to hide their contents from network providers, cybercriminals, and intelligence services who might gain access to them via hacked routers, an email server, or by recording a message during transmission. "In the wake of Snowden's whistleblowing and countless hacked email servers, this is very much a realistic scenario," stresses Prof Dr. Sebastian Schinzel from the Department Electrical Engineering and Computer Science at FH Münster.

The intercepted message is manipulated by the attacker as he adds his own malicious commands in encrypted form. Thus altered, the message is sent to one of the recipients or to the sender, i.e. where the data is stored that's necessary for deciphering it.

After the message has been deciphered, the inserted commands cause the victim's email program to establish a communication connection with the attacker the next time the email is opened. This form of communication is pretty much standard when, for example, images or design elements in emails are loaded. Via that connection, the decoded email is then sent to the attacker who can read them. The researchers named this novel attack method "Exfiltration with Malleability Gadgets".

Enterprise, journalist, whistleblower

The email encryption standards S/MIME – short for Secure/Multipurpose Internet Mail Extensions – and OpenPGP have been in use since the 1990s. S/MIME is frequently deployed by enterprises that encrypt all outgoing and decrypt all incoming emails. OpenPGP is preferably used by individuals, for example, by journalists in conflict areas or by whistleblowers like Edward Snowden.

The underlying cryptography hasn't been updated since the 1990s, even though better techniques have long been available. "This type of cryptography has been broken more than once in other Internet standards, e.g. in TLS, short for Transport Layer Security, a protocol for the encryption of online data transmission. We have now demonstrated for the first time that it is also vulnerable as far as email encryption is concerned," explains Prof Dr. Jörg Schwenk from the Chair for Network and Data Security at RUB.

In its current version, S/MIME is not suitable for secure communication

In the case of S/MIME, the successful attack has shown that the current standard is not suitable for secure communication. "OpenPGP can be configured and used securely; however, this is often not the case as we showed in our practical analyses and should therefore be considered insecure," says Jörg Schwenk.

Now, the Internet Engineering Task Force, a developer-independent international organisation, is called upon to provide a new standard, according to the researchers. Following their successful attack, the research team have informed the developers of all tested email programs of the security gap identified by them. Measures have been taken to close it, in order to minimise the risk of a successful genuine attack.

Provided by Ruhr-Universitaet-Bochum

Citation: Email encryption standards hacked (2018, May 14) retrieved 1 May 2024 from https://phys.org/news/2018-05-email-encryption-standards-hacked.html