

## Re: [openpgp] Spoofing OpenPGP and S/MIME Signatures in Emails

Stephen Farrell <stephen.farrell@cs.tcd.ie> | Tue, 30 April 2019 13:19 UTC | [Show header](#)

Hiya,

On 30/04/2019 13:29, ilf wrote:

> <https://github.com/RUB-NDS/Johnny-You-Are-Fired>  
> <https://raw.githubusercontent.com/RUB-NDS/Johnny-You-Are-Fired/master/paper/johnny-fired.pdf>  
>

Great work, thanks! I guess that's another fine demonstration that code that's not really used in anger enough tends to have lots of frailties;-)

A comment and a question:

- I think it'd be a fine thing if this were to be presented at an IETF meeting - if some of the authors are going to be at one of those (or would present remotely) then contacting the security area directors and asking for a slot at some saag session would be a fine thing.
- I wasn't clear how to interpret the missing combinations from Table 2, e.g. does the lack of mention of the Linux/TB/Enigmail combination mean that it was not vulnerable to the attacks or that it was not tested? (Or that it's almost certainly vulnerable but you'd already broken so much so well, it wasn't worth specifically documenting;-)

Cheers,

S.

>  
>  
> \_\_\_\_\_  
> openpgp mailing list  
> [openpgp@ietf.org](mailto:openpgp@ietf.org)  
> <https://www.ietf.org/mailman/listinfo/openpgp>  
>

Attachment: [0x5AB2FAF17B172BEA.asc](#)Attachment: [signature.asc](#)[\[openpgp\] Spoofing OpenPGP and S/MIME Signature...](#) ilf

[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Stephen Farrell  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Marcus Brinkmann  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Peter Gutmann  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Albrecht Dreß  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Albrecht Dreß  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Marcus Brinkmann  
[Re: \[openpgp\] Spoofing OpenPGP and S/MIME Signa...](#) Marcus Brinkmann

[Hide Navigation Bar](#)v2.1.2 | [Report a Bug](#) | [By Email](#)