E-Mail Security and Privacy

How to handle the most common issues

Tobias Dussa
WP8-T1

Webinar, September 2020

Public

www.geant.org

Game Plan

- Recap on what e-mail really is and is not.
- Bad things that come upon users of e-mail.
- Things that users can do proactively to improve the situation.
- Questions/discussion/open mike session.

Recap: Previously on “Your Life with E-Mail”

What is E-Mail?

- A means for users of computer systems to exchange text-based messages.
- Defined in RFC 822 (1982-08-13) or, to be a bit more generous, in RFC 733 (1977-11-21).
- Essentially, text files are moved from the Mail User Agent (MUA) of the sender via one or more Mail Transport Agents (MTA) to the appropriate Mail Delivery Agent (MDA) of the receiver’s system.

So What is the Problem?

- Mail in itself is not authenticated. In principle, everybody can send mails that look like they have been sent from any given mail address.
- Every intermediate system that handles a given e-mail can **read** it (obviously) and **change** it.
- MUAs are trying to be smart about displaying more complex content (HTML, PDF, ...) and occasionally trip over details or create privacy issues.

What Does Mail Look Like?

- Generally, an e-mail consists of two parts: The mail header and the mail body.
- Both parts can be empty when a mail is sent.
- The header may contain metadata:
  Sender, recipient, time, user agent, …
  In particular, every MTA that handles a mail **adds** one or more header lines containing “routing information”.
- The body must not be changed (by MTAs).
- Crucially, mail is routed based on the **envelope address**, **not** the “To:” header.

Things that will come upon you and make your life miserable if you use e-mail

The Bad, the Ugly, and the Very Ugly

Types of mail you will get but not want:

- Spam,
- phishing,
- backscatter.

Depending on some details, these are anything between a mild nuisance and a serious security problem.

Spam

Spam (junk, unsolicited bulk e-mail or UBE, unsolicited commercial e-mail or UCE, ...) is

- generally harmless (unless you count lost time and/or resources),
- unavoidable (mail addresses are public) and
- almost never a security problem
- ... unless it carries malware or URLs to malware
- ... or causes availability issues by overflowing mailboxes.

What to Do about Spam

Best course of action:

- Ignore or delete the mail.
- … unless you have a spam filter that is capable of learning from identified spam, in which case feed it with the spam mail.
- **DO NOT** respond!
- (… unless you are bored and feel like chatting up Nigerian princes or Iraqi generals who for some reason need **YOU** to help them move lots of money out of their countries.)

Phishing

Phishing mails are designed to make you do something you really don’t want to do.

- Generally, the purpose is to get access to your account and/or computer.
- May or may not contain malware.
- Recognizing well-made phishing mail is really, really, really, **really** hard.
- Fortunately, a lot of phishing mails are badly-made.

What to Do about Phishing

- If you have identified a mail as a phishing attempt: Excellent! Consider letting your local security team know about it. Otherwise, ignore or delete it.
- If you have already done something you wish you hadn’t done (opening an attachment of a strange mail, sending your username and password to a stranger), **talk to your local security people immediately**.

What Else to Do about Phishing

If you are the security or admin team for an organisation:

- You will benefit from maintaining a clear picture of what is happening, so it is probably a good idea to tell people how to forward phishing mail to you with intact headers.
- Consider registering with the “I Got Phished” service (https://igotphished.abuse.ch/) or getting in touch with the Anti-Phishing Working Group (https://apwg.org/).

Backscatter

Backscatter are e-mails sent in reply to you because of spam mails you have allegedly sent:

- Non-delivery notices (bounces), mailing list notices, autoresponder replies, angry mails sent by spam recipients who don’t understand how the entire spiel works.
- In many (most?) cases, this does **not** mean you have a security problem, just that someone sent spam in your name.

What to Do about Backscatter

There really is just one important thing to do:
Verify that your sender address was faked.

- Try to get a hold of the original spam message, inspect the headers.
- If the headers look like your account or machine was indeed used to send the spam mails: Go see your security team.
- Otherwise: Get a coffee and wait for the storm to blow over.

(Incomplete) Header Example

```
Received: from smtp.dfn-cert.de ([193.174.12.171])
        by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 3j9ctm_WAnGc; Mon, 21 Sep 2020 17:23:24 +0200 (CEST)
Received: from goggles.dfn-cert.de (unknown [IPv6:2001:638:714:2c30:3::1])
        (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
        (Client CN "Tobias Dussa", Issuer "DFN-Verein [...] CA" (verified OK))
        by smtp.dfn-cert.de (Postfix) with ESMTPS id 3288C65BEB;
        Mon, 21 Sep 2020 17:23:24 +0200 (CEST)
To: Captain Kirk <kirk@enterprise.gov>
From: The Emperor of China <emperor@imperialpalace.cn>
Date: Sun, 05 May 1850 17:23:22 +0800
```

What you can do to improve the situation

Basic Transport-Layer Hygiene

Always force properly secured connections for sending and receiving mail whenever you need to authenticate:

- IMAP**S** (port 993) instead of IMAP (port 143),
- POP3**S** (port 995) instead of POP (port 110),
- SMTP**S** aka submission**s** (port 465) instead of SMTP (port 25) or submission (port 587).
- If the above are not available, then use STARTTLS (on the regular ports).
- If STARTTLS is not available either, consider changing your mail provider.

Mail User Agent Configuration

- Carefully consider whether you want your MUA to render HTML or other content – more complexity means more attack surface for malware.
- HTML rendering hides true URL targets.
- Disable automatic loading of HTML objects because `img` tags are sometimes used to track whether a mail has been opened.
- Disabling HTML for outbound mail is a very, very good idea as well.

Enhanced Privacy

- If mail content is sensitive, consider encrypting and/or signing your e-mails:
  - **Encrypting** keeps messages private,
  - **signing** makes them tamper-proof.

  (If your content is **really** sensitive, consider not sending it via e-mail at all.)
- Two competing standards:
  - S/MIME and
  - PGP/MIME.

S/MIME and PGP/MIME

- Both make use of public-key cryptography:
  - Every user has (at least) one pair of keys, a **public** key and a **private** (or **secret**) key.
  - The public key is, well, public and meant to be distributed.
  - The secret key is secret and must only be known to the user.
  - The public key can decrypt what was encrypted with the secret key and vice versa.
- Problem: How to find the correct public key for a given recipient?

S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME uses a Public-Key Infrastructure (PKI).

- Public keys are enclosed in X.509 certificates.
- Certificates are issued by CAs: “Certificate Authorities” or “Certification Authorities”.
- CAs do (more or less) comprehensive identity verification → you can assume a certificate to be correct if you trust the issuing CA.
- Your OS/browser/MUA comes with a set of trusted CAs.

PGP/MIME (Pretty Good Privacy/MIME)

- Public keys are not embedded in certificates but can be signed by other users.
- The idea is that if sufficiently many people attest to a public key’s correctness, then you can assume it is correct (“Web of Trust”).
- Completely decentralized: No need to trust any central entity, but you are on your own with regard to trust management.

So… S/MIME or PGP/MIME?

A tough question to answer in general.

- In some ways, S/MIME is easier for the user (trust management, MUA support, required level of technical expertise).
- … but you have to **get** an X.509 certificate from somewhere so that both you and your correspondent trust the issuing CA.
- (CAcert.org offers certificates verified with a somewhat consistent and documented degree of scrutiny free of charge.)

More Pros and Cons

- Trust models of S/MIME and PGP/MIME are completely different → you might have a preference for whatever reason.
- Ultimately, the choice might not be yours to make, because the recipient of your e-mails may have preferences or constraints that limit your choices.

Common Problems of E-Mail Encryption

Both approaches share some pitfalls:

- Most importantly, encrypted e-mails are **gone** if you lose your private key. No, really. You cannot recover from that.
- Webmailers are completely out of the picture and will not work.
- MUA support is okayish at best, a nightmare at worst. Be prepared to run into all sorts of problems.

More Challenges

- Snooping adversaries cannot read encrypted e-mails, but virus scanners and spam filters cannot read them either.
- Searching in your mail archive is a lot harder.
- Make sure to tell your MUA to **also** encrypt outgoing mail with **your** public key if you store a local copy. If you don’t, you will not be able to read the mails you have sent.

Even More Challenges

- Need your colleagues to read your mail while you are on vacation? Think through this scenario before rolling out encryption. Key escrow is non-trivial.
- If you want to play it even safer, you can put your private key on a hardware token.

What About Signatures?

Signatures are nowhere near as troublesome as encryption.

- If your MUA is configured properly (read: if it appends signatures as separate MIME attachments), then the recipient's MUA can always display the mail as before even if it has no idea what this funny "signature attachment" is supposed to be.
- In some corner cases, signed mails will cause an intermediate MTA/MDA to trip and fall over. This is rare nowadays though.

Bottom Line

- If your e-mail contains sufficiently sensitive information that it should really not be read by someone else, **encrypt** your mails and be prepared to meet at least some of the problems above.
- In general, **signing** all outgoing e-mails is safe and a good idea.
- If you care about your data, **create offline backups** of your private key.

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).