CIA Lab Assignment: Mail Transfer Agents (2)*

A. Bakker N. Sijm J. van der Ham M. Pouw†

Feedback deadline:
October 10, 2017 10:00 CET

Abstract

This afternoon we will be looking at mailing loops, virtual domains and other mail related things. Note that your MTA must be up and running before you can start working together, so be sure to communicate with each other when to start.

1 Mailing Loops

Create an email loop within your own group by sending email from domain to domain using email aliases.

1. Now send an email to the loop using your own email address and show what happens on your MTA (logs, error message)
2. Can you change the behaviour of your MTA in response to this loop?

2 Virtual Domains

An MTA can be a mail server for more than one domain. It can receive and send mail as if each of the domains has a dedicated MTA. Since the domain only exists within the MTA, it is called virtual.

3. (a) Create a new subdomain within your domain and add an MX entry to it.
   (b) Then extend your MTA configuration to handle virtual domains, and have it also handle the email for the newly created domain.
   (c) Show how you test this.

*Based on earlier work by E.P. Schatborn and A. van Inge. Version October 3, 2017.

†Arno.Bakker@os3.nl,mick@os3.nl

3 SPAM and Security

For many people unsolicited commercial email, or rather SPAM, is a big problem. There are many ways to filter SPAM, each one having advantages and disadvantages. Examples include domain keys, SPF records, DNS block lists, greylisting, reverse checks, tarpitting, Bayesian filters, whitelists, etc.

A lot of viruses and malware are transported over email (as well as the World Wide Web). Because viruses can cause a lot of trouble, discarding viral messages is a nice service to offer to your users.

4. (a) Write a small paragraph that highlights the advantages and disadvantages of SPF and DomainKeys Identified Mail (DKIM).
   (b) What would you choose at a first glance and why?
   (c) Configure your system to support one of the two. Your system must support it for both sending and receiving email. You might need additional software packages or patches.
   (d) Provide full email/MTA headers to prove that SPF/DKIM were implemented correctly on your system (sending and receiving).

5. Investigate what generic anti-spam open source software packages are out there, choose one, download it (compile it if necessary) and configure your MTA to use it. Show that it works. Make sure that in your MTA group there are 2 different anti-spam solutions implemented!

Remember to keep an exact log of your actions, highlighting the problems you've encountered and how *you* solved them.

Somewhat related to the filtering of SPAM is the authentication and encryption of SMTP sessions. There are numerous SMTP extensions like SMTP-AUTH or TLS/SSL that take care of authentication and/or encryption. SMTP-AUTH[1] is primarily used for authentication using a username/password combination. The STARTTLS command starts the encryption during an SMTP session. These methods are often combined. By using TLS the outside world cannot see how the SMTP-AUTH is established.

6. Investigate these methods and add authentication to your MTA. Show that it works.

4 Extra Assignments (Optional)

7. Also add transport encryption to your MTA.