CIA Practicum Assignments
Mail Transfer Agents (2)

E.P. Schatborn N.P.H. Sijm A. van Inge C. Dumitru

September 28, 2012

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 Introduction

Before you start take some time and read RFC1855.

2 Mailing-loops

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

→ Now send an email to the loop using your own email address and see what happens on your MTA.

→ Can you change the behavior of your MTA in response to this loop?

→ What else does an MTA do to prevent email loops?

3 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.

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

4 SPAM and Viruses

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.

Nowadays, most viruses and malware are transported over the world wide web. Some years ago, however, their most important means of transport was email. Because viruses can cause a lot of trouble, discarding viral messages is a nice service to offer to your users.

→ Write a small paragraph that highlights the advantages and disadvantages of SPF and domain keys. What would you chose at a first glance and why ? Configure your system to support and check for one of the two. You might need additional software packages or patches. Provide full email/MTA headers to prove that SPF/DKeys were implemented correctly

→ Investigate what generic antispam open source software packages are out there, chose one, download it (compile it if necessary) and configure your MTA to use it. Make sure that in your MTA group there are at least 2 different antispam solutions implemented!

→ Perform the same for an open source antivirus solution and test it!

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

5 Extra Assignments

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.

→ Investigate these methods and add authentication to your MTA.

→ Install a mailing list software and ask your group members to sign up. When do you think it's better to use top-posing ?

[1] SMTP-AUTH is a Simple Authentication and Security Layer (SASL) profile. SMTP-AUTH is described in RFC2554 and SASL in RFC2222.