The Safety precautions and Design of Mail System

Fang Lei
HuangShan University, College of Information & Engineering, An Hui, Huang Shan, 245021.China.

Abstract. Through the introduction of the current mainstream Mail protocol, this paper analyzes its advantages, disadvantages and application environment. Combined with the security strategies and application requirements, we summarize its practical application in production environment and further elaborate the hierarchical security management requirements of today’s mail system.

1. Preface
As we all know, the Internet era has brought about a positive impact on global development, which is hard to underestimate, greatly improving the efficiency and quality of information exchange and sharing. At the same time, Email loaded on the Internet has already become one of the most important tools in business communication, and the traditional era of surface mail has become a memory. If someone else is using the surface mail, it is definitely not the pursuit of efficiency, but there are other meanings of use. Of course, today’s express is an upgraded version of surface mail. However, it is mainly used for the transmission of visible and significant items. It is not suitable for the transmission of information, and it cannot be compared with E-mail in terms of transmission efficiency.

2. A brief Introduction the Application of Mainstream Mail protocol
Due to the importance of e-mail, the pioneers finally released the SMTP e-mail protocol standard in 1982 after more than ten years endeavor. At the same time, the e-mail protocol has caught up with the rapid development of the Internet. With the gradual improvement and promotion of e-mail protocol, people have become dependent on e-mail which has become an indispensable tool in people's daily work. Therefore, it is necessary for us to understand it deeply and improve it according to the development needs.

At present, SMTP/POP3 is the most mature and the highest utilization on the Internet, while MAPI, which we are familiar with, is the most common one used in Intranet. However, because it was originally designed by Microsoft and officially put into use in 1991, MAPI was mainly used in an intranet environment with other similar products of Microsoft. Later, Microsoft introduced RPC OVER HTTP technology and promoted MAPI to the Internet. But what needs to be explained here is that all systems that require regular email communication with others must adhere to the commonly recognized protocol standards, otherwise they cannot communicate with other systems that use these protocols. Therefore, most of the current mail systems on the Internet use the international standard protocol SMTP/POP3 system, and it is still difficult to be compatible with the MAPI mail system. Based on the third party protocol of “translation”, they can all exist on the Internet at the same time. The specific application can be shown in Figure 1:
It should be noted that the mail protocol is mainly responsible for the control of the successful exchange process of each mail. A real complete mail transmission process is very complex, and it must be completed with the cooperation of other protocols, which can be briefly explained by following diagram:

![Figure 2. Schematic Diagram of Mail protocol Transmission Control](image)

3. **A brief Introduction the mechanism of SMTP/POP3**
SMTP (Simple Mail Transfer Protocol) is called the Simple Mail Transfer Protocol and aims to provide users with efficient and reliable mail transmission. An important feature of SMTP is that it can relay mail in transit, that is, mail can be relayed via the host on different networks, which can worked in two situations: one is that e-mail is transmitted from client to server; the other is that e-mail is transmitted from one server to another. SMTP is a request/response protocol that monitors 25 port to receive mail requests from users and establishes an SMTP connection to the remote mail server.
There are two working modes of SMTP: sending SMIP and receiving SMIP. The specific working method is as follows: After sending SMTP receiving the mail request from the user, it is determined whether the mail is a local mail or not. If it is a local mail, it will be directly sent to the user's mailbox. Otherwise, it will query the MX record of the remote mail server from DNS and establish a two-way transmission channel between the remote receiving SMTP. Thereafter, the SMTP command will be sent by the sending SMTP and received by the receiving SMTP, and the reply will be sent in the opposite direction. Once the delivery channel is established, the SMTP sender sends the mail command to indicate the mail sender. An OK reply is returned if the SMTP receiver can receive the message. Then SMTP sender issues RCPT command again to confirm whether the mail has been received or not. If the SMTP receiver receives, an OK reply is returned. If it cannot be received, a reject reply is issued (without aborting the entire mail operation), and both parties repeat this multiple times. A special sequence is received when the receiver receives the full message, and an OK reply is returned if the receiver successfully processes the message. In the whole transmission process, the system needs to use five essential commands: HELO, MAIL, RCPT, DATA and QUIT. HELO is used to declare the sender's identity, MAIL is used to represent the sender's address, RCPT is used to inform the recipient's address, while DATA and QUIT are used to start and end content input respectively. All commands are completed between the sender and the first MAIL transfer agent (TMA). The following is a transmission diagram.

![Diagram of SMTP Transmission Mode](image)

The full name of pop is post office protocol, which is used for receiving e-mail. It uses TCP port 110 by default. Since it is commonly used in the third edition, it is called POP3 which adopts client/server working mode. When the client needs the service, the client's software will establish a TCP connection with the POP3 server. After that, it will go through the three working states of the POP3 protocol. The first is the authentication process, confirming the username and password provided by the client, and then transferring it after the authentication is passed. In this state, users can receive their own mail or delete the mail. After the corresponding operation is completed, the client issues the quit command and then enters the update state to delete the mail marked with delete from the server side. By this time, the whole POP process is completed. The most common commands are: USER (verify the user name), PASS (verify the password), LIST (list the email number in the mailbox), RETR (LIST the body of a specific email), DELE (delete a specific email), and QUIT (quit the session). Compared with SMTP, POP3 work mechanism is simpler with only three processes. It usually runs on the same host as SMTP to facilitate management and maintenance.

4. Application Features of Microsoft MAPI
The full name of MAPI is the Messaging Application Programming Interface, translated as “message application interface”, but from a protocol point of view, we usually call it as MAPI protocol, because it is the popular name of MAPI/RPC Protocol. And in Microsoft, they also called it as “Exchange RPC” and “Outlook-Exchange Transport Protocol”. In my opinion, “Outlook-Exchange Transport Protocol” is the most vivid and easy to understand. It is mainly used as a very important information Exchange Protocol between Outlook and Exchange Server. The difference between MAPI and SMTP/POP3 can be found in the following table:
Table 1. The Difference of Application Function with MAPI and SMTP/POP3

| Applications           | MAPI | SMTP/POP3 | Explanation                                      |
|------------------------|------|-----------|--------------------------------------------------|
| Sending email          | Yes  | Yes       |                                                   |
| Receiving email        | Yes  | Yes       |                                                   |
| Calendar management    | Yes  | No        | Manage personal or other work plans               |
| Task management        | Yes  | No        | Manage individual or others’ task plans          |
| Conference Booking     | Yes  | No        | Schedule a meeting with others                   |
| Diary management       | Yes  | No        | Manage personal diary                            |
| Mail rule              | Yes  | No        | Flexible management and classification of sent or received mail |
| Contact management     | Yes  | No        | Detailed management of contact information and compatibility with third-party applications |
| Multi-person resource sharing | Yes  | No        | Flexible authorization management for personal mail or others |
| Centralized mail storage | Yes  | No        |                                                   |
| -----------------------|------|-----------|--------------------------------------------------|

It can be seen from the above table that the advantage of using MAPI protocol is obviously higher than that of SMTP/POP3. It is not only simple to send and receive mail, but also almost all office requirements can be realized through it, especially the promotion of RPC OVER HTTP application. Even if you leave the Office with NOTEBOOK, you can also work in the Internet as in the Intranet environment. But at the same time, it needs to be explained: because MAPI is the protocol for communication between Outlook and Exchange Server, it only supports Outlook series products on Windows platform at present, while SMTP/POP3 does not have so many restrictions. As long as the server side starts SMTP/POP3 service, it can be said that all the client software supports SMTP / POP3. The main reason is that the background of the MAPI and the SMTP / POP3 is different. The former is Microsoft's own product, and the latter is an international standard, supported by more products.

5. Security Requirements for Mail System in Practical Production Environment

Based on the previous acquaintance of the operation mechanism of SMTP / POP3 and MAPI, we can see that in terms of security, SMTP/POP3 faces much bigger challenges than MAPI. The main reasons are as follows:

In the early days of protocol customization, the security challenges faced by the Internet environment were not as complex and changeable as they are today, and more robust security mechanisms were not developed in order to facilitate and efficiently exchange mail. When we realized this problem, it was too late. However, we are fortunate that the upgraded version of ESMTP/POP4 has appeared and is being promoted, and the corresponding security design is a hot issues of research[1]-[4].

(2)Since SMTP/POP3 is an open protocol, it can be said that the interested technicians are familiar with its operating mechanism. Therefore, many people currently use the “legal” SMTP sending mechanism to carry out spam activities. According to international anti-spam organization observation: the world Internet mail flow of spam has reached 80%, and even in Europe, North America has reached 90%, which shows how harmful it is. But at the same time, we are glad that mail manufacturers at home and abroad have already cooperated with anti-spam organizations. Close cooperation has been carried out to curb spam, and governments have begun to value and support this work. At present, the most authoritative anti-spam organization in foreign countries is http://www.spamhaus.org/, and the domestic one is http://www.anti-spam.cn/. And then how to build a more secure e-mail system in such a complex Internet environment? I would like to use the
following diagram to illustrate that the overall thinking should be combined with comprehensive prevention, so as to build a secure email system:

![Diagram of Anti-spam Strategy]

**Figure 4. A Brief Sketch of the Anti-spam Strategy**

In figure①, ②, ③ is a simple mail receiving process: in stage ①, before server2 is ready to receive Server1, the sender's identity information (usually the information used includes the legality of IP address, the authenticity of email address, the standardization of DNS related information, etc.) will be checked with the information provided by domestic and foreign anti-spam organizations. If it does not conform to the requirements of the identity of the definition of Server2, then it carries on the corresponding processing operations, such as refused to receive, delete, feedback and other action. In the second stage, the recipient’s “intranet anti-mail detection system” will check the sender information with the information provided by the anti-spam organization at home and abroad again before receiving the mail sent by Server2, and carry out corresponding processing to strengthen the mail security. In the third stage, users usually install anti-spam software, which will monitor the user’s email environment at all times and deal with the email with its own “anti-spam database”.

Of course, this is just a simple diagram, and the actual environment will be much more complicated than this. Because it is difficult to use a standard to measure whether an email is “real spam” or not. And many innocent emails are treated as spam, which also affects the normal delivery of emails. Therefore, this double-edged sword often makes mail system administrators feel very distressed. After a long period of time, the system conducts repeated actual production environment tests on the level of “strict”, “high”, “medium”, and “low”, and finally the user’s complaints are calm. But this is not the end, because “spear” and “shield” are still developing, and they have not stopped. At the same time, they also bring commercial value to spam producers, and even some of them are also “spear” and “shield”.

6. The Practical Application of Combined with SMTP/POP3 and MAPI features

Combined with the advantages of SMTP / POP3 and MAPI, and according to the user’s requirements for mail security, in the actual system construction process, we customized a set of safe, efficient, stable and practical mail system for a public institution. The main system configuration is as follows:

(1) According to the overview in Table 1, it is not difficult to find that using MAPI will bring a lot of office convenience to users. By using the requirements of multi-functional applications, we can fully support the user's office, so in the intranet of this unit, we use the mail system of MAPI Technology: exchange server, which will allow users to work by mail as they wish and use other functions. At the same time, in order to allow other mobile users to enjoy such convenience when they leave the office, we extended the MAPI (RPC OVER HTTP) function of Exchange, and then...
published it through the gateway, so that outgoing users can use all the functions provided by Exchange Server anytime and anywhere, just like working in the office. What needs to be added is that if the VPN connection is used, the same effect can be achieved, and in this respect, it can be selected according to the actual environment.

(2) In the previous section, we only realized the mail communication and other auxiliary functions between our intranet employees. From the above mentioned concept that if we need to communicate with all users of the Internet by mail can only use servers that can support SMTP / POP3 very well. (It needs to be added that Microsoft Exchange server does not completely support SMTP / POP3, but because of Microsoft's own consideration, it focuses on the development and continuous improvement of Mapi, and simply "kidnaps" SMTP / POP3. Therefore, in the application development of SMTP / POP3, it is far less abundant than other manufacturers.) Therefore, we choose the current mainstream MDaemon server products, which are mainly characterized by rich, flexible management functions, and rich anti-spamp functions, and strong database portability. Then we put MDaemon server completely on the Internet to communicate smoothly with all SMTP / POP3 servers on the Internet, while at the same time ensuring email security and anti-spamp effects, the following key configurations are performed on MDaemon Server and Exchange Server:①retransmission the messages received by each mail account in MDaemon server and forward them to the corresponding mail account in exchange server.②Forward (relay) the mail sent by each mail account in exchange server to MDaemon server, and send the mail to Internet as MDaemon server.③Configuring anti-spamp policies on MDaemon Server and Exchange Server respectively. Through the ① and ② configurations, the real location of the mail server can be well hidden. Even if the MDaemon server is attacked or stolen, it will not affect the normal operation of the exchange server where the mail data is stored. At the same time, the SMTP / POP3 function can be enabled immediately as a temporary replacement scheme to provide mail services for users. And through the ③ point configuration, the user can maximize the spam filtering. In order to improve this, we will install and configure anti-spamp programs in each client to control spam flexibly and effectively.

(3) In the process of realizing the whole e-mail architecture, some security problems are also mentioned, but in the actual operating environment, the security requirements analysis, security policy design and implementation process should be carried out according to the user application system. For the nature of the institution and the dependence of the user on the mail system, a full range of dynamic design and dynamic management is required(The so-called dynamic, that is, the existing security policy is updated and managed at any time according to various human factors and non-human factors changes in the internal and external networks). The following diagram is a common security policy reference model. Among the eight security policy requirements, we used the last seven items. Since the “computer room electromagnetic shielding” is usually used in a highly confidential machine room, it is not used here.

Figure 5. A Schematic Diagram of the Mail System Architecture of an Institution
The last seven items of use are as follows:

1) The “computer room video surveillance” mainly uses the monitoring system to record the 24-hour video of the personnel entering and leaving the computer room, so that the personnel can investigate and collect evidence in case of human sabotage.

2) The “gateway configuration audit” is mainly used to periodically perform security audits and log check on the gateway configuration to prevent illegal users from intruding into the intranet to threaten the mail system.

3) “Server hardware test” mainly checks and analyzes the running status of all hardware on the server regularly, repairs in advance, replaces or upgrades accessories.

4) “Operating system security audit” mainly includes permission audit of all system accounts, update of patches, analysis of logs, early detection and elimination of potential risks.

5) “Mail system security audit” is mainly used to audit permissions of all mail system accounts, update patches, analyze logs, detect and eliminate hidden risks in advance.

6) “Anti-virus and anti-spam strategy” mainly configures and manages the anti-virus and anti-spam filtering of the system.

7) The final “system and mail backup strategy” is the last layer of protection against disaster recovery. If the previous protection fails or an irresistible force occurs, the existing backup files can be used for rapid recovery. Therefore, the last layer of protection is very important in the whole security policy, and it is also used high frequently in actual environment. Therefore, we specially adopt the Veritas backup system of Symantec company, which is also very convenient to use. Although it is an invisible burden to managers, this kind of investment is very necessary for managers!

7. Conclusion
This paper introduces the current mainstream e-mail protocol. Combined with the security strategies and application requirements, the thesis elaborates the hierarchical security management requirements of today’s mail system by its practical application in production environment.

Reference
[1] YIN Chen , ZHANG Ning. Potential security risk of the E-mail system and its prevention solutions[J]. Journal of Nanjing University of Technology (NATURAL SCIENCE EDITION),2005,(04)
[2] YU Chuying, Li Jianzhong. Design and Implementation of A Sescure Mail Server which Supports A Great Number of Users[J]. Journal of Shantou University(NATURAL SCIENCE EDITION), 2005,(04)
[3] Ji Xing, Chen Xiaomin,Gu Xunrang. Model of Secure Email System Based on Double Authentications[J]. Computer Engineering, 2005, (22).
[4] Xu Li. Security Defense of Enterprise Mail System[J]. China Computer&Network, 2004,(17)