فصل دوم

مفاهیم پایه

این فصل به مفاهیم پایه ای می‌پردازد. نحوه عملکرد سیستم پست الکترونیکی، پروتکل‌های پست الکترونیکی من جمله pop3، imap، smtp و mime و همچنین سرآیندهای پست الکترونیکی شرح داده می‌شوند. در انتهای این فصل انواع حملات و نتایج آنها را بررسی می‌کنیم تا در فصل بعد از آن استفاده کنیم.

۲-۱ اصول پست الکترونیکی

در این قسمت به نحوه عملکرد سیستم پست الکترونیکی می‌پردازیم و اجزای مختلف این سیستم را بررسی می‌کنیم.

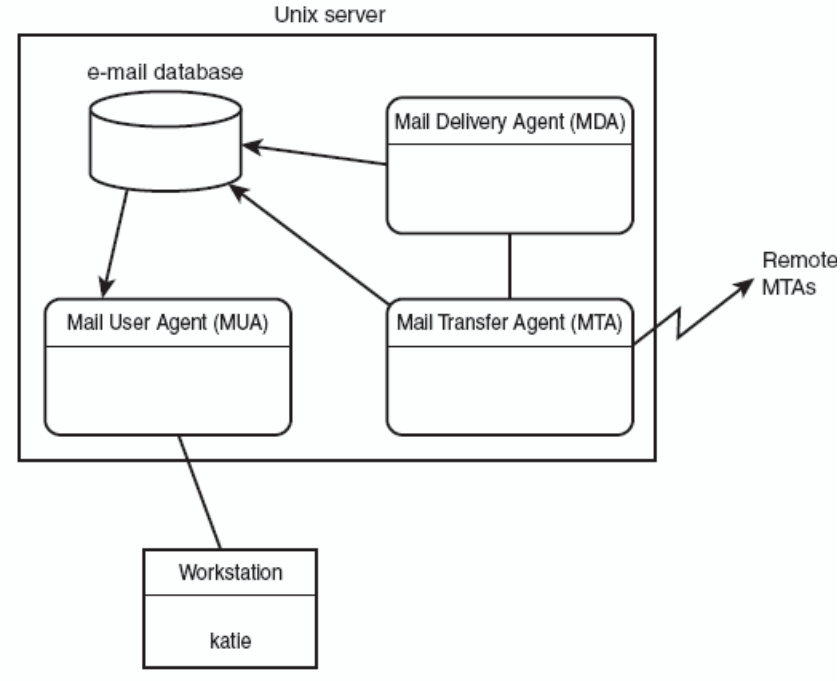
۲-۱-۱ سیستم‌های پست الکترونیکی لینوکسی[1]

از دهه ۱۹۷۰ به بعد، سیستم عامل لینوکس به یکی از محبوب‌ترین سیستم عامل‌های دنیا تبدیل شد[2]. اکثر پست الکترونیکی سرورهای اینترنتی، از سرورهای لینوکسی استفاده می‌کنند.

یکی از مهم‌ترین ابداعات سیستم عامل لینوکس، ماژولار کردن نرم افزارهاست. بجای داشتن یک برنامه غول پیکر که کنترل کردن تمام قطعات مورد نیاز برای انجام یک کار را انجام می‌دهد، برنامه‌های کوچک‌تری ایجاد می‌شود تا با یکدیگر بتوانند کار کنند. هر برنامه قطعات کوچک‌تری را کنترل می‌کند تا تمام کار در نهایت انجام شود. این فلسفه در سیستم سرورهای پست الکترونیکی لینوکسی نیز استفاده می‌شود. وظایف پست الکترونیکی به چند قطعه تقسیم شده و به برنامه‌های مجزا تخصیص داده می‌شود. شکل ۲-۱ نشان می‌دهد که چگونه اکثر سرورهای پست الکترونیکی متن باز[2]، وظایف پست الکترونیکی را در یک سیستم لینوکسی ماژوله بندی کرده اند.

---

[1] linux
[2] Open Source



شکل (۲-۱) : محیط ماژولار پست الکترونیکی در یونیکس

همان‌طور که در شکل ۲-۱ می‌بینید، یک سیستم پست الکترونیکی لینوکسی از سه بخش عمده زیر تشکیل شده است[23]:

- The Mail Delivery Agent (MDA)

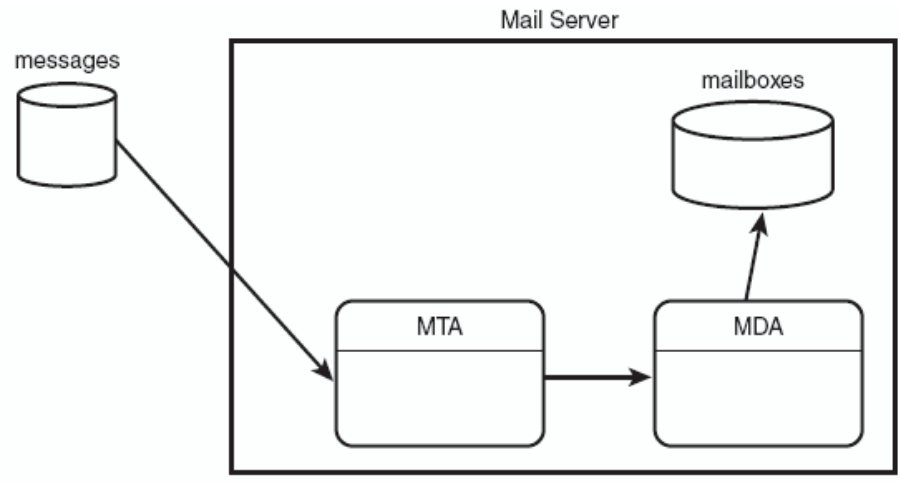
- The Mail Transfer Agent (MTA)

- The Mail User Agent (MUA)

البته برخی از بسته‌های سرور پست الکترونیکی موجود، نقش MTA و MDA را تلفیق کرده‌اند و برخی دیگر نقش MDA و MUA را تلفیق کرده‌اند.

MDA

وظیفه MDA، تحویل دادن پیام‌ها به کاربران محلی می‌باشد[23]. MDA بر روی پیام‌هایی تمرکز دارد که مقصدشان، کاربر بر روی پست الکترونیکی سرور محلی می‌باشد. MDAپیام‌ها را از MTA می‌گیرد، به MDA تحویل می‌دهد و تعیین می‌کند که پیام‌ها چگونه برسند.



شکل (۲-۲) : استفاده از MDA در سرور پست الکترونیکی

سه ویژگی عمده MDA عبارتند از:

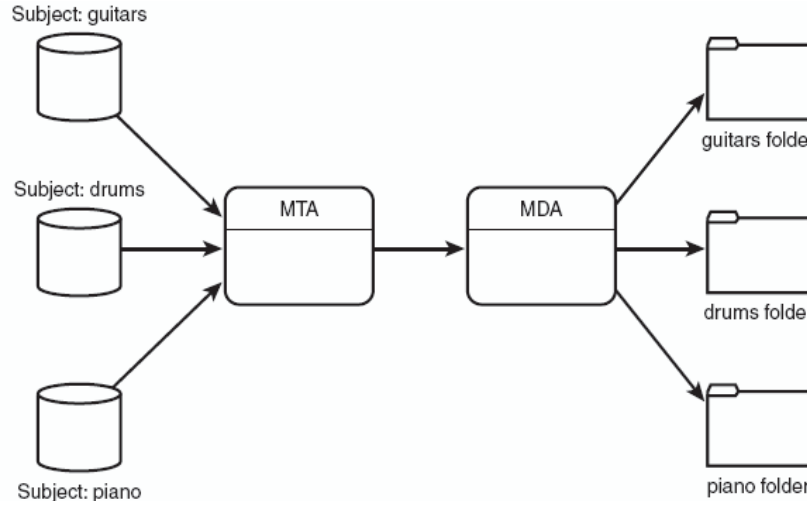
- فیلترگذاری خودکار پست الکترونیکی[۱]
- پاسخگویی خودکار پست الکترونیکی[۲]
- مقداردهی اولیه برنامه توسط پست الکترونیکی[۳]

فیلترگذاری خودکار پست الکترونیکی

این قابلیت باعث می‌شود که درون پیام‌های ورودی جستجو کنیم و هنگامی که یک عبارت منطبق شد، پیام را درون پوشه خاصی در ناحیه پست الکترونیکی، ذخیره کنیم[23]. همچنین این قابلیت می‌تواند پیام‌های ناخواسته را فیلتر کند.

---

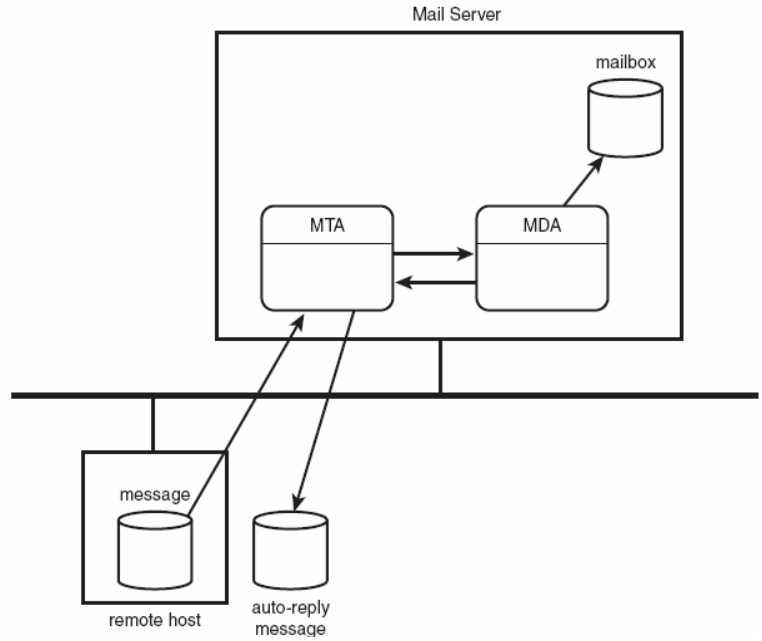
[1] Automatic Mail Filtering
[2] Automatic Mail Replying
[3] Automatic Program Initialization By Mail



شکل (۲-۳) : فیلترگذاری خودکار پست الکترونیکی

پاسخگویی خودکار پست الکترونیکی

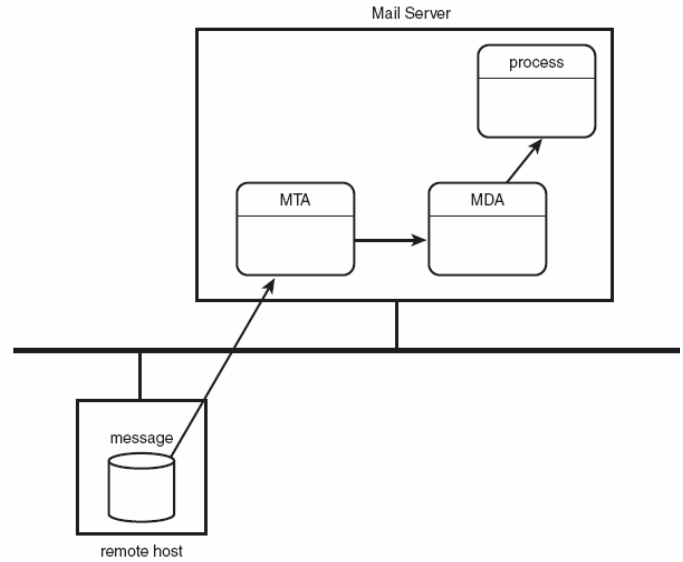
برنامه‌های MDA به کاربران پست الکترونیکی اجازه می‌دهند تا پیام‌های پاسخ را بر اساس سرآیند پیام، بفرستند[23].



شکل (۲-٤) : پاسخگویی خودکار پست الکترونیکی

مقداردهی اولیه برنامه توسط پست الکترونیکی

برنامه‌های MDA به کاربران پست الکترونیکی اجازه می‌دهند تا کاربران پست الکترونیکی، برنامه ای را بر اساس سرآیند پیام در یافتی، اجرا کنند[23].



شکل (۲-۵) : مقداردهی اولیه برنامه توسط پست الکترونیکی

MTA

MTA مسئول کنترل و تعامل با پیام‌های پستی ورودی و خروجی می‌باشد[23]. برای هر پیام پستی خروجی، MTA آدرس مقصد گیرنده را مشخص می‌کند. اگر مقصد، ماشین محلی باشد، MTA آن را به صندوق پستی[1] محلی یا MDA محلی، تحویل می‌دهد. ولی اگر مقصد سرور پست الکترونیکی راه دور[2] باشد، MTA یک اتصال با MTA راه دور، برقرار می‌کند. برای انتقال پیام‌ها، پروتکل‌های مختلفی استفاده می‌شود ولی رایج‌ترین آنها SMTP می‌باشد.

سه ویژگی عمده که یک MTA بایستی از آنها به خوبی پشتیبانی کند :

- امنیت

[1] mailbox
[2] remote

- آسانی پیکربندی

- سرعت پردازش پیام

معروف‌ترین بسته‌های پست الکترونیکی لینوکسی موجود، عبارتند از[2]:

- Sendmail

- Qmail

- Postfix

Sendmail محبوبیتش را به این خاطر بدست آورد که بسیار روان است. Qmail ایده برنامه پست الکترونیکی ماژولار را اخذ کرد و MTA خود را به صورت ماژولار نوشت. درQmail نیاز دارید که User-IDهای متفاوتی بر روی سرور پست الکترونیکی، اضافه کنید. هر ماژول، تحت یک User-id متفاوت، اجرا می‌شود. اگر نفوذ گر، یک ماژول را تحت سلطه خود در آورد، بر روی ماژول‌های دیگر، تأثیری نخواهد داشت. ویژگی امنیتی qmail، بهترین مزیت qmail محسوب می‌شود.

قابلیت اعتماد، ویژگی دیگر qmail می‌باشد. به صورتی که پیام موجود در صف پیام‌ها، گم نمی‌شود. همچنین qmail می‌تواند از ویژگی Maildir style بهره گیرد که از گم شدن و خراب شدن پیام‌ها جلوگیری می‌کند.

Qmail از فایل‌های پیکربندی گوناگونی استفاده می‌کند که هر کدام برای یک ویژگی به وجود آمده‌اند. این مانع به وجود آمدن یک فایل پیکربندی بزرگ می‌شود[12].

درPostfix نیاز دارید که User-IDهای متفاوت را بر روی سرور پست الکترونیکی، اضافه کنید. بر خلاف qmail که از User-Id مجزا، برای هر ماژول استفاده می‌کند، postfix هر ماژول را تحت یک user-id، اجرا می‌کند. به‌هرحال اگر نفوذ گری، یک ماژول را تحت سلطه خود در آورد، بر روی ماژول‌های دیگر، تأثیری نخواهد داشت.

یکی از بهترین ویژگی‌های postfix، سادگی آن است. بجای داشتن یک فایل پیکربندی پیچیده بزرگ یا فایل‌های پیکربندی فراوان کوچک، دو فایل پیکربندی وجود دارد که برای اجرا شدن، از کاربر پارامتر می‌گیرند[12].

در فصل مخاطرات، به شرح گسترده تری از این سه بسته پست الکترونیکی خواهیم پرداخت و مخاطرات آنها را بررسی می‌کنیم.

MUA

MUAها پیام‌ها را دریافت نمی‌کنند. آنها فقط پیام‌هایی را که در صندوق پستی کاربر هستند، نمایش می‌دهند[23]. همچنین بسیاری از MUAها، قابلیت ایجاد پوشه‌های متفاوت را برای ذخیره پیام‌ها، به کاربر می‌دهند.

تفاوت برنامه‌های MUA، بر دو اصل استوار است: محل ذخیره پیام‌ها و چگونگی نمایش پیام‌ها.

محل ذخیره پیام‌ها

دو فلسفه برای محل ذخیره سازی پیام‌ها وجود دارد[23]. فلسفه اول می‌گوید که وقتی کاربر پست الکترونیکی خود را می‌خواند، آن پیام از سرور بارگذاری[1] شده و بر روی سیستم کاربر قرار گیرد. اشکال کار این فلسفه این است که کاربر اگر از روی کامپیوتر دیگری، پست الکترونیکی خود را چک کند، چون پیام از روی سرور، حذف شده است قادر نخواهد بود پیام را بخواند. ولی خوبی این فلسفه این است که کار مدیر سیستم[2] را کم می‌کند. در فلسفه دوم پیام و پست الکترونیکی، از روی سرور پاک نمی‌شود و تنها یک کپی از آن به کاربر ارسال می‌شود و در این صورت، کاربر قادر است از روی هر کامپیوتری پست الکترونیکی خود را بخواند. ولی در عین حال، مشکل این روش، بار سنگینی است که بر روی دوش مدیر سیستم قرار می‌دهد.

چگونگی نمایش پیام‌ها

MUAها به گونه ای متفاوت با یکدیگر، پیام‌ها را نمایش می‌دهند[23]. برخی فقط به حالت متن ساده، پیام‌ها را نمایش می‌دهند. ولی برخی قابلیت نمایش بر اساس اسناد HTMLی که گرافیک را پشتیبانی می‌کنند، را نیز دارند. برای ایجاد این قابلیت بسیاری از MUAها، MIME را پشتیبانی می‌کنند. MIME این قابلیت را ایجاد می‌کند تا نسخه‌های مختلفی از پیام، وجود داشته باشد. در نهایت، کار MUA این است که MIME، پیام را نگاه می‌کند، اگر حالت متنی ساده باشد، آن را به خروجی متنی می‌دهد و اگر MIME، بیانگر حالت گرافیکی باشد، MUA آن را به خروجی گرافیکی، برای نمایش به کاربر می‌دهد.

---

[1] download
[2] administrator

۲-۱-۲ پروتکل‌های پست الکترونیکی

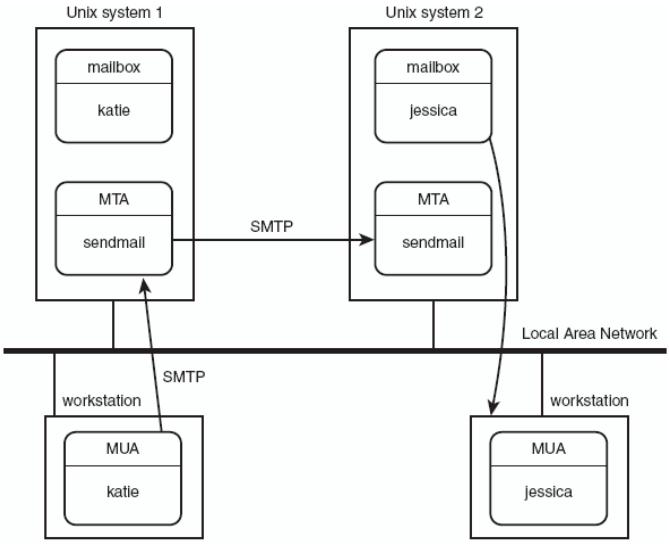
در قسمت‌های قبلی به معرفی MDA، MTA و MUA پرداختیم و وظیفه هر یک را بررسی کردیم. اکنون پروتکل‌های مورد استفاده در MDA، MTA و MUA را معرفی اجمالی کرده و شرح آنها را به قسمت‌های بعد کتاب موکول می‌کنیم.

پروتکل‌های MTA

برنامه‌های MTA می‌بایست قادر باشند با MTAهای راه دور دیگر، ارتباط برقرار کنند تا بتوانند پیام‌ها را منتقل نموده و همچنین اطلاعات مورد نیاز برای شناسایی پیام‌های راه دور را منتقل کنند. این کار توسط پروتکل smtp یا esmtp[1] انجام می‌گیرد.

پروتکل SMTP

پروتکل smtp به عنوان متد اولیه برای انتقال پیام‌ها در اینترنت، توسط سرورهای MTA ایجاد شد[25][24]. smtp از دستورات ساده‌ای برای ایجاد یک اتصال به MTA و انتقال اطلاعات و داده‌ها استفاده می‌کند. شکل ۲-٦ نمایشگر این مسئله است.



شکل (۲-٦) : اتصال smtp بین دو ایستگاه کاری

[1] Extended Simple Mail Transfer Protocol