امنیت پست الکترونیکی

سید حسین رجاء

انتشارات پندار پارس

سرشناسه : رجاء، سیدحسین، 1362 -
عنوان و نام پدیدآور : امنیت پست الکترونیکی/ حسین رجاء.
مشخصات نشر : تهران : پندار پارس: مانلی، 1390.
مشخصات ظاهری : xi، 160 ص.: مصور، نمودار.
شابک : 978-600-6529-00-4 :45000 ریال
وضعیت فهرست نویسی : فیپا
موضوع : پست الکترونیکی -- پیش‌بینی‌های ایمنی
موضوع : پست الکترونیکی
رده بندی کنگره : TK5105/139073 8الف3ر /
رده بندی دیویی : 692/004
شماره کتابشناسی ملی : 2596427

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوچه رشتچی، شماره 14، واحد 16 **www.pendarepars.com**

تلفن: 66572335 - تلفکس: 66926578همراه: 09122452348 **info@pendarepars.com**

نام کتاب : **امنیت پست الکترونیکی**

ناشر : **انتشارات پندار پارس ناشر همکار: مانلی**

تالیف : **سید حسین رجاء**

چاپ نخست : **زمستان 90**

شمارگان : **1000 نسخه**

طرح جلد : **محمد اسماعیلی هدی**

لیتوگرافی، چاپ، صحافی : **ترام‌سنج، فرشیوه، خیام**

قیمت : **4500 تومان** **شابک** : 978-600-6529-00-4

به‌نام خداوند جان و خرد

پیش‌گفتار

فن‌آوری پست الکترونیکی، با توجه به استفاده روز افزون از آن در عصر اطلاعات، به یکی از ملزومات زندگی بشر، برای مکاتبات و مراسلات بین افراد، تبدیل شده است. با توجه به این مسئله، نکته قابل اهمیت در مورد پست الکترونیکی این است که سرور و سرویس پست الکترونیکی و پیام‌ها و مکاتبات رد و بدل شده بین افراد، دارای امنیت قابل قبولی باشد تا افراد با اطمینان خاطر از این فن‌آوری، استفاده کنند.

ابتدا به بررسی نحوه عملکرد سیستم پست الکترونیکی و معرفی پروتکل‌های آن می‌پردازیم. با بررسی صورت گرفته مشخص شد که برای ارزیابی مخاطرات سیستم پست الکترونیکی، روش خاصی ارائه نشده است.

با بررسی روش‌های ارزیابی سایر سیستم‌ها و نقاط ضعف و قوت آنها، از روش آقای کانوری که روشی برای ارزیابی در حیطه امنیت شبکه می‌باشد، برای ارزیابی مخاطرات پست الکترونیکی استفاده می‌کنیم. با ارائه جداول خاص و استفاده از فرمول کانوری، به بررسی مخاطرات می‌پردازیم که معیار کار ما برای ارزیابی مخاطرات می‌باشد. پس از آن، به معرفی و بحث بر روی مخاطرات موجود در سرور و سرویس پست الکترونیکی می‌پردازیم.

سپس به مکانیزم‌های امن کردن مخاطرات سرور و سرویس پست الکترونیکی می‌پردازیم. میزان کاهش مخاطره را با به‌کارگیری مکانیزم‌ها و راهکارهای موجود، به صورت مطالعه موردی و به وسیله آزمایش‌هایی بدست می‌آوریم. در نهایت و در فصل نتیجه گیری، پست الکترونیکی را از لحاظ امنیت و نوع سازمان، دسته‌بندی کرده و مکانیزم‌های ایمن سازی آن را ارائه می‌دهیم.

مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه‌مند به حوزه پست الکترونیکی می‌باشند.

این کتاب با توجه به مطالعات علمی و تجربه فنی نگارنده در سرورهای پست الکترونیکی Qmail، Postfix، Sendmail، Exim و Exchange Server تألیف شده است. بدیهی است که مطالب این کتاب، خالی از اشکال نمی‌باشد و نظرات خوانندگان، ما را در بهبود سطح علمی و فنی کتاب، یاری خواهد کرد؛ لذا از خوانندگان محترم درخواست می‌شود هرگونه پیشنهاد و انتقادی در جهت بهبود و اصلاح محتویات کتاب را به آدرس الکترونیکی hosseinraja@dspri.com ارسال نمایند.

در نهایت بر خود لازم می‌دانم از موسسه تحقیقاتی داده‌سنجی پیشرفته، جناب مهندس مقدسی و جناب مهندس سید محمد رجاء، که اینجانب را در مراحل مختلف تألیف این کتاب یاری رسانده‌اند، کمال تشکر را داشته باشم.

سید حسین رجاء

پاییز 1390

فهرست

فصل اول

مقدمه

1-1 طرح مسئله

سال‌ها پیش، زمانی که پست الکترونیکی و رایانه‌ای وجود نداشت و سیستم مراسلات به صورت کاغذی و به شکل نامه بود، افراد از فاش شدن محتوای نامه خود هراس داشتند. مسائل مالی، از بین رفتن آبرو و حیثیت اشخاص، مسائل سیاسی، اجتماعی و فرهنگی از جمله دلایلی بودند که فکر امن کردن مراسلات و سیستم آن را به وجود آورد.

با پیشرفت علم و ورود به عرصه رایانه، بشر سیستم جدیدی برای مراسلاتش به وجود آورد. سیستم جدید که همان پست الکترونیکی بود، کار نامه کاغذی را با سرعتی بسیار بالاتر انجام می‌داد. همانند سیستم سنتی، مسئله‌ای که وجود داشت، بحث امنیت پیام‌های رد و بدل شده و همچنین امنیت سیستم ارسال مراسلات بود. البته اهمیت امنیت سیستم الکترونیکی، نسبت سیستم سابق، فزونی می‌یابد. در عصر اطلاعات، بسیاری از تراکنش‌ها چه مالی و چه غیرمالی، به صورت الکترونیکی انجام می‌شوند، تبادل داده‌ها از طریق اینترنت صورت می‌گیرد و سرقت و دست‌کاری و لو رفتن داده‌ها می‌تواند هزینه ای گزاف از حیث آبرویی، مالی، سیاسی، اقتصادی و فرهنگی داشته باشد.

در حوزه مراسلات الکترونیکی که پست الکترونیکی باشد، نیز این مسئله وجود دارد و بسی حائز اهمیت است[1].

در حوزه پست الکترونیکی، پروتکل‌ها و مکانیزم‌های مختلفی وجود دارد و درون این پروتکل‌ها و مکانیزم‌ها، انواع مخاطرات وجود دارد. مسئله مهم آن است که:

- مخاطرات را بشناسیم.
- چگونه این مخاطرات را ارزیابی کنیم.
- چگونه این مخاطرات را، از طریق مکانیزم‌های موجود، ایمن نماییم و مخاطره را کاهش دهیم.

- راهکار ایمن سازی پست الکترونیکی، بر اساس تقسیم‌بندی سازمان‌ها و ارزیابی صورت گرفته، ارائه دهیم.

افرادی مانند بولم[2] و اسمیت[12]، مخاطراتی را که برای پست الکترونیکی وجود دارند، به دو دسته کلی مخاطرات سرور پست الکترونیکی[1] و مخاطرات سرویس پست الکترونیکی تقسیم‌بندی کرده‌اند. در این کتاب، از این دسته‌بندی استفاده می‌کنیم. میزان مخاطرات را با فرمولی که ارائه داده ایم، بررسی کرده و میزان کاهش درصد مخاطره را، با راهکارها و مکانیزم‌های موجود، محاسبه می‌کنیم.

در مخاطراتی که برای سرور پست الکترونیکی وجود دارد می‌توان به موارد زیر اشاره کرد:

- فعال نبودن برخی ویژگی‌ها بر روی سرور پست الکترونیکی، می‌تواند باعث به مخاطره افتادن سرور و سوء استفاده از آن گردد. این ویژگی‌ها را بررسی کرده و نحوه فعال کردن آنها را بیان می‌کنیم.
- هنگامی که یک سرور پست الکترونیکی، تلاش می‌کند یک نامه مرتبط به سرور پست الکترونیکی دیگر را، به سرور پست الکترونیکی بفرستد و سرور، پیام را پذیرفته و به سرور پست الکترونیکی دیگر بفرستد، Open Relay اتفاق می‌افتد. اما سوء استفاده از این مسئله، موجب شده است که تمهیداتی در نظر گرفته شود تا جلوی این مسئله گرفته شود[3]. در اینجا مکانیزم‌های رله کردن گزینشی، ارائه می‌شود.
- با مواجه شدن با حجم انبوه پست‌های spam، ممکن است سرور از کار بیفتد[4]. از ابتدای تولد اینترنت، متدهای زیادی برای جلوگیری از spam، معرفی شده است[5]. سه متد کلی برای بلوک کردن spamها، تا به حال معرفی شده است.
- ویروس‌ها عنصر خطرناکی هستند. اثر تخریبیشان بسیاری از مدیران شبکه را مجبور کرده است تا دنبال راهی برای متوقف کردن آنها بیابند[6].

در مخاطراتی که برای سرویس پست الکترونیکی وجود دارد، می‌توان به موارد زیر اشاره کرد:

- نفوذکنندگان و spammerها تکنیک‌های مختلفی استفاده می‌کنند تا اطلاعاتی در مورد سیستم پست الکترونیکی و کاربران آن بدست آورند، ولی تکنیک‌هایی وجود دارد که کمک می‌کند تا با این مشکل، مبارزه کنید. با غیر فعال کردن برخی دستورات و همچنین نصب فایروال پست الکترونیکی، می‌توانید جلوی حملات و کاوشگری‌ها را بگیرید.

---

[1] Email Server

- متد رایج اجازه دادن به میزبان‌های راه دور، که بتوانند پیام‌ها را از طریق پست الکترونیکی سرور رله کنند، استفاده از یک متد تایید هویت می‌باشد. متد تایید هویت، به صورت منحصربه‌فرد می‌تواند پست الکترونیکی سرور راه دور را مشخص کند، به نحوی که پست الکترونیکی سرورتان بتواند مشخص کند اجازه دارد پیام‌ها را رله کند یا خیر. یکی از مشهورترین متدهای تایید هویت اتصالات شبکه، SASL[1] می‌باشد که به بررسی آن می‌پردازیم[8][7].
- بسیاری از بسته‌های MTA[2] برای دریافت پیام‌ها، از پروتکل‌های pop3[3] یا imap[4]بهره می‌گیرند[10][9]. مشکل این پروتکل‌ها این است که آنها اطلاعات را به صورت متن اسکی، بدون هیچ رمز نگاری ارسال می‌کنند. برای کمک کردن به این‌گونه مسائل، پروتکل SSL[5] به وجود آمد که به میزبان‌های شبکه اجازه می‌دهد تا داده‌ها را قبل از ارسالشان در طول شبکه، رمز کنند[11]. در این کتاب به شرح این پروتکل و پروتکل‌های مشابه آن می‌پردازیم.
- بسیاری از شرکت‌ها، نرم افزار کلاینتی پست الکترونیکی تحت وب، منتشر کرده‌اند که کاربر را قادر می‌سازد از طریق وب، پست الکترونیکی خود را بخواند. پیاده سازی‌های بسیار زیاد و محبوبی مانند Hotmail، Yahoo! و Gmail وجود دارد که کاربران می‌توانند از طریق پویش گر وب[6]، به سرور پست الکترونیکی متصل شوند[12]. Webmail به خودی خود امن نیست و باید راهکارهای ایمن سازی را برای آن پیاده سازی کنیم.

با ارائه جدول و فرمولی خاص، به سنجش و بررسی مخاطرات می‌پردازیم که در اخذ راهکارهای امنیتی کمک قابل توجهی می‌کند.

---

[1] Simple Authentication and Security Layer
[2] Mail Transfer Agent
[3] Post Office Protocol version 3
[4] Internet Message Access Protocol
[5] Secured Socket Layer
[6] Web Browser

2-1 اهداف

مضامین اصلی که در کتاب مورد بحث قرار خواهد گرفت، به شرح زیر است:

- بررسی نحوه عملکرد سیستم پست الکترونیکی.
- بررسی و معرفی پروتکل‌های پست الکترونیکی، همانند pop، imap، smtp[1] و mime[2]
- بررسی مخاطرات موجود برای سرور پست الکترونیکی.
- بررسی مخاطرات موجود برای سرویس پست الکترونیکی.
- ارائه جدول مخاطره و فرمول خاص، برای محاسبه مخاطرات.
- بررسی راهکارها و مکانیزم‌های تأمین امنیت سرور پست الکترونیکی.
- بررسی راهکارها و مکانیزم‌های تأمین امنیت سرویس پست الکترونیکی.
- بررسی میزان تأثیر راهکارها و مکانیزم‌ها و محاسبه میزان تقلیل مخاطره، به صورت موردی.
- ارائه دسته‌بندی پست‌های الکترونیکی، چگونگی ایمن سازی آنها و نتیجه گیری.

3-1 پرسش‌ها و فرضیات

مسئله‌ای که در قسمت طرح مسئله ارائه شد، مجدداً برای تاکید ذکر می‌کنیم:

در حوزه پست الکترونیکی، پروتکل‌ها و مکانیزم‌های مختلفی وجود دارد و درون این پروتکل‌ها و مکانیزم‌ها انواع مخاطرات وجود دارد. مسئله مهم آن است که:

- مخاطرات را بشناسیم.
- چگونه این مخاطرات را ارزیابی کنیم.
- چگونه این مخاطرات را، از طریق مکانیزم‌های موجود، ایمن نماییم و مخاطره را کاهش دهیم.

---

[1] Simple Mail Transfer Protocol
[2] Multipurpose Internet mail extensions

- راهکار ایمن سازی پست الکترونیکی، بر اساس تقسیم بندی سازمان‌ها و ارزیابی صورت گرفته، ارائه دهیم.

حال با توجه به مسئله موجود، پرسش‌ها و فرضیاتی پدید می‌آید که بایستی آنها را مطرح کنیم.

پرسش‌های موجود برای این تحقیق، عبارتند از:

- آیا مخاطرات موجود در پروتکل‌ها و مکانیزم‌های پست الکترونیکی را می‌توان شناخت؟
- آیا می‌توان این مخاطرات را ارزیابی کرد؟
- آیا روشی برای ارزیابی مخاطرات پست الکترونیکی وجود دارد؟
- آیا می‌توان از روش‌های ارزیابی موجود در دیگر سیستم‌ها، برای ارزیابی پست الکترونیکی استفاده نمود؟
- نقاط قوت و ضعف روش‌های ارزیابی در سیستم‌های دیگر چیست؟
- آیا پارامترهای موجود در ارزیابی مخاطرات سایر سیستم‌ها، با مکانیزم‌ها و پروتکل‌های سیستم پست الکترونیکی نیز رابطه دارند؟
- آیا می‌توان مخاطرات موجود در پست الکترونیکی را با روش‌های موجود، ایمن نمود؟
- آیا می‌توان میزان کاهش مخاطره را پس از ایمن سازی محاسبه کرد؟
- آیا می‌توان راهکاری جامع بر اساس تقسیم بندی سازمان‌ها و میزان مخاطره ارائه داد؟

فرضیه‌های موجود در این کتاب، عبارتند از:

- سیستم پست الکترونیکی که دارای مکانیزم‌ها و پروتکل‌های مختلفی می‌باشد. این مکانیزم‌ها و پروتکل‌ها، حاوی مخاطراتی می‌باشند و می‌توان این مخاطرات را شناسایی کرد.
- می‌توان مخاطرات موجود در سیستم‌های پست الکترونیکی را ارزیابی کرد.
- می‌توان از روش‌های ارزیابی مخاطراتی که در سایر سیستم‌ها وجود دارد، برای سیستم پست الکترونیکی نیز استفاده نمود.
- پارامترهای موجود در ارزیابی مخاطرات سایر سیستم‌ها، با مکانیزم‌ها و پروتکل‌های سیستم پست الکترونیکی نیز رابطه دارند.
- می‌توان مخاطرات موجود در پست الکترونیکی را با روش‌های موجود ایمن نمود.

- می‌توان میزان کاهش مخاطره را، پس از ایمن سازی محاسبه کرد.
- می‌توان راهکاری جامع بر اساس تقسیم بندی سازمان‌ها و میزان مخاطره، ارائه داد.

4-1 تحقیقات مرتبط

در این کتاب، پس از بررسی مخاطرات سرور و سیستم پست الکترونیکی، با ارائه جدول و فرمولی خاص، مخاطرات را مورد ارزیابی قرار می‌دهیم. با بررسی صورت گرفته، در حوزه مخاطرات سیستم‌های پست الکترونیکی و ارزیابی آن، روش خاصی ارائه نشده است اما در حوزه مخاطرات سیستم‌های دیگر، تحقیقاتی صورت گرفته و روش هایی ارائه شده است.

استون برنر و همکارانش، در حوزه مخاطرات سیستم‌های بر مبنای IT، فرمولی ارائه داده‌اند که بسیاری از افراد در ارزیابی مخاطرات، از آن استفاده می‌کنند. این فرمول از دو پارامتر احتمال کلی[1] و تأثیر[2] استفاده می‌کند[13]. فرمول در قالب توصیه‌نامه‌ای از سازمان NIST[3] ارائه شده است و افراد مختلف با تغییر نام پارامترها، فرمول را به همان شیوه ارائه شده، استفاده می‌کنند. برای مثال در حوزه امنیت نرم افزار و شبکه، مک گراو[4] فرمولی ارائه داده است که از دو پارامتر انتظار کاهش تنها[5] و نرخ رخداد در سال[6]، برای محاسبه مخاطره استفاده می‌کند[14]. این فرمول، در واقع همان پارامترهای تغییر نام یافته‌ای است که در فرمول استون برنر و همکارانش ارائه شده است. البته افرادی وجود دارند که از فرمول‌های دیگر و پارامترهای اضافه تری استفاده کرده‌اند. برای مثال در حملات SQL injection، مادان[7] و همکارانش فرمولی برای ارزیابی مخاطره، ارائه داده‌اند که از 5 پارامتر پتانسیل خرابی[8]، قابلیت تکثیر[9]، قابلیت استفاده[10]، کاربران مورد تأثیر[11] و قابلیت شناسایی[12]

---

[1] LIKELIHOOD
[2] impact
[3] National Institute of Standards and Technology
[4] McGraw
[5] single loss expectancy
[6] Annualized rate of occurrence
[7] Madan
[8] Damage Potential
[9] Reproducibility
[10] Exploitability
[11] Affected User
[12] Discoverability

استفاده می‌کند[15]. شرکت سیسکو[1] برای ارزیابی مخاطرات در IPSهای سری 4200، از 3 پارامتر شدت[2]، وفاداری[3] و نمره ارزش هدف[4] استفاده می‌کند[16].

کانوری فرمولی برای محاسبه مخاطرات حملات معروف شبکه ای، مانند سیل ریزی[5]، دست‌کاری[6]، جعل[7] و دیگر حملات رایج ارائه داده است[17]. این فرمول از 4 پارامتر سختی شناسایی[8]، آسانی استفاده[9]، فراوانی[10] و تأثیر[11] استفاده می‌کند.

در این کتاب از فرمولی که کانوری برای ارزیابی مخاطره ارائه داده است، در ارزیابی مخاطرات پست الکترونیکی استفاده کرده‌ایم. پارامترهای مناسب و همچنین وزن دار بودن پارامترها، در این انتخاب نقش مهمی داشته است. پس از آن، به روزترین و جدیدترین مکانیزم‌های تأمین امنیت سرور و سیستم پست الکترونیکی را مورد بررسی قرار داده‌ایم و با انجام آزمایش‌هایی، میزان کاهش این مخاطرات را به صورت موردی بدست آورده‌ایم. در نهایت، پست الکترونیکی را از لحاظ مخاطره و سازمان‌ها دسته بندی کرده و با توجه به نتایج بدست آمده از فصل قبل، راهکارهای ایمن سازی ارائه داده‌ایم.

از آنجا که این کتاب، ترکیبی از مباحث مختلف در حوزه پست الکترونیکی و راهکارهای ایمن سازی سرور و سرویس پست الکترونیکی می‌باشد، می‌توان آن را نگاهی جامع به مبحث امنیت در سرور و سرویس پست الکترونیکی دانست. البته کتاب‌ها و مقالاتی در این زمینه وجود دارد که هر یک وارد یک بحث جزئی از مباحث امنیت پست الکترونیکی شده‌اند.

به عنوان مثال در حوزه رمزنگاری[12] پست الکترونیکی، جین و همکارانش به تأمین امنیت پست الکترونیکی از طریق رمزنگاری و فشرده سازی[13]، راهکاری ارائه داده‌اند[18]. فارل بحثی در عدم

---

[1] Cisco
[2] Sevirity
[3] Fidelity
[4] Target Value-Rating
[5] flooding
[6] manipulate
[7] spoof
[8] Detection difficulty
[9] Ease of Use
[10] Frequency
[11] Impact
[12] Encription
[13] Compressing

نیاز به رمزنگاری پست الکترونیکی ارائه داده است[19]. در حوزه کرم‌های[1] پست الکترونیکی، زو مدلی برای کرم‌های پست الکترونیکی و مقابله با آن، ارائه داده است.[20] همچنین در حوزه spam، دآمبرا تحقیقاتی دارد و به مسائلی همچون لزوم پرداخت دولت‌ها به مبحث spam [21] و مقایسه سرعت تشخیص spam توسط انسان و رایانه می‌پردازد[22].

در این کتاب، پس از بررسی مخاطرات و ارائه فرمول و جدولی برای سنجش مخاطرات، به روش‌ها و مکانیزم‌های نوین تأمین امنیت و میزان کاهش درصد مخاطرات پرداخته‌ایم. در نهایت، راهکاری جامع برای تأمین امنیت سرور و سرویس پست الکترونیکی، ارائه داده‌ایم.

1-5 ساختار کتاب

ساختار این کتاب شامل 6 فصل می‌باشد.

- فصل اول در مورد طرح مسئله، اهداف و کارهای مرتبط می‌باشد.
- فصل دوم به مفاهیم پایه ای می‌پردازد. نحوه عملکرد سیستم پست الکترونیکی بررسی می‌گردد و پروتکل‌های پست الکترونیکی من جمله pop3، imap، smtp و mime شرح داده می‌شوند. همچنین حملات را دسته بندی کرده و نتایج حملات را بررسی می‌کنیم.
- در فصل سوم، فرمول و جدول مخاطره ای ارائه می‌دهیم که از آن برای ارزیابی مخاطرات پست الکترونیکی، استفاده می‌کنیم. این فصل به مخاطرات پست الکترونیکی می‌پردازد، که شامل دو بخش مخاطرات در سرور پست الکترونیکی و مخاطرات در سرویس پست الکترونیکی می‌باشد. به مواردی همچون نا امن بودن سرور پست الکترونیکی، دستورات ناامن، عدم امنیت بسته[2]های پست الکترونیکی همچون sendmail، postfix و qmail، open relay، spam، ویروس‌ها، سرقت و خواندن داده‌ها، امن نبودن سرورهای pop3 و imap و فقدان امنیت webmailاشاره می‌کنیم. برای بررسی مخاطرات، از جدول مخاطره و فرمولی که ارائه داده‌ایم، استفاده می‌کنیم.
- فصل چهارم، راهکارهای پیشنهادی برای رفع مخاطرات سرور و سرویس پست الکترونیکی را ارائه می‌دهد. در این فصل به مباحثی همچون امن کردن سرور پست الکترونیکی، امن کردن بسته‌های پست الکترونیکی من جمله postfix، sendmail و qmail،

---

[1] Worms
[2] Package

ممانعت از open relay، بلوکه کردن spam، فیلتر کردن ویروس، رله کردن گزینشی[1]، SASL، رمزنگاری داده‌ها توسط پروتکل‌هایی همانند SSL، TLS[2] و PGP[3]، استفاده از دیوارهای آتش[4] پست الکترونیکی، امن کردن سرورهای pop3 و imap و امن کردن webmail می‌پردازیم. با انجام آزمایش‌هایی، میزان کاهش این مخاطرات را به صورت موردی، توسط راهکارها و مکانیزم‌ها بررسی کرده‌ایم.

- فصل پنجم، به ارائه دسته بندی پست الکترونیکی و چگونگی ایمن سازی آنها و نتیجه گیری می‌پردازد.
- فصل ششم حاوی مراجع و منابع می‌باشد.

[1] Selective Relaying
[2] Transport Layer Security
[3] Pretty Good Protection
[4] Firewall

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.

2-1 اصول پست الکترونیکی

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

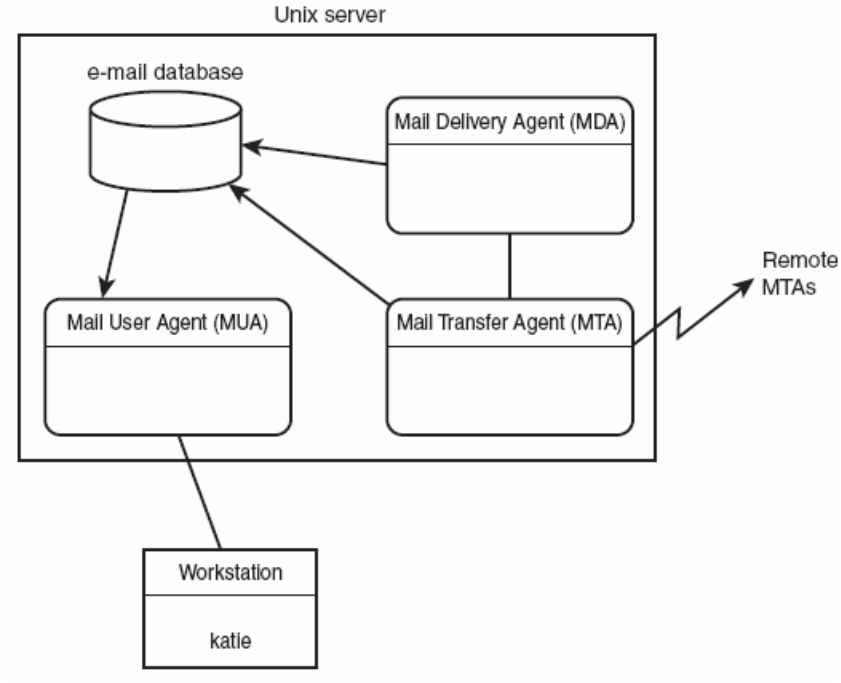
2-1-1 سیستم‌های پست الکترونیکی لینوکسی[1]

از دهه 1970 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 2-1 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 (2-1) : محیط ماژولار پست الکترونیکی در یونیکس

همان‌طور که در شکل 2-1 می‌بینید، یک سیستم پست الکترونیکی لینوکسی از سه بخش عمده زیر تشکیل شده است[23]:

- The Mail Delivery Agent (MDA)

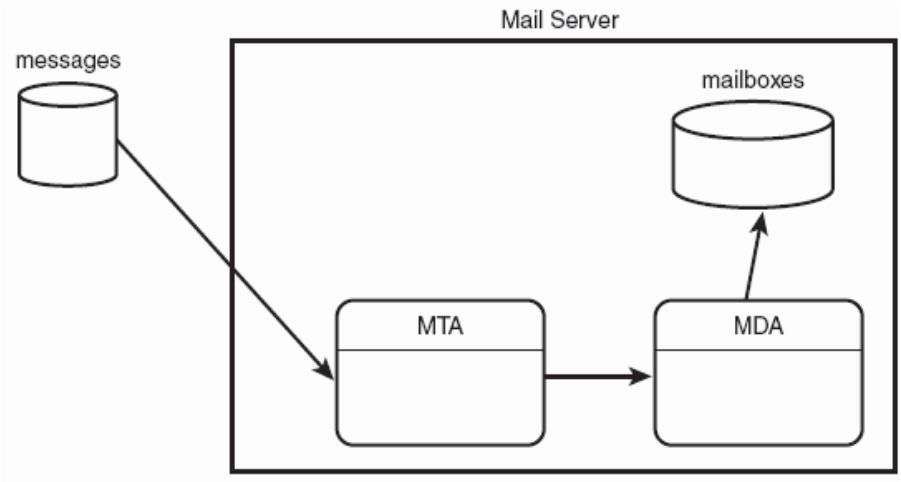
- The Mail Transfer Agent (MTA)

- 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 (2-2) : استفاده از MDA در سرور پست الکترونیکی

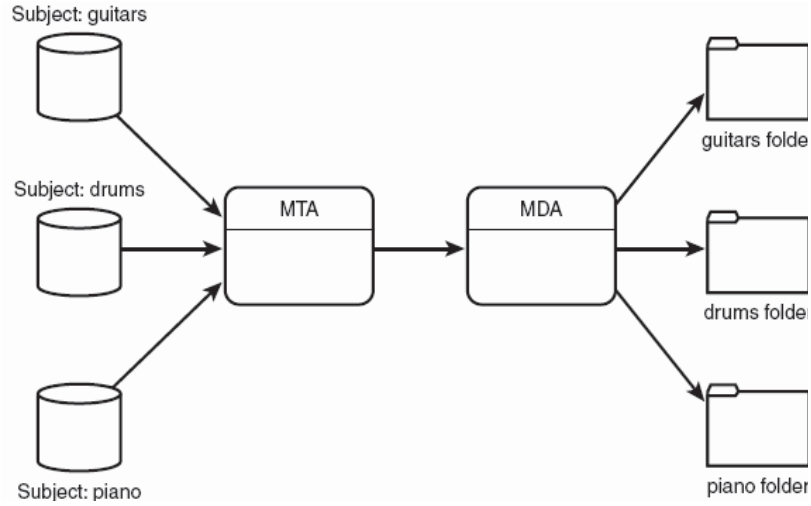
سه ویژگی عمده MDA عبارتند از:

- فیلترگذاری خودکار پست الکترونیکی[1]
- پاسخگویی خودکار پست الکترونیکی[2]
- مقداردهی اولیه برنامه توسط پست الکترونیکی[3]

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.

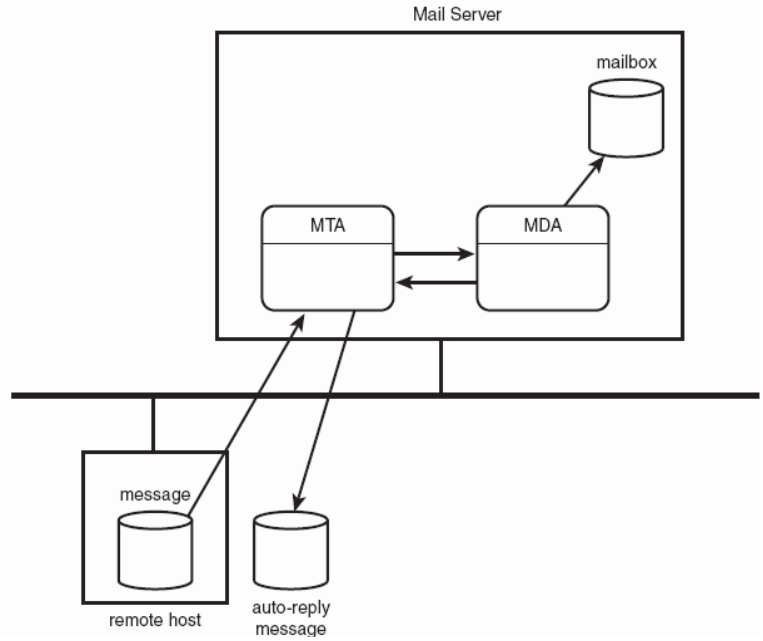
[1] Automatic Mail Filtering
[2] Automatic Mail Replying
[3] Automatic Program Initialization By Mail



شکل (2-3) : فیلترگذاری خودکار پست الکترونیکی

پاسخگویی خودکار پست الکترونیکی

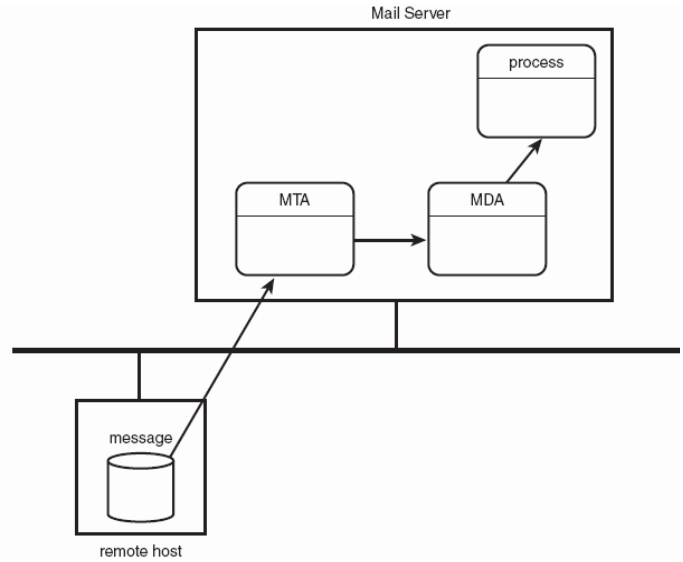
برنامه‌های MDA به کاربران پست الکترونیکی اجازه می‌دهند تا پیام‌های پاسخ را بر اساس سرآیند پیام، بفرستند[23].



شکل (2-4) : 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 (2-5) : 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

2-1-2 پروتکل‌های پست الکترونیکی

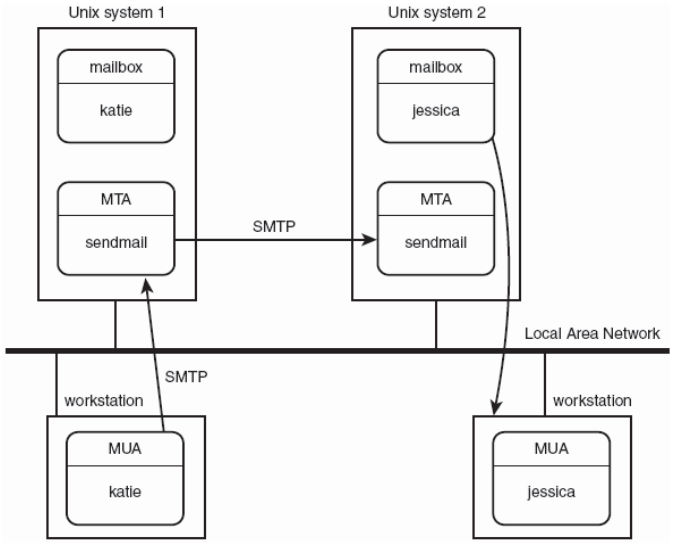
در قسمت‌های قبلی به معرفی MDA، MTA و MUA پرداختیم و وظیفه هر یک را بررسی کردیم. اکنون پروتکل‌های مورد استفاده در MDA، MTA و MUA را معرفی اجمالی کرده و شرح آنها را به قسمت‌های بعد کتاب موکول می‌کنیم.

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 2-6 نمایشگر این مسئله است.



شکل (2-6) : اتصال smtp بین دو ایستگاه کاری

[1] Extended Simple Mail Transfer Protocol