کارگزار پست الکترونیکی امن

فهرست

شرح فنی ۵

کارگزار نامه الکترونیکی امن و مقیاس‌پذیر ۶

بیان ضرورت و چالش‌ها با ملاحظات پدافند غیرعامل ۱۴

با پیشرفت ارتباطات در دنیای امروز و پیدایش اینترنت، ابزارهای ارتباطی میان انسان‌ها نیز الکترونیکی شده است. با توجه به اهمیت این مقوله در دنیای ارتباطات و نیاز به محصولات بومی که نیازهای امنیتی و قابلیت پشتیبانی از حجم بالای کاربر را برآورده سازد، در این کتابچه توصیف فنی یک «کارگزار نامه الکترونیکی امن و مقیاس‌پذیر» ارائه شده است. در توصیف ارائه شده برای کارگزار هدف دو ویژگی عمده مد نظر است که سعی شده است تا جهت نیل به آن ها راه حل های بومی مطلوب ارائه گردد. این دو ویژگی شامل «پوشش تعداد زیاد کاربر» و «تأمین امنیت حداکثری» با استفاده از روش های مختلف از جمله فراهم کردن زیر ساخت کلید عمومی، امکانات امنیتی رمزنگاری و امضای رقمی است.

آغاز

با ظهور اینترنت و فراگیر شدن امکانات و تسهیلات فراهم شده توسط آن، ابزارهای ارتباطی فیزیکی میان انسان‌ها، جای خود را به ابزارهای ارتباطی الکترونیکی مانند نامه‌های الکترونیکی داده است.

در این کتابچه، به بررسی یک کارگزار نامه الکترونیکی امن و مقیاس‌پذیر مطلوب پرداخته می‌شود. این کارگزار باید دو هدف زیر را برآورده نماید.

۱. ارائه یک راه حل بومی بطوریکه کارگزار نامه الکترونیکی تعداد زیادی کاربر را پوشش دهد.
۲. ارائه یک راه حل امن که کارگزار نامه الکترونیکی را در مقابل هرزنامه‌ها، ویروس‌ها و انواع حملات مانند DoS[۱] مقاوم نماید. از طرفی در ابزار واسط مبتنی بر وب[۲] یا وب‌میل[۳]، امکانات امنیتی رمزنگاری به

---

[۱] Denial of Service

[۲] Web Client

[۳] Web Mail

نحوی فعال گـردد کـه بتـوان بـرای برقـراری ارتبـاط در آن، از امضـای رقمی بهره گرفت.

شرح فنی

از دید منطقی یک کارگزار نامه عموماً از مؤلفه‌های اصلی زیر تشکیل می‌شود.

- عامل تحویل نامه‌ها (MDA[۱]): این جزء برای ارسال نامه‌ها به کاربران محلی مورد استفاده قرار می‌گیرد.
- عامل ارسال نامه‌ها (MTA[۲]): این جزء برای مدیریت نامه‌های ورودی و خروجی به این کارگزار نامه الکترونیکی مورد استفاده قرار می‌گیرد.
- عامل کاربر نامه‌ها(MUA[۳]): این جزء برای نمایش نامه‌های دریافتی برای کاربران مختلف مورد استفاده قرار می‌گیرد.
- مخزن نامه‌های الکترونیکی: این جزء نامه‌های موجود در صندوق‌های پستی کاربران را نگه‌داری می‌کند. مخزن نامه‌ها می‌تواند برای تسریع جستجو از پایگاه داده‌ها نیز استفاده نماید؛ اما برای نگه‌داری از نامه‌ها، بکارگیری پایگاه داده‌ها پیشنهاد نمی‌گردد.

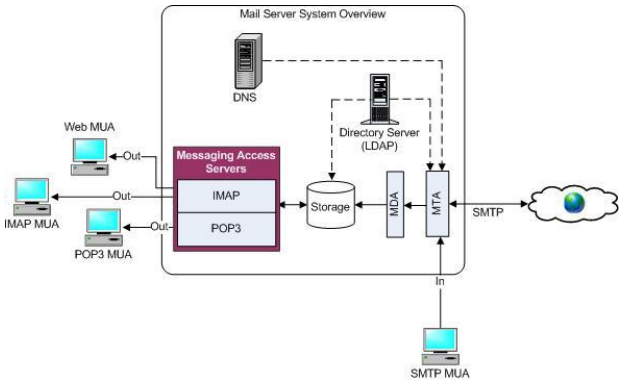
نحوه استقرار و ارتباط این اجزاء در شکل۱ بیان شده است.

---

[۱] Mail Delivery Agent

[۲] Mail Transfer Agent

[۳] Mail User Agent



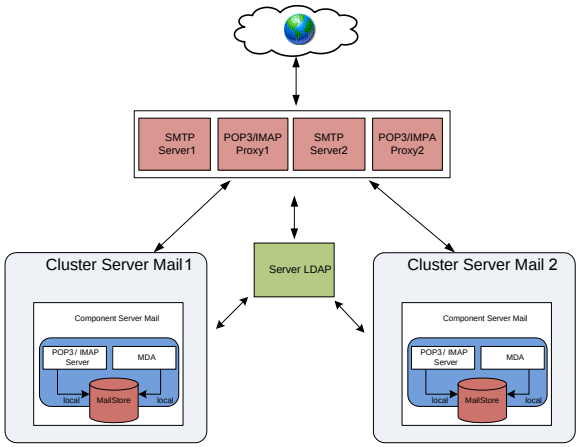
شکل ۱. ساختار یک کارگزار نامه

کارگزار نامه الکترونیکی امن و مقیاس‌پذیر

با توجه به اهداف اشاره شده در کارگزار نامه بومی، معماری کارگزار با در نظر گرفتن دو ویژگی مقیاس‌پذیری و امنیت ارائه شده است. مقیاس‌پذیری با بکارگیری خوشه‌بندی و تقسیم وظایف و امنیت با استفاده از الزامات امنیتی مورد نیاز با استفاده از تمهیدات خاص در نظر گرفته شده است. در ادامه ابتدا به مقوله مقیاس‌پذیری و سپس مقوله امنیت را مورد بررسی قرار خواهیم داد.

- مقیاس‌پذیری در کارگزار نامه

برای مقیاس‌پذیر نمودن کارگزار نامه، می توان از روش خوشه‌بندی استفاده نمود. خوشه‌ها بر اساس کاربران طراحی می شوند؛ به این ترتیب که هر خوشه وظایف مربوط به دسته‌ای از کاربران را بر عهده دارد. این معماری بصورت لایه ای بوده، در لایه نخست، یک یا چند پروکسی IMAP و POP۳ و تعدادی کارگزار SMTP قرار گرفته است.



معماری نمونه برای یک کارگزار نامه مقیاس پذیر

پروکسی‌های IMAP و POP۳ هریک وظیفه ارجاع درخواست‌های دریافت نامه‌ها و بررسی کردن صندوق‌های پستی را برعهده دارند. این پروکسی‌ها از طریق تونل‌سازی[۱] عمل کرده و وظیفه دارند پس از تشخیص خوشه مرتبط و برقراری ارتباط میان کاربر و کارگزار، تمام پیام‌های پروتکلی رد و بدل شده میان کلاینت کاربر و کارگزار IMAP یا POP۳ موجود در هر خوشه را میان آنها تبادل نمایند. کارگزاران SMTP موجود در لایه نخست، از این منظر که باید خوشه‌ای را که نامه باید در انباره موجود در آن ذخیره شود، تشخیص دهد، شبیه به پروکسی‌های IMAP و POP۳ عمل می‌کند. نوع کارکرد این مؤلفه به صورت ذخیره و ارجاع[۲] است. به این معنا که کارگزار SMTP نامه را

[۱] Tunneling

[۲] Store and Forward

گرفته ابتدا ذخیره و پس از تعیین خوشه مرتبط آنرا به MDA موجود در هر خوشه تحویل می‌دهد.

اطلاعات مربوط به کاربران باید در یک انباره قرار گیرد. برای این منظور باید از یک کارگزار مناسب استفاده گردد. کارگزار LDAP[۱] از یک ساختار درختی برای ذخیره اطلاعات کاربری استفاده می‌کند. این کارگزار برای نگهداری اطلاعات کاربری در یک کارگزار نامه بسیار مناسب است؛ زیرا به نحوی طراحی شده است که خواندن از این کارگزار بسیار سریع و نوشتن روی آن نسبتاً کند است. با توجه به اینکه در یک کارگزار نامه الکترونیکی، معمولاً اطلاعات کاربری مانند نام کاربری و محل نگهداری نامه‌ها به ندرت تغییر می‌کنند، نیاز به نوشتن به ندرت پیش می‌آید.

هر خوشه، حاوی یک انباره است که در آن صندوق‌های پستی کاربران نگهداری می‌شود. این انباره از نوع SAN[۲] انتخاب شده است. ویژگی این نوع انباره این است که اطلاعات موجود در آن را به صورت RAID[۳] نگهداری می‌کند. به این ترتیب، از طرفی به خوبی از داده‌ها نگهداری و پشتیبان گیری می‌شود و از طرف دیگر دسترسی به آن سریع تر خواهد بود. هر خوشه شامل یک MDA و یک کارگزار IMAP و POP۳ نیز هست که به ترتیب وظیفه تحویل نامه به صندوق پستی و تحویل نامه به کاربر از صندوق پستی را برعهده دارند.

---

[۱] Lightweight Directory Access Protocol

[۲] Storage Area Network

[۳] Redundant Array of Inexpensive Disks

- امنیت در کارگزار نامه الکترونیکی مقیاس‌پذیر

محرمانگی[1]، صحت[2] و دسترس‌پذیری[3] به عنوان سه رکن اصلی امنیت اطلاعات شمرده می‌شوند. این سه رکن امنیتی، در سامانه های تبادل نامه الکترونیکی نیز مانندسامانه‌های دیگر نقش مهم دارند و به دو شکل خود را نشان می‌دهند. شکل اول آن ها در حوزه خود کارگزار نامه الکترونیکی است که به صورت غیر مستقیم به کاربران صدمه می زنند. شکل دوم آن ها در نامه‌های الکترونیکی است که مستقیماً به کاربر ضربه وارد می کنند.

محرمانگی در حوزه امنیت کارگزار نامه الکترونیکی مربوط به حفظ اطلاعات کارگزار می‌شود و در مواردی مانند آدرس‌های کارگزار و پیکربندی آن باید مورد حفاظت قرار گیرند. لذا باید جلوی نشت اطلاعاتی که به سود نفوذگران بوده و به آنها در جهت نفوذ به کارگزار کمک می‌کند، گرفته شود. منظور از صحت در حوزه کارگزار نامه الکترونیکی، تضمین آن است که پیکربندی کارگزار نامه به صورت صحیح است به نحوی که نامه‌ها صحیح و سالم به گیرندگان واقعی خود برسند و یا اینکه محرمانگی کاربران از طریق تغییر پیکربندی صورت نگیرد. دسترس‌پذیری نامه الکترونیکی در حوزه کارگزار نامه، به معنای در دسترس نگه داشتن کارگزاران نامه و آمادگی همیشگی آنها برای

---

[1] Confidentiality

[2] Integrity

[3] Availability

ارائه سرویس است. از جمله تهدیداتی که می‌توانند امنیت سامانه کارگزار نامه الکترونیکی را به خطر اندازند، وبروس‌ها و هرزنامه‌ها هستند. ویروس‌ها تهدیدی بسیار جدی برای کارگزار نامه هستند به این دلیل که می‌توانند باعث وارد کردن بار زیاد ویرانگر به کارگزار و پایین آوردن کامل آن شوند. تهدید عمده دیگر برای امنیت سامانه کارگزار نامه، هرزنامه‌ها هستند به خاطر باری که به سامانه وارد می‌کند تهدید برای کارگزار به حساب می‌آیند.

محرمانگی نامه الکترونیکی، به معنای اطمینان از حفظ کردن نامه از فاش شدن محتوای آن و دسترسی غیرمجاز به محتوا و اطلاعات مربوط به سرآیند آن است. منظور از صحت نامه الکترونیکی، تضمین آن است که نامه توسط شخص غیرمجازی خراب و یا تغییر داده نشده است. دسترس‌پذیری نامه الکترونیکی به معنای ایجاد اطمینان از در دسترس باقی نگهداشتن کارگزاران نامه است که به معنی قادر بودن کاربران برای سرویس‌گیری از کارگزار نامه است. وبروس‌ها و هرزنامه‌ها در این حوزه نیز تهدیداتی جدی هستند زیرا ویروس‌ها می‌توانند با خراب کردن داده‌ها، کاربر را تهدید کنند و هرزنامه ها نیز به خاطر احتمال به همراه داشتن ویروس و یا درخواست‌هایی که کلاه‌برداران به این وسیله برای دریافت اطلاعات شخصی افراد می‌کنند، در حوزه تهدید برای کاربران، دارای اهمیت است.

کارگزار نامه الکترونیکی مقیاس‌پذیر ارائه شده در بخش قبل بمنظور تأمین امنیت و پایداری خود به بعضی الزامات امنیتی نیاز دارد. از جمله این الزامات عبارتند از:

- احراز هویت

در حوزه کارگزار نامه، احراز هویت، فرآیندی برای شناسایی کاربران[1] خدمات نامه است که مستقل از نشانی شبکه‌ای[2] آنها کار می‌کند. وجود این فرآیند، کارگزار نامه را قادر به تبادل نامه میان کاربرانی می‌کند که از نشانی شبکه‌ای آنها اطلاعی در دست نیست. به‌منظور برقراری فرآیند احراز هویت در کارگزار نامه، گزینه‌های متعددی در دسترس است که سه روش زیر از جمله آن هاست.

- مکانیزم احراز هویت شناسه کاربری/گذرواژه؛ واضح که به علت حساسیت، گذرواژه رسانه‌ای امن برای این نوع احراز هویت مورد نیاز است.
- مکانیزم احراز هویت چالش و پاسخ[3]
- مکانیزم احراز هویت کربروس که هم برای کاربر و هم احراز هویت در وب‌میل بکار گرفته می‌شود.

---

[1] منظور از کاربران خدمات نامه، در حقیقت، ابزارهای سمت‌کاربر جهت ارسال و دریافت نامه است.

[2] IP address

[3] Challenge Response

- ضد هرزنامه و ضد ویروس

سامانه مورد استفاده به این منظور باید توانایی حفاظت در برابر ویروس و هرزنامه را داشته باشد و نیز از طیف وسیعی از کارگزاران نامه الکترونیکی پشتیبانی کند.

- دسترس‌پذیری بالا

برای داشتن دسترس‌پذیری بالا معیار زمان قطعی/خرابی[1] تعریف می‌شود. برای کم کردن زمان قطعی/خرابی ، با دو سیاست مختلف مواجه هستیم.

- سعی شود که سیستم کم‌تر در معرض قطعی/خرابی قرار گیرد.
- سعی شود در صورت قطعی/خرابی سیستم، در سریع‌ترین زمان ممکن آنرا عملیاتی و به عبارت دیگر بالا آورد.

که البته تلفیق هر دو روش پیشنهاد می گردد تا مزایای هر دو مورد استفاده قرار گیرد. با در نظر گرفتن این دو استراتژی، دو دسته تمهید باید برای کارگزار نامه الکترونیکی امن در نظر گرفت. دسته اول دسته‌ای است که موجب شود همواره سامانه به صورت آرام و بدون اشکال به کار ادامه دهد؛ که در این صورت، باید همواره میزان بار روی سامانه به صورت مشخص و

---

[1] Down time

از یک مقدار حداکثری فراتر نرود و برای این کار باید اجزای مختلف کارگزار نامه را به صورت افزونه استفاده کرده و به کمک ابزارهایی مانند متوازن کننده بار و پروکسی از آنها بهره گرفت. دسته دوم راهکارهایی را شامل می‌شود که پس از خرابی جزئی از سامانه، وظایف جزء خراب را در اسرع وقت عملیاتی می‌کنند. برای لحاظ نمودن این مورد، از پشتیبان‌هایی استفاده می‌شود تا داده‌های پشتیبان گرفته شده قبل از آنرا بازگرداند و با داده‌های جدید همگام و به‌روز نمود.

- امکانات رمزنگاری

یک زیرساخت کلید عمومی یا به اختصار یک PKI[۱] امکان تأمین بعضی تسهیلات مدیریتی گواهی‌نامه‌ها را می‌دهد. بعضی از این تسهیلات مدیریتی شامل صدور[۲]، لغو[۳]، ذخیره، بازیابی[۴] و اعتماد به گواهی‌نامه‌ها است. استفاده از زیرساخت‌های کلید عمومی در کارگزار نامه دو کاربرد اساسی دارد. کاربرد اول در ایجاد رسانه‌های امنی است که روی بستری مانند SSL[۵]/TLS[۶] بنا شده‌اند و کاربرد دوم در ایجاد یک زیرساخت اعتمادی میان

---

[۱] Public Key Infrastructure

[۲] Issue

[۳] Revoke

[۴] Retrieve

[۵] Secure Sockets Layer

[۶] Transport Layer Security

کاربرانی که از کارگزار نامه الکترونیکی خدمات می‌گیرند نقش دارد.

- امن‌سازی

امن سازی یا مستحکم سازی فرآیندی است که در آن باید به صورت یک چرخه سامانه را مورد بررسی قرار داد و آسیب‌پذیری‌های احتمالی و جاری آنرا شناسایی و مستند نمود. سپس با توجه به مسایل زمان و هزینه، آنها را اولویت‌بندی کرده و رفع نمود. نکته شایان ذکر در مورد امن سازی این است که این فرآیند یک فرآیند دائمی است و باید به صورت دوره‌ای انجام شود؛ لذا هیچگاه به پایان نمی‌رسد.

بیان ضرورت و چالش‌ها با ملاحظات پدافند غیرعامل

کارگزاران نامه یکی از نقاط حساس در شاهراه اطلاعاتی دنیای مجازی هستند. تأمین کنندگان برای ارائه خدمات، نیاز به محصولات قابل اطمینان، امن، پایدار و با ظرفیت بالا دارند تا بتوانند کیفیت خدمات را برای انبوه کاربران تضمین نمایند. اکثر محصولات فعلی موجود در بازار قابلیت ارائه خدمات به حجم کم از کاربران را دارند و یا از نظر امنیتی دچار مشکل هستند. لذا نگاه جدی به تولید محصول بومی برای کاربران زیاد در مقیاس بالا و همراه با امکانات امنیتی کافی در راه حل‌های موجود چه از نظر امکانات برقراری ارتباط به زیرساخت PKI و چه از نظر عملکرد، در این زمینه مطرح است. تا بتوان امکان سرویس‌دهی به تعداد زیاد کاربران بدون کاهش کارایی از جمله کندشدن سامانه و یا کمبود حافظه را

فراهم کرد و از طرف دیگر امکان امن‌سازی ارتباطات میان کاربران استفاده‌کننده از کارگزار نامه الکترونیکی با استفاده از مخزن کلیدهای PKI فراهم شود.

- امن‌سازی

مستحکم‌سازی یا Hardening فرآیندی برای مستحکم کردن یک سامانه یا خدمت اطلاعاتی در مقابل تهدیدهای متعارف است. بر اساس این تعریف باید تأکید کرد که مستحکم‌سازی یک فعالیت (task) نبوده و یک فرآیند است. بنابراین در تمام طول عمر یک سامانه و نه فقط تولید آن اجرا خواهد شد. البته ممکن است در زمان تولید سامانه به دلیل بالا بودن آسیب‌پذیری‌های سامانه نسبت به زمان نگهداری، بسیار گسترده‌تر و پر حجم‌تر باشد. برای مستحکم‌سازی سامانه باید فرآیندی تدوین شود که با اجرای آن در زمان تولید و سپس در زمان نگهداری تا حد امکان به یک سامانه مقاوم در برابر ناامنی‌ها دست یابیم.

در فرآیند مستحکم‌سازی به ترتیب انجام کارها در یک چرخه برای مستحکم کردن یک سامانه پرداخته می‌شود. فرآیند مستحکم‌سازی را می‌توان به چهار مرحله تقسیم کرد.

۱. شناسایی آسیب‌پذیری‌های سامانه موجود
۲. برنامه ریزی رفع آسیب‌پذیری‌ها
۳. اجرای برنامه رفع آسیب‌پذیری‌ها
۴. بررسی آسیب‌پذیری‌های رفع شده