دانشکده مهندسی
گروه برق

پایان‌نامه کارشناسی

گرایش:مخابرات

عنوان :بررسی و مقایسه الگوریتم‌های رمزنگاری

استاد راهنما:جناب آقای مهندس مصطفوی

نگارش:میثم احمدی

بهمن ۸۹

فهرست

۱)مقدمه

تا یکی دو دهه قبل شبکه های کامپیوتری معمولاً در دو محیط وجود خارجی داشت:

- محیطهای نظامی که طبق آئین نامه های حفاظتی ویژه بصورت فیزیکی حراست می شد و چون سایت های ارتباطی خودشان هم در محیط حفاظت شدهٔ نظامی مستقر بود و هیچ ارتباط مستقیم با دنیای خارج نداشتند، لذا دغدغهٔ کمتری برای حفظ اسرار و اطلاعات وجود داشت. (نمونه بارز این شبکه *ARPANET* در وزارت دفاع آمریکا بود)
- محیط های علمی و دانشگاهی که برای مبادله دستاوردهای تحقیقی و دسترسی به اطلاعات علمی ازشبکه استفاده می کردند و معمولاً بر روی چنین شبکه هایی اطلاعاتی مبادله می شد که آشکار شدن آن ها لطمهٔ چندانی به کسی وارد نمی کرد.(اداراتی هم که اطلاعات محرمانه و سری داشتند معمولاً از کامپیوترهای *Mainframe* استفاده می کردند که هم مدیریت و حراست ساده تری نیاز دارد و هم کنترل کاربران آن بصورت فیزیکی ساده است)

با گسترش روز افزون شبکه های به هم پیوسته و ازدیاد حجم اطلاعات مورد مبادله و متکی شدن قسمت زیادی از امور روزمره به شبکه های کامپیوتری و ایجاد شبکه‌های جهانی چالش بزرگی برای صاحبان اطلاعات پدید آمده است. امروز سرقت دانشی که برای آن هزینه و وقت، صرف شده یکی از خطرات بالقوه شبکه های کامپیوتری به شمار می آید.

در جهان امروز با محول شدن امور اداری و مالی به شبکه های کامپیوتری زنگ خطر برای تمام مردم به صدا درآمده است و بر خلاف گذشته که خطراتی نظیر دزدی و راهزنی معمولاً توسط افراد کم سواد و ولگرد متوجه مردم بود امروزه این خطر توسط افرادی تحمیل می شود که با هوش و باسوادند(حتی با هوش تر از افراد معمولی) و قدرت نفوذ و ضربه به شبکه را دارند. معمولاً هدف افرادی که به شبکه های کامپیوتری نفوذ یا حمله می کنند یکی از موارد زیر است:

- تفریح یا اندازه گیری ضریب توانایی فردی یا کنجکاوی (معمولاً دانشجویان!)
- دزدیدن دانشی که برای تهیه آن بایستی صرف هزینه کرد (راهزنان دانش)
- انتقام جویی و ضربه زدن به رقیب
- آزار رسانی و کسب شهرت از طریق مردم آزاری (بیماران روانی)
- جاسوسی و کسب اطلاعات از وضعیت نظامی و سیاسی یک کشور یا منطقه
- رقابت ناسالم در عرصهٔ تجارت و اقتصاد

- جا به جا کردن مستقیم پول و اعتبار از حسابهای بانکی و دزدیدن شماره کارتهای اعتبار
- کسب اخبار جهت اعمال خرابکاری و موذیانه (توسط تروریستها)

بهر حال امروزه امنیت ملی و اقتدار سیاسی و اقتصادی به طرز پیچیده ای به امنیت اطلاعات گره خورده و نه تنها دولتها بلکه تک تک افراد را تهدید می کند. برای ختم مقدمه از شما سئوال می کنیم که چه حالی به شما دست می دهد وقتی متوجه شوید که شماره حساب بانکی یا کارت اعتباریتان توسط فرد ناشناس فاش شده و انبوهی هزینه روی دست شما گذاشته است؟ پس به عنوان یک فرد مطلع از خطراتی که یک شبکه کامپیوتری را دنبال می کند این فصل را دنبال کنید.

۱-۱) سرویس‌های امنیتی در شبکه‌ها

تهدید های بالقوه برای امنیت شبکه های کامپیوتری بصورت عمده عبارتند از:

- فاش شدن غیر مجاز اطلاعات در نتیجهٔ استراق سمع داده ها یا پیامهای در حال مبادله روی شبکه
- قطع ارتباط و اختلال در شبکه به واسطه یک اقدام خرابکارانه
- تغییر و دستکاری غیر مجاز اطلاعات با یک پیغام ارسال شده

بایستی با مفاهیم اصطلاحات زیر به عنوان سرویسهای امنیتی آشنا باشید:

الف) محرمانه ماندن اطلاعات[۱]: دلایل متعددی برای یک سازمان یا حتی یک فرد عادی وجود دارد که بخواهند اطلاعات خود را محرمانه نگه دارد.

ب) احراز هویت[۲]: بیش از آنکه محتوای یک پیام یا اطلاعات اهمیت داشته باشد باید مطمئن شوید که پیام حقیقتاً از کسی که تصور می کنید رسیده است و کسی قصد فریب و گمراه کردن (یا آزار) شما را ندارد.

ج) سلامت داده ها[۳] : یعنی دست نخوردگی و عدم تغییر پیام و اطمینان از آنکه داده ها با طلاعات مخبر مثل یک ویروس کامپیوتری آلوده نشده اند.

د) کنترل دسترسی[۱]: یعنی مایلید دسترسی افرادی ا که مجاز نیستند، کنترل کنیدو قدرت منع افرادی را که از دیدگاه شما قابل اعتماد به شمار نمی آیند از دسترسی به شبکه داشته باشید.

---

۱ .*Confidentality*

۲. *Authentication*

۳ . *Integrity*

ه) در دسترس بودن[۲]: با این تفاضیل، باید تمام امکانات شبکه بدون دردسر و زحمت در اختیار آنهایی که مجاز به استفاده از شبکه هستند، باشد و در ضمن هیچ کس نتواند در دسترسی به شبکه اختلال ایجاد کند.

زمانی که یکی از سرویسهای امنیتی پنج گانه فوق نقض شود می گوییم به سیستم حمله شده است. معمولاً یک شبکه کامپیوتری در معرض چهار نوع حمله قرار دارد:

- حمله از نوع وقفه[۳]: بدین معنا که حمله کننده باعث شود شبکه مختل شده و مبادلـه اطلاعـات امکان پذیر نباشد.
- حمله از نوع استراق سمع[۴]: بدین معنا که حمله کننده به نحوی توانسته اطلاعات در حال تبادل روی شبکه را گوش داده و بهره برداری نماید.
- حمله از نوع دستکاری داده ها[۵] : یعنی حمله کننده توانسته به نحوی اطلاعاتی را که روی شبکه مبادله می شود تغییر دهد یعنی داده هایی که در مقصد دریافت می شود متفاوت با آن چیزی باشد که از مبدأ آن ارسال شده است.
- حمله از نوع افزودن اطلاعات[۶]: یعنی حمله کننده اطلاعاتی را که در حال تبادل روی شبکه است تغییر نمی دهد بلکه اطلاعات دیگری را که می تواند مخرب یا بنیـانگزار حمـلات بعـدی باشـد، بـه اطلاعات اضافه می نماید (مثل ویروس ها)

به حمله ای که هنگام شروع با بروز اختلال در شبکه علنی می شود و در کار ارسال یا دریافت مشکل ایجاد می کند "حمله فعال" می گویند. برعکس حمله ای که شبکه را با اختلال مواجـه نمـی کنـد و ظاهراً مشکلی در کار ارسال و دریافت به وجود نمی آورد "حملهٔ غیـر فعـال"[۷] نامیـده مـی شـود و از خطرناکترین انواع حمله ها به شبکه به شمار می رود.

در ادامه این فصل دو راه کلی برای حراست و حفظ امنیت اطلاعات در یک شبکه کامپیوتری معرفـی می شود:

۱.*Access Control*

۲.*Availability*

۳.*Interruption*

۴.*Interception*

۵.*Modification*

۶.*Fabrication*

۷.*Passive*

- حراست و حفاظت داده ها و شبکه از طریق نظارت بر اطلاعات و دسترسی ها به کمک سیستم هایی که "دیوار آتش[1]" نامیده می شود.
- رمز گذاری اطلاعات به گونه ای که حتی اگر کسی آنها را دریافت کرد نتواند محتوای آن را بفهمد و از آن بهره برداری کند.

برای تمایز دو مورد فوق مثال عامیانه زیر بد نیست:

چون احتمال سرقت همیشه وجود دارد اولاً شما قفلهای مطمئن و دزدگیر برای منزل خود نصب می کنید و احتمالاً نگهبانی می گمارید تا ورود و خروج افراد را نظارت کند (کاری که دیوار آتش انجام می دهد) ثانیاً چون باز هم احتمال نفوذ می دهید لوازم قیمتی و وجه نقد را در گوشه ای مخفی می کنید تا حتی در صورت ورود سارق موفق به پیدا کردن و بهره برداری از آن نشود. با تمام این کارها باز هم اطمینان صد در صد وجود ندارد چرا که هر کاری از یک انسان باهوش بر می آید.

۲)دیوار آتش

دیوار آتش سیستمی است که در بین کاربران یک شبکه محلی و شبکه بیرونی (مثلاً اینترنت)قرار می گیرد و ضمن نظارت بر دسترسی ها، در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد.

مدلی ساده برای یک سیستم دیوار آتش در شکل (۱) ارائه شده است. در این ساختار هر سازمان شبکه داخلی خود را با دنیای خارجی قطع کرده و هر نوع ارتباط خارجی از طریق یک دروازه که در شکل (۱) نشان داده شده، انجام شود.

۱ *Fire wall*

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

مراجع

مجموعهٔ مراجع زیر می توانند برای دست آوردن جزییات دقیق و تحقیق جامع در مورد مفـاهیم تعریـف شده مفید واقع شوند .

۱.*"Computer Networks" , Andrew S.Tanenbaum, Third Edition, Prentice-Hall,* ۱۹۹۶.

۲.*RFC*۱۲۴۴ *"Site Security Handbook"*

۳.*RFC*۱۱۱۴ *"Privacy Enhancement for Internet Electronic Mail : Part II--Certificate-Based Key Management [Draft]," Kent, S.T.; Linn, J.:*۱۹۸۹.

۴.*RFC*۱۱۰۸ *"Security Options for the Internet Protocol,"* ۱۹۹۱.