رمزنگاری اطلاعات

۱- غلامرضا سینگر ، ۲- حسن ارفعی نیا
۱- دانشجوی کارشناسی ارشد شبکه های کامپیوتری دانشگاه آموزش عالی لیان واحد بوشهر
۲- استاد گروه کامپیوتر ، دانشگاه آموزش عالی لیان واحد بوشهر ، حسن ارفعی نیا
بوشهر
Email: resing7777@gmail.com
Email: h.arfaeinia@gmail.com

چکیده

امروزه در دنیای دیجیتال حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام‌ها ومبادلات تجاری ایفا می‌نماید. برای تامین نیازهای امنیتی تراکنش امن، از رمز نگاری استفاده می‌شود . با توجه به اهمیت این موضوع و گذار از مرحله سنتی به مرحله دیجیتال آشنایی با روش‌های رمز گذاری ضروری به نظر می‌رسد. هدف از انجام تحقیق حاضر آشنائی با رمزنگاری اطلاعات و بررسی الگوریتم های آن می باشد. این مطالعه به روش کتابخانه ای و مطالعه مروری می باشد.

واژه‌های کلیدی: رمز– رمزنگاری - امنیت اطلاعات– الگوریتم

۱- مقدمه

با گسترش شبکه های کامپیوتری و نقل و انتقال اطلاعات تکنیک های مختلف رمزنگاری اطلاعات مورد توجه قرار گرفته اند . در این بین تکنیک هایی که بتواند محرمانه بودن پیغام را طوری تامین کند که تهدید کننده نتواند به اصل متن پی ببرد اهمیت پیدا می کند.[۱]

با اتصال شبکه داخلی سازمانها به شبکه جهانی ، داده های سازمانها در معرض دسترسی افراد و میزبانهای خارجی قرار می گیرد . اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حیاتی از مهم ترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است . راه های مختلفی نظیر محدود کردن استفاده از اینترنت ، رمزنگاری داده ها ، و استفاده از ابزار امنیتی برای میزبان های داخلی و برقراری امنیت شبکه داخلی اریه شده است. [۲]

یکی از مهم ترین مباحث در امنیت شبکه و رایانه رمزنگاری است . رمزنگاری دانشی است که به بررسی و شناخت اصول و روش های انتقال یا ذخیره اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال ارتباطی یا محل ذخیره اطلاعات ناامن باشد) می پردازد . رمز نگاری از زمانهای قدیم برای حفظ اطلاعات ، همخوانی اطلاعات فرستاده شده و دریافت شده ، تصدیق هویت و سندیت استفاده میشد و این اصول در هر نوع رمزنگاری رعایت شود . حفظ اطلاعات و رازداری به این معنی است که فقط فرستنده و گیرنده محتوای پیغام را بفهمند ممکن است افراد دیگر نتوانند محتوای ان را بفهمند اما از دید انها محتوای ان باید کاملا نامفهوم باشد. [۳]

رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمز نگاری است. استفاده از علم رمز نگاری دارای یک سابقه طولانی دارد، کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت. از این روست که رمزنگاری داده‌ها با توجه به پیشرفت‌های اخیر تحول یافته والگوریتم‌های نوینی به همین منظور طراحی گردیده است.[۳]

۲- مبانی نظری

۲-۱- تعریف رمزنگاری

رمزنگاری عبارت است از بهم ریختگی اطلاعات به طوری که برای کسی قابل فهم نباشد . فن آوری رمزنگاری امکان مشاهده ، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیر مجاز را سلب می‌نماید . از رمزنگاری به منظور حفاظت داده‌ها در شبکه‌های عمومی نظیر اینترنت استفاده می‌گردد . در این رابطه از الگوریتم‌های پیشرفته ریاضی به منظور رمزنمودن پیام‌ها و ضمائم مربوطه ، استفاده می‌شود. [۴]

۲-۲- تاریخچه رمزنگاری

یکی از اولین شکل‌های رمزنگاری، رمز سزار نامیده می‌شود زیرا ژولیوس سزار از آن برای ارتباطات محرمانه استفاده می‌کرده است. سوئتونیوس در زندگی‌نامه ژولیوس سزار می‌گوید: «اگر او می‌خواست چیزی محرمانه بنویسد، آن را به صورت رمزی می‌نوشت و برای این کار، ترتیب حروف را در الفبا، تغییر می‌داد. اگر کسی می‌خواست این نوشته‌ها را رمزگشایی و معنی آن‌ها را استخراج کند، می‌بایستی حرف چهارم حروف الفبا را با حرف اول جایگزین می‌کرد و با این کار ترتیب کل حروف الفبا را تغییر می‌داد».توصیف سوئتونیوس از رمز سزار، شامل دو مؤلفه رمزنگاری است که در بالا به آن‌ها اشاره کردیم؛ الگوریتم و کلید. الگوریتم رمز سزار بسیار ساده است: هر حرف با حرف دیگری در حروف الفبا جایگزین می‌شود. کلید رمز سزار این بود که هر حرف باید با چندمین حرف در حروف الفبا جایگزین می‌شد. همانطور که سوئتونیوس می‌گوید، کلید رمز سزار، جایگزینی هر حرف با سه حرف عقب‌تر بود. مشخص است که ژولیوس سزار می‌توانست هر بار، رمز و کلید را تغییر دهد. برای مثال، می‌توانست کلید را به این صورت تعریف کند که هر حرف با پنج حرف عقب‌تر، جایگزین شود. با رمزنگاری به شیوه سزار می‌توانید هر پیامی را که بخواهید، به صورت محرمانه منتقل کنید. بر خلاف رمز سزار، اگر از یک سیستم دارای عبارات کد استفاده کنید، فردی که پیام را دریافت می‌کند، باید سندی از همه عبارات کد در اختیار داشته باشد و نمی‌توان هر پیامی را با این سیستم انتقال داد. برای مثال، ممکن است در یک سیستم رمزنگاری بر اساس عبارت کد، «چوب دستی» به صورت «تفنگ ژ۳» کدگشایی شود ولی هیچ رمزی برای عبارت «سلاح ضد تانک» تعریف نشده باشد و در نتیجه، امکان مخابره این پیام به صورت رمزی با چنین سیستمی وجود ندارد[۸]

این در حالی است که در سیستم رمز سزار، یک الگوریتم ثابت وجود دارد و با استفاده از آن می‌توان هر پیامی را که فکرش را بکنید، رمزنگاری کرد و هر کسی که این الگوریتم را بداند، می‌تواند پیام شما رمزگشایی کند. یکی دیگر از مزیت‌های رمز سزار در مقایسه با سیستم رمزنگاری با استفاده از عبارات کد، امنیت بالاتر و راحت بودن استفاده از آن است زیرا نیازی به یک سند قطور از عبارات کد ندارد.رمز سزار به «رمز جانشینی» نیز معروف است زیرا در این سیستم، هر حرف، جانشین حرف دیگری می‌شود. انواع دیگری از رمز جانشینی وجود دارند که در آن‌ها، چندین حرف یا کل یک کلمه، جایگزین می‌شوند.در بیشتر طول تاریخ، از رمز جانشینی برای انتقال پیام‌های محرمانه دولتی و نظامی استفاده می‌شد تا اینکه ریاضی‌دانان عرب در دوران قرون وسطی، دانش رمزنگاری را کمی به جلو برند. با این حال، اکثر سیستم‌های رمزنگاری که پیش از دوران مدرن توسعه یافته‌اند، بسیار ساده هستند زیرا پیش از اختراع و توسعه کامپیوترها، انجام تبدیلات ریاضیاتی برای رمزگشایی پیام‌ها، بسیار زمان‌بر بود. در واقع، رمزنگاری به موازات توسعه کامپوترها پیشرفت کرده است. چارلز بابیج که ایده «ماشین تفاضلی»

او زمینه‌ساز توسعه کامپیوترهای مدرن شد، به رمزنگاری علاقه‌مند بود. در طول جنگ جهانی دوم، آلمان‌ها از نوعی وسیله الکترومکانیکی به نام «ماشین انیگما» برای رمزنگاری پیام‌ها استفاده می‌کردند و آلن تورینگ معروف نیز تیمی در بریتانیا تشکیل داد تا ماشین مشابهی برای رمزگشایی پیام‌های آلمان‌ها توسعه دهند که کار آن‌ها، زمینه‌ساز توسعه کامپیوترهای مدرن شد. با اختراع و توسعه کامپیوترهای مدرن، رمزنگاری به شکل دیوانه‌واری پیچیده شد ولی به مدت چندین دهه، فقط جاسوس‌ها و نظامی‌ها از آن استفاده می‌کردند[۸]

۲-۳- انواع مدل رمزنگاری

۱- رمزنگاری کلید عمومی و امنیت
۲- رمزنگاری کلید عمومی و تشخیص هویت
۳- رمزنگاری کلید عمومی و غیرجعلی بودن اطلاعات[۱]

۲-۴- ویژگی های مدل رمزنگاری

عدم استفاده از کلیدهای مشابه (در رمزنگاری و رمزگشایی)

هر کاربر دارای یک زوج کلید (عمومی ، خصوصی) می‌باشد . از کلید عمومی به منظور رمزنگاری داده و از کلید خصوصی به منظور رمزگشائی داده استفاده می‌گردد.

این مدل رمزنگاری تقریبا ۵۰۰ مرتبه کندتر از رمزنگاری کلید خصوصی (متقارن) است.

از مدل رمزنگاری عمومی به منظور مبادله کلید خصوصی و امضای دیجیتال استفاده می شود[۱]

۲-۵- موارد کاربرد رمزنگاری

موارد متعددی از اطلاعات حساس که نباید در دسترس دیگران قرار گیرد ، وجود دارند . اینگونه اطلاعات جهت حفاظت باید رمزنگاری گردند . این اطلاعات شامل :

۱- اطلاعات کارت اعتباری
۲- شماره‌های عضویت در انجمن‌ها
۳- اطلاعات خصوصی
۴- جزئیات اطلاعات شخصی
۵- اطلاعات حساس در یک سازمان[۵]

۲-۶- روش های رمزگذاری

- روش متقارن

در این روش هر دو طرفی که قصد ردو بدل اطلاعت را دارند از یک کلید مشترک برای رمز گذاری و نیز بازگشایی رمز استفاده می کنند .در این حالت باز گشایی و رمز گذاری اطلاعات دو فرایند معکوس یک دیگر می باشند .مشکل اصلی این روش این است که کلید مربوط به رمز گذاری باید بین دو طرف به اشتراک گذاشته شود و این سوال پیش می اید که دو طرف چگونه می توانند این کلید را به طور امن بین یک دیگر رد و بدل کنند. انتقال از طریق انترانت و یا به صورت فیزیکی تا حدی امن می باشد اما در انتقال ان در اینترنت به هیچ وجه درست نمی باشد .در این قبیل سیستم ها ،کلید های رمز نگاری و رمز گشایی یکسان هستند و یا رابطه ای بسیار ساده با هم دارند.این سیستم ها را سیستم های متقارن یا "تک کلیدی"می نامیم.به

دلیل ویژگی ذاتی تقارن کلید رمز نگاری و رمزگشایی،مراقبت و جلوگیری از افشای این سیستم ها یا تلاش در جهت امن ساخت انها لازم است در بر گیرنده جلو گیری از استراق سمع و ممانت از دستکاری اطلاعات باشد[۹]

- روش نامتقارن

این روش برای حل مشکل انتقال کلید در روش متقارن ایجاد شد .در این روش به جای یک کلید مشترک از یک جفت کلید به نام های کلید عمومی و خصوصی استفاده می شود .در این روش از کلید عمومی برای رمز گذاری اطلاعات استفاده می شود. طرفی که قصد انتقال اطلاعات را به صورت رمز گذاری شده دارد اطلاعات را رمز گذاری کرده و برای طرفی که مالک این جفت کلید است استفاده می شود .مالک کلید،کلید خصوصی را پیش خود به صورت محرمانه حفظ می کند.در این دسته ،کلید های رمز نگاری و رمز گشایی متمایزند و یا اینکه چنان رابطه پیچیده ای بین انها حکم فرماست که کشف کلید رمز گشایی با در اختیار داشتن کلید رمز نگاری ،عملا نا ممکن است[۹]

۲-۷- مقایسه رمز نگاری الگوریتم های متقارن و الگوریتم های کلید عمومی

بحث های زیادی شده که کدام یک از این الگوریتم ها بهترند اما جواب مشخصی ندارند. البته بررسی هایی روی این سوال شده به طور مثالNeedham وSchroederبعد از تحقیق به این نتیجه رسیدند که طول پیغامی که با الگوریتم های متقارن می تواند رمزنگاری شود از الگوریتم های کلید عمومی کمتر است.وبا تحقیق به این نتیجه رسیدند که اگوریتم های متقارن الگوریتم های بهینه تری هستند .اما وقتی که بحث امنیت پیش می اید الگوریتم های کلید عمومی کارایی بیشتری دارند و به طور خلاصه می توان گفت که الگوریتم های متقارن دارای سرعت بالا تر و الگوریتم های کلید عمومی دارای امنیت بهتری هستند. در ضمن گاهی از سیستم ترکیبی از هر دو الگوریتم استفاده می کنند که به این الگوریتم ها الگوریتم های ترکیبیگفته می شود .اما اگر به طور دقیق تر به این دو نگاه کنیم انگاه متوجه خواهیم شد که الگوریتم های کلید عمومی و الگوریتم های کلید متقارن دارای دو ماهیت کاملا متفاوت هستند و کار برد های متفاوتی دارند به طور مثال در رمزنگاری های ساده که حجم داده ها بسیار زیاد است از الگوریتم متقارن استفاده می شود زیرا داده هابا سرعت بالا تری رمز نگاری و رمز گشایی شوند .اما در پروتکل هایی که در اینترنت استفادهمی شود،برای رمز نگری کلید هایی که نیاز به مدیریت دارند از الگوریتم های کلید عمومی استفاده می شود[۶]

۲-۸- کلید های مورد استفاده در رمزگذاری

وقتی یک سندXMLیا بخشی از آن رمز گذاری می شود آن قسمت با عنصر <EncryptedData>تعویض می شود .این عنصر ممکن است شامل نوع رمز گذاری باشد که گیرنده از این اطلاعات استفاده می کند .مثلا اطلاعاتی شامل اینکه آیا کل سند رمزگذاری شده یا قسمتی از آن و همچنین اینکه نوع اطلاعات رمزگذاری شده متن است یا تصویر و غیره...

می توان مشخصات کلید مشترک را درون خود سند درون عنصر <EncryptedKey> قرارداد. اطلاعات واقعی که رمز گذاری شده اند درون عنصر <ChiperData>قرار می گیرند. درداخل این قسمت نیز یک عنصر <CipherValue> قرار دارد که شامل اطلاعات واقعی رمز گذاری شده می باشد .

۲-۹- روش های انتقال کلید طبق استاندارد W3C

سه روش برای انتقال کلید موجود می باشد:

۱.می توان کلید درون همان سند قرار داد، عناصر <EncryptedData> و یا <EncryptedKey> می توانند یک عنصر <ds:Keyinfo> داشته باشند که مشخص کننده جزییات کلید می باشد .خود این عنصر شامل عناصر زیر می باشد :

-عنصر<ds:KeyValue>که مقدار ان همان کلید عمومی یا کلید رمز گذاری شده می باشد.

-عنصر<dsKeyName>که به یک عنصر<EncryptedKey>اشاره می کند.

-عنصر<ds:RetrievalMethod>که متد باز یابی کلید را مشخص می کند.

۲.می توان یک فایل دیگر که شامل عنصر <EncryptedKey>می باشد ضمیمه سند کرد که در این حالت درون سندxmlعنصر <Data Reference>یا<KeyReference>قرار می گیرد که به آن ضمیمه اشاره می کند.

۳.در روش سوم در هیچ قسمت از سند XMlبه کلید اشاره ای نمی شود و مسیر کلید از قبل مشخص می باشد[۷]

۲-۱۰- امضای دیجیتالی

معرفی امضای دیجیتالی برای اینکه هویت فرستنده سند تایید شود و نیز برای اطمینان از اینکه سند در طول مدت انتقال به گیرنده دستکاری نشده است از امضای دیجیتالی استفاده می شود. می توان کل یک سند ویا قسمتی از ان را امضا کرد .به طور کلی سه دلیل برای استفاده از امضای دیجیتالی وجود دارد که شامل :

۱.استفاده از کلید عمومی این اجازه را به هر شخص می دهد که کلید خود را به سمت فرستنده اطلاعات بفرستد و سپس گیرنده پس از دریافت اطلاعات ان را توسط کلید خصوصی خود باز گشایی می کند .بنابراین امضای دیجیتالی این امکان را می دهد که فرستنده یا گیرنده مطمئن شوند که اطلاعات از محل یا شخص مورو نظر دریافت می شود.

۲.اطلاعات در طول مدت انتقال ممکن است توسط دیگران دستکاری شود برای اینکه از صحت اطلاعات رسیده مطمئن شویم نیاز به یک امضای دیجیتالی در این حالت احساس می شود.

۳.رد کردن اطلاعات فرستاده شده .گیرنده اطلاعات برای این که مطمئن شود فرستنده بعد از اطلاعاتی که فرستاده اعلام بی خبری نکند و انها را رد نکند از فرستنده یک امضا درخواست می کند تا شاهدی بر این ادعا باشد.

برای پیاده سازی یک امضای دیجیتالی نیاز به سه الگوریتم داریم:

- یک الگوریتم برای ایجاد کلید
- الگوریتم برای ایجاد امضا
- الگوریتم برای تایید امضا

برای ایجاد یک امضای دیجیتالی باید یک عددchecksum برای سند مورد نظر محاسبه شود. فرض کنید Bobقصد ارسال یک پیام به Aliceرا دارد،Bob پیام خود را همراه با امضای دیجیتالی برای Alice می فرستد .این امضای دیجیتالی توسط کلید خصوصی که مالک آن Bobمی باشد ایجاد شده است .در سمت دیگر Alice با استفاده از الگوریتم تایید امضا و کلید عمومی که از Bob دریافت کرده صحت امضا و این که امضا از طرفBob می باشد را تایید می کند[۱۰]

۲-۱۰-۱- علامت گذاری امضا

در این قسمت مقدار digest برای عنصر<signedinfo> محاسبه شده و درون عنصر <signatureValue> قرار می گیرد .

- اضافه کردن مشخصات کلید

می توانید مشخصات کلید خود را درون عنصر <KeyInfo> قرار دهید ولی این قسمت الزامی نیست و ممکن است شما نخواهید که این مشخصات معلوم گردد.

- تایید یک امضای دیجیتالی

مراحل تایید Verify یک امضای دیجیتالی به صورت خلاصی در زیر آورده شده است :

-تایید امضای عنصر<SignedInfo>.برای این منظور ابتدا دوباره مقدار digest برای این عنصر را طبق الگوریتم مشخص شده در عنصر <SignatureMethod>محاسبه نموده و از کلید عمومی برای این کار استفاده می شود و برای تایید آن مقدار محاسبه شده را با مقدار معرفی شده در عنصر <SignatureValue>مقایسه می کنیم

-اگر مرحله قبل بدون مشکل تایید شد حالا به ازای هر منبع معرفی شده در عنصر <DigestValue>مقایسه می کنیم[۱۰]

۲-۱۱- محافظت از داده ها با رمزنگاری

بی شک اطلاعات، یکی از ارزشمندترین دارایی های سازمان ها و کسب و کارهای امروز است و نگرش اصولی مدیران به این موضوع ، دغدغه حفاظت از این دارایی ها را در ذهن آن ها ایجاد خواهد نمود. نتایج تحقیقات انجام شده، بیانگر این واقعیت است که سالانه نیمی از کاربران کامپیوتر، اطلاعات خود را به اشکال مختلف از دست می دهند . بروز نقص در تجهیزات ذخیره سازی داده ها، خطاهای انسانی، سرقت کامپیوترها، حملات ویروسی و خطاهای نرم افزاری و نیز حوادثی نظیر آتش سوزی و زلزله ، از شایع ترین عوامل تخریب و از دست دادن اطلاعات و داده های کامپیوتری و دیجیتال است.

۲-۱۲- آیا رمزنگاری بهترین راه حفاظت از داده ها است؟

با وجود تلاش های زیادی که آژانس امنیت ملی آمریکا در جهت کرک کردن تکنولوژی های رمزنگاری انجام داده است کارشناسان امنیتی بر این باوردند که رمزنگاری ، هنوز هم بهترین راه کار برای حفظ امنیت آنلاین است.کارشناسان معتقدند که با پیاده سازی درست تکنولوژی ها ، رمزنگاری می تواند امنیتی غیر قابل نفوذ ایجاد کند، چرا که در صورت پیاده سازی نادرست فرایند های آن، سطح امنیتی می تواند به حدی پایین آید که هکرها بتوانند در ظرف چند ساعت آن ها را رمزگشایی کنند . اغلب ایمیل ها ، جستجوها در وب و تماس های تلفنی به طور اتوماتیک رمزنگاری نمی شوند بنابراین NSA براحتی می تواند با اسکن ترافیک آنلاین به آن ها دسترسی پیدا کند آسیب پذیری عمده ای که در رابطه با ترافیک رمز شده وجود دارد مربوط به مدیریت key استkey های رمزنگاری شده بسیار طولانی هستند و در واقع پسوردهایی هستند که بصورت تصادفی تولید شده اند و برای رمزنگاری و رمزگشایی ترافیک اینترنت مورد استفاده قرار می گیرند . بنابراین سرقت key ها مانند سرقت یک پسورد است[۹]

بسیاری از کمپانی ها ممکن است به استفاده از تکنولوژی های open source نظیر Open SSL روی آورند که در این صورت کدها همیشه برای توسعه دهندگان آشکار می باشد و تمامی تغییرات قابل مشاهده ، بررسی و پیگیری است . در نتیجه می توان مطمئن شد که آسیب و تهدیدی عمدی وجود ندارد.[۹]

۲-۱۳- رمزنگاری و مدیریت داده ها با Protectorion ToGo

همیشه بحث های فراوانی درباره اهمیت امنیت داده ها و چگونگی امن نگه داشتن فایل ها از گزند هکرها و سارقین وجود داشته . البته که هیچ کس نمی خواهد اطلاعات خصوصی او در دست افراد نا به کار قرار بگیرد . بنابراین ، بهتر است قبل از آنکه دیر شود ، از راهکارهای امنیتی مطلوب استفاده شود . خوشبختانه تعداد زیادی برنامه رایگان یا ارزان برای این کار در دسترس هست که می توان با آنها فایل های خصوصی را در یک محیط امن و رمزگذاری شده، قرار داد. یکی از برنامه هایی که اخیرا برای ویندوز مورد توجه قرار گرفته ، Protectorion ToGo است . هر چند مثل سایر برنامه ها نمی توان تضمین کرد که این برنامه داده های شما را از گزند افراد یا سازمان های فوق توانمند حفظ کند ولی برای نگهداری اطلاعات بانکی ، رمزها ، اطلاعات ورود به حساب های مختلف و سایر اطلاعات حساس ، گزینه ای مناسب است . این برنامه رایگان از استاندارد رمزنگاری AES-256 bit استفاده می کند و ویژگی مدیریت داده ها را نیز در خود دارد.

Protectorion ToGo در اصل طراحی شده تا داده های قرار گرفته بر روی درایو های یو اس بی فلش یا درایوهای اکسترنال را محافظت کند و کیست که نیاز به جا به جایی این درایوها را در زندگی روزمره خود حس نکند ؟ این برنامه نیاز به هیچ نوع نصبی ندارد که این ویژگی آن را برای استفاده بر روی درایوهای قابل حمل ، بسیار مناسب می کند.[۹]

۲-۱۴- روش های رمزنگاری و کنترل حملات سایبری

جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است . این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد. مارتین لیبیکی ، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی ، در کتاب «جنگ اطلاعاتی چیست ؟» می‌نویسد «تلاش برای درک مفهوم جنگ اطلاعاتی مانند این است که چند نفر نابینا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست . جنگ اطلاعاتی نیز شامل بخش‌های مختلف و متعددی می شود .» تلاش برای داشتن نگرش جامعه نگرانه در تعریف جنگ اطلاعات نکته این است که باید حتماً به آن توجه شود. مگان برنز در سال ۱۹۹۹ با نگرشی کلی تریف زیر را ارئه می‌دهد «جنگ اطلاعاتی طبقه یا مجموعه‌های از تکنیک‌ها شامل جمع آوری ، انتقال، حفاظت ، ممانعت از دسترسی ، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند[۱۰]

۲-۱۵- انواع نفوذ گران در جنگ سایبر

۱-White hat hackers

گروه نفوذگران کلاه سفید هر کسی که بتواند ازسد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند . هکرهای کلاه سفید متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا می کنند و به مسوولان گزارش می‌دهند .

۲- hackers- Black

گروه نفوذگران کلاه سیاه اشخاصی هستند که وارد کامپیوتر قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن ویروس و غیره می‌پردازند .

3-Gray hat hackers

گروه نفوذگران کلاه خاکستری اشخاصی هستند که حد وسط دو تعریف بالا می‌شوند .

4-Pink hat hackers

گروه نفوذگران کلاه صورتی این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند . گروه نفوذ گران کلاه قرمزعده ای متخصص که اطلاعاتی نادرست را به شبکه های اینترنت وارد می کنند.[۱۱]

۲-۱۶- کریپتو گرافی

رمزنگاری با کریپتوگرافی به عنوان یک روش موثر برای حفاظت از اطلاعات حساس استفاده می شود اطلاعاتی مانند اطلاعات طبقه بندی شده نظامی ، اطلاعات حساس موسسات مالی ، کلمات عبور که بر روی سیستم های رایانه یی ذخیره شده اند و داده هایی که بر روی اینترنت و یا از طریق امواج رادیویی انتشار می یابند . در حقیقت این روش جزو پایه ای ترین علوم در کار کامپیوتر محسوب می شود . زیرا هر جا احتیاج به انتقال (و یا بایگانی) اطلاعاتی است که ارزشمند هستند ، این بحث مطرح می شود که ایا این اطلاعات را می توان دور از دسترس دیگران نگه داشت . سامانه عمومی کریپتوگرافی شامل مسیر پیام کریپتوگرافی است این سامانه خود شامل فرایندهای رمزنگاری ، انتفال و رمزگشایی به همراه روشهای توزیع متغیرهای عددی و یا کلید است که انتقال رمز را کنترل می کند[۱۲]

۲-۱۷- انواع رمزنگاری در سیستم های استاندارد امن

فرایند رمزنگاری با استفاده از جا به جایی ، چرخش و یا روشهای عددی (و یا ترکیبی از آنها) ، متن عادی را به متن رمز شده تبدیل می کند . متغیرهای کلید ، که الگوریتم های تبذیل را کنترل می کند ، ایجاد توانایی تغییر در تبدیل را فراهم کرده و بنابراین به طور مستقیم بر قدرت الگوریتم در برابر حملات تاثیر گذار خواهد بود[۱۵]

۱- الگوریتم های محرمانه

این الگوریتم ها ، امنیت را از طریق الگوریتم های پنهان و یا ایجاد کانال ارتباطی فراهم می اورند . این الگوریتم روش ساده در رمزنگاری است که برای اجرای ان نیازی به کلید برای هر پیامی است که قصد داریم ان را رمزنگاری کنیم . مخفی کردن داده شاخه ای از رمزنگاری است که داده را از طریق پنهان کردن متن رمز شده در یک محیط ارتباطی مخفی ، محافظت می کند . متن رمز شده ممکن است در داخل متن ، صوت و یا تصویر پنهان شود به طوری که جریان داده دست نخورده به نظر برسد[۱۵]

۲- الگوریتم های عمومی

رمزنگاری انبوه یکی از پرکاربردترین روش های استفاده از رمزنگاری برای داده ها با حجم بالاست که باید از یک مسیر انتقال شناخته شده منتقل شوند . (مانند ارتباطات ماهواره ای ، خطوط زمینی ، خطوط بی سیم ، شبکه های رایانه ای محلی و یا گسترده). الگوریتم های عمومی روش عملی برای استاندارد کردن سامانه های رمزنگاری به روش های مختلف جهت رمز کردن داده ها با حجم متوسط به بالا است . در این روش هر چند که الگوریتم برای عموم شناخته شده است ، اما کلید مخفی باقی می ماند. روش ایجاد کلید در سامانه های رمزنگاری ، شامل دو متد اصلی برای الگوریتم های عمومی است . سامانه های کلاسیک کلید مخفی که در چند دهه پیش توسط ارتش به کار گرفته می شد ، روشی برای توزیع کلید مخفی به فرستنده و گیرنده و همزمانی استفاده از کلیدها برای یک پیام خاص بود . در روش عمومی از یک معماری متقارن جهت استفاده از کلید در دو سمت فرستنده و گیرنده به کار گرفته می شود و یک هماهنگی در این دو سمت وجود دارد . الگوریتم رمز داده به عنوان بهترین الگوریتم کلید مخفی شناخته شده که قادر است بلوکهای ۶۴ بیتی داده را توسط کلید ۵۶ بیتی رمزنگاری کند[۱۵]

۳- امضای دیجیتال

فرایند رمزنگاری علاوه بر طبقه بندی ، روشی برای تشخیص هویت پیام از طریق یک مولفه داده رمز شده به نام امضای دیجیتال به شمار می رود . امضای دیجیتال هویت فرستنده را اثبات و تایید می کند که هیچ مهاجمی پیام را تغییر نداده است. مفاهیم رمزبا کلید عمومی ، اساس ایجاد امضای دیجیتال است.

۴- مدیریت کلید

تولید ، ذخیره سازی ، توزیع و مراقبت کلی از کلید ، حفاظت امنیت کلید سامانه رمز ، ضروری و حیاتی می باشد . یکی از روشهای مستقیم دسترسی غیر مجاز ، استفاده از کلیدهای لو رفته است . به همین دلیل لایه های امنیتی فیزیکی ، اطلاعاتی و ادراکی باید عملیات مراقبت از مدیریت کلید را به همراه انچه که در زیر عنوان شده است ، انجام دهند .

۱- سیاست امنیت کلید : یک سیاست امنیتی معین برای کنترل کلید در تمام دوران عمر کلید (تولید ، توزیع ، فعالیت و تخریب) باید تعریف و استفاده گردد .

۲- سلسله مراتب لایه های کلید : کلید باید در لایه های مختلف تعریف شود که لایه های بالاتر ان جهت رمز کردن لایه‌های پایین تر ، استفاده می شود .

۳- جدایی کلید : کلید باید قابلیت تفکیک به مولفه مختلف ، جهت توزیع در چند کانال ، و یا نگهداری توسط افراد مختلف را داشته باشد (جهت ایجاد امنیت بالاتر) . در عین حال که تولید ان توسط یک سامانه انجام می شود .

-کنترل طول عمر کلید – دوران اعتبار کلیدها (دوران رمز) بر حسب زمان ، حالت سامانه و یا متغیرهای دیگر تعریف می شود و باید به همراه کلید برای کاربران ارسال گردد .

۴- ضمانت کلید : بعضی سامانه ها ، توانمندی ضمانتی داشته به این صورت که داده ها در یک محدوده تاریخی توسط یک «فرد سوم معتبر» به منظور انجام تغییرات بعدی بر روی کلیدهای استقرار و رمزگشایی پیام ها ، در مواقعی که به طور قانونی از طریق سازمان های دولتی اجازه ان داده شود ، قرار می گیرند . ضمانت استاندارد رمز امریکا ، یک روش جهت ضامن کلیدها تعریف کرده است[۱۳]

۲-۱۸- مراحل دفاع

همواره اشکال متفاوتی در برخورد با فعالیت های مجرمانه در یک فضای سایبر وجود دارد. در اینجا لازم است که دو مرحله از مراحل دفاع بررسی شود[۱۴]

- جلوگیری

عبارت است از شناسایی راه های نفوذ وحمله و مقابله با آنها جهت افزایش ضریب امنیت ، ایمنی و پایداری . از جمله روشهای جلوگیری می توان به موارد ذیل اشاره نمود : طراحی امن و ایمن و پایدار سیستم ها : در صورتیکه امنیت جزو معیارها و اصول طراحی سیستم ها ، قرار بگیرد ، سیستم ها بسیار امن تر و ایمن تر و پایدارتر از قبل خواهند بود.

متوقف نمودن حملات : از دیگر راه های جلوگیری از حملات ، متوقف نمودن آنها می باشد این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم ، میسر است[۱۴]

- مدیریت حادثه ، محدود کردن خرابی ها

روش های مدیریت حوادث و محدود نمودن اثرات زیانبار حوادث ، راه هایی هستند که با استفاده از آنها می توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم. تعیین آثار ، نشانه ها و هشدارها : بدین معنی که وقتی حمله ای اتفاق می افتد ، ابتدا در گام اول باید آثار و خطراتی که این حمله میتواند داشته باشد را شناسایی کنیم ، زیرا با شناسایی آثار یک حمله می توانیم ازپیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند ، جلوگیری کنیم .

امن ، ایمن و پایدار کردن سیستم ها : جهت جلوگیری از نفوذهای بیرونی ، ضروری است تا موانعی ایجاد کنیم. از قدیمی ترین موانع نفوذ ، استفاده از کلمه عبور است که البته روش های جدیدتر ، استفاده از تکنیک هایی مانند دیوار آتش و یا پروکسی سرور ها است. البته همان طورکه شیوه های رمزنگاری شکست خوردند ، شیوه های جدید نیز میتواند منجر به شکست شوند . در مورد حملات فیزیکی نیز لازم است که ابتدا تمام حملات و نفوذهایی که می تواند انجام شود را ، شناسایی کنیم . مثلاً در مورد یک شبکه اطلاعاتی، باید استراتژی های فیزیکی مناسب جهت امن ، ایمن و پایدار نمودن مراکز داده آن اتخاذ نمود .

خاموشی و تخصیص مجدد : یک راه حل دیگر این است که سیستم به طور کامل یا به طورجزئی خاموش شود و دوباره تخصیص مجدد شود . سیستمی که متوجه شود تحت یک حمله قرار دارد ، باید موانع و دفاعهایی از خود را بنا نهد که شاید در مواقع عادی از آنها استفاده نمی کند و سعی کند قسمتهایی از سیستم را که مواجه با حمله شده اند ، ایزوله کند. البته مراحل خاموش کردن و تخصیص دهی مجدد باید به صورت بلادرنگ و به سرعت انجام گیرد .

پشتیبانی : نکتهٔ قابل توجه این است که باید همواره از اطلاعات جمع آوری شده ، قبل از هر حمله ای پشتیبانی کنیم . این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده اند ، به دست می آید . بسیاری از روش های دفاع ، نیاز به این دارند که حالت صحیح سیستم قبل از حمله را ، جهت تسهیل در بازیابی و تجدید مجدد بدانند . این روش برای مواقعی است که حملات براساس نقطهٔ شروع دقیق و مشخصی انجام می شود و پشتیبانها به طور منظم گرفته می شوند. بسیاری از حملات موذیانه به کندی و بطور محرمانه ، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند ، ایجاد می کنند (یعنی در اینگونه از حملات ما زمان دقیق سالم بودن اطلاعات را نداریم و تاثیر حملات هنوز ایجاد نشده است). در این حالت ، جهت ایجاد فضای سالم ، سیستم های سازمان باید خودشان برنامه هایی تهیه نسخه پشتیبان داشته باشند[۱۴]

۳- بحث و نتیجه گیری

همانطور که دیدید، رمزنگاری به هیچ وجه موضوع تازه‌ای نیست و حتی ژولیوس سزار نیز برای مخابره پیام‌های خودش به فرماندان نظامی از رمزنگاری استفاده می‌کرده است. با اینکه رمزنگاری تا همین چند دهه گذشته فقط کاربرد نظامی و جاسوسی داشته است اما امروزه تقریبا در تمامی جنبه‌های زندگی روزمره ما کاربرد دارد. با گسترش کاربرد اینترنت و استفاده از شبکه‌های باز برای مخابره اطلاعات حساس و محرمانه مثل گذرواژه‌های حساب‌های بانکی، اهمیت رمزنگاری در زندگی روزمره انسان بیشتر و بیشتر شد و امروزه تقریبا تمامی اطلاعاتی که بر بستر اینترنت منتقل می‌کنیم، رمزنگاری می‌شوند. تکنیک‌های بسیار زیادی برای رمزنگاری وجود دارد ولی به طور کلی می‌توان این تکنیک‌ها را در دو دسته رمزنگاری متقارن، رمزنگاری نامتقارن جای داد. رمزنگاری متقارن همان روشی است که ژولیوس سزار از آن استفاده می‌کرد اما روش دیگر، از توابع ریاضیاتی یک طرفه استفاده می‌شود.

مراجع

[۱]ستایشی، س، مقدمه ای بر رمزنگاری اطلاعات ، ماهنامه پردازش ، ش ۵۷ ، ۱۳۸۹.
[۲]وفایی، مجید، مقدمه ای بر رمزنگاری اطلاعات ، ماهنامه پردازش ، ش ۳۹ ، ۱۳۸۹.
[۳]زارعی فر، م ع، الگوریتم رمزنگاری اطلاعات ، ماهنامه پردازش ، ش ۳۹ ،۱۳۸۹.
[۴]امنیت وب ، سایت اطلاع رسانی امنیت اطلاعات ایران ، فروردین ۱۳۸۹ .
[۵]جاوید، م، امنیت اطلاعات ، تهران، علوم رایانه ، ص ۱۸، ۱۳۸۹.
[۶]یادگاری، م، محافظت از داده ها با رمزنگاری ، تهران ، انتشارات جام جم ، ص ۳۲ ، فروردین ۱۳۹۰.
[۷]زرگر ، م. محافظت از داده ها با رمزنگاری، تهران ، انتشارات جام جم ، ص ۳۸ ، فروردین ۱۳۹۰ .
[۸]ایران ، گروه مشاوران مهندسی نیرانا ، "عصر فناوری اطلاعات " تهران ، ص ۴، ۱۳۸۹.
[۹]خراشادی زاده، ح، محافظت از داده ها با رمزنگاری ،تهران، انتشارات جام جم ، ۱۳۸۸ .
[۱۰]محمودی ، ف ، روش های رمزنگاری و کنترل حملات سایبری ، تهران ، انتشارات عصر فناوری اطلاعات ، مرداد ۱۳۹۱.
[۱۱]ایران ، فرهنگستان زبان و ادبیات فارسی ، دفتر هفتم واژگان مصوب ، تهران ، ۱۳۸۲.
[۱۲]وود، ل ، رمزنگاری و چالش های پیش رو ، ترجمه محمد جعفر کاظمی ، تهران ، انتشارات فناوری دانش ، بهمن ۱۳۸۹.
[۱۳]کاظمی، م ج ، پایگاه خبری فناوری اطلاعات، تهران ، انتشارات جام جم ، ص ۴۲ ، ۱۳۹۲.
[۱۴] K. Yanagimoto, T. Hasegawa, M Takano " A New Encoding Approach Realizing High Security and High Performance Based on Double Common Encryption Using Static Keys and Dynamic Keys",NTT West Corporation 6-2-82 Shimaya, Konohana-kuOsaka 554-0024, Japan.
[۱۵] C.S. Brès, Y.-K. Huang, I. Glesk, and P.R. Prucnal. Scalable asynchronous incoherentoptical CDMA [Invited]. J. Opt. Netw., 6:599–615, 2007.