به نام خدا

امنیت در تجارت الکترونیک

(رشته فناوری اطلاعات و امنیت اطلاعات)

Electronic Commerce Security

ویژه دانشجویان

تدوین : مهندس علی ثاقب موفق

امنیت در تجارت الکترونیک

مقدمه:

با رشد روز افزون اطلاعات و سیستم های مبتنی بر اطلاعات، امنیت اطلاعات نیز اهمیت یافته است. حال امنیت از ابعاد مختلف می تواند مهم باشد که یکی از آنها اقتصادی است. همواره منافع مالی و اقتصادی ترغیب کننده بسیار قوی برای هرگونه اقدام خرابکارانه بوده است. یعنی یکی از اهداف هکر ها و مخرب های سیستم ، هدف مالی و اقتصادی بوده است که در کنار هدف های سیاسی، آزار و اذیت و اجتماعی ،جزو مهمترین اهداف آنها نیز به شمار می آید و بخش عمده ای از هکر ها با هدف مالی اقدام به هک کردن سیستم های مالی و بانکی و یا کشف شماره های کارت اعتباری و یا نفوذ به نرم افزارهای مربوطه به مبادلات مالی و تراکنش های آن می نمایند که همان تجارت الکترونیک محسوب می شود.

لذا با توجه به همه گیر شده کاربردهای فناوری اطلاعات منجمله کسب و کار الکترونیک، ضروری است تا به موضوع امنیت آن نیز توجه ویژه ای شود.

۱. مسایل مهم امنیتی در تجارت الکتریکی

برای انجام داد و ستدهای الکترونیکی، باید به مسایل امنیتی توجه شود تا مشکلی برای خریدار و فروشنده پیش نیاید. پس باید به سرویس های امنیتی کارآمد برای منابع و ارتباطات اندیشید. در این بخش مهم ترین مسایل ایمنی همراه با خطرات و تدابیر رویارویی با آنها به طور خلاصه بیان شده است .اما گفتنی است که با وجود این سرویس ها و تدابیر، هنوز هم امنیت صد در صد برای تجارت الکترونیکی به دست نیامده است .

۱–۱ تایید هویت یا اصالت

که به موجب آن، فرد یا سازمان بتواند هویت خود را اثبات کند، فرآیندی است که تضمین می کند یک هویت همان است که ادعا می شود. سرویس های تایید هویت، درستی یا نادرستی هویت طرف های بازرگانی در معامله را آشکار می کنند. واژگان رمز،گواهی ها روش های زیست سنجی از خطر جعل هویت می کاهند .

۱–۲مجوز

سیستم با استفاده از مجوز می تواند دسترسی به منابع را پس از تایید هویت مبادله گران کنترل کند. تشخیص مجوز فرایندی است که روشن می کند یک سرویس گیرنده اجازه انجام چه کارهایی را دارد و یک هویت چه جایگاهی در دسترسی به منابع خواهد داشت.

رخداد خطرات دسترسی بدون مجوز به منابع سیستم با ایجاد محدودیت به کمک لیست های کنترل دستیابی برای تعیین اینکه چه کسانی اجازه دستیابی به منابع را دارند کاهش می یابد .

۱–۳ محرمانگی و خصوصی بودن

محرمانه نگه داشتن محتویات پیام های مبادله شده میان طرف های مجاز را تضمین می کند. سرویس های خصوصی بودن از آشکار شدن داده ها و اطلاعات شخصی کاربران برای افراد و سازمانهای غیر مجاز، جلوگیری می کند. این سرویس ها تضمین می کنند که داده فرستاده شده روی شبکه تا زمانی که در راه است خوانده نشود .برای اینکار، این گونه سرویس ها حفاظت پیام ها را در برابر سو استفاده، رهگیری و شنود تامین می کنند. به کمک رمز نگاری پیام ها، دسترسی غیرمجاز به پیام ها توسط افراد درون سازمانی یا برون سازمانی، با رهگیری هنگام مخابره دشوارتر می شود .

۱–۴ تمامیت یا درستی داده ها

برای جلوگیری از دستکاری، یا حذف ناخواسته پیام ها می باشد. سرویس های تامین تمامیت اطلاعات می کوشند تا داده فرستاده شده در شبکه، در طول راه دچار دگرگونی یا گم نشود. بدون این سرویس ها، یک شخص غیر مجاز ممکن است یک بسته یا پیام را از شبکه بگیرد، آنرا تغییر دهد و دوباره در جریان اندازد، بدون اینکه تغییرات برای گیرنده بسته یا پیام آشکار شود. با تایید بسته و رمز نگاری پیام ها می توان بروز اشتباه تصادفی یا متغلبانه در هنگام ورود داده ها ونیز تخریب و تغییر پیام ها را کاهش داد .

۱–۵ عدم انکار ارسال و دریافت پیام

توانایی تضمین اینکه، طرفین معامله نتوانند محتویات پیام مبادله شده را انکار کنند. با سرویس های انکار ناپذیری، فرستنده و گیرنده نمی توانند ارسال و دریافت پیام را انکار کنند. تایید اصالت پیام با آمیزه ای از آنچه که کاربر می داند، آنچه که کاربر در اختیار دارد و یا ویژگی های فیزیکی کاربر مانند روش های زیست سنجی در برابر جعل هویت و انکار پیام ها به بازرگانان یاری می رساند .

۱–۶ در دسترس بودن

امکان دسترسی به داده ها در زمان و مکان مناسب همراه با ایمنی از دسترسی غیر مجاز به داده را تامین می کند. از خطرهای تهدید کننده این ویژگی می توان خطای شبکه، قطع برق، اشتباهات عملیاتی، اشتباهات کاربردی، خطای سخت افزار، خطای نرم افزار سیستم و ویروس ها را نام برد که با گزینش راه های ارتباطی جایگزین، پیش گیری از قطع برق، آزمایش کیفیت نرم افزار و سخت افزارها، محدود ساختن دسترسی و تامین سیستم پشتیبانی داده ها از آنها کاسته می شود.

در ادبیات تجارت الکترونیک و در ارتباط با امنیت اطلاعات در شبکه‌های اینترنت سه موضوع مهم به شرح زیر مطرح می‌باشند:

۱-۶-۱_ Authentication .که عبارت است از احراز هویت طرفین فرآیند تجاری.

۱-۶-۲_ Encryption .که به‌مفهوم رمزنگاری می‌باشد. هر رکورد اطلاعاتی می‌باید به‌گونه‌ای رمزنگاری شود تا سایر افراد نتوانند آن‌را خوانده یا در آن تغییراتی را اعمال نمایند.

۱-۶-۳ _Authorization .پس از احراز هویت و رمزگشایی رکورد دریافتی متقاضی موضوع بعدی، محدوده دستیابی به رکوردهای بانک‌های اطلاعاتی و مجموعه عملیاتی که از قبل تعیین گردیده است تحت عنوان مجوز دستیابی یا Authorizationمی‌باشد که آن‌هم از اهمیت ویژه‌ای برخوردار است.

فرآیند رمزگذاری و رمزگشایی داده‌ها توسط یک کلید و مجموعه‌ای از الگوریتم‌های رمزنگاری صورت می‌پذیرد. در فرآیند مذکور پیامی که می‌باید رمز گردد و به آن Plaintext Message گفته می‌شود ابتدا به ردیفی از بلوک‌های چندبیتی (n-bit blocks) تقسیم می‌گردد. سپس فرآیند الگوریتم رمزنگاری (encipher algorithm) با استفاده از یک کلید و بلوک‌های فوق به‌عنوان داده‌های ورودی پس از اجرای فرآیندهای تعریف‌شده در الگوریتم رمزگذاری، بلوک‌های رمزشده نظیربه‌نظیر را با همان طول به عنوان خروجی جهت انتقال روی شبکه اینترنت دراختیار قرار می‌دهد و متعاقباً در سمت گیرنده، الگوریتم‌های رمزگشا (cipher algorithm) با استفاده از همان کلید، بلوک‌های رمزشده cyphertext block را تبدیل به پیام اولیه می‌نمایند. در الگوریتم‌های پیشرفته رمزگذاری زنجیره رمزگذاری (cipher chaining)یعنی عملیات رمزگذاری و رمزگشایی روی هر بلوک، بستگی به محتویات بلوک قبلی دارد.

باید توجه داشت که در این روش الگوریتم‌های مذکور دراختیار همگان قرار دارد و سالهاست که از آنها استفاده می‌گردد. آنچه که مهم است دانستن کلید توسط طرفین فرآیند تجاری می‌باشد. قابل ذکر است که علاوه بر بکارگیری شیوه فوق در انتقال داده‌ها در ذخیره‌سازی داده‌ها نیز از این الگوریتم‌ها استفاده می‌گردد. نکته قابل تعمق در این روش توزیع کلید روی اینترنت است.

اگر قصد خرید اینترنتی از یک فروشگاه الکترونیکی را دارید باید با چشمانی باز این کار را انجام دهید .ما نمی خواهیم خرید اینترنتی را یک کار عجیب و سخت جلوه دهیم اما وقتی شما به صورت فیزیکی هم خرید می کنید مطمئنا از یک مکان معتبر خریدهای خود را انجام می دهید. خرید الکترونیکی شاید ساده ترین و لذت بخش ترین کاری باشد که شما در اینترنت می توانید انجام دهید به شرطی که به یک سری نکات مهم توجه داشته باشید.

۲.خرید از فروشگاه های معتبر

قبل از خرید در مورد فروشگاهی که می خواهید از آن خرید کنید. تحقیق کنید فروشگاه های معتبر عموما آدرس پستی، تلفن و مشخصات خود را به طور دقیق بر روی وب سایت شان درج می کنند. دقت کنید که فروشگاهی که از آن خرید می کنید یک فروشگاه فعال است یا یک وب سایت رها شده. درنظر داشته باشید تعداد زیادی وب سایت رها شده در اینترنت وجود دارند که روزی به مشتریان خود سرویس دهی می کردند اما به علل مختلف بی استفاده مانده اند. اگر از طریق تبلیغات با فروشگاه آشنا شدید تقریبا می توان اطمینان داشت که فروشگاه موردنظر فعال است، اما اگر به طور اتفاقی وارد فروشگاه شدید باید بررسی بیشتری نمایید.

معمولا وب سایت های فعال بخش اخبارشان به روز است و به عنوان یکی از نشانه های به روز بودن فروشگاه می توان درنظر گرفت است و یا اینکه بررسی کنید اطلاعات تکمیلی در مورد کالا به همراه قیمت دقیق و شرایط و هزینه های ارسال درج شده باشد معمولا فروشگاه هایی که یک شعبه فیزیکی دارند بسیار مطمئن تر از فروشگاه هایی هستند که فقط به صورت مجازی پایه گذاری شده اند و آمارها نیز نشان می دهد اعتماد افراد به فروشگاه هایی که شعبه فیزیکی دارند بیشتر است زیرا احتمال کلاهبرداری و یا اینکه کالای خریداری شده به دست شما نرسد کمتر است و اگر مشکلی پیش بیاید می توانید به آدرس فروشگاه مربوطه مراجعه کنید.

۳.انتخاب روش خرید مناسب

وقتی از یک فروشگاه مجازی معتبر خرید می کنید معمولا انتخاب های متعددی برای نحوه خرید و دریافت کالا برای شما وجود خواهد داشت از جمله پرداخت وجه به صورت آنلاین، خرید به صورت پستی، واریز به حساب و ... همیشه سعی کنید روشی برای خرید خود انتخاب کنید که کمترین ریسک پذیری را داشته باشد.

۴.خرید به صورت آنلاین

معمولا فروشگاه هایی که ارائه دهنده سرویس های آنلاین هستند خدمات پرداخت اینترنتی خود را از یکی از بانک های معتبرکشور دریافت می کنند و بانک ها نیر معمولا بابت ارائه این نوع سرویس از فروشگاه ها مبالغی بابت ضمانت دربافت می کنند تا در مواردی که از فروشگاه مربوطه شکایتی صورت گرفت، مورد اجرا قرار دهند. استفاده از این سیستم بیشتر در مواقعی مناسب است که شما محصول خود را می خواهید به صورت الکترونیکی دریافت کنید مانند خرید کارت اینترنت و غیره. در پرداخت های آنلاین همیشه وقتی می خواهید مرحله پرداخت وجه را از طریق کارت انجام دهید وارد سایت دومی خواهید شد که سایت بانک دریافت کننده وجه است که عموما سایت های بانک سامان به آدرسsb ۲۴ com.و یا سایت بانک پارسیان به آدرس pec.ir و یا سایت معتبر دیگر بانک ها می باشد.

دقت کنید بسیاری از سارقان اینترنتی با راه اندازی سایت هایی شبیه سایت های بانک ها و آدرس های شبیه به آنها اقدام به کلاهبرداری نموده اند. اگر از مرورگر IE استفاده می کنید، بعد از ورود به صفحه پرداخت الکترونیکی بانک، تصویر یک قفل زرد رنگ پایین صفحه مشاهده می شود روی آن قفل دوبار کلیک کنید تا گواهینامه سایت بانک مذبور باز شود. در قسمت Issuedto آدرس بانک نوشته شده است. مثلا اگر وارد درگاه بانک پارسیان شده باشید باید www.pec.ir داخل این قسمت نوشته شده باشد ولی اگر وارد قسمت پرداخت شدید و این قفل زرد رنگ را ندیدید، یا نام داده شده در قسمت Issuedto درست نبود، شماره کارت و رمز خود را وارد نکنید چون نشان دهنده این است که این سایت از نظر امنیتی تایید شده نیست و یا اصلا سایت بانک نمی باشد و اطلاعات شما در اختیار افراد دیگری قرار خواهد گرفت.

۵.شیوه خرید از طریق واریز به حساب

در این روش برای خرید یک کالا باید ساعت ها در صف بانک بایستید تا مبلغ را به حساب فروشگاه واریز کرده سپس شماره فیش را در وب سایت وارد کنید تا محصول موردنظر را برای شما ارسال کنند. این شیوه یکی از بدترین شیوه های خرید اینترنتی است و حتی شاید

نتوان آن را یک خرید اینترنتی قلمداد کرد. زیرا استفاده از تجارت الکترونیک باید باعث سرعت و سهولت در خرید گردد، اما در این روش شما دردسر بیشتری نسبت به خرید فیزیکی خواهید داشت. از نظر امنیتی هم استفاده از این روش خرید غیرعاقلانه است در پرداخت های الکترونیکی تمام سوابق تراکنش های مالی شما در سیستم ثیت می شود و حتی مشخص است که این کالا در چه تاریخی و از چه فروشگاهی و با چه قیمتی خریداری شده است.

اما در حالتی که شما به حساب فرد مبلغی واریز می کنید ممکن است هیچ وقت چیزی به دست شما نرسد و چون شما مبلغ را در بانک واریز کرده اید و این فروشگاه اینترنتی برای بانک شناخته شده نیست و فروشگاه ضمانتی هم به بانک نداده است اثبات اینکه شما مبلغی را بابت خرید محصول خاصی که در اینترنت وجود داشته پرداخت کرده اید مشکل تر است و ردیابی آن سخت تر و یا اگر بر فرض فیش بانکی را گم کنید که اوضاع وخیم تر خواهد شد.

بسیاری از سارقان از این روش نیز برای کلاهبرداری های اینترنتی خود استفاده می کنند و با راه اندازی یک سایت و ارائه یک محصول با قیمت وسوسه انگیز و ارائه شماره حساب از مشتریان می خواهند مبالغ را واریز کنند .معمولا این افراد درخواست مبالغ اندکی از مشتریان می کنند، به طور مثال ۳ تا ۵ هزار تومان. به همین خاطر بیشتر افراد وقتی چیزی بدستشان نمی رسد در پی شکایت نمی روند، اما درنظر بگیرید این افراد از هزاران نفر به این شیوه کلاهبرداری می کنند و مبالغ کلانی به جیب می زنند!

۶.خرید پستی

شاید بتوان گفت امن ترین روش خرید اینترنتی استفاده از سیستم پست خرید شرکت پست باشد که امروزه اغلب فروشگاه نیز از این سرویس استفاده می کنند .شما با استفاده از این شیوه می توانید محصول خود را سفارش دهید و محصول موردنظر توسط شرکت پست برای شما ارسال شده و سپس مبلغ کالا را به مامور پست تحویل می دهید. می بینید که در این روش شما با اطمینان خاطر و بدون اینکه پولی را از پیش پرداخت کرده باشید می توانید محصول خود را خریداری کنید. استفاده از این روش برای کالاهایی که ماهیت فیزیکی دارند بسیار مناسب است. همیشه سعی کنید در فروشگاهی که امکان خرید پستی وجود دارد از این روش استفاده کنید البته از این شیوه در محصولاتی که ماهیت فیزیکی ندارند مانند کارت اینترنتی و اطلاعات و حق عضویت و ... نمی توان استفاده کرد و باید از شیوه پرداخت آنلاین استفاده شود.

گرچه سالهاست که واژه ی تجارت الکترونیک وارد ادبیات کسب و کار شرکت ها شده است، اما تجارت موبایل پدیده ای نسبتاً نوین است. توانایی استفاده از اینترنت ورای زمان و مکان از طریق تلفن های همراه فرصت های جدیدی را برای فروش، تعامل و تبادلات تجاری پدید آورده است .چنانچه شرکت ها بتوانند به مشتریان خود خدمات فردی و مطابق با انتظارات و سلیقهء ایشان را ارائه دهند طبعاً زمینه مناسبی برای توسعهء این سبک از تجارت پدید خواهد آمد.

تحقیقات متنوعی در حوزهء رضایت و وفاداری مشتری در تجارت الکترونیک به عمل آمده است که "رضایت الکترونیکی" و "وفاداری الکترونیکی" نامیده می شوند. عواملی که منجر به رضایت و وفاداری الکترونیکی می شوند به شرح زیر قابل اشاره اند: راحتی، فرایند خرید، قابلیت اطمینان سایت، اطلاعات، خدمات مشتری، قیمت، امنیت.

راحتی به عواملی همچون سهولت کاربری، سهولت دسترسی و جابجایی در سایت، سهولت درک محتوای سایت، مفید بودن سایت و کارکرد فروشگاه مجازی اشاره دارد .به عبارت دیگر گردش در سایت نباید موجب زحمت برای کاربر شود.

فرایند خرید دو بعد سفارش و تحویل را دربر می گیرد. در فرآیند سفارش، کارآیی سفارش، وضوح فرایند سفارش، زمان تراکنش و زمان پاسخگویی فروشگاه مطرح است و در فرایند تحویل زمان تحویل، سلامت محصول و کیفیت محصول در زمان تحویل مد نظر است. به بیان ساده، مشتری باید به راحتی این فرایند را طی کرده و احساس کند که همهء مراحل به روشنی تشریح شده است.

قابل اعتماد بودن سایت وب به جوانب سیستم و قابل اعتماد بودن سیستم، محصول، رقابت پذیر بودن در حوزهء ایجاد ارزش، تنوع محصولات، منحصر به فرد بودن محصولات و گارانتی کیفیت می پردازد. به عبارت دیگر فرد باید اطمینان داشته باشد که محصولات ارائه شده از طریق این سایت کیفیت لازم را دارند و می تواند بدون هیچگونه نگرانی نسبت به خرید از سایت اقدام نماید.

از بعد اطلاعاتی، سایت باید مفید بوده و اطلاعات کافی در حوزهء قبل از خرید ارائه دهد. همچنین تصویر ارائه شده از سایت باید مطابق با انتظارات باشد.

امنیت سایت از لحاظ حفظ اطلاعات مشتریان و امن بودن تبادلات مد نظر است .تعداد پنجره هایی که اطلاعات فردی را بررسی می کنندو میزانی که سایت اطلاعات مربوط به حراست از اطلاعات خصوصی افراد را مورد تاکید قرار می دهد، همگی در این حوزه مطرح اند.

قیمت با توجه به وجود امکان مقایسه در لحظه با دیگر سایت ها اهمیتی دو چندان می یابد (البته در صورتی که قیمت محصولات در سایت لحاظ شود.)

سطح خدمات مشتری به میزان تعامل با مشتری، قابلیت تطبیق سفارشات با ویژگی های مورد نظر مشتری بستگی پیدا می کند. قابل رویت بودن سایت به نحوی که سایت شناخته شده باشد و در موتورهای جستجو به راحتی یافت شود، اشاره دارد.

در حوزهء تجارت موبایل نه تنها کلیهء عوامل فوق مطرح است، بلکه باید در نظر داشت که هزینه اتصال به اینترنت بالاتر از هزینه های خطوط معمول می باشد و در عین حال، برخلاف سایت های معمول اینترنتی در این سبک از تجارت، مشتری از طریق پورتال های موبایل به سایت مورد نظر خود وصل می شود و به همین لحاظ در اینجا خدمات مبتنی بر مکان، مشتری، و سفارش مشتری موضوعیت می یابد.

بدین ترتیب عوامل زیر در مورد تجارت موبایل نیز در نظر گرفته می شود:

۱ – رفتار مشتری به میزان جدیت و قصد وی در خرید و همچنین در دسترس بودن امکانات مورد نظر در مکان ها و زمان های مختلف بستگی دارد.

۲ – قابل رویت بودن اطلاعات با توجه به اندازهء محدود صفحه نمایش موبایل از عوامل مهم در انتخاب دستگاه های همراه به عنوان کانال خرید محسوب می شود.

در عین حالی که عوامل تفاوت و مشترک بین این دو سبک از تجارت وجود دارد، اولویت های مشتریان در رده بندی این عوامل یکسان نیست.

۷. عوامل کلیدی در تجارت الکترونیک:

قابل رویت بودن

امنیت

فرایند خرید

راحتی

سفارشی سازی

عوامل کلیدی در تجارت موبایل

قابل اعتماد بودن محتوا

در دسترس بودن

فرایند خرید

برداشت از هزینه/قیمت تراکنش موبایل

خدمات مشتری

سه ویژگی موردنظر مشتری در تجارت موبایل (قابل اعتماد بودن محتوا، در دسترس بودن، برداشت از هزینه تراکنش موبایل) صرفاً در تراکنش های موبایل مدنظر است که قبلاً در تجارت الکترونیک به این شدت مطرح نبود.

۸. مشکلات امنیت در تجارت الکترونیکی

درخصوص تجارت الکترونیک که در فضای مجازی انجام می شود. تامین امنیت داده های الکترونیک پیچیده و مشکل است. با استفاده از خدمات امنیتی این اطمینان برای افراد ایجاد می شود که دسترسی به سیستم تجارت الکترونیک و داده های آن تنها محدود به افراد مجاز و مطابق با سیاست های امنیتی عنوان شده از طرف وب سایت فرستنده است. بعنوان مثال اطلاعات شخصی و شماره کارت اعتباری در صورت عدم حفاظت ممکن است در جریان انتقال توسط عوامل غیر مجاز دستکاری شوند. انجام خدمات امنیتی در رفع دغدغه های مرتبط با ریسک های حوزه امینت و حریم خصوصی تاثیر گذار است. باید تضمین کرد که فرستنده و گیرنده بتوانند متن پیغام را ببینند، متن داده در طول انتقال دستکاری نشود، فرستنده یاگیرنده نتواند ارسال و دریافت داده را انکار کند. در اینجا سه روش رمزنگاری، امضاء دیجیتال و گواهی دیجیتال که به افزایش چشمگیر امنیت در تجارت الکترونیک منجر می شود، بررسی می شود.

۹.روش های افزایش امنیت

در ذیل به سه روش افزایش امنیت اشاره می شود:

۱_الگوریتم های رمزنگاری

۲_امضاء دیجیتال

۳_گواهی دیجیتال

۹–۱ الگوریتم های رمز نگاری:

یکی از ابزارهای فنی ایجاد امنیت در تجارت الکترونیکی، رمزنگاری داده ها می باشد. در ذیل سه الگوریتم رمزنگاری شرح داده شده است:

الگوریتم متقارن Symmetric Algorithms

الگوریتم نامتقارن Asymmetric Algorithm

الگوریتم های Hash Hash Algorithms

۹–۲ الگوریتم های متقارن:

فرستنده داده را رمزنگاری کرده و برای گیرنده می فرستند. برای اینکه گیرنده بتواند داده ارسالی را بخواند باید کلیدی که داده با آن رمزنگاری شده است را داشته باشد. الگوریتم های متقارن برای رمزنگاری و رمزگشایی داده ها فقط از یک کلید استفاده می کنند. این کار موجب محرمانگی در انتقال داده ها می شود. به این الگوریتم، الگوریتم یک کلیدی هم گفته می شود. از الگوریتم های متقارن می توان DES – Data Encryption Standard , AES – Advanced Encryption Standard , Blowfish را نام برد.

نقاط ضعف الگوریتم های متقارن را می توان موارد زیر ذکر کرد:

۱_ مبادله کلید (key exchange) : انتقال کلید بین فرستنده و گیرنده کار بسیار دشواری است.

۲_ نگهداری کلید (key holder) : فرستنده به ازای هر گیرنده باید یک کلید داشته باشد و نمی تواند تمامی فایل های خود را با یک کلید ارسال کند. لذا به تعداد هر دو نفر باید یک رمز تعریف شود. اگر تعداد گیرندگان زیاد باشد ، نگهداری کلیدها به سختی امکان پذیر است.

۳_ اعتماد به کلید (key trust): اگر دو گیرنده کلیدهایشان را به یکدیگر بدهند، فرستنده مطلع نمی شود. درصورتیکه فرستنده نخواهد داده ای که به گیرنده ای می فرستد، گیرنده دیگر آنرا ببیند، اگر دو گیرنده کلیدهایشان را با هم رد و بدل کرده باشند، می توانند ببینند.

از نقاط قوت این الگوریتم می توان به جابجایی بسیار سریع داده ها اشاره کرد.

۹–۳ الگوریتم های نا متقارن:

این الگوریتم بسیار مشهور را زوج کلیدی یا دو کلیدی نیز می نامند. در این روش داده با یک کلید رمز می شود و سپس با زوج کلید آن، می توان آن را رمز گشایی کرد. هر فرستنده یک جفت کلید تولید می کند. یکی از کلیدها، کلید عمومی یا public key است و صاحب کلید، آن را در اختیار سایرین قرار می دهد و با آن رمزنگاری صورت می گیرد. کلید دیگر، کلید خصوصی و private است و فقط در

اختیار خودش (صاحب کلید) است و برای رمز گشایی استفاده می شود. در صورتیکه فرستنده بخواهد متن رمز شده ای را برای گیرنده بفرستد، باید کلید عمومی گیرنده را داشته باشد. فرستنده داده را با کلید عمومی گیرنده رمز کرده، ارسال می کند. چون گیرنده کلید خصوصی آن کلید عمومی را دارد، تنها کسی است که می تواند متن رمز شده را باز کند. یعنی اگر حتی این متن رمز شده در اختیار کس دیگر قرار گیرد (حتی خود فرستنده) چون جفت کلید مربوط به رمزگشایی را ندارد، امکان بازکردن رمز را ندارد. در نتیجه محرمانگی به طور کامل برآورده می شود.

در این روش، مشکل مبادله کلید حل شده است ولی مشکل نگهداری کلید همچنان وجود دارد. به دلیل امکان لو رفتن کلید خصوصی مشکل اعتماد به کلید نیز باقیست. الگوریتم های نامتقارن درعمل سرعتشان تقریبا هزاربار کند تر از الگوریتم متقارن است. زیرا نیاز به قدرت پردازش محاسباتی بیشتری دارند. معروف ترین الگوریتم های نامتقارن عبارتند از RSA-Rivest, Shamir , and Adelman و Diffie Hellman .

برای حل مشکل سرعت و در عین حال حفظ محرمانگی، فرستنده با روش الگوریتم متقارن یک کلید خلق می کند. این کلید را با کلید عمومی گیرنده رمزنگاری می کند و می فرستد. در نتیجه فقط گیرنده قادر به رمزگشایی و رسیدن به کلید متقارن است. از این به بعد فرستنده ، داده را با روش متقارن که بسیار سریعتر است، رمزنگاری و ارسال می کند. برای حفظ محرمانگی به طور متناوب کلیدهای متقارن جدید ایجاد می کند و دوباره رمزنگاری می کند و می فرستد تا فرستنده با کلید جدید رمزگشایی کند.

۹–۴ الگوریتم HASH

فرستنده با استفاده از این الگوریتم عمل رمزنگاری را به طور یک طرفه بر روی داده ها انجام می دهد و با استفاده از تابعی به اصطلاح از فایل hash می گیرد. (از خصوصیات فایل hash شده این است که از این فایل نمی توان به فایل اصلی رسید و همچنین اگر یک فایل چندین بار به تابع hash داده شود، خروجی یکسان است.

در صورت تغییر حتی یک بیت در فایل، فایل hash جدید کاملا متفاوت از قبلی است. با این عمل یک چکیده از متن اصلی به دست می آید که به آن Digest می گویند. فرستنده ، متن اصلی و چکیده را با سایر سرویس های امنیتی مانند امضاء دیجیتال و یا گواهی دیجیتال برای گیرنده می فرستد. گیرنده با رمز های متقارن یا گواهی دیجیتال و یا رمز دیجیتال و یا هر دو، متن اصلی را کشف می نماید. برای اطمینان از دست نخوردن متن ، گیرنده متن را با استفاده از تابع hash می کند. حال دو متن digest را در اختیار دارد و این دو را با هم مقایسه می کند. در صورتیکه کوچکترین بیتی بین راه عوض شده باشد. مشخص می شود. در نتیجه موضوع صحت و یکپارچگی برآورده می شود. از مهمترین الگوریتم های Hash می توان MD4 – Message Digest و , MD5 و SHA-1, SHA-2 Secure Hash Algorithm را نام برد. در این روش همچنیین مشکل کلید و اطمینان به کلید وجود دارد. برای حل این مشکلات از CA: Certificate Authority استفاده می شود.

۹–۵ امضاء دیجیتال:

امضاء سبب رسمیت یافتن، تایید سند و ایجاد التزام به مندرجات آن است. امضاء کننده با امضای یک نوشته هویت خود را بعنوان نوسینده مشخص می کند و جامعیت آن را تایید می کند. لذا در بستر مبادلات الکترونیک و در خصوص تامین امنیت پیام ها، امضا اهمیت اساسی و اجتناب ناپذیری پیدا می کند. امضای دیجیتال، ابزار اعتبار بخشیدن به اسناد الکترونیکی می باشد که منجر به سندیت بخشیدن به یک رکورد الکترونیکی از طریق رمز نگاری نامتقارن می شود.

هنگامیکه فرستنده بخواهد داده ای را امضاء کند، با استفاده از الگوریتم Hash از متن اصلی Digest تهیه می کند و آن را با کلید خصوصی خودش رمز می کند. با این کار امضای مربوط به آن داده تهیه می شود (در نتیجه امضای هر سند متفاوت با سند دیگر است؛ در نتیجه هر سند امضای منحصر به فرد خود را دارد. امضا را همراه با داده اصلی برای گیرنده ارسال می کند. از آنجائیکه کلید خصوصی باید بصورت محرمانه توسط صاحب آن نگهداری شود برای امنیت، می توان آن را بر روی کارت هوشمند (smart card) ذخیره کرد. در سال های اخیر کارتهای هوشمند قویتر و امن تر شده اند.

گیرنده جهت کنترل صحت امضا، ، امضای دیجیتالی را با کلید عمومی فرستنده که قبلا دریافت کرده است، رمزگشایی می کند. از داده فرستاده شده Hash تهیه می کند و آن را با امضای رمزگشایی شده مقایسه می کند. چنانچه نتیجه یکسان بود، امضاء پذیرفته می شود.

امضای دیجیتال بصورت خودکار و توسط کامپیوتر تولید می شود. با توجه به اینکه کلید خصوصی فقط در اختیار دارنده آن است و داده یا استفاده از آن رمزنگاری شده است، در نتیجه احراز هویت و انکار ناپذیری برآورده می شود. بدلیل استفاده از الگوریتم Hash یکپارچگی داده حفظ می شود. امضای دیجیتال در مورد محرمانگی کاربردی ندارد.

۹-۶ گواهی دیجیتال :

این سوال پیش می آید که چطور می توان اطمینان کرد که کلید عمومی متعلق به کسی است که ادعا می شود. به عبارت دیگر، هویت فرستنده و صحت امضای وی به چه نحو اثبات می شود؟ برای حل این مساله، مرجع ثالثی به نام " مرجع گواهی" Certificate Authentication وجود دارد که گواهی دیجیتال را به منظور تایید هویت امضاء کننده، صادر می کند. اگر کسی تقاضا برای دریافت گواهی دیجیتال داشته باشد، یک درخواست که شامل مشخصات درخواست کننده و نوع درخواست است به همراه کلید عمومی خود به مرجع گواهی ارسال می کند. مرجع گواهی از این فایل Hash تهیه و با کلید خصوصی خودش امضا می کند. یک نسخه از گواهی را به درخواست کننده می دهد و نسخه دیگر را نزد خودش نگه می دارد. این گواهی شامل نام و کلید عمومی درخواست کننده، تاریخ انقضای کلید عمومی، نام و امضای مرجع گواهی و عدد سریال گواهی می باشد.

هنگامیکه کسی بخواهد ارتباط رمز شده ای را برقرار کند، گواهی را به گیرنده ارائه می دهد. گیرنده باید چندین مورد را بررسی کند: تاریخ اعتبار منقضی نشده باشد، مرجع صدور گواهی را قبول داشته باشد و لیست CRL- Certificate Revocation List را بررسی کند. (این لیست شامل گواهی های باطل شده می باشد). در گواهی دیجیتال ، محرمانگی داده ها و انکار ناپذیری حفظ می شود.

۱۰. ضرورت استفاده از گواهی دیجیتال:

به دلیل اینکه تجارت الکترونیک در فضای مجازی انجام می شود و عملیات آن برای طرفین ملموس نیست، حفظ امنیت داده ها بعنوان یکی از راه های جلب اعتماد مشتریان به تجارت الکترونیک از اهمیت بالایی برخوردار است. یکی از راه های مقابله با تهدیدات، رمزنگاری داده های ارسالی می باشد. الگوریتم متقارن نوعی الگوریتم رمزنگاری است که سرعت آن تقریبا ۱۰۰۰ برابر الگوریتم نامتقارن است ولی نگهداری کلیدهای فراوان سبب ایجاد اشکالاتی می کند. با این دو الگوریتم می توان مشکل بالا را حل کرد. سرعت را بالا برد و در عین حال محرمانگی و یکپارچگی را هم حفظ کرد. الگوریتم Hash یکپارچگی و عدم انکار را برآورده می کند ولی داده ها به صورت محرمانه منتقل نمی شوند. در الگوریتم های رمز نگاری مشکل تشخیص صحت هویت فرستنده به قوت خود باقی است. به کمک امضای دیجیتال و گواهی دیجیتال این مشکل به خوبی مرتفع می شود. امضای دیجیتال در مورد محرمانگی کاربردی ندارد ولی سایر قابلیت های را دارد.

۱۱. امنیت در تجارت الکترونیکی

بی اعتمادی نسبت به امنیت تجارت الکترونیکی ممکن است ما را به سمت همان تجارت سنتی بکشاند که ناشی از شنیده های زیاد از هکرها و حمله به سایت ها و اطلاعات شخصی کاربران است. چالش بین آرامش و سادگی و استفاده آسان همواره بوده است و نهایتا به نفع آسایش و راحتی شده است.

راهبرد امنیت تجارت الکترونیکی شامل دو موضوع است :

۱_حمایت از جامعیت و صحت اطلاعات تجاری در شبکه و سیستمهای آنها

۲_انجام تراکنش های امن بین مشتری و تجارت

ابزار اصلی آن نیز استفاده از فایروال است که باعث می شود صرفا کاربران خارجی با هویت مشخص به شبکه حمایت شده تجارت الکترونیک دسترسی داشته باشند. البته طراحی اصلی آن برای سرویس های خاص است. (مثل email و دسترسی وب) به طوریکه بین اینترنت و شبکه داخلی قرار می گیرد. فایروال اکنون نقطه اصلی دفاع در امنیت کسب و کار است ولی به هر حال بخش کوچکی از معماری امنیت کسب و کار محسوب می شود چرا که تونل Smtp و Icmp اجازه می دهد که اطلاعات از پورت ها عبور کند. از آنجائیکه emailهای , inbound و outband اجازه عبور email از فایروال را می دهند. ویروس iloveyou به شبکه های دارای فایروال نفوذ می کند. مایکروسافت یک Patch برای ویروس iloveyou نوشته است که آنرا disable و حمله ddos برای سایت های مهم تجاری را مسدود می کند. بیشتر موارد امنیتی در اینترنت در نقاط انتهایی شبکه رخ می دهد نه بر روی backbone.

کرم های Codered و Nimda از فایروال عبور می نمایند چرا که از طریق پورت های سرور وب به سیستم دسترسی دارند. امنیت تراکنش ها برای مشتریان مهم و حیاتی است و بستگی به توانایی سازمان متولی آن در اطمینان بخشی به حریم شخصی کاربران دارد. تعیین هویت، جامعیت و دسترسی پذیری و بلوک کردن حملات ناخواسته از جمله این موارد هستند. حریم خصوصی تعاملات توسط مونیتورینگ شبکه غیر معتبر مورد تهدید واقع می شود که این موضوع توسط تجهیز نرم افزاری به نام برنامه های sniffer انجام می شود.

این برنامه ها در نقاط پایینی اتصالات شبکه به احتمال بیشتری یافت می شوند. راه هایی برای دفاع از آنها و تهدیدات در مقابل آنها وجود دارد . مثل رمزگذاری و توپولوژی شبکه سوئیچ شده. تراکنش ها خواهان برداشتن هر رد و جاپایی از تعاملات واقعی داده از سایت های میانی هستند. البته ثبت پیام های ایشان چیز دیگری است و برای اصلاح تعاملات واقعی اتفاق می افتد. گره ها و نود های میانی که داده را handle می کنند نباید آنها را حفظ و نگهداری نمایند بجز هنگامی که می خواهند داده را بازپخش کنند. رمزگذاری و encryption رایج ترین روش اطمینان از این اعتماد هست.

جامعیت تراکنش مستلزم روشی است که از تغییر ناخواسته تراکنش ها در هر روش انتقال به سمت مشتری و یا از سمت مشتری ممانعت بعمل آورد. کدهای چک کردن خطا (error checking code) یکی از این روش ها است. تکنیک های رمزنگاری مثل secret key , public key و امضای دیجیتال رایج ترین روش اطمینان بخشی برای حریم خصوصی تراکنش ها هستند. ضعف مشترک این تکنیک ها این است که برای پشتیبانی کلیدها از سوء استفاده یا تغییرات، بستگی به امنیت سیستمهای نقاط انتهایی دارند. در ادامه به آسیب پذیری های مدل client server می پردازیم.

با توجه به اینکه دسترسی و داده ها در سیستم های سروری هستند و در آنجا زندگی می کنند لذا حمله های هکری اولیه به سمت سیستم های سرور هدایت می شد. پس از آنکه admin های سیستم با تجربه شده اند برای هکرها سخت بود تا به سرورها نفوذ کنند و سپس هکرها تمرکز خود را به سمت خوراندن شبکه در سرور بردند. آنها به خرابکاری خود روی سرورها ادامه دادند که این از طریق شنود جریان ترافیک cleartext به سمت سرور و یا به خارج از سرور بود. رمزگذاری ترافیک شبکه ، تبدیل شبکه به توپولوژی سوئیچ شده و فیلتر سازی دسترسی های ناشناخته برخی از اقدام های متقابل به این حمله sniffer است. در پاسخ به این کار، هکرها به طور ساده به سمت لبه client شیفت می کنند و این همان جایی است که بسیاری از معماری های امنیت شبکه فرو می ریزد.

وقتی که به معماری متداول و شایع os در لبه client توجه می کنیم، ما مشاهده می کنیم یک os استفاده شده در سرور که همچنین روی سیستم client استفاده می شود یا در pc/macintosh که در client وقتی سرور و client مشابه باشند مکانیزم های دفاع مورد استفاده آنها نیز مشابه هست. حال اگر سیستم عامل Client و معماری آن بر اساس win9x یا mac os باشد ، سپس دفاع موثری در دسترس نخواهد بود. این پلت فرم سیستم عامل، امنیت built in طراحی شده ای ندارد و اجازه می دهد که هر کسی با دسترسی به سیستم قادر به حصول دسترسی و کنترل آن باشد. این معماری های os همچنان حساس به برنامه های حمله ای ویروس و تروجان خواهند بود.

دو تهدید مهم مدل client server تجارت الکترونیک ، برنامه های ویروس و اسب تروجان هستند. ویروس ها به طبع خود ویرانگر هستند اما برنامه های اسب تروجان تهدید های جدی تری می باشند، چرا که نه تنها رفتن به سمت سیستم دیگر را تسهیل میکنند بلکه اجازه حملات جامعیت داده را نیز می دهند.

۱۱–۱ ویروس ها Viruses :

ویروس ها، از آنجائیکه امنیت داخلی سیستم های client را مورد توجه قرار می دهند. عمومی ترین تهدید برای سیستمهای client محسوب می شوند. خراب کردن یک سیستم pc/mac مستلزم دسترسی به سیستم و داشتن مجوزهای خاص نوشتن کد در نواحی سیستمی حساس است.

طراحی سیستم عامل یک رویداد را در نسخه های قدیمی win 9x , mac , 8x منتشر کرده است. سیستم عامل هایی مثل nt , 2000 همچنان بر روی این نوع حمله آسیب پذیر هستند و دارای قابلیت هایی از محدود نمودن کسانی است که می توانند ویروس را فعال کنند. ویروس های مشهوری مثل irok , kak , resume , iloveyou , Melissa تاثیری روی سیستم عامل یونیکس ندارند. ویروس ها به system privilege برای اثر بخشی نیاز دارند. به طور کلی اسکیم های دسترسی ارائه شده در vms , unix و سایر سیستم های عامل چند کاربره از virus و تخریب کل سیستم جلوگیری می کند. و فقط یک فایل خاص کاربر را خراب می کند.

۱۱-۲ اسب های تروجان :

ابزارهای هکری backoffice , netbus , bo2k اجازه می دهند که یک کاربر راه دور هر اطلاعاتی را که روی pc هدف قرار گرفته را کنترل، آزمایش و مونیتور نماید. آنچه که آنها را به طور مخصوص فریب می دهد این است که آنها قادر به استفاده از pc هدف برای ارسال اطلاعات بر روی شبکه همانطور که کاربر قانونی آنرا انجام می دهد، هستند. یعنی مثل کاربر عمل می کند.

ابزارهایی تجاری مثل vncviewer , cucme هستند که همان کار را انجام می دهند. هکرهای زیادی هستند که وب سایت را کشف می کنند از قبیل , www.rootshell.com , www.cultedeadcow.com , www.portwolf/trojans.htm . www.insecure.org , http://the.pimmed.com جائیکه هر کس می تواند یک کپی از برنامه های اسب تروجان ذکر شده در بالا را دانلود نماید.

بخش خوب داستان این است که force اجازه می دهد به admin های سیستم تا از این ابزارها برای مدیریت راه دور تعداد زیاد ایستگاه های کاری استفاده نماید. این ابزار پشتیبانی مناسب sys admin معمولی است جائیکه تعداد زیادی ماشین نسبت به sysadmin وجود دارند. اما بخش بد داستان این است که force اجازه می دهد به کاربران بد تا این ابزارهای را برای اهداف سرور خود مثل جعل اسناد، تغییر داده و برای استراق سمع استفاده کنند.

یک برنامه کنترلی راه دور واقعی روی کامپیوتر قربانی غیر مضنون نصب شده است . قربانی دارای یک mini cam متصل به pc اش است و هکر می تواند ببیند آنچه داخل اتاق اتفاق می افتد. شخص گیج و حیرت زده می شود . شما می توانید ببینید دسک تاپ قربانی را با علائم سیاه شده برای اهداف گویا و روشنگر پنجره yahoo messanger که آشکار می کند به قربانی که ماشین او توسط شخص دیگری گرفته شده است. پیامی فرستاده می شود . هکر دارای کنترل کامل کامپیوتر است . هکر می تواند موس را حرکت دهد و هر برنامه ای را اجراء نماید. هر فایل را اصلاح و یا حذف کند از سیستم قربانی. بعلاوه هکر می تواند ببیند هر چیزی را که قربانی روی کامپیوتر انجام داده است.

این نوع برنامه ها نسبت به ویروس ها بسیار برای تجارت الکترونیک خطرناک هستند. از آنجائیکه بسیاری از کامپیوترهای خانگی بدون پشتیبان و یا حمایت کم به اینترنت متصل می شوند و از این نوع حمله محافظت نمی شوند. بنابراین حامیان تجارت الکترونیک بایستی روش هایی را برای فراهم نمودن ابزارها و تغییر فرهنگ کامپیوترهای شخصی به منظور امنیت محکم تر در نقاط پایانی Client ها پیدا کنند. این ابزارهای هک برای نصب روی pc ساده ترین هستند و روش های ترجیح داده شده تحویل توسط email هست.

دانش کامپیوتر واقعی غیر از اینکه چطور استفاده کنیم از مرورگر وب مورد نیاز وجود ندارد. این نوع از برنامه های مونیتورینگ می تواند به سادگی هر سیستم رمزگزاری را تبدیل نماید. از آنجائیکه آنها داده های قبل از رمز نگاری را Capture می کنند.

طراحی فیلترها برای کشف این ابزارها مشکل خواهد بود از آنجائیکه کد منبع به همراه هر یک از این ابزارها فراهم می باشد. مکانیزم های دفاع در این حالت کاهش واکنش نسبت به proactive بودن است. تفاوت اصلی بین حمله هدفمند pc dh mac و اونی که هدف آن سیستم های nt یا یونیکس است ، پهناوری سیستم در دامنه دومی آن نسبت به مبتنی بر کاربر بودن اولی است. استثناء حالتی است که کاربر admin یا کاربر root سیستم nt یا unix مورد هدف قرار بگیرد . این نوع ابزارها یک تهدید جامعیت داده و اتقلال جنبه های تجارت الکترونیکی را قرار می دهند.

بزرگترین تهدید تجارت الکترونیک کدام است؟

ویروس ها آزاردهنده ترین تهدید جهان تجارت الکترونیک هستند . آنها عملیات تجارت الکترونیک را خراب می کنند و بایستی طبقه بندی شوند. بعنوان یک ابزار dos و " از کارانداختن سرویس " . برنامه های کنترل از راه دور اسب ترجان و معادل های تجاری آنها جدی ترین تهدید در تجارت الکترونیک هستند. برنامه های اسب ترجان اجازه می دهد که جامعیت داده و حملات فریب از یک سیستم client به ظاهر معتبر شروع و حل و رفع آن می تواند بسیار پیچیده باشد.

یک هکر می تواند دستورات فریب را از یک سیستم قربانی شروع نماید و سرور تجارت الکترونیک نمی تواند بفهمد که دستور تغلبی است یا واقعی. Password protection و ارتباطات client server رمزگذاری شده و اسکیم های رمزگذاری کلید شخصی و عمومی همه اینها خنثی می شوند. برنامه تروجان اجازه می دهد که هکر همه cleartext ها را ببیند قبل از اینکه رمزگذاری شوند.

۱۲. مباحث حریم خصوصی:

سوء استفاده از حریم خصوصی مصرف کننده به سطح دولت و تجارت و مصرف کننده مربوط می شود. شرکت Bank crop آمریکا برای اعمال فریبنده خود در سال ۱۹۹۹ تحت تعقیب قرار گرفت که اطلاعات حساس مشتریان را در اختیار قرار می گذاشت تا آنها برای تبلیغات در طرح های دندانپزشکی از آن استفاده نمایند.

۱۳. حملات از کار انداختن سرویس توزیع شده:

کسب و کارهایی که یک تراکنش مبتنی بر وب را باز پخش می کنند و به آسیب پذیری در ddos ادامه می دهند. اسکریپت حمله dos ، رایج ترین ، موثر ترین و ساده ترین پیاده سازی حمله موجود روی web است. در این جا، خرابی واقعی بر روی سایت قربانی انجام نمی

شود. مسیرهای دسترسی به آن به طور ساده با پاکت های ورودی انباشته می شود. در صورتیکه پاکت های ورودی سفارشات مشتریان واقعی باشند، این برای هر تاجر و بیزینس من، یک رویا است. ولی اگر هدف حمله dos قرار گرفته باشند ، می تواند بدترین کابوس باشد.

حملات dos اولیه توسط یک ماشین در مقابل دیگری شلیک می شوند. حمله ddos جدیدترین انقلاب در حمله های dos است و موفقیت آن بستگی دارد به ناتوانایی سایت های میانی برای کشف ، بازداشتن و از بین بردن نفوذ شبکه به آنها. سایت های بیشتری برای ایجاد یک حمله ddos در برابر یک سایت قربانی در دسترس می شوند و سایت های میانی بیشتری شرکت داده می شوند.

حمله ddos به دانشگاه Minnesota بیش از ۲ بیلیون پاکت تحت ۳۰۰ سیستم در ۱۰ دقیقه تولید شد. حمله dos به طور شیطنت آمیزی ساده است. هر پاکت منتقل می شود روی اینترنت که شامل یک منبع و آدرس مقصد است. ساده ترین مثال این است که یک تراکنش icmp , ping داشته باشیم.

تراکنش اصلی عبارت است از:

۱_سیستم منبع یک پاکت "ping" به هدف می فرستد. این پاکت icmp_echo_request است که شامل آدرس منبع فرستنده و آدرس هدف دریافت کننده است.

۲_ اگر سیستم هدف قادر به پاسخ باشد، یک پاسخ به سمت آدرس مبداء لیست شده در پاکت ping می فرستد این یک پاکت icmp_echo_request_reply است.

یک پاکت ping برای تعیین اینکه ببیند آیا سایت هدف online است مورد استفاده قرار می گیرد.

حمله اصلی به نام smurf نامیده می شود و به طور ساده آدرس مبداء پاکت icmp_echo_request را با آدرس هاست غیر از فرستنده اصلی عوض می کند.

سایت منبع ناآگاه و جدید یک پاکت Reply را دریافت و از آن چشم پوشی می کند. این فرایند زمان پردازش را مصرف می کند. وقتی سایت منبع صدها هزار از این پاکت ها دریافت کند در واقع حمله dos واقع می شود. حمله smurf را Ddos یک گام جلوتر می گیرد. به نحوی که کل شبکه ها درگیر می شوند و مصالحه می کنند و slave daemon روی ماشین های خاص نصب می شوند. این slave daemon ها می توانند یک icmp , syn , udp یا حمله سیل آسایی smurf را راه اندازی کنند. اما صرفا در فرمان سیستم master که شرکت داده می شوند.

هکر فرمان حمله را به master ها می فرستد. هر کدام بازپخش می کنند فرمان را به slave daemon ها. ممکن است ده ها هزار ماشین باشد که هر یک بازپخش کنند که حمله به یک سایت ایجاد کنند. موفقیت ddos بستگی به شکست شبکه های مشارکت کننده در کشف و از بین بردن برنامه های master , slave دارد. این شکست ممکن است به دلایل زیر باعث شود:

۱_فقدان تجربیات admin سیستم

۲_ فقدان استاندارد اساسی امنیت برای هر ماشین

۳_فقدان نرم افزار جلوگیری از تهاجم برای توجه دادن به admin یا تصمیم مدیریتی که درگیر نشود.

برنامه های TFN , DDOS نامیده می شوند و Trinoo, win_trinoo و تنوع بسیاری از این نوع برنامه های اولیه وجود دارد که مفهوم آنها یکسان است. خطرناک ترین آنها در win_trinoo , win 9x نامیده می شود . زیرا میلیون ها سیستم ویندوز نسبت به سرور وجود دارد.

چرا حملات ddos خطرناک است؟ آیا سایت ها آسیب پذیرند؟ سایت های اینترنتی آسیب پذیرند اگر مدیران سایت ها patch های استاندارد نگهداری را انجام نداده باشند و سیستم هایشان را با ابزارهای کشف تهاجم به طور مرتب مانیتور نکنند. همه آسیب پذیری ها با patch های ارائه شده توسط فروشنده vendor_supplied اصلاح و درست میشود.

بهره برداری موفقیت آمیز از هر یک از این ضعف ها، کنترل کامل ماشین را به هکر می دهد. نشان می دهد که سیستم استاندارد نگهداری امنیت روی تعداد زیادی از ماشین ها انجام نشده است. این فقدان آمادگی ، مرحله ای برای حملات ddos اخیر است.

۱۴. پاسخگویی امنیت سایت های تجارت الکترونیکی:

حملات ddos به خاطر اینکه سایت ها در کشف اولیه سیستم های آنها با مشکل مواجه شده اند کار می کنند. حال اگر سیستم استاندارد نگهداری اجرا شود از حضور کامپیوترهای مشارکت کننده در حمله جلوگیری می شود. داشتن سایت هایی که مصالحه کننده ها را کشف می کنند می توانند خودشان را بعنوان شرکای نا آگاه جدید در حمله قلمداد کنند. آموزش ناظرین سیستم مناسب ساده ترین روش مواجهه با این نوع حمله ها است. امنیت سایت بستگی به امنیت سیستم های داخلی و امنیت شبکه خارجی دارد.

سایت های تجارت الکترونیک برای رسیدن به اطمینان بخشی حریم خصوصی مشتری و منابع شرکت که از طرف سایت های اینترنتی دیگر مورد حمله واقع نشود. نیاز به معماری امنیت خودشان را دارند. صنعت تجارت الکترونیک یک تنزل بزرگ را در کوشش خود برای آرام کردن ترس مشتریان درباره امنیت تحمل خواهد شد وقتی که مشخص شود که سایت cd universe برای چند ساعت قبل از حمله کشف شده. بر روی مهاجمان باز است و مشکل بیشتر از آنجا است که تحقیقات امنیتی آشکار کرده است که حفره امنیتی به خوبی شناخته شده است و patch فروشنده برای بستنه آن سوراخ امنیتی در دسترس هست. تجارت الکترونیک با حملات ddos زمین گیر نمی شود اما سایت های تجاری شخصی از آن متاثر می شوند. توسعه دهندگان نرم افزاری نیاز به طراحی نرم افزاری دارند که برای امنیت و ایمنی مهندسی شده باشد.

بروز رسانی اتوماتیک امینیتی ویژگی دیگر است که باید برای کمک به محدود نمودن برد این حمله ها مورد استفاده قرار گیرد. برنامه آموزشی مناسب برای ناظرین سیستم، ساده ترین و موثر ترین روش برای جلوگیری از توافق گر های بزرگ امنیتی است. گروه بازرسی نیاز به بازنگری روش های امنیتی برای اطمینان از ابزارهای خود با سیاست شرکت و استاندارد های امنیتی اینرتنت عمومی دارند.

۱۵. امن سازی برنامه های کاربردی

را ه های مختلفی برای نفوذ به شبکه و سیستم تجارت الکتورنیکی است که البته بخش عمده از آن بر روی برنامه های کاربردی سمت client است و البته در برنامه های کاربردی سمت سرویس دهنده server نیز امکانات تخریبی وجود دارد.

امنیت بر روی پست الکترونیک:

اتصال بین یک کاربر و سرویس دهنده در اینترنت از میان تعدادی سیستم غیر مرتبط به طرفین این ارتباط گذر می کند و در هر نقطه اتصال، ترافیک قابل مانیتور می باشد و عدم رمزگذاری اطلاعات در اینترنت، محرمانگی را از دست می دهد. یکی از روش های متداول ارتباط پست الکتورنیک است که موضوعاتی امنیتی بر آن مترتب است.

امن سازی پیغام های الکترونیکی:

ایمیل ها می توانند توسط تجهیزاتی مانند پروتکل آنالایزر در طول مسیر انتقالشان مورد شنود برای دستیابی به موضوعات مهم درون آنها مثل کلمه و رمز عبور قرار گیرند. ایمیل ها براحتی قابل جعل می باشند و یک فرد هکر می تواند با تغییر فیلد ارسال کننده در ایمیل ها آنها را به شکلی که از طرف فرد مطمئن و معتبری ارسال شده اند جلوه دهد.

لذا امن سازی و رمزنگاری ایمیل ها این امکان را می دهد که تنها توسط افراد مورد نظر قابل فهم و دریافت باشد که شامل امضاء الکترونیکی می تواند باشد که در این صورت گیرنده مطمئن می شود که ایمیل از جانب شخص شما است.

ابزار نرم افزاری PGP این امکان را در اختیار می دهد که رمزگذاری، رمزگشایی و امضاء الکترونیکی بر روی اطلاعات داخل کامپیوتر و ایمیل ها انجام گیرد و روش آن نامتقارن می باشد و شامل مراحل تولید کلید (زوج کلید عمومی و خصوصی) ، مدیریت کلید (نگهداری کلید عمومی دیگران به صورت محلی) رمزگذاری و رمزگشایی ایمل ها (دوستان شما می توانند با کلید عمومی شما پیغام ها را رمزگذاری کنند و شما هم می توانید با کلید خصوصی خودتان این پیغام هار ا از رمز در آورید) امضاء ایمیل ها (می توان با استفاده از کلید خصوصی خود پیغام های ارسالی را امضاء نمود و دوستان هم با داشتن کلید عمومی می توانند این امضاء را رمزگشایی کنند و از اینکه شما ارسال کننده واقعی ایمیل هستید مطمئن گردند.

نرم افزار S/MIME هم شبیه PGP می باشد، با این تفاوت که کاربران به تاییدیه های ایجاد شده توسط PKI اعتماد می کنند. و برای استفاده از آن باید از برنامه های کاربردی که S/MIME را قادر به استفاده می کنند و همچنین دسترسی به یک تائیدیه PKI ، استفاده کنید. که این تاییده می تواند درون سازمانی یا برون سازمانی باشد.

۱۶. نقاط آسیب پذیر پست الکترونیک:

همچنان که نقاط آسیب پذیر بر روی نرم افزارها وجود دارد بر روی ایمیل نیز موجود است. ایمیل علاوه بر نقاط آسیب پذیری برای تخریب خودش امکان استفاده از این نقاط آسیب پذیر برای تخریب دیگر امکانات سیستم مثل پاک کردن اطلاعات کامپیوتر را هم دارد. برای محافظت از شبکه و سازمان در مقابل نقاط آسیب پذیر پست الکترونیک، باید از ویروس یاب های بروز شده استفاده نمائید. سرور درگاه ایمیل می تواند با اسکن کردن ایمیل های ورودی ، این درگاه را ایزوله کرده و یا ویروس های متصل به ایمیل هار را اجازه ورود به شبکه ندهد. همچنین باید کاربران شبکه در خصوص نقاط احتمالی حمله به وسیله ایمیل و عدم باز نمودن آنها را آموزش یابند. ارتباط با

فروشندگان و رهگیری وصله های و نصب آنها بر روی سیستم ها و شبکه کمک شایانی به حفاظت از آنها در مقابل تهدیدات ناشی از ایمیل می کند.

۱۷. انواع ایمیل های مخرب:

۱۷–۱ ایمیل های Spams **:** ایمیل های ناخواسته مثل تبلیغات تجاری که به آدرس های زیادی ارسال می گردند و برای محافظت در مقابل آنها باید از نرم افزارهای فیلتر کننده در درگاه سرور ایمیل و تک تک کامپیوترهای شبکه استفاده شود و همچنینی آموزش های کاربری شامل؛ عدم پاسخگویی به اسپم ها ، عدم پست آدرس ایمیل در داخل صفحات وب، برای استفاده از گروه های خبری از آدرس دوم ایمیل استفاده نمائید، عدم ارائه آدرس ایمیل به جاهای متفرقه و استفاده از فیلتر های اسپم.

۱۷–۲ ایمیل های Scams : ایمیل های ناخواسته که هدف خاص آنها سرقت پول، کالاها و سرویس های می باشد و از قربانب تقاضای پول و یا اطلاعات کارت اعتباری و حساب بانکی می کنند که عموما به شیوه فریب می باشد. راهکار آن نیز تنظیم سیاست نامه امنیتی ،رعایت محرمانگی اطلاعات مالی و آموزش ایمیل های اسکم به کاربران (مثل فرصت های تجاری، پولسازی از طریق ایمیل های عمده، نامه های زنجیره ای، برنامه کار در خانه ، سلامتی و رژیم، درآمد بدون تلاش، کالای مجانی، فرصت های سرمایه گذاری، وام ها و یا اعتبارهای تضمین شده و اصلاح اعتبار)

۱۷–۳ ایمیل های Hoaxes **:** ایمیل های هواکس حاوی اطلاعات غلط ولی قابل باور هستندو معمولا از سوی یک شخص برای تعداد زیاد کاربر ارسال می شود تا اینکه ایده و یا دیدگاهی را در آنها به باور برساند و معمولا از گیرنده درخواست می شود که آن را برای دوستان خود نیز ارسال نماید و گاها باعث تخریب اطلاعات هارد می شود.

به عنوان مثال به شما اعلام می شود که کامپیوتر شما ویروسی است و نام فایل ویروسی را هم اعلام می کنند درحالیکه آن نام فایل جزو فایل های اصلی سیستم عامل است. برای محافظت در برابر این نوع ایمیل ها باید سیاست نامه امنیتی داشته باشید و آنرا به کاربران نیز آموزش دهید. برخی عنوان مورد استفاده در ایمیل های Hopax شامل کلماتی مثل فوری، مهم، خطر، هشدار ویروس، به دوستان خود بگوئید، این یک hoax نیست، پر آمد ناگوار، تاریخچه است که همگی آنها بهئنحوی کاربران ناآگاه را می تواند فریب دهد.

۱۸. امنیت بر روی وب:

ضعف طراحی و برنامه نویسی برنامه های کاربردی منجر می شود که مهاجمین بتوانند به وبت سایت نفوذ نمایند که مخاطرات و روش های مقابله با آنها ذکر می شود:

۱۸–۱ SSL/TLS : پروتکل های لایه سوکت امن و امنیت لایه انتقال برای پیاده سازی امنیت در تبادلات کلاینت/سرور در اینترنت بکار برده می شود که توسط شرکت نت اسکیپ ارائه شده است و مبتنی بر رمزگذاری کلیدهای غیرمتقارن است که توسط شرکت RSA ارائه شده است. SSL/TLS ارتباطات اینترنتی را در مقابل استراق سمع، مداخله و جعل محافظت می کند و کلاینت و سرور می توانند

با استفاده از آن همدیگر را احراز هویت کرده و پیغام ها را به شکل رمزگذاری شده در اینترنت انتقال دهند. همچنین امکان احراز هویت سرور برای کلاینت ، مبادله الگوریتم رمزگذاری مشترک، احراز هویت کلاینت برای سرور،استفاده از رمزگذاری غیرمتقارن برای ارسال رمزهای اشتراکی و برقراری یک اتصال رمزگذاری شده است.

۱۸-۲ HTTPS : ارتباطات وب با بکارگیری HTTP اجرا می شوند. ارتباطات وبی که به وسیله SSL/TLS امن شده است با عنوان HTTPS نامیده می شود. مرورگرهای وب که ارتباطات HTTPS را نشان می دهند از علامت Https:// استفاده می کنند.

۱۸-۳ Buffer Overflow : بافر به فضای داده ای اطلاق می شود که بوسیله هر دو عنصر تجهیزات سخت افزاری و پروسس های نرم افزاری به اشتراک گذاشته می شود. سرریز بافر زمانی است که یک برنامه تلاش می کند داده های بیشتر از ظرفیت بافر را وارد نماید و باعث می شود داده های اضافی به بافرهای کناری ریزش کند و باعث خرابی آنها شود و ممکن است ناشی از ضعف برنامه و یا با هدف تخریب باشد. یک مهاجم از این روش برای دراختیار گرفتن کامپیوتر مهاجم استفاده می کند و بهترین راه جلوگیری از آن طراحی و برنامه نویسی امن می باشد.

۱۸-۴ Active Content : برای مهیج نمودن صفحات وب، محتوی های فعال ایجاد می شوند که شامل برنامه ها و یا کدهای اجرایی کوچک است که به داخل مرور گر ها ارائه می شود. مثل محتوی های ویدئویی و انیمیشن بر روی صفحات وب. دو نوع مرسوم محتوی های فعال جاوا اسکریپت ها و اکتیو ایکس ها هستند. محتوی فعاب برای اجرای یک اسکریپت داخل سیستم کلاینت طراحی شده اند که متاسفانه برخی اسکریپت ها باعث عملکرد های مخرب در سمت کلاینت می شوند. که شامل java applet , java script active x, signing active content, هستند.

۱۸-۵ Java Applet : جاوا زبان برنامه نویسی است که توسط سان میکرو سیستم ارائه شده و برنامه های کوچکی در این زبان جاوا اپلت نامیده می شوند که بر روی بیشتر مرورگرهای سمت کلاینت اجرا می گردند و به طور مثال نت اسکیپ و اینترنت اکسپلورر این برنامه های کوچک را پشتیبانی می کند. برای اجرای آنها بر روی سیستم عامل xp باید ماشین مجازی جاوا را اجرا نمود و متاسفانه مهاجمین می توانند از این امکان برای حمله به کلاینت استفاده کنند و راهکار آن غیر فعال سازی امکان پشتیبانی جاوا از طریق نت اسکیپ و یا اینترنت اکسپلورر است .

۱۸-۶ Java Script : شرکت نت اسکیپ جاوا اسکریپت را بوجود آورد و بسیاری از مروز گرها مثل نت اسکیپ و اینترنت اکسپلورر جاوا اسکریپت را پشتیبانی می کنند. جاوا اسکریپت نوعا داخل صفحات HTML قرار می گیرد و معمولا برای دریافت اطلاعات ورودی از کاربر است و متاسفانه می تواند مورد سوء استفاده توسط مهاجمین قرار گیرد و راه حل آن این است که می توان جاوا اسکریپت را بر روی کامپیوتر غیر فعال نمود و یا مرور گر را با آخرین وصله های امنیتی بروز نمائید که البته در این حالت از استفاده های مفید آن نیز محروم می شویم.

۱۸-۷ Active X : این تکنولوژی برای ایجاد محتوی فعال توسط مایکروسافت برای استفاده در اینترنت اکسپلور بوجود آمده است و در حال حاضر در هیچ مرورگر دیگری پشتیبانی نمی شود و می تواند داده های ورودی کاربر را دریافت نماید که تنظیم و غیر فعال نمودن آن از طریق اینترنت اکسپلورر امکان پذیر است.

۱۸-۸ Signing Active Content: برای امنیت سایت ها، برخی شرکت ها نسبت به امضاء محتوی فعال و پیاده سازی آن اقدام نمودند و قبل از ارسال این محتوی فعال آنها را امضای دیجیتال کرده و تائیده های امضاء را از مرکز CA دریافت می کنند. مایکروسافت از تکنولوژی Authenticode برای بررسی صحت امضاء قبل از ارسال محتوی فعال استفاده می می کند.

۱۸-۹ COOKIES : کوکی عبارت است از مقدار کوچکی از اطلاعات که یک وب سرور در مورد یک کاربر روی کامپیوتر خود کاربر نگهداری می کند. مثل تبلیغاتی که یک کلاینت دریافت کرده است و این به وب سرور کمک می کند که تبلیغات متفاوتی غیر از تبلیغاتی که برای کاربر قبلا ارسال شده را به نمایش گذارد. برخی کوکی ها برای ثبت علایق کاربران وقتی به وب متصل می شوند و برخی برای پشتیبانی از وضعیت اطلاعات بکار می روند. متاسفانه کوکی های هم می توانند توسط مهاجمین مورد سوء استفاده قرار گیرند که برای بدست آوردن اطلاعات مهم در مورد کاربران شبکه، سازمان و مسائل امنیتی شبکه باشد.مهاجم می تواند با نوشتن یک اسکریپت، کوکی های داخل کلاینت را به سمت سیستم خود هدایت نماید. برای محافظت از کلاینت ها در برابر تخریب های ناشی از کوکی بایستی از آنها برای اطلاعات محرمانه استفاده نشود و حتی الامکان از ssl/tls برای محافظت از اطلاعات داخل کوکی ها استفاده شود.

۱۸-۱۰ CGI : برای تولید محتوی فعال می باشد و برای انجام کارهایی مثل وارد کردن داده، جستجو، فانکشن بازیابی در دیتا بیس مورد استفاده قرار می گیرد. این برنامه ها می توانند مورد حمله برای تخریب وب سروها قرار گیرد و بر خلاف جاوا اسکریپت و اکتیوایکس که بر روی کلاینت اجرا می شود این برنالمه بر روی وب سرور اجرا می گردد.

اجرای چندین باره یک برنامه CGI از طریق مرور گر های چند گانه وب، هرگاه یک برنامه CGI توسط مرور گری اجرا می شود بخشی از ظرفیت منابع سیستمی بر روی وب سرور را برای اجرا در اختیار می گیرد. حال اگر مهاجمی به کرات دستور اجرای این برنامه را بروی مرورگر خود بدهد، ظرفیت منابع سروری مورد استفاده قرا می گیرد و این عاملی برای پایین آمدن سرعت سرویس دهنده وب سرور خواهد بود. این برنامه ممکن است دارای حفره های امنیتی باشد و مهاجمین از آن استفاده نمایند. ارسال داده های جعلی به سمت برنامه های CGI که می تواند باعث تخریب برنامه گردد.

برای اینکه یک سرور قادر به اجرای برنامه های CGI باشد باید بر روی سرور اجازه خواندن و اجراء را در دایرکتوری برنامه CGI بدهید. اما باید از غیر فعال سازی امکان نوشتن در این دایرکتوری مطمئن شوید. برای محافظت از وب سرور در مقابل مخاطرات ناشی از برنامه های CGI می توان به موارد : ایجاد محدودیت در برنامه های CGI ، نصب برنامه CGI با شرایط حداقل اجازه ، پاک کردن تمام برنامه های CGI به صورت پیش فرض در درون وب سرور ، بررسی برنامه های CGI در جهت پیدا کردن حفره های امنیتی آنان، اشاره نمود.

۱۱-۱۸ Instant Messaging : پیغام گذاری لحظه ای IM برای انتقال صحبت، فایل و صدا بین کاربران به طور مستقیم بر روی وب مورد استفاده قرار می گیرد. این برنامه ها برای اجرا و استفاده بسیار راحت هستند اما دارای شرایطی هستند که توسط مهاجمین برای تدارک حمله مورد استفاده قرار می گیرند از جمله مشکلات؛ انتقال داده های رمز نشده ای مثل کلمه و رمز عبوراست. IM به کاربران اجازه انتقال فایل ها را جدا از سیستم ایمیل که دارای ویروس یاب هست را می دهد و چون فایل ارسالی از طریق ایمیل ارسال نمی شود لذا مورد بررسی ویروس یاب هم قرار نمی گیرد. لذا هکر می تواتند نقاط ضعف سیستم را مثل سر ریز بافر شناسایی نماید. اشکال برنامه ای در یک طرف ممکن است باعث شود تا طرف دیگر کنترل برنامه را دراختیار گیرد .

راه حل و اجتناب از آن طرفا با استقاده از IM امن امکان پذیر می باشد، حذف کامل IM در سازمان، انحصار در استفاده از IM هایی که برای استفاده مجاز می باشد ، استفاده از برنامه IM با قابلیت رمز گذاری ، تنظیم نظام نامه امنیتی برای استفاده از IM مثلا اینکه از این طریق انتقال فایل انجام نشود ، آموزش کاربران برای آگاهی آنان از خطرات IM ، استفاده از ویروس یاب های بروز شده برای تمامی استفاده کنندگان IM ، دریافت آخرین وصله های امینینتی نرم افزارهای .IM از جمله روش های اجتناب از تهیدیدات IM است.

منابع:

۱. بررسی و تحلیل چالش های امنیت در تجارت الکترونیک و راههای مقابله با آن . مهرنوش ترابی و کرشا زمانی دانشگاه شیراز

۲. آشنایی با امنیت تجارت الکترونیکی . محمد رضا داوری