بسم الله الرحمن الرحیم

رایانه امن در محیط ویندوز

شرکت مهندسی پیام‌پرداز

مرداد ماه ۸۹

این پیشنهاد توسط شرکت پیام‌پرداز تهیه شده است و هرگونه استفاده از تمام یا بخشی از آن منوط به اجازه کتبی از این شرکت می‌باشد.

فهرست

عنوان **صفحه**

۱- مقدمه..... ۱
۲- نیازمندی‌های امنیتی..... ۱
۲-۱- احراز اصالت کاربر..... ۲
۲-۲- محرمانگی و صحت داده‌های ذخیره شده..... ۲
۲-۳- محرمانگی و صحت داده‌های مبادله شده..... ۲
۳- راه حل‌های امن‌سازی..... ۳
۳-۱- ورود امن به ویندوز..... ۳
۳-۲- امن‌سازی فایل‌ها و پرونده‌ها..... ٤
۳-۳- امن‌سازی رسانه‌های ذخیره‌سازی..... ٤
۳-۴- امن‌سازی پست الکترونیک..... ٥
۳-۵- امن‌سازی بستر شبکه..... ٥
۴- جمع‌بندی..... ٦

۱- مقدمه

امروزه دامنه تحولات ناشی از گسترش فناوری اطلاعات، نه تنها زیرساخت‌های جامعه و حوزه‌های اداری و سازمانی را تحت تاثیر قرار داده بلکه در زندگی شخصی و به طور خاص کاربردهای روزانه افراد نیز بروز یافته است. در حال حاضر رایانه و کاربردهای متنوع آن به عنوان عنصر لاینفک زندگی اکثر افراد جامعه تلقی می‌گردد و بهمین دلیل باید ملاحظات بیشتری در استفاده و بهره‌گیری از آن مورد توجه قرار گیرد. از جمله مهمترین این ملاحظات توجه به تهدیداتی است که رایانه‌های شخصی را در بر می‌گیرد. این تهدیدات می‌توانند با بروز خسارت‌های فراوان، هزینه‌های زیادی را به صاحبان خود تحمیل کنند. از این رو شناخت این تهدیدات و راه‌های مقابله با آن‌ها می‌تواند بسیار مهم و ضروری باشد.

هدف از این نوشتار مروری سریع بر تهدیدات امنیتی پیش رو در استفاده از رایانه‌های شخصی و ارایه راه‌کارهایی برای امن‌سازی آن می‌باشد. در ارایه راه‌حل‌های امن‌سازی از محصولات شرکت مهندسی پیام‌پرداز بهره‌گیری شده است. این شرکت با بیش از ۱۴ سال تجربه موفق در اجرای طرح‌های پژوهشی و کاربردی در زمینه امنیت فناوری اطلاعات و با برخورداری از متخصصین و کارشناسان خبره، هم اکنون سبد متنوعی از محصولات امنیت فضای تبادل اطلاعات را در اختیار دارد.

۲- نیازمندی‌های امنیتی

به منظور ارایه راه‌کارهای مناسب امن‌سازی لازم است ابتدا نیازمندی‌های امنیتی در استفاده از رایانه‌های شخصی شناسایی گردد. در این راستا تهدیدات و حملات قابل انجام بر روی رایانه‌ها باید مد نظر قرار گیرند.

۲-۱- احراز اصالت کاربر

در سیستم عامل ویندوز به صورت معمول برای احراز اصالت[1] کاربر از نام و کلمه عبور استفاده می‌شود. این روش که اصطلاحا به عنوان روش احراز اصالت یک‌عاملی[2] نامیده می‌شود دارای ضعف‌های زیادی است. به عنوان مثال انتخاب کلمات عبور ضعیف توسط کاربران، حمله دیکشنری و حمله جستجوی کامل[3] نمونه‌هایی از تهدیدات روش احراز اصالت یک عاملی هستند. برای رفع این مشکلات روش‌های احراز اصالت دوعاملی[4] پیشنهاد می‌شود که در آن علاوه بر کلمه عبور (یا اصطلاحا *PIN*[5]) از یک توکن سخت‌افزاری امنیتی[6] نیز برای بررسی هویت کاربر استفاده می‌شود.

۲-۲- محرمانگی و صحت داده‌های ذخیره شده

اطلاعات ذخیره شده بر روی هر رایانه شامل انواع فایلها و پوشه‌ها معمولا به صورت فاش بر روی هارد دیسک و یا سایر رسانه‌های جانبی ذخیره می‌گردد. از آنجا که امکان دسترسی غیرمجاز به ابزارهای ذخیره‌سازی به انحای مختلف مثل دسترسی عادی، دسترسی از طریق شبکه، سرقت و ... وجود دارد لذا امکان مشاهده اطلاعات حساس و نیز امکان تغییر و دستکاری داده‌های ارزشمند و نهایتا نقض حریم خصوصی به راحتی وجود دارد. بنابراین لازم است با استفاده از روشهای رمزنگاری، از محرمانگی[7] و صحت[8] اطلاعات ذخیره شده بر روی رایانه اطمینان حاصل کرد.

۲-۳- محرمانگی و صحت داده‌های مبادله شده

معمولا کاربران اطلاعات خود را از روش‌های گوناگون از قبیل ارسال *Email*، به‌اشتراک‌گذاری داده‌ها در شبکه، انتقال فایل با استفاده از مودم و ... مبادله می‌کنند. از آنجا که بستر تبادل داده‌ها اعم از شبکه‌های داخلی و شبکه‌های عمومی نظیر اینترنت در دسترس عموم قرار داشته و امکان شنود اطلاعات حساس و یا تغییر و دستکاری داده‌های ارزشمند در حین تبادل و یا درهنگام ذخیره بر روی سرورهای میانی وجود دارد لذا باید محرمانگی و صحت اطلاعات حساس مبادله شده بین کامپیوترهای کاربران نیز با روش‌های مدرن رمزنگاری تامین گردد.

---

[1] *Authentication*
[2] *One-Factor*
[3] *Brute Force*
[4] *Two-Factor*
[5] *Personal Identity Number*
[6] *Security Token*
[7] *Confidentiality*
[8] *Integrity*

۳- راه حل‌های امن‌سازی

در ادامه با توجه به نیازمندیهای امنیتی مطرح شده، راه‌کارهای امن‌سازی پیشنهادی مورد بحث قرار می‌گیرند.

کلیه راه‌کارهای مطرح شده از یک ماژول امنیت سخت‌افزاری با نام **کیا** به عنوان پایه زیربنایی امنیت استفاده می‌کنند. محصول **کیا** که یک توکن امنیتی از نوع *USB* است برای اولین بار در کشور در سال ۱۳۸۳ به وسیله شرکت پیام‌پرداز عرضه گردید. مراحل طراحی، توسعه و تولید این محصول به صورت کامل در داخل شرکت پیام‌پرداز و زیر نظر تیم‌هایی متشکل از متخصصین امنیت، سخت‌افزار و نرم‌افزار انجام گرفته است.

۳-۱- ورود امن به ویندوز

مطمئناً تشخیص صحیح هویت و احراز اصالت فرد، اولین قدم در راستای تخصیص منابع و تفویض اختیارات و دسترسی‌های لازم به او می‌باشد. در حقیقت بیشتر حملات سعی دارند که با کسب اختیارات بیشتر، به منابع مهمتر و حیاتی‌تری دست یابند تا با سوء استفاده از آن خساراتی را به بار آورند.

یکی از نرم‌افزارهای قابل استفاده برای احراز اصالت قوی فرد، نرم‌افزار **کیان** برای ورود امن به ویندوز است که فرایند *Login* به رایانه را به صورت دوعاملی تبدیل می‌کند. با نصب نرم‌افزار، پنجره *Login* ویندوز تغییر یافته و کاربر برای ورود به ویندوز نیاز به یک توکن سخت‌افزاری (که قبلا برنامه‌ریزی شده) به همراه *PIN* فعال‌سازی توکن دارد. این محصول را می‌توان بر روی هر کامپیوتر محلی یا عضو شبکه *Domain* نصب کرده و از ورود افراد غیر مجاز به کامپیوترها جلوگیری نمود. نرم‌افزار **کیان** از توکن سخت‌افزاری **کیا** به عنوان عامل دوم احراز هویت استفاده می‌کند.

یک راه حل دیگر برای ورود امن به ویندوز راه حل *Smart Card Logon* است که شرکت مایکروسافت در داخل ساختار *Active Directory* تعبیه کرده و امکان تشخیص هویت کاربران از طریق گواهی دیجیتال را فراهم می‌سازد. گواهی دیجیتال کاربر به وسیله یک مرکز صدور گواهی[1] (*CA*) که با *Active Directory* ارتباط دارد صادر می‌شود. با انجام تنظیمات ساده‌ای بر روی کامپیوترهای متصل به دامنه‌ی *Active Directory* کاربران می‌توانند گواهی دیجیتال خود را بر روی یک کارت هوشمند ذخیره (*Enroll*) نمایند و برای ورود به سیستم از این کارت هوشمند استفاده کنند. بدین ترتیب ورود به سیستم عامل ویندوز به صورت دو عاملی در می‌آید. ویندوز برای عملیات ورود، از کتابخانه‌ی *CSP* جهت

[1] *Certificate Authority*

ارتباط با فراهم‌کنندگان خدمات کارت‌های هوشمند[1] استفاده می‌نماید.

بسته‌ی زیرساخت کلید عمومی[2] (*PKI*) ماژول **کیا** با ارائه‌ی کتابخانه‌ی *CSP* و معرفی آن به سیستم عامل، این امکان را فراهم می‌سازد که گواهی‌های دیجیتال کاربران به وسیله‌ی سیستم ثبت گواهی[3] ویندوز بر روی توکن **کیا** ذخیره شده و در هنگام ورود به سیستم خوانده و استفاده شود. با توجه به حافظه‌ی امن **کیا** و حفاظت دوعاملی (به وسیله توکن و شناسه‌ی شخصی یا *PIN*)، اطلاعات ورود به سیستم کاربر کاملاً محفوظ و غیر قابل دسترس برای افراد غیر مجاز خواهد بود.

۳-۲- امن‌سازی فایل‌ها و پرونده‌ها

برای جلوگیری از افشای ناخواسته داده‌ها یا دستکاری و تغییر غیرمجاز آن‌ها بایستی تمهیدات لازم برای محدود کردن دسترسی به اطلاعات در نظر گرفته شود. هر چند با استفاده از سرویس کنترل دسترسی ویندوز تا حد زیادی می‌توان دستیابی افراد غیرمجاز به اطلاعات را محدود نمود ولی این سرویس از قدرت بازدارندگی کافی برخوردار نیست و مدیران شبکه یا دیگر کاربران با سطح دسترسی *Administrator* می‌توانند از آن عبور نمایند. یک راه حل مناسب برای امن‌سازی اطلاعات استفاده از روش‌های رمزنگاری است. در این راستا نرم‌افزار رمزکننده **پاس** پیشنهاد می‌گردد که در محیط *Shell* برنامه *Explorer* ویندوز کار می‌کند و امکانات رمزنگاری را از طریق *Context Menu* به راحتی با یک کلیک راست در اختیار کاربر قرار می‌دهد. این نرم‌افزار با استفاده از ماژول امنیتی **کیا** کار می‌کند و اطمینان لازم از محرمانگی و صحت فایل‌ها را به کاربر ارایه می‌نماید. نرم‌افزار **پاس** می‌تواند برای بایگانی امن فایل‌های کاربر بر روی رایانه و نیز برای مبادله امن فایل‌ها بین کاربران به کار رود. نرم‌افزار **پاس** به دو گونه مختلف ارایه شده است. گونه ۱ این محصول از الگوریتم رمز استاندارد *AES* (با طول کلید ۱۲۸ بیت) برای رمزنگاری استفاده می‌کند. گونه ۲ به یک الگوریتم رمز اختصاصی (با طول کلید ۲۵۶ بیت) مجهز شده و امکانات بیشتری را ارایه می‌نماید.

۳-۳- امن‌سازی رسانه‌های ذخیره‌سازی

ابزارهای ذخیره‌سازی داده‌ها همچون هارد کامپیوتر، فلش‌های *USB*، *CD* و دیگر رسانه‌های قابل حمل[4]، اطلاعات الکترونیکی افراد و سازمان‌ها را در بر می‌گیرند. با توجه به سادگی دسترسی غیرمجاز به این ابزارهای ذخیره‌سازی، باید با مکانیزم‌های مناسب رمزنگاری، از افشای اطلاعات حساس درایوها

[1] *Smart Card Service Provider*
[2] *Public Key Infrastructure*
[3] *Certificate Enrollment*
[4] *Removable Disk*

جلوگیری نمود.

اگرچه در این حالت امکان استفاده از نرم‌افزارهای رمزکننده فایل مطابق بخش قبل برای رمز تک تک فایل‌ها وجود دارد ولی در صورتی که بخواهیم حجم انبوهی از فایل‌ها و پوشه‌ها مثلا کل اطلاعات موجود بر روی یک پارتیشن را رمز نماییم راه حل بهتر استفاده از رمزکننده‌های درایو است. در این راه حل یک درایو مجازی امن بر روی رایانه تشکیل می‌شود که هر فایل یا پوشه‌ای در آن قرار گیرد به طور شفاف رمز می‌شود.

نرم‌افزار رمزکننده دیسک **هدا** محصولی از شرکت پیام‌پرداز است که با استفاده از این راه حل سرویس امنیتی خود را ارایه می‌کند. با استفاده از این نرم‌افزار می‌توان دیسک‌های فیزیکی موجود بر روی رایانه اعم از پارتیشن‌های هارد، دیسک فلاپی و یا *Flash Disk* را رمزنگاری نمود. همچنین این نرم‌افزار می‌تواند مبتنی بر یک فایل *Image* که بر روی هر رسانه‌ای قابل ذخیره‌سازی است پارتیشن مجازی امن ایجاد کند. این نرم‌افزار از توکن امنیتی **کیا** برای ذخیره‌سازی امن کلیدهای رمزنگاری استفاده می‌نماید. بدین ترتیب در صورت در اختیار داشتن ماژول کیای معتبر و *PIN* مربوطه، می‌توان به اطلاعات ذخیره شده در درایوهای امن دسترسی داشت.

۳-۴- امن‌سازی پست الکترونیک

پست الکترونیک به دلیل هزینه کم و سرعت زیاد از همگانی‌ترین سرویس‌های اینترنت محسوب می‌شود. نامه‌های الکترونیک در طی مسیر خود از مبدا تا مقصد اعم از سوییچهای شبکه و یا سرورهای *Email* مبدا یا مقصد، به راحتی قابل مشاهده، تغییر، حذف و یا حتی جعل می‌باشند.

برای امن‌سازی کاربرد پست الکترونیک معمولاً از پروتکل *S/MIMIE* مبتنی بر زیرساخت رمزنگاری کلید عمومی (*PKI*) استفاده می‌شود. این پروتکل در نرم‌افزارهای سرویس‌گیرنده پست الکترونیک همچون *Microsoft Outlook*، *Netscape* و *Mozilla Thunderbird* پشتیبانی می‌شود. این نرم‌افزارها به ترتیب با حمایت از استاندارد *CSP* و *PKCS#11* امکان کار با توکن‌های امن را نیز پدید می‌آورند. بدین ترتیب می‌توان از ماژول سخت‌افزاری **کیا** به عنوان یک توکن امنیتی برای ذخیره مطمئن کلید خصوصی استفاده نمود.

۳-۵- امن‌سازی بستر شبکه

در حال حاضر اکثر کامپیوترها به شبکه‌های محلی یا گسترده متصل هستند و داده‌های خود را با سایر کامپیوترها از بسترهای ارتباط خصوصی یا عمومی عبور می‌دهند. به منظور امن‌سازی ارتباط رایانه‌های داخل یک شبکه محلی و یا اتصال یک رایانه راه دور با یک شبکه محلی از یک بستر عمومی

نظیر اینترنت، می‌توان از محصول رمزکننده شبکه **سدید** استفاده نمود. این محصول با ایجاد شبکه اختصاصی مجازی[1] (*VPN*) در لایه پیوند داده[2]، اطلاعات مبادله شده در بستر شبکه را رمز می‌نماید. نرم‌افزار **سدید** برای ذخیره‌سازی اطلاعات حساس خود از قبیل کلید و ... از توکن امنیتی **کیا** استفاده می‌کند.

یک راه حل دیگر برای امن‌سازی ارتباطات *Client/Server* در شبکه‌های *LAN* یا *WAN* استفاده از محصول **کیهان** است. این محصول توسط شرکت پیام‌پرداز طراحی و پیاده‌سازی شده و از اجزای نرم‌افزاری و سخت‌افزاری مختلفی تشکیل می‌شود. به منظور امن‌سازی شبکه، یک سرویس‌دهنده کیهان در جلوی سرورهای حساس سازمان قرار گرفته و بر روی هر یک از کامپیوترهای کاربران نرم‌افزار *Client* کیهان نصب می‌شود. ضمنا برای هر کاربر یک توکن امنیتی **کیا** توسط مدیر سیستم برنامه‌ریزی شده و در اختیار وی قرار می‌گیرد. هر کاربر برای ارتباط با سرورهای اصلی ابتدا لازم است از طریق سرور کیهان احراز اصالت شده و اجازه دسترسی وی صادر گردد. فرایند احراز اصالت کاربر با استفاده از یک پروتکل احراز اصالت اختصاصی و به صورت دوعاملی (با بکارگیری ماژول کیای کاربر و *PIN* وی) انجام می‌گیرد. پس از احراز اصالت موفقیت‌آمیز کاربر، یک تونل امن در لایه شبکه بین کامپیوتر کاربر و سرور کیهان برقرار می‌شود که کلیه داده‌های مبادله شده درون آن رمز گردیده و بدین ترتیب سرویس‌های محرمانگی و صحت تامین می‌شود.

۴- جمع‌بندی

همانگونه که اشاره گردید ماژول سخت‌افزاری کیا به عنوان پایه زیربنایی امنیت در همه محصولات نرم‌افزاری معرفی شده مورد استفاده قرار گرفته است. به همراه هر توکن امنیتی کیا (مدل *W*) نرم‌افزارهای زیر به صورت رایگان عرضه می‌شود:

- نرم‌افزار کیان برای ورود امن به ویندوز
- نرم‌افزار رمزکننده فایل پاس گونه ۱
- بسته *PKI* کیا برای بکارگیری توکن کیا در سرویس‌های *Email* امن و *Smart Card Logon*
- نرم‌افزار کلاینت کیهان برای امن‌سازی کاربردهای *Client/Server* شبکه

علاوه بر نرم‌افزارهای فوق، محصولات زیر نیز بر روی توکن امنیتی کیا قابل ارایه است:

- نرم‌افزار رمزکننده فایل پاس گونه ۲

[1] *Virtual Private Network*
[2] *Data Link*

- نرم‌افزار رمزکننده دیسک هدا
- نرم‌افزار رمزکننده شبکه سدید (نسخه میزبان)

بنابراین با اختصاص یک توکن امنیتی کیا به هر کاربر و با بهره‌برداری مناسب از نرم‌افزارهای اشاره شده، می‌توان به یک رایانه امن دست یافت.