تولید قفل

و روش های شکستن آن ها

فهرست

انواع قفل ها..... ۵

۱ – قفل های سخت افزاری..... ۵

۲ – قفل های نرم افزاری..... ۶

روش های قفل گذاری نرم افزاری..... ۸

۳ – قفل‌های روی CD..... ۱۱

روش های قفل گذاری روی CD..... ۱۲

۴ – قفل‌های اینترنتی..... ۱۳

تکنیک های شکستن قفلهای نرم افزار..... ۱۴

یکی از دغدغه های امروز در حوزه فناوری اطلاعات و فضای سایبر برقـراری امنیت است. روشهای متنوعی برای برقراری امنیت وجود دارد. یکی از این روش‌ها استفاده از انواع قفل‌ها بر روی نرم افزار، سخت افزار، لوح فشرده و غیره مـی‌باشـد. دراین کتابچه به بررسی انواع قفل و روشهای ساخت و شکستن آنها می‌پردازیم.

آغاز

در جنگ‌های رودررو و فیزیکی، ایجاد بسترهای امنیتی، بیشتر در قالب سنگر، خاک‌ریز و ... معنای واقعی پیدا می‌کند، ولی در جنگ‌های سایبری که در جهت سرقت، نابودسازی و تغییر اطلاعات محرمانه انجام می‌شود، ایجاد بستر امنیتی در قالب سرویس‌های امنیتی مانند فایروال، آنتی‌ویروس، سیستم تشخیص‌نفوذ، آنتی اسپم، سیستم ضد جاسوسی، و همچنین استفاده از قفل‌ها و ... معنا پیدا می‌کند. امروزه یکی از دغدغه های مهم در عرصه اطلاعات جلوگیری از نفوذ به سیستم-هاست. به همین دلیل تخصص تولید قفل و روشهای شکستن آن به عنوان یکی از شاخه های مهم امنیتی، اهمیت دوچندانی یافته است و تا حدی که با داشتن قفل های مناسب می توان پایداری سیستم را در مقابل حملات مختلف حفظ نمود.

انواع قفل ها

۱ – قفل های سخت افزاری

۲ – قفل های نرم افزاری

۳ – قفل‌های CD ، DVD و ...

۴ – قفل‌های اینترنتی

۱ – قفل های سخت افزاری

چنانچه از سخت افزار خاصی برای قفل گذاری استفاده شود، به آن قفل سخت افزاری می گوییم. این قفلها بعضی به صورت یک رابط، بر روی پورت پارالل سیستم نصب می شوند که البته هر دو نوع آن عملکرد مشابه دارند. بخش اصلی قفل، از یک حافظه قابل پاک شدن تشکیل شده که با توجه به نوع و حجم آن، دارای عملکردی متفاوت می باشد و عمدتاً به یکی از دو روش زیر عمل می کند.

الف) روش اول قفل گذاری سخت افزاری

روش اول قفل گذاری به این صورت است که تولید کننده نرم افزار یک یا چند بایت از اطلاعات را در قفل نوشته و برنامه در هنگام اجرا آن را چک می کند. در صورتیکه قفل وجود داشته باشد، برنامه به کار خود ادامه می دهد و اگر قفل وجود نداشته باشد و یا اطلاعات خوانده شده از روی قفل صحیح نباشد، برنامه متوقف شده و با اعلام خطا، از اجرای صحیح، سرباز می زند. این نوع قفل ها دارای ساختاری ساده، حافظه ای در حد چند بایت، و قیمتی ارزان هستند. استفاده از این قفل ها بسیار ساده بوده و نیاز به تخصص خاصی ندارد، تنها کافیست که نرم افزار ویژه قفل را (که توسط شرکت تولید کننده قفل ارایه شده) اجرا نمود. در ابتدا که قفل فاقد اطلاعات است، اول یک کلمه دلخواه، به عنوان کلمه عبور درخواست کرده و سپس با توجه به نوع قفل، یک یا چند کلمه اطلاعات را دریافت

و در حافظه قفل ثبت می کند. پس از ثبت اطلاعات در قفل، تولید کننده نرم افزار، اطلاعات ثبت شده در یک برنامه چک می کند که نحوه چک کردن اطلاعات، با توجه به نوع قفل متفاوت است. در بعضی فقط اطلاعات درون قفل چک می شود و در بعضی دیگر، در مرحله اول وجود قفل چک شده و در مرحله بعدی، اطلاعات درون آن چک می شود .

ب) روش دوم قفل گذاری سخت افزاری

روش دیگر قفل گذاری به این صورت است که تولید کننده نرم افزار، بخش کوچکی از برنامه را در حافظه قفل قرار می دهد که در این حالت، چنانچه قفل وجود نداشته باشد برنامه به هیچ وجه، قادر به اجرا و ادامه کار نخواهد بود. این نوع قفل ها، دارای ساختاری کمی پیچیده، حافظه ای بعضا تا چند کیلو بایت، و قیمتی نسبتاً گران هستند. استفاده از این قفل ها، به سادگی نوع قبلی نیست. البته نحوه کلی کار مشابه روش قبلی است. با اجرای نرم افزار ویژه قفل و وارد نمودن کلمه عبور، باید نام فایلی را که می خواهیم بر روی آن قفل بزنیم، مشخص کنیم، تا بخشی از آن در قفل ثبت گردد.

۲ – قفل های نرم افزاری

با توجه به نوع کاربرد برنامه، اندازه، قابلیت کپی برداری از آن بر روی دیسک، تحت شبکه بودن برنامه و... می توانیم از انواع روش هایی که جهت حفاظت از نرم افزار در نظر داریم (و متعاقباً توضیح داده خواهد شد) استفاده کنیم. چگونگی استفاده از قفل منتخب به شرایط زیر بستگی دارد:

الف) اعتقاد طراح نرم افزار به اینکه کاربر حتماً باید آن را خریداری کند تا از امکانات آن مطلع شود

در این حالت قفل نرم افزاری در ابتدای شروع به کار برنامه کنترل می گردد حتی طراح می تواند در مواقع حساس نیز قفل را مجدداً کنترل کند و یا در حالتی

که طراح واقعاً سخت گیر باشد، می تواند در زمان هـای مشخصـی از وجـود قفـل اطمینان حاصل نماید (مثلاً هر ۴ ثانیه). البته در این حالت طراح باید روشی را کـه جهت کنترل قفل استفاده می کند، نیز در نظر بگیرد.

ب) اعتقاد طراح نرم افزار به این که کاربر می تواند از نـرم افـزار بـه عنـوان نسخه نمایشی نیز استفاده کند.

طراح در این حالت می بایست در مکان های خاصی از برنامه، قفل را کنتـرل کند. مثلاً در یک برنامه حسابداری مـی تـوان تمـام بخـش هـای سیسـتم را آزاد گذاشته (یعنی برنامه نیازی به قفل نداشته باشد) اما در صورتی که کاربر مایـل بـه استفاده از امکانات گزارش گیری سیستم باشد، قفل نرم افزاری درخواسـت گـردد. مزیت این روش بر روش قبلی این است که دیگر نیاز به طراحـی نسـخه نمایشـی جهت مشاهده کاربران وجود ندارد. در انتها طراح باید موارد زیر را نیز در نظر گرفته و با توجه به برنامه مورد نظر یکی را انتخاب کند.

- **محدودیت در تعداد کپی (Copy Limited)**

در این حالت برنامه نصب کننده نرم افزار، فضای مشخصـی در دیسـک را بـا روش خاصی فرمت کرده و تعداد مجاز نسخه برداری را در آن درج می کند. بـدین طریق با هر بار کپی کردن برنامه، یک واحد از این عدد کم می شود و هنگامی که تعداد مجاز آن به صفر رسید، دیگر نمی توان برنامه را بر روی سیستم نصب نمود.

- **استفاده از دیسـکت، در هنگـام اجـرای برنامـه (Required Disk)**

در این حالت، دیسکت مورد نظر، یا به روش خاصی فرمت می شود و سـپس در هنگام اجرا، اطلاعات روی آن بررسی می شود و یا اینکه قسمتی از دیسـکت را بصورت فیزیکی و عمدی خراب می کنند و در اینجا، در واقع همان صدمه ای کـه

به عمد، بر سطح دیسکت وارد شده است، به عنوان قفل و محافظ نرم افـزار عمـل می کند. از این پس برای انتقال برنامه از یک سیستم به سیستم دیگر، این فلاپـی مانند قفل سخت افزاری عمل می کند و می بایست مختصـات آن توسـط برنامـه تایید شود و چنانچه این فلاپی در درایو نباشد، برنامه اجرا نخواهد شد.

روش های قفل گذاری نرم افزاری

در ادامه چند نمونه از روشهای قفل گذاری نرم افـزاری و نحـوه طراحـی آن آورده شده است.

۱ – قفل گذاری با استفاده از شماره سریال اصلی دیسکت

سیستم عامل جهت هر دیسـکت یـک شـماره سـریال واحـد (UNIQUE) اختصاص می دهد، بطوریکه شماره سریال هر دو دیسـکت بـا هـم یکـی نیسـتند. بنابراین همین خود یک راه تشخیص دیسکت کلید (قفل) می باشد.

۲ – قفل گذاری با استفاده از مشخصات سیستم

در این نوع قفل نرم افزاری، برنامه قبل از اجـرا ابتـدا مشخصـات سیسـتم را خوانده (که اینکار از طریق مراجعه به بخش های خاصی از حافظه و یا مراجعه بـه اطلاعات BIOS انجام می شود.) سپس آنرا با فایلی که قبلا توسط نویسـنده نـرم افزار بر روی کامپیوتر کپی گردیده، مقایسه مـی کنـد و در صـورت عـدم برابـری، اجـرای برنامـه پایـان مـی پـذیرد. درصـد اطمینـان ایـن نـوع قفـل ۷۵٪-۶۵٪ می باشد .

۳ – قفل با استفاده از موقعیت فایل روی هارد دیسک

این نوع قفل فقط بر روی هارد دیسک قابل استفاده بوده و بـه ایـن صـورت است که فایل اجرایی به موقعیت خود بر روی هارد حساس می باشد چرا که قبل از اجرا ابتدا موقعیـت خـود را از روی سـکتورهای ROOT خوانـده و سـپس شـماره

کلاستر اشاره گر به خودش را بدست می آورد، سپس آنرا با شماره کلاستری که قبلا توسط برنامه نویس بر روی یکی از فایل های برنامه (ممکن است بصورت کد شده باشد) قرار داده شده، مقایسه کرده و در صورت برابر بودن اجرا می شود. ضریب اطمینان این نوع قفل نیز ۸۰٪-۷۰٪ می باشد.

۴ – قفل با استفاده از فرمت غیر استاندارد

این شیوه یکی از رایج ترین قفل های نرم افزاری است که هنوز هم بصورت جدی مورد استفاده قرار می گیرد. سیستم عامل جهت دسترسی به اطلاعات یک دیسکت از فرمت خاصی (۱۸ سکتور در هر تراک) استفاده می کند اما اگر یک تراک به صورت غیر استاندارد فرمت شود، (مثلا ۱۹ سکتور در تراک) سیستم عامل دیگر توانایی استفاده از سکتورهای غیرمجاز را نخواهد داشت و بنابراین تمام نرم افزارهای تحت سیستم عامل مزبور نیز از سکتورهای مخفی استفاده نکرده، در نتیجه امکان کپی برداری از آنها بسیار ضعیف است. از همین روش جهت طراحی قفل مورد نظر استفاده می شود. قفل نرم افزاری Copy Control که معروفترین در نوع خود می باشد، از همین روش استفاده می کند. این قفل فقط جهت فلاپی دیسک قابل استفاده می باشد و درصد اطمینان در این روش حدود ۹۵٪-۸۵٪ می باشد .

۵ – قفل با استفاده از شماره سریال ساختگی

این روش قفل گذاری که قویترین قفل می باشد، بصورت مخلوطی از روش های ۱ و ۴ می باشد یعنی ابتدا تراک خاصی را بصورت غیر استاندارد فرمت کرده و سپس اطلاعات خاصی را درون آن قرار می دهند (شماره سریال فرضی). این قفل فقط جهت فلاپی دیسک قابل استفاده بوده و ضریب اطمینان آن حدود ۹۸٪-۹۰٪ می باشد.

۶– قفل های اکتیو ایکس

در واقع یک اکتیو ایکس که مانع اجرای برنامه در شرایط خاصی شود را قفل اکتیو ایکس می نامند. این نوع قفل مانند سایر کامپوننت های برنامه نویسی است. برنامه نویس به سادگی آن را بر روی فرم برنامه خود قرار می دهد و با تنظیم پارامترها و خصوصیات آن، سبب فعالیت آن می شود. این اکتیو ایکس قبل از قرار گرفتن فرم اصلی در حافظه، شروع به کار می کند و اگر برای اولین بار اجرا می شود برحسب اندازه حافظه، شماره ی سریال و سرعت پردازنده کد ویژه ای تولید می کند این کد تولید شده وابسته به خصوصیات کامپیوتر است بنابراین کد برگشتی این اکتیو ایکس بر روی هر سیستمی متفاوت خواهد بود. پس از ارائه کد، کد معادل آن را از کاربر درخواست می کند. کاربر با ارائه کد تولید شده به شرکت تولید کننده نرم افزار کد معادل آن را دریافت می کند. این کد را کاربر یا از طریق تلفن یا از طریق پست الکترونیکی و یا اینترنت دریافت می کند در صورتیکه کد معادل دریافت شده پس از کد شدن معادل کد ارائه شده باشد یا به عبارتی دیگر کد ارائه شده از طرف کامپیوتر مکمل کد دریافت شده از شرکت باشد اکتیو ایکس اجازه می دهد که برنامه بدون اشکال شروع به کار کند. کاربر نیز می تواند بارها از این کد بر روی کامپیوتر خود (کامپیوتری که کد دریافت کرده) استفاده کند. پس از ورود کد، این کد در مکانی از سیستم مثلاً رجیستری یا یک فایل بصورت کد شده قرار می گیرد و هر بار کامپیوتر برنامه را اجرا کند به جای درخواست کد از کاربر، کد را از رجیستری یا فایل پس از کدیابی مورد استفاده قرار می دهد.

نقاط ضعف:

- قفل های اکتیو ایکس نیاز به دریافت کد از شرکت دارند یعنی اینکه باید کاربر حتماً به نحوی با شرکت تولید کننده تماس بگیرید و نمی تواند برنامه را پس از خرید بلافاصله استفاده کند.

- قفل های اکتیو ایکس تنها بر روی یک سیستم اجرا می شوند و باید برای دریافت کد برای هر کامپیوتر اقدام شود (دشواری در نصب های تعداد بالا)
- قفل های اکتیو ایکس ممکن است با فرمت کردن، پارتیشن بندی تغییر یابد که نمی تواند شرکت دقیقاً حدس بزند که این قفل برای این سیستم بوده یا واقعاً تغییر کرده. در اکثر قفلهای ساخته شده تغییرات این کد بسیار مشاهده شده است.
- با صدمه دیدن قطعه ای در کامپیوتر و یا تعویض یک قطعه برنامه تصور می کند که سیستم تغییر یافته است مثلاً با تغییر حافظه سیستم.

نقاط قوت:

- امنیت بالا برای برنامه نویس از نظر کپی برداری با تعداد بالا.
- دارای بیشترین امنیت نسبت به سایر قفل های نرم افزاری یا CD.
- سازگاری بسیار بالا نسبت به سایر قفل های نرم افزاری.
- قابلیت آمارگیری فروش برنامه توسط شرکت ارائه کننده کد معادل قفل های CD را میدهد.

۳ – قفل‌های روی CD

با متداول شدن CDو یا لوح فشرده به عنوان بهترین، ارزان ترین و آسان ترین روش مبادله و تکثیر اطلاعات نیاز به حفاظت از آن در برابر تکثیر غیرمجاز هر چه بیشتر احساس شد.

روش های قفل گذاری روی CD

۱- یک روش قفل گذاری اجرای برنامه از روی CD است. در این حالت برنامه هنگام اجرا، به CD رجوع کرده و نقاط خاصی از آن را چک می کند. این نقاط بخش هایی هستند که به صورت فیزیکی علامت گذاری شده اند و در واقع به نوعی صدمه دیده اند و معمولاً این خرابی با تابش اشعه لیزر انجام می شود. به این ترتیب به اصطلاح نقاط معینی از CD لیزرسوز می شود. این نقطه یا نقاط، به عنوان قفل CD عمل می کند و از عمل تکثیر یا کپی برداری و همچنین استفاده غیرمجاز از آن جلوگیری به عمل می آورد.

۲- قفل های حجمی، در این روش فایل های CD را به حدود چند گیگا بایت افزایش می دهند که امکان کپی شدن روی هارد را نداشته باشند. یکی از ساده ترین و عمومی ترین روش هایی که تاکنون برای حفاظت از CD دیده شده است افزایش مجازی طول چند فایل درون CD می باشد به نحوی که آنها تا چند صد مگا بایت به نظر می رسند. برای انجام چنین کاری تنظیمات مربوط به طول آن فایل را در Image بر روی هم قرار می گیرند ولی برنامه حجم واقعی هر فایل را می داند و عمل خواندن را تا آن نقطه انجام می دهد. بنابراین برنامه بخوبی کار می کند.

۳- یکی از روش های نادر و کمیاب برای حفاظت از CDها کنترل بر روی درایو CDمی باشد. از این روش بیشتر در حفاظت بازی ها استفاده می شود و نحوه ایجاد آن به دانش بالایی نیاز دارد. روش آن بدین نحو است که اطلاعاتی نادرست (عمدی) در قسمت ECC (تصحیح خطا) یک سکتور داده نوشته می شود. CD نویس‌های استاندارد بصورت خودکار این خطاها راهنگام نوشتن تصحیح می کنند در هنگام خواندن، برنامه سکتور داده را بصورت RAW و بدون تصحیح خطا در حافظه برای تطبیق با داده های اصلی بار می کند و در صورت تناقض با داده های اصلی برنامه اجرا نمی شود.

۴- متداول ترین روشی کـه بـرای محافظـت از CDدیـده مـی شـود. ایجـاد فاصله‌هایی (gaps) غیراستاندارد ما بین تراک های صوتی و قرار دادن انـدیس هـا در مکان هایی دور از انتظار است. CDکه با این روش قفل گـذاری مـی گـردد در بسیاری موارد توسط نرم افزارهای کپی برداری معمولی و CDنویس هـایی کـه از at once Disc پشتیبانی نمی کنند غیرقابل کپی برداری اسـت. ولـی بـا پیشـرفت تکنولوژی این روش نیز بسرعت در حال کناره گیری است.

۵- امروزه قرار دادن فاصله خالی یا سوراخ گذاری بر روی CDمتـداول شـده است. بدین نحو بسیاری از برنامه ها که قصد خواندن یک تراک از ابتدا تا انتهـا را دارند با مشکل مواجه می شوند.

۶- با استفاده از دسـتکاری TOC سـی دی. یـک قفـل سـاز سـعی دارد بـا دستکاری TOC اطلاعاتی دروغین را به CDپیوند بزند. TOC در واقع اولین تراک از CD می باشد که اطلاعات CD مثل اندازه فایل ها بر روی CD، چگونگی قـرار گرفتن آنها و... را در خود نگهداری می کند.

۴ – قفل‌های اینترنتی

در این روش نرم‌افزار به یک سایت در شبکه اینترنـت وصـل مـی شـود و در صورت تأیید کاربر توسط آن سایت، اجازه کار با نرم‌افزار به کاربر داده می شود.این قفل‌ها در صورتی که به درستی استفاده شوند دارای امنیت بالا و قیمت ارزان مـی باشند. شکستن اینگونه قفل‌ها بسیار مشکل است، البته به شـرط آنکـه از آنهـا بـه درستی استفاده شود. یکی دیگر از قابلیت های اینگونه قفـل‌هـا توانـایی شناسـایی کاربر می باشد، تولید کننده نرم‌افـزار مـی توانـد عـلاوه بـر نـام کـاربر، اطلاعـات شناسایی دیگری مانند نام کاربر، سن، پست الکترونیکی و غیـره را دریافـت کننـد، همچنین فروش آنلاین نرم‌افزار به هر جای دنیا به راحتی امکان پذیر است.

تکنیک های شکستن قفلهای نرم افزار

۱.تغییرJMP: بعضی از نرم افزارها طوری نوشته می شوند تا فقط در صورت وارد شدن شماره سریال صحیح ، برنامه به مرحله بعد برود و در غیر این صورت در همان مرحله بماند و یا از برنامه خارج شود. وقتی این نوع برنامه به کد اسمبلی تبدیل می شود، در کد اسمبلی دو دستور JMP داریم که یکی از آن ها در صورت مساوی بودن عدد وارد شده با شماره سریال صحیح رخ می دهد و دیگری در صورت وارد شدن شماره سریال اشتباه. حال اگر جای این دو JMP عوض شود، نرم افزار با هر عددی به جز شماره سریال اصلی از آن مرحله خواهد گذشت. بنابراین در این روش قفل شکن بدون پی بردن به شماره سریال صحیح با ایجاد تغییر در برنامه باعث می شود هر شماره سریال دلخواه، به عنوان شماره سریال صحیح تشخیص داده شود.

۲.یافتن شماره سریال از داخل کد برنامه: در این روش وقتی یک شماره سریال توسط کاربر وارد شد ، نرم افزار باید آن را با شماره سریال صحیح مقایسه کند تا به صحت یا اشتباه بودن آن پی ببرد. بنابراین در لحظه مقایسه ، شماره سریال صحیح می بایست در جایی موقتا ذخیره شود تا امکان مقایسه ایجاد شود. این مکان موقتی می تواند محل خاصی از RAM یا جایی در هارددیسک ویا در رجیسترهای داخلی پردازشگر باشد. قفل شکنان حرفه ای قادرند با استفاده از نرم افزارهایی که هر نوع تغییر در RAM و هارددیسک و ....را ثبت می کنند، شماره سریال واقعی را بیابند.

۳. Brute force attack: در این روش قفل شکنان برنامه ای را می نویسند که بتواند تمامی حالت های ممکن یک شماره سریال را وارد نرم افزار کرده و بالاخره شماره سریال واقعی را بیابد. البته استفاده از این روش ممکن است چند روز و یا بیشتر طول بکشد.

٤.کد رجیستر کردن (Registration Code): قفل شکنان برای کد رجیستر کردن توسط نرم افزار debugger مکان محاسبه کد از روی نام استفاده کننده را پیدا می کنند و به رابطه ریاضی بین این دو پی می برند.

٥.محدودیت زمانی Time trial: قفل شکنان برای از کار انداختن محدودیت زمانی از دو روش استفاده می کنند: آن ها یا روتین های چک کردن زمان را در برنامه پیدا کرده، آن را غیرفعال می کنند و یا زمان را طوری تغییر می دهند تا نرم افزار به تمام شدن دوره زمانی از پیش تعیین شده، پی نبرد. برای این کار معمولا برنامه ای می نویسند تا قبل از اجرا ی نرم افزار اصلی، زمان کامپیوتر را تغییر دهد.