Intelligent Boards Electronic Co.

شرکت الکترونیکی بردهای هوشمند

قفل سخت افزاری

Safe

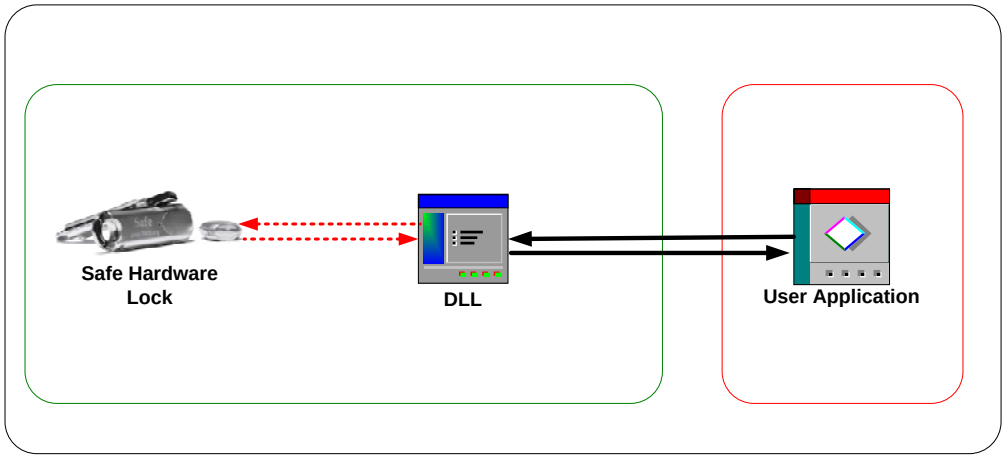
نگارش ۳.۱

www.ibSecurity.com

با توجه به گسترش روز افزون تولید نرم افزارها در زمینه های مختلف و همچنین رعایت نشدن قانون کپی رایت در کشور ما، شرکت های تولید کننده نرم افزار، بسته به نوع و قیمت محصولاتشان روشهای مختلفی را برای تأمین امنیت اعمال می کنند. برای نرم افزارهای ارزان قیمت، از روش های نرم افزاری استفاده می شود. این روشها دارای امنیت پایینی هستند؛ چرا که راههای نفوذ به آنها سالهاست کشف شده است. همچنین این گونه روشها معمولاً نیاز به ارتباط مستقیم مصرف کننده ی نرم افزار با تولید کننده ی آن دارند. در این میان قفل های سخت افزاری به دلیل ماهیت غیر قابل کپی شدن از امنیت بسیار بالاتری برخوردارند؛ البته باید توجه داشت که در صورت استفاده از قفل سخت افزاری نیز تولید کننده ی نرم افزار باید نکات امنیتی را رعایت کند و برای تولید نرم افزاری امن ارتباط تنگاتنگی با تولید کننده ی قفل سخت افزاری داشته باشد.

قفل Safe یک سخت افزار الکترونیکی می باشد که می تواند تا حد زیادی امنیت یک نرم افزار را افزایش دهد. تمامی مراحل طراحی و تولید قفل سخت افزاری Safe در شرکت الکترونیکی بردهای هوشمند انجام شده است؛ کارشناسان این شرکت تلاش زیادی برای بالا بردن امنیت آن و همچنین راحتی استفاده از آن را انجام داده اند. همچنین این شرکت آماده است که در زمینه های امنیتی به مشتریان خود مشاوره دهد.

این قفل با استفاده از یک DLL که در حقیقت رابط نرم افزاری آن با برنامه نویس می باشد، می تواند توابع متعددی را اجرا کند. نحوه ی ارتباط DLL با برنامه و قفل سخت افزاری در شکل زیر نشان داده شده است.



در زیر برخی از قابلیت های قفل سخت افزاری Safe به همراه شرح مختصر هر کدام بیان شده اند:

شمارنده تعداد دفعات اتصال قفل به رایانه، عدم دسترسی به اطلاعات قفل حتی توسط شرکت سازنده ی قفل، فضای داده ی ۲۵۶ بایتی غیر فرار برای ذخیر ه ی اطلاعات کلیدی، قابلیت برنامه ریزی پارامترهای مختلف قفل توسط برنامه نویس، رمز عبور ۳۲ بیتی و شماره ی سریال ۶۴ بیتی برای هر قفل و قابل برنامه ریزی توسط کاربر، امکان استفاده از ثبت زمانی (تاریخ و ساعت اولین استفاده، آخرین استفاده و تاریخ انقضاء)، قابلیت استفاده چندین برنامه به طور همزمان از قفل، عدم نیاز به نصب درایور و . . . .

شماره منحصر بفرد (DeviceID) : این شماره برای هر قفل تولید شده یک عدد منحصر بفرد بوده و می توان از آن به عنوان شناسه ی یک قفل استفاده کرد. این پارامتر به صورت فقط خواندنی، درهنگام ساخت توسط شرکت سازنده بر روی هر قفل تولید شده تنظیم می گردد و برنامه نویس فقط می تواند مقدار آن را از قفل بخواند. لازم به ذکر است که تابع استفاده شده برای بازیابی این شماره از روی قفل، نیازی به ارسال رمز عبور ندارد.

شمارنده تعداد دفعات اتصال قفل به رایانه : قفل سخت افزاری Safe طوری طراحی شده است که می تواند به صورت خودکار تعداد دفعات اتصال قفل به رایانه را مشخص کند. در قفل یک متغیر وجود دارد که هر زمان تغذیه ی برق آن وصل شد، این متغیر یک واحد افزایش می یابد. لازم به ذکر است اگر قفل به رایانه متصل باشد و رایانه روشن و سپس خاموش شود یا در هنگام جدا شدن و متصل شدن مجدد قفل، این متغیر افزایش می یابد. برای بازیابی این پارامتر نیز نیازی به رمز عبور قفل نخواهید داشت.

فضای داده ی ۲۵۶ بایتی : در قفل سخت افزاری Safe، فضای داده ی ۲۵۶ بایتی در نظر گرفته شده است. این حافظه از نوع غیر فرار بوده و با جدا شدن قفل از رایانه پاک نمی شود؛ برنامه نویس می تواند اطلاعات کلیدی برنامه خود را در این بخش ذخیره کرده و در مواقع مورد نیاز استفاده نماید. همچنین طراح نرم افزار می تواند از این قابلیت به عنوان یک پارامتر امنیتی در نرم افزار استفاده کند؛ چرا که قفل سخت افزاری یک ماژول جدا از برنامه و غیر قابل کپی برداری است. به همین دلیل توصیه می شود که برنامه نویسان و طراحان نرم افزار به طور مناسب از این قابلیت استفاده نمایند. لازم به یاد آوری است که در صورت نیازِ طراحان نرم افزار به مقدار بیشتری از حافظه، می توانند با اعلام در خواست خود، از یک قفل اختصاصی با ظرفیت حافظه ی بیشتر بهره مند گردند.

رمز عبور ۳۲ بیتی : برنامه نویس برای ارتباط با قفل و اجرا کردن توابع موجود روی آن نیاز به داشتن رمز عبور (Password) دارد. این پارامتر توسط کاربر و با استفاده از برنامه ی مدیریت قفل (LockManager) بر روی قفل تنظیم می شود و در هنگام استفاده در برنامه این رمز عبور باید به عنوان یکی از پارامترهای تابع، به قفل مورد نظر ارسال شود. توابع موجود بر روی قفل در صورتی به درستی اجرا می شوند که این مقدار با رمز ذخیره شده بر روی قفل یکسان باشد. نکته ی قابل توجه در مورد این پارمتر این است که به منظور جلوگیری از تلاش افراد غیر مجاز برای دسترسی به این رمز عبور، اگر به هر نحوی، بیش از سه مرتبه رمز عبور اشتباه به قفل ارسال شود، قفل به صورت سخت افزاری و به طور خودکار از کار می افتد و دیگر به هیچ تابعی حتی با رمز صحیح پاسخ نخواهد داد. لازمه ی برقراری ارتباط مجدد با قفل جدا کردن قفل از رایانه و اتصال مجدد آن می باشد. با

این روند اگر شخص غیر مجازی بخواهد به صورت آزمایش و خطا این رمز را کشف کند، عملاً تلاش بیهوده ای خواهد نمود. در عین حال که رمز عبور به امنیت برنامه کمک شایانی می کند، این پارامتر تنها پارامتر امنیتی قفل نبوده و موارد دیگری نیز (از قبیل شماره سریال، الگوریتم امنیتی یک طرفه و ....) وجود دارند که با ترکیب آنها می توان به سطح امنیت بالایی دست یافت.

شماره ی سریال : این پارامتر یک عدد ۶۴ بیتی می باشد که توسط برنامه نویس بر روی قفل تنظیم می شود و در الگوریتم تشخیص قفل به صورت مستقیم شرکت می کند. طراح نرم افزار همچنین می تواند شماره های متفاوتی را برای نسخه های متعدد نرم افزار و یا برای نرم افزاری های متعدد خود تولید و تنظیم کند و با استفاده از این شماره های متفاوت، بین نرم افزار های گوناگون خود تفاوت قائل شود بدین ترتیب، علاوه بر پارامتر DeviceID (که در هنگام تولید و به صورت فقط خواندنی بر روی قفل تنظیم می شود) این مقدار نیز می تواند یک شماره ی منحصر بفرد قابل برنامه ریزی توسط برنامه نویس برای شناسایی بهتر قفل سخت افزاری ایجاد نماید. نحوه ی تنظیم این پارامتر و نیز چگونگی بکار گیری آن در مستندات مربوطه و همچنین در ادامه متن آمده است.

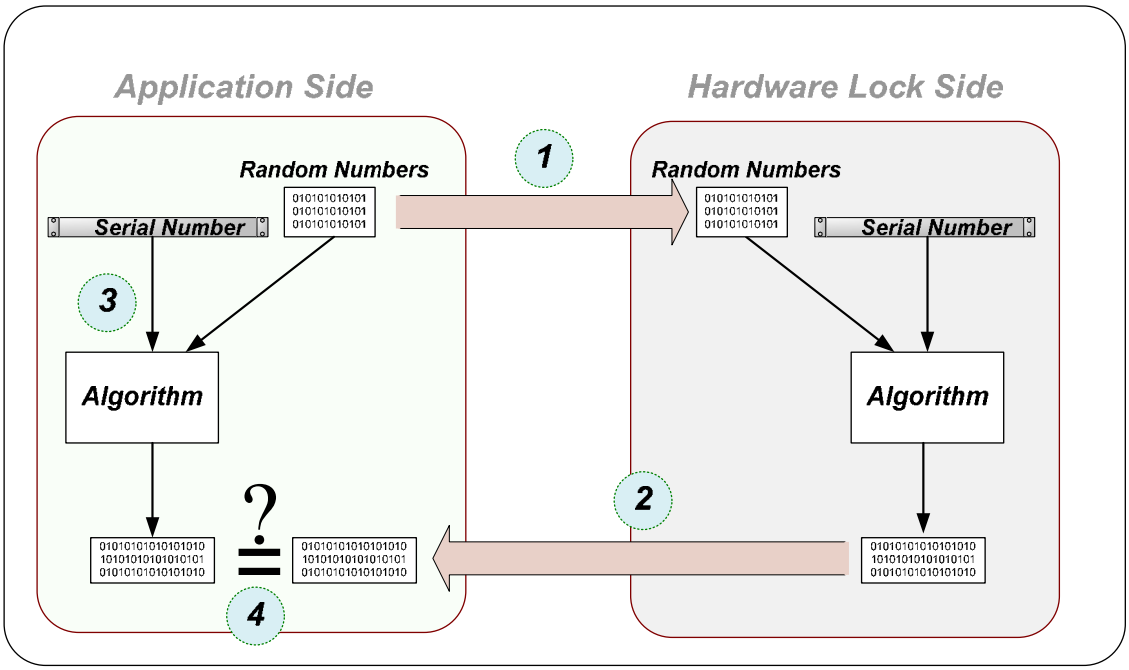
امکان استفاده از ثبت زمانی : در قفل سخت افزاری Safe می توان مقادیری از قبیل تاریخ و ساعت اولین استفاده، آخرین استفاده و تاریخ انقضای قفل را تنظیم کرد. لازم به توضیح است که تنظیم کردن و مدیریت این مقادیر صرفاً در دست برنامه نویس بوده و وی باید در مواقع مناسب این مقادیر را تنظیم و از آنها به طور مناسبی استفاده کند. به طور مثال تنظیم تاریخ انقضای قفل، توسط برنامه نویس تنظیم می شود و مسئولیت از کار انداختن (یا مدیریت) نرم افزاری که تاریخ انقضای آن گذشته باشد، بر عهده شخص برنامه نویس یا طراح نرم افزار می باشد.

عدم نیاز به نصب درایور : اکثر سخت افزارهایی که به نوعی با رایانه ارتباط برقرار می کنند، قبل از شروع به کار نیاز به نصب درایوری دارند که شرکت سازنده ی آن سخت افزار تولید کرده است. این درایورها برای ارتباط نرم افزار با سخت افزار لازم و ضروری هستند. قفل سخت افزاری Safe طوری طراحی شده است که نیاز به نصب هیچ گونه درایوری نداشته و به صورت Plug & Play کار می کند.

قابلیت استفاده چندین برنامه به طور همزمان از قفل : قفل سخت افزاری Safe و نرم افزار های مربوط به آن طوری طراحی شده اند که چندین برنامه به طور همزمان می توانند از قفل استفاده کنند و این امر هیچ گونه مشکل همزمانی را ایجاد نخواهد کرد. این قابلیت هنگامی مشخص می شود که شرکت تولید کننده ی نرم افزار بخواهد چندین نرم افزار خود را که به یک مشتری عرضه می نماید، تنها با یک قفل محافظت نماید که در این صورت از ارائه قفل به ازای هر نرم افزار جلوگیری می شود و می توان تنها با یک قفل امنیت چندین نرم افزار را تأمین کرد.

نحوه استفاده از شماره سریال : شماره ی سریال، یک عدد ۶۴ بیتی است که توسط طراح نرم افزار بـر روی قفل تنظیم (Set) می شود. این مقدار در الگوریتم امنیتی قفل شرکت می کنـد و یکـی از پارامترهـای مهـم قفـل است. چگونگی استفاده از این پارامتر در این متن و در سایر مستندات مربوط به قفل سخت افزاری، کاملاً توضـیح داده شده است.

در قفل سخت افزاری Safe یک الگوریتم قدرتمند و یک طرفه پیاده سازی شده است. الگوریتم یک طرفـه بـه این معنی است که با داشتن خروجی و خود الگوریتم نمی توان به ورودی های آن پی برد. نحوه ی ارتباط برنامه با این الگوریتم در شکل زیر نشان داده شده است :



همان طور که در شکل ملاحظه می کنید، شماره سریال هم در قفل سخت افزاری و هم در برنامـه وجـود دارد. در حقیقت شماره سریال، قبل از استفاده از قفل سخت افزاری توسط برنامه ی LockManager بـر روی حافظـه ی موجـود در آن ثبـت مـی شـود. برنامـه نـویس بـا اسـتفاده از دسـتورالعمل خاصـی کـه در اختیـار او قرار می گیرد، تعدادی عدد تصادفی (Random) تولید کرده و با استفاده از تابع خاصی (که در DLL مربـوط بـه قفل وجود دارد،) این مقادیر را به قفل سخت افزاری می فرستد. قفل سخت افزاری بلافاصله شماره سریال و اعـداد تصادفی را در داخل الگوریتم امنیتی گذاشته و بر اساس ترکیب آن دو، مقادیری را تولید کرده و به برنامه بـر مـی گرداند. در این هنگام برنامه، کاری شبیه به کار سخت افزارِ قفل را انجام می دهد؛ یعنی همان اعدادِ تصادفیِ تولید شده، به علاوه ی شماره سریال قفل را داخل همان الگوریتم گذاشـته و خروجـی الگـوریتم را بـا خروجـی مقـادیر بازگشتی از قفل مقایسه می کند؛ در صورتی که این اعداد با هم برابر باشند می توان نتیجه گرفت که دقیقاً همـان

قفل مورد نظر بر روی رایانه وجود دارد یا خیر. لازم به ذکر است که کُد (Source) مربوط به این الگوریتم تماماً در اختیار برنامه نویس قرار گرفته و فاش شدن این کُد برای سایرین هیچ مشکل امنیتی را برای برنامه و قفل سخت افزاری ایجاد نمی کند. البته این مطلب به شرطی درست است که برنامه نویس یا تنظیم کننده ی قفل سخت افزاری، به هیچ وجه شماره سریال و رمز عبور قفل سخت افزاری را در اختیار دیگران قرار ندهد. لازم به ذکر است که شماره سریال و رمز عبور قفل، به ترتیب مقادیر پیش فرض FFFFFFFFFFFFFFFF و FFFFFFFF را دارند. همان طور که ملاحظه می کنید اعداد فوق در مبنای HexaDecimal (شانزده شانزدهی) می باشند و هر کدام به ترتیب ۶۴ و ۳۲ بیت طول دارند

برنامه نویسان زبانهای متفاوت هیچ گونه نگرانی در مورد طرز استفاده از قفل، چک کردن قفل و نوشتن الگورتیم امنیتی فوق را نخواهند داشت؛ چرا که کُد نمونه برای اکثر زبانهای رایج برنامه نویسی بر روی CD مربوط به قفل سخت افزاری وجود دارد. همچنین تعدادی از نکات مهم امنیتی که برنامه نویس یا طراح نرم افزار باید آنها را مد نظر قرار دهد تهیه شده و به همراه سایر مستندات قفل سخت افزاری بر روی CD ضمیمه موجود می باشد. مطلب بسیار مهم اینکه تمامی موارد امنیتی لازم در مراحل طراحی و پیاده سازی قفل سخت افزاری رعایت شده است و این قفل دارای امنیت بالایی می باشد؛ اما از آنجاییکه امنیت نرم افزار رابطه ی مستقیمی با همکاری طراحان نرم افزار و تولید کننده ی قفل سخت افزاری دارد، اکیداً توصیه می شود که طراحان نرم افزار نکات امنیتی برنامه هایشان را با دقت رعایت کنند، چرا که صِرف استفاده از قفل سخت افزاری (و توجه نکردن به مسائل امنیتی) تأثیر زیادی در جلوگیری از Crack شدن برنامه ندارد.

شرکت الکترونیکی بردهای هوشمند

تهران – خیابان ولیعصر – بالاتر از پارک ساعی – کوچه چمن – پلاک ۲

تلفن : ۰۲۱-۸۸۸۷۳۵۰۲ ۰۲۱-۸۸۸۷۳۵۰۳

www.ibSecurity.com