شرکت صنایع پیشرفته سهند (سهامی خاص)

اندیشه نگار پارس
Andisheh Negar Pars

Sahand Server Descriptions

SAHAND SR220-G1

2U Rackmount

2U Rackmount with 1+1 1600W CRPS
Dual Socket P+ (LGA 4189), supports 3rd Gen Intel® Xeon® Scalable processors
16+16 DIMM slots (2DPC), supports DDR4 RDIMM, LRDIMM, RDIMM/LRDIMM-3DS, Intel® Optane™ Persistent Memory 200 series
12 hot-swap 3.5"/2.5" drive bays, 2 fixed 2.5" SATA drive bays
4 FH PCIe4.0 x16, 2 FH PCIe4.0 x8, 1 low-profile PCIe4.0 x16, 1 low-profile PCIe4.0 x8
Supports 2 M.2 (PCIe3.0 x4 or SATA 6Gb/s)
2 RJ45 (1GbE) by Intel® i350-AM2
1 OCP NIC 3.0 (PCIe4.0 x16)
Baseboard Management Controller (BMC)

www.sahand-tech.ir
info@sahand-tech.ir

باسمه‌تعالی

شرحی بر کارگزار SAHAND SR220-G1

تولید شرکت صنایع پیشرفته سهند (سهامی خاص)

۱- مقدمه

تردیدی نیست که امروزه کارگزارهای کامپیوتری(Computer Server) [۱] نقشی بنیادی در زیرساخت‌های حیاتی هر کشوری از جمله کشور عزیز ما ایفاء می‌کنند. کارگزارها در واقع فراهم آورنده‌ی بستر اصلی ذخیره‌سازی و پردازش حجم عظیم داده‌هایی هستند که تمام شئون زندگی بشر در دنیای امروز درگیر آن است. نمونه‌هایی از کاربردهای کارگزارها عبارت است از [۱][۲]: ذخیره سازی اطلاعات حساس کشور از اطلاعات دولتی و اقتصادی گرفته تا اطلاعات شخصی افراد، ارائه‌ی خدمات برخط مانند خدمات بانکی، وب سایت‌ها، شبکه‌های اجتماعی و ایمیل، فراهم‌سازی توانایی مدیریت اطلاعات به ویژه در حوزه‌های امنیتی و نظارتی و فراهم‌سازی بستر توسعه و رشد اقتصادی مانند ایجاد فرصت‌های شغلی مرتبط با فناوری اطلاعات.

با توجه به نیاز جدی کشور به برخورداری از تعداد بسیار زیاد کارگزار در تمامی بخش‌های دولتی و خصوصی واضح است که اقدام به تولید کارگزار در داخل کشور می‌تواند در جلوگیری از خروج ارز و رشد تولید داخلی گامی بسیار مؤثر باشد. اما اهمیت تولید کارگزار در داخل کشور تنها محدود به مزایای اقتصادی و رشد تولید داخلی نیست و بحث بسیار مهم دیگر حفاظت از امنیت زیرساخت‌های حیاتی کشور است [۴]. در این نوشتار با ذکر دلایل فنی شرح داده خواهد شد که چگونه استفاده از کارگزارهای تولید شده توسط شرکت‌های خارجی خواه ناخواه به معنای آن است که قابلیت کنترل و امنیت داده‌های کشور به دست این شرکت‌ها سپرده شود که این امر قطعاً برای امنیت کشور مخاطره ایجاد می‌کند. به این ترتیب هر نوع تولید کارگزار در داخل کشور باید رفع نگرانی‌های امنیتی برای زیرساخت‌های ذخیره‌سازی و پردازش داده را در اولویت قرار دهد.

در راستای موارد بیان شده شرکت صنایع پیشرفته سهند اقدام به تولید کارگزار SAHAND SR220-G1 نموده است تا بتواند پاسخگوی نیازهای روزافزون داخل کشور به کارگزارهایی باشد که نه تنها از نظر توانایی ذخیره‌سازی داده و قدرت محاسباتی توانایی بالایی داشته باشد بلکه لازمه‌های امنیت، حفاظت و مراقبت از داده‌ها را نیز مورد توجه جدی قرار دهد. خط تولید مربوط به این کارگزار هم‌اکنون در منطقه ویژه اقتصادی فرودگاه بین‌المللی پیام برای فرآیند تولید آماده شده است. همچنین بخش ثابت‌افزار (Firmware) این کارگزار شامل واحد UEFI BIOS [۵] و همچنین BMC [۶] که نقش کلیدی و بنیادی در تأمین امنیت داده‌ها در کارگزارها را دارند بطور کامل در داخل کشور و با همکاری دانشگاه صنعتی شریف تولید شده است و به این ترتیب کد منبع (Source Code) ثابت‌افزار تجاری این کارگزار در داخل کشور موجود است. وجود کد منبع ثابت‌افزار کارگزار در داخل کشور این اطمینان را می‌دهد که نه تنها آسیب‌پذیری‌های امنیتی عمدی (مانند: Backdoor) [۷] در ساختار و طراحی کارگزار قرار داده نشده باشد بلکه اجازه‌ی پیاده‌سازی مکانیسم‌های امنیتی سفارشی توسط نهادهای داخل کشور را فراهم می‌آورد. در واقع تیم تحقیق و توسعه‌ی شکل گرفته با همکاری دانشگاه صنعتی شریف اجازه‌ی اعمال توسعه و سفارشی‌سازی در جنبه‌های گوناگون این کارگزار را فراهم می‌کند. نکته‌ی قابل توجه دیگر این است که شرکت صنایع پیشرفته سهند به همراه محققین دانشگاه صنعتی شریف در طراحی معماری بخش مادربورد نیز درگیر بوده است که این مسئله (درگیری در طراحی معماری مادربورد) از لازمه‌های کسب قابلیت طراحی ثابت‌افزار BMC است [۸] که همانطور که بیان شد بطور کامل در داخل کشور صورت گرفته است.

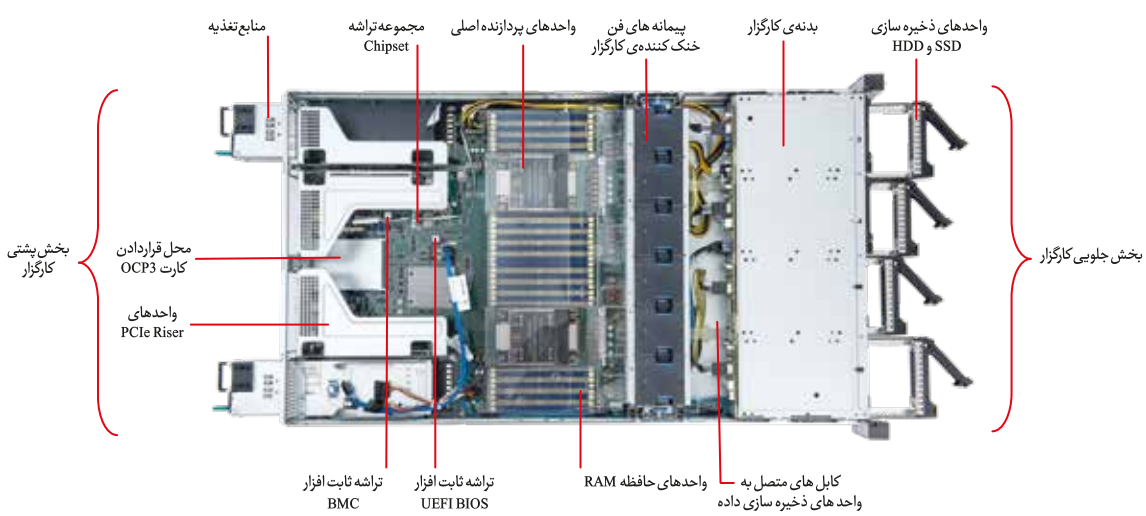
لازم به ذکر است که واحدهایی از این کارگزار طبعاً باتوجه به توجیه اقتصادی که وجود دارد از خارج از کشور خریداری شده یا به برخی از شرکت‌های خارجی سفارش داده شده است تا تهیه گردد که البته همانطور که در این نوشتار خواهیم دید (و در مراجع

متعدد از جمله مرجع مورد ارجاع بیان شده است) [۹] این کار رویه‌ای شناخته شده برای تمامی تولید کنندگان مطرح کارگزار در دنیا است. اما نکته‌ی کلیدی این است که نظارت شرکت صنایع پیشرفته سهند بر روند کارهایی که برون‌سپاری شده است، طراحی معماری و ساختار کارگزار در داخل کشور و همچنین تولید صد در صد ثابت‌افزار در داخل کشور مانع از آن است که نگرانی‌های امنیتی که برای کارگزارهای تولید خارج از کشور وجود دارد، در اینجا مطرح باشد. در واقع بخش عمده و اصلی ارزش افزوده در روند تولید کارگزار SAHAND SR220-G1 بدون تردید حاصل فعالیت نیروها و متخصصین داخلی است و می‌توان به جرأت ادعا نمود قابلیت‌های امنیتی و سفارشی‌سازی که این کارگزار برای مصرف‌کنندگان داخل کشور ارائه می‌کند، در میان کارگزارهای موجود در بازار نظیری ندارد.

در ادامه‌ی این نوشتار ابتدا به نقش و میزان مشارکت شرکت صنایع پیشرفته سهند در تولید کارگزار SAHAND SR220-G1 پرداخته می‌شود. سپس در بخش ۳ ویژگی‌های خاص و منحصر به فرد این کارگزار به ویژه از منظر تأمین امنیت داده‌ها که برای کشور ما بسیار حیاتی است بیان می‌شوند. در بخش ۴ ویژگی‌های این کارگزار از منظر قابلیت‌های محاسباتی و کارآیی بیان می‌گردد و در نهایت در بخش ۵ خلاصه و جمع‌بندی از بحث ارائه می‌شود.

۲- مشارکت و نقش شرکت صنایع پیشرفته سهند در تولید کارگزار SAHAND SR220-G1

در ابتدا یک نگاهی داریم بر اینکه یک کارگزار از چه بخش‌هایی تشکیل شده است و چه کارهایی باید برای تولید یک کارگزار انجام گیرد و سپس به سهمی که شرکت صنایع پیشرفته سهند در این تولید دارد، پرداخته می‌شود. بخش‌های اصلی تشکیل دهنده‌ی یک کارگزار، همانطور که در شکل ۱ نمایش داده شده‌اند، عبارتند از [۱۰][۱۱]: پردازنده‌ی اصلی، مادربورد، ثابت‌افزار UEFI BIOS، ثابت‌افزار BMC، حافظه RAM، واحدهای ذخیره‌سازی داده SSD و HDD، بخش‌های الکترومکانیکی شامل واحدهای منبع تغذیه، بدنه کارگزار و سیستم خنک کننده و اتصالات درونی کارگزار. در واقع از کنار هم قرار گرفتن همین اجزاء است که یک کارگزار تشکیل می‌گردد. نکته‌ی قابل توجه این است که اگر کارگزارهای تولید شده توسط شرکت‌های مطرح دنیا مانند شرکت HP را مورد بررسی قرار دهیم به سادگی مشخص می گردد که هیچ تولیدکننده‌ی کارگزاری نیست که تمام این قطعات و واحدها را خود تولید کند [۹]. به عنوان مثال به سادگی می‌توان مشاهده نمود که در کارگزارهای HP پردازنده‌های اصلی بطور معمول تولید شرکت Intel هستند، واحدهای SSD به کاررفته تولید شرکت‌های دیگر مانند Samsung هستند و حتی طراحی مادربوردها معمولاً از شرکت‌های دیگر مانند شرکت Intel دریافت شده و تولید آن عمدتاً به کارخانه‌های تولید بوردهای الکترونیکی واقع در آسیای شرقی برون سپاری می‌شود [۱۳].



شکل ۱: بخش‌های تشکیل دهنده‌ی یک کارگزار

اینکه تمامی قطعات یک کارگزار را یک تولیدکننده‌ی واحد ایجاد نمی‌کند یک نقیصه نیست بلکه یک رویه و تصمیم منطقی است که سه دلیل اصلی را می‌توان برای آن ذکر نمود [۹][۱۳]:

دلیل اول) صرفه‌ی اقتصادی: برای یک تولیدکننده‌ی کارگزار حتی تولیدکنندگان مطرح در کشورهای پیشرفته‌ی صنعتی مقرون به صرفه است که به جای اینکه خود به تولید بوردهای الکترونیکی اقدام کنند آن را به شرکت‌های تولید کننده‌ی بورد که معمولاً در کشورهای آسیای شرقی قرار دارند بسپارند [۱۳] و به این ترتیب هزینه‌ی تولید کاهش قابل توجهی خواهد داشت. این انتخاب به دلیل وجود یک نقص نیست بلکه بطور عمده به صرفه‌ی اقتصادی باز می‌گردد.

دلیل دوم) تخصصی بودن کار: کارگزارها سیستم‌های پیچده‌ای هستند که تولید هرکدام از اجزاء تشکیل دهنده که از آن‌ها نام برده شد حقیقتاً تخصص‌های دانشی بسیار متفاوتی را می‌طلبد. به عنوان مثال در حالیکه بحث معماری پردازنده‌ها برای خود یک علم و تخصص بسیار گسترده است. بحث سیستم‌های ذخیره‌سازی داده مانند واحدهای SSD نیز امروزه برای خود یک علم و تخصص بسیار گسترده دیگر است که با حوزه‌ی قبلی یعنی بحث معماری پردازنده‌ها متفاوت است. به همین ترتیب، علم و تخصص مهندسی ثابت‌افزار (Firmware Engineering) نیز یک زمینه‌ی بسیار گسترده و متفاوت دیگری است که با هر دو مورد قبلی تفاوت‌های جدی دارد. به همین دلیل شرکت‌های مطرح در این حوزه به جای اینکه در تمام این تخصص‌های گسترده و متفاوت ورود کنند که می‌تواند موجب اتلاف هزینه و تحلیل توانایی مدیریتی گردد، ترجیح می‌دهند که به شکل تخصصی کار کنند و در نتیجه در یک یا حداکثر دو حوزه از موارد ذکر شده ورود کنند [۹].

دلیل سوم) قابلیت اطمینان: در بحث مهندسی قابلیت اطمینان (Reliability Engineering) این یک امر کاملاً شناخته شده است که اگر یک شرکت به جای تهیه‌ی قطعات از شرکت‌های تخصصی گوناگون، خود مستقیماً به تولید یک قطعه اقدام کند، می‌تواند به شدت و در حد چندین مرتبه‌ی بزرگی (Order of Magnitude) موجب افت در قابلیت اطمینان و افزایش نرخ خطا در سیستم تولید شده گردد. این امر تا آن اندازه شناخته شده است که امروزه در بسیاری از استانداردهای محاسبه‌ی قابلیت اطمینان مانند MIL-HDBK-217 [۱۳] در روابط ریاضی که برای محاسبه‌ی نرخ خطا یا قابلیت اطمینان به کار می‌روند، در نظر گرفته می‌شود. واضح است که کارگزارها به دلیل به کار گرفته شدن در زیرساخت‌های حیاتی و کاربردهای حساس نیازمند سطوح بسیار بالای قابلیت اطمینان هستند.

حال که متوجه شدیم منطقاً قابل قبول نیست که یک تولیدکننده‌ی کارگزار خود اقدام به تولید تمامی اجزاء کارگزار کند، خوب است به این مسئله بپردازیم که شرکت صنایع پیشرفته سهند بر تولید کدام بخش‌های کارگزار به شکل تخصصی تمرکز کرده است و کدام بخش‌ها را برون‌سپاری کرده یا از خارج از کشور تهیه می‌کند. در واقع مشارکت شرکت صنایع پیشرفته سهند در تولید کارگزار را می‌توان در شش قسمت بیان نمود که در ادامه بیان شده‌اند:

۱) تولید ثابت‌افزار UEFI BIOS کارگزار بطور ۱۰۰٪ توسط شرکت صنایع پیشرفته سهند و با مشارکت محققین دانشگاه صنعتی شریف در داخل کشور صورت گرفته است. برای پی‌بردن به اهمیت این بخش لازم است تأکید گردد که شرکت‌های بسیار بزرگ و مطرحی در دنیا بطور تخصصی فقط برروی تولید همین قسمت از کارگزار کار می‌کنند که از جمله می‌توان به شرکت Phoenix Technologies ونیز شرکت Insyde Software اشاره نمود که در واقع شرکت دوم (Insyde Software) نقش اصلی تولید UEFI BIOS برای کارگزارهای شرکت HP را برعهده دارد. خوب است دقت شود که حتی شرکت‌های شناخته شده در حوزه مهندسی کامپیوتر همچون Intel و IBM امروزه از تولیدکنندگان مطرح ثابت‌افزار BIOS نیستند. همچنین می‌توان گفت این قسمت، البته در کنار واحد BMC که در ادامه شرح داده خواهد شد، نقطه‌ی کلیدی امنیت کارگزارها است [۱۴] به نحوی که برای تأمین امنیت زیرساخت‌های حیاتی کشور هیچ چاره‌ای به جز ورود مستقیم به تولید این قسمت در داخل کشور وجود ندارد. در مورد حجم پیچیدگی کار نیز باید بیان نمود که امروزه واحد UEFI BIOS از نظر پیچیدگی قابل مقایسه با یک سیستم‌عامل کامل است (البته UEFI BIOS با سیستم‌عامل متفاوت است و فقط برای اینکه دیدی از حجم پیچیدگی داده شود این مثال آورده شده است) و

فقط هسته‌ی مرکزی آن توسط شش میلیون خط برنامه‌نویسی سطح پایین و درگیر در جزئیات سخت‌افزار توصیف می‌گردد [۱۵]. با توجه به اینکه این بخش بطور ۱۰۰٪ در داخل کشور تولید شده است، به جرأت می‌توان ادعا نمود که شرکت صنایع پیشرفته سهند اولین تولیدکننده در کشور است که کد منبع تجاری واحد UEFI BIOS را بطور کامل در اختیار دارد که این مسئله اهمیت بسیار زیادی از منظر تأمین امنیت کارگزارها دارد. چراکه می‌توان به این ترتیب مطمئن بود که آسیب‌پذیری‌های عمدی (مانند درب پشتی Backdoor) در آن قرارداده نشده است و همچنین وجود کامل کد منبع اجازه‌ی هر نوع سفارشی‌سازی برای مشتریان داخل کشور را فراهم می‌آورد.

۲) تولید ثابت‌افزار BMC کارگزار بطور ۱۰۰٪ توسط شرکت صنایع پیشرفته سهند و با مشارکت محققین دانشگاه صنعتی شریف در داخل کشور صورت گرفته است. لازم به ذکر است که حوزه‌ی کاری این ثابت‌افزار با حوزه‌ی ثابت‌افزار پیشین یعنی ثابت‌افزار UEFI BIOS به کل متفاوت است و اهداف طراحی و ساختار کاملاً متفاوتی دارد. این بخش از جمله قسمت‌هایی است که شرکت HP نیز تولید آن را خود انجام می‌دهد که البته معمولاً شرکت HP از این محصولِ خود با نام واحد ILO یاد می‌کند [۱۶] و در واقع بخش بسیار مهمی از ارزش افزوده شرکت HP در تولید کارگزار است. برای پی‌بردن به اهمیت این بخش نیز لازم است تأکید گردد که امروزه شرکت‌های Google و Facebook نظر به اهمیت فوق‌العاده‌ی ثابت‌افزار BMC از منظر امنیت کارگزار تولید این ثابت افزار را پی‌گیری نموده‌اند و سعی کرده‌اند که مستقل از تولیدکنندگان دیگر خود به این بحث وارد شوند [۱۷]. همانطور که در بند قبل برای ثابت‌افزار UEFI BIOS بیان شد در مورد ثابت‌افزار BMC نیز برای تأمین امنیت زیرساخت‌های حیاتی کشور هیچ چاره‌ای به جز ورود مستقیم به تولید این قسمت در داخل کشور وجود ندارد. در مورد حجم پیچیدگی کار خوب است بیان گردد که اگرچه واحد BMC یک بخش از کارگزار است ولی خود یک کامپیوتر تمام‌عیار، کامل و مستقل است که پردازنده‌ی مرکزی، حافظه و واحدهای ذخیره‌سازی خود را دارد و از سیستم‌عامل خود (که معمولاً مبتنی بر لینوکس نهفته است) استفاده می‌کند و وظیفه‌ی کنترل و مدیریت کامل کارگزار را برعهده دارد [۶][۸][۱۰].

۳) شرکت صنایع پیشرفته سهند با همکاری محققین دانشگاه صنعتی شریف در طرح معماری و سازمان (Organization) مادربورد مشارکت داشته‌اند هرچند که تولید بورد الکترونیکی آن به شرکت‌های خارجی واگذار شده است. از دلایل اصلی ورود شرکت صنایع پیشرفته سهند و محققین دانشگاه صنعتی شریف به طرح معماری و سازمان کارگزار نیازی است که برای تولید ثابت‌افزار BMC (و تاحد نسبتاً کمتری برای تولید ثابت‌افزار UEFI BIOS) وجود داشته است [۸]. همانطور که در دو بند قبلی مشاهده شد ورود صد در صدی به تولید ثابت‌افزارهای BMC و UEFI BIOS با توجه به هدف تأمین امنیت برای ما الزامی بوده است. اما نکته‌ی مهم این است که ثابت‌افزار واحدهای BMC و UEFI BIOS به حدی درگیر جزئیات سخت‌افزاری، پیاده‌سازی و معماری مادربورد است [۸] که امکان انجام این کار بدون مداخله در طرح و سازمان مادربورد وجود ندارد و لذا انجام این قسمت نیز الزامی بوده است.

۴) به جهت تأمین امنیت کارگزارها شرکت صنایع پیشرفته سهند با همکاری محققین دانشگاه صنعتی شریف دست به طراحی و پیاده‌سازی یک واحد جدید و افزودن آن به عنوان بخشی از کارگزار نموده است که نام واحد (Security Features Controller) SFC بر آن نهاده شده است. در حال حاضر واحد مشابهی در هیچکدام از کارگزارهای موجود در بازار قرار ندارد و این بخش با این هدف طراحی و تولید شده است که مدیریت امنیت کارگزار را بطور کامل در اختیار تولیدکننده داخل کشور قرار دهد و امکان حملات امنیتی در لایه‌های پایین (حملات در سطح ثابت‌افزار یا حتی در سطح سخت‌افزار) به کارگزارها را حداقل کند. این واحد در واقع بطور اختصاصی و برای اولین بار در کارگزار SAHAND SR220-G1 به کار گرفته شده است و با توجه به اینکه ثابت‌افزار آن نیز بطور کامل در داخل کشور طراحی و تولید شده است امکان توسعه و سفارشی‌سازی آن در آینده برای پوشش دادن یا ارائه دادن کاربردهای امنیتی دیگر نیز وجود دارد.

لازم به ذکر است مجموعه‌ی شرکت صنایع پیشرفته سهند بر این باور است که تولید محصولات داخلی نباید صرفاً با الگوبرداری از محصولات خارجی باشد (هرچند که این الگوبرداری قطعاً بسیار مثبت است و اهمیت خود را دارد) و نیاز است که با توجه به

اقتضائات و نیازهای خاصی که در کشور وجود دارد و تفاوت‌هایی که نیازهای داخل کشور ما با سایر نقاط جهان دارد تولیدکنندگان داخلی دست به ابتکار عمل برای حل مسائل داخلی بزنند. در واقع می‌توان تولید واحد SFC و افزودن آن به معماری و سازمان کارگزار را در همین راستا دانست. در حقیقت کشور ما بنابه‌دلایل گوناگون، از جمله عدم برقراری ارتباط با شرکت‌های تولیدکننده‌ی خارجی ثابت‌افزار کارگزار یا قرارداشتن در معرض حملات امنیتی طراحی شده توسط سازمان‌های تخصصی، نیازهای امنیتی ویژه‌ای دارد و وجود یک واحد سخت‌افزاری (و البته مجهز به ثابت‌افزار خاص خود) مانند SFC در درون کارگزار می‌تواند یکی از راهکارهای مهم برای پرداختن به این امر باشد.

۵) کارگزارها دارای بخش‌های مکانیکی بسیار مهمی هستند که از جمله می‌توان به شاسی، بدنه، سیستم تهویه و خنک‌کنندگی و پنل فیزیکی آن‌ها اشاره نمود [۱۱]. همچنین کارگزارها دارای اتصال‌های بسیار زیاد و متعدد در درون خود با انواع کابل‌ها و اتصال‌های استاندارد هستند (مانند اتصال‌های SATA، کابل‌های USB، اتصال‌های پهن با شکل Ribbon و ...) که ویژگی‌های مهندسی و فنی بسیار پیچیده و تخصصی دارند. شرکت سهند قصد دارد که تمامی این اجزاء را به تولیدکنندگان داخلی در صورت وجود برون سپاری نماید. هرچند که ورود این اجزاء از خارج از کشور نیز امکان پذیر است.

۶) از مراحل بسیار مهم در تولید کارگزارها که حجم فعالیت بسیار زیادی را به خود اختصاص می‌دهد، بدون تردید مجتمع‌سازی (Integration) و آزمون (Test) کارگزارها است [۱۸][۱۹]. واضح است که اجزاء ذکر شده در این نوشتار باید در کنار یکدیگر قرار گیرند تا کارگزار را تشکیل دهند. همچنین لازم است که این اجزاء هم پیش از فرآیند مجتمع‌سازی مورد آزمون قرار گیرند تا یک واحد مشکل‌دار در کارگزار قرارداده نشود و هم پس از مجتمع‌سازی باید کارگزار کامل مورد آزمون‌های متعدد از منظر کارآیی و حتی امنیتی قرار گیرد. تمامی این مراحل در تولید کارگزار SAHAND SR220-G1 بطور ۱۰۰٪ توسط شرکت صنایع پیشرفته سهند و در خط تولید کارخانه انجام می‌گیرد. در پایان این بخش مجدداً و صراحتاً ذکر می‌گردد که پردازنده و واحدهای SSD و HDD قرار داده شده در کارگزار SAHAND SR220-G1 از شرکت‌های خارجی تهیه خواهد شد. همچنین تولید بورد الکترونیکی مادربورد و تولید واحدهای RAM به شرکت‌های خارجی برون‌سپاری می‌گردد هرچند که شرکت صنایع پیشرفته سهند در روند طراحی آن‌ها (بیشتر در طرح مادربورد و تاحدی کمتر در طرح واحدهای RAM) مداخله دارد و تأکید می‌گردد که این رویه‌ای شناخته شده برای تولید کارگزار در تمام دنیا است [۹]. شکل ۲ بطور خلاصه موارد مشارکت تولید داخل و شرکت سهند در تولید کارگزار و همچنین موارد برون‌سپاری شده و خرید خارجی را نمایش می‌دهد.

شکل ۲: موارد مشارکت تولید داخل و برون‌سپاری یا خرید از خارج در تولید کارگزار SAHAND SR220-G1

۳- ویژگی‌های خاص و منحصر به فرد کارگزار SAHAND SR220-G1

کارگزار SAHAND SR220-G1 تولید شرکت صنایع پیشرفته سهند دارای ویژگی‌های است که حقیقتاً آن را در میان کارگزارهایی که در کشور مورد استفاده هستند، منحصر به فرد و خاص می‌نماید. در این بخش این ویژگی‌ها معرفی شده و مختصراً شرح داده می‌شوند.

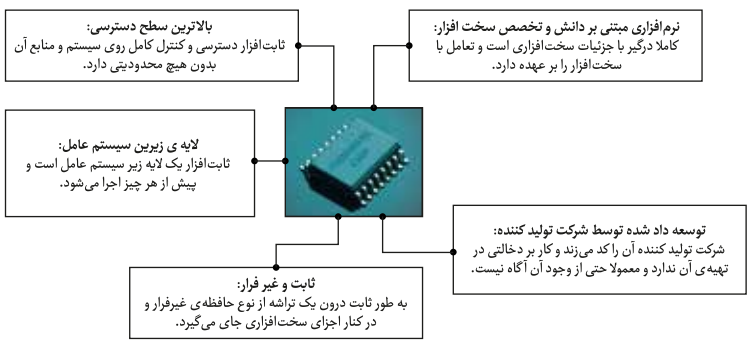
ویژگی ۱) تولید واقعی ثابت‌افزار در داخل کشور و در نتیجه تملک کد منبع (Source Code) بدون Crack نمودن کد باینری ثابت‌افزارهای تولید خارج

تاکنون در داخل کشور تمایل برای تغییر ثابت‌افزار مادربورد کارگزار وجود داشته است. اما، باتوجه به پیچیده بودن انجام این کار و نیاز به دانش پیشرفته و تیم‌های حرفه‌ای، تمامی این تلاش‌ها متأسفانه به شکل Crack نمودن کد باینری ثابت‌افزارهای تولید خارج از کشور بوده است. چنین کاری به هیچ عنوان تولید یک ثابت‌افزار جدید محسوب نمی‌شود و با این روش نمی‌توان مکانیسم‌های جدیدی (مانند مکانیسم‌های امنیتی) را به ثابت‌افزار اضافه نمود و تنها می‌توان تغییرات بسیار سطحی در ثابت‌افزار (از جمله تغییر برخی از پیغام‌ها یا تصاویر) ایجاد نمود. به‌علاوه crack نمودن ثابت‌افزار به دو دلیل عمده موجب افزایش مشکلات امنیتی می‌گردد:

۱) Crack نمودن ثابت‌افزار معمولاً نیازمند خاموش کردن برخی مکانیسم‌های محافظتی ثابت‌افزار مانند Boot یا Secure Boot Guard [۲۰] است که این کار شدیداً موجب افزایش آسیب‌پذیری امنیتی کارگزار می‌گردد.

۲) Crack نمودن سیستم‌های کامپیوتری معمولاً موجب بروز ناپایداری و رفتارهای ناشناخته در آن می‌گردد که افراد crack کننده به دلیل عدم دستیابی به اطلاعات کامل از پیاده‌سازی سیستم و در دست نداشتن کد منبع (Source Code) نمی‌توانند تحلیلی در مورد پیامدهای آن داشته باشند [۲۱].

از آنجایی که ثابت‌افزار کارگزار SAHAND SR220-G1 به شکل کامل در داخل کشور و با همکاری شرکت صنایع پیشرفته سهند و دانشگاه صنعتی شریف تولید شده است کد منبع (Source Code) آن بطور کامل موجود است و به این ترتیب تحلیل و تسلط بسیار بالایی برروی طراحی و تولید ثابت‌افزار حاصل شده است. به این ترتیب ما در اینجا یک محصول اصیل (Genuine) داریم و نه یک محصولی که از Crack و اعمال تغییرات با پیامدهای ناپایدار کننده در محصولات خارجی حاصل شده باشد.



شکل ۳: ویژگی‌های مهم ثابت‌افزار

ویژگی ۲) اطمینان از عدم وجود آسیب‌پذیری امنیتی عمدی در ثابت‌افزار کارگزار

یکی از خطرات مهم امنیتی این است که تولید کنندگان یک سیستم کامپیوتری (و از جمله یک کارگزار) هنگام طراحی آن راه‌هایی را برای نفوذ احتمالی خود در آینده و یا در صورت نیاز در سیستم قرار می‌دهند. به چنین اقلامی، قراردادن درب پشتی (Backdoor) گفته می‌شود و معمولاً در ثابت‌افزار سیستم انجام می‌گیرد [۷] چراکه:

الف) ثابت‌افزار را شرکت تولید کننده ایجاد می‌کند (برخلاف نرم‌افزارهایی که می‌توانند از منابعی جدای از تولید کننده‌ی سیستم کامپیوتری تهیه گردند).

ب) هرآنچه که یک سیستم کامپیوتری در دست کاربر و مشتری انجام می‌دهد در واقع تحت مدیریت و اجرای ثابت‌افزار آن قرار دارد.

پ) ثابت‌افزار بخشی است که دسترسی نامحدود به تمامی امکانات سیستم دارد بدون آنکه ابزارهایی مانند ویروس‌کش‌ها یا دیواره‌های آتش بتوانند محدودیتی برای آن ایجاد کنند.

ت) کاربر و یا مدیر یک سیستم توانایی تغییر ثابت‌افزار به آنچه مورد نظر خود است (مثلاً مانند انتخابی که در مورد سیستم‌عامل وجود دارد) را ندارد و ثابت‌افزار همواره همان چیزی است که تولید کننده تصمیم می‌گیرد.

برخی از ویژگی‌های مهم ثابت‌افزار در شکل ۳ نمایش داده شده است. با توجه به اینکه ثابت‌افزار کارگزار SAHAND SR220-G1 بطور کامل و صد در صد تولید داخل کشور است این اطمینان وجود دارد که شرکت‌ها و نهادهای امنیتی خارج از کشور هیچ درب پشتی درون آن ندارند.

ویژگی ۳) تشخیص و متوقف‌سازی وسائل جانبی تقلبی و غیراصل

امروزه یکی از مشکلات مهم در سیستم‌ها و کارگزارهای کامپیوتری ارائه‌ی محصولات تقلبی و غیراصل است [۲۲]. فروش واحدهای مستعمل و دسته دوم به عنوان تجهیزات نو و همچنین ارائه‌ی برخی از محصولات به شکل تقلبی به جای محصولات دیگر از کارهایی است که متأسفانه به شکل قابل توجهی در بازار وجود دارد. استفاده از چنین محصولاتی می‌تواند خطرات جدی در کارگزارها را به دنبال داشته باشد و از جمله می‌تواند موجب کاهش جدی قابلیت اطمینان (Reliability) و دسترسی‌پذیری (Availability) در کارگزارها گردد و خسارات جدی و اختلال در خدمت‌رسانی را موجب گردد. لازم به ذکر است که مشکلات مربوط به قابلیت اطمینان و دسترسی‌پذیری چیزی نیست که از ابتدا به چشم بیاید و مالکان و یا کاربران کارگزار بتوانند متوجه آن شوند. بلکه این مشکلات متأسفانه آسیب خود را هنگامی که کارگزار به طور جدی به کار گرفته شده و مشغول ارائه‌ی خدمات است، نشان می‌دهند. از جمله ویژگی‌های مهم کارگزار SAHAND SR220-G1 این است که قابلیت شناسایی محصولات جانبی غیرمعتبر در آن در نظر گرفته شده است و به این ترتیب اجازه نمی‌دهد که کارگزارها به دلیل استفاده از محصولات غیراصلی و تقلبی آسیب‌پذیر بوده و دچار اختلال در خدمت‌رسانی گردند.

ویژگی ۴) مجهز به Sahand Secure Boot با اولویت بالاتر از UEFI Secure Boot برای پیشگیری از اعمال قدرت شرکت‌های خارجی

یکی از مهمترین امکانات موجود در کارگزارهای امروزی ویژگی موسوم به UEFI Secure Boot [۲۰] است که وظیفه‌ی آن جلوگیری از حملات امنیتی Bootkit است. لازم به ذکر است که حملات امنیتی Bootkit شاخه‌ای از حملات امنیتی Rootkit بوده و بسیار مخرب هستند به گونه‌ای که اگر این حمله علیه یک کارگزار رخ دهد، فرد یا سازمان حمله کننده اختیار کامل سرور را به دست می‌گیرد [۲۳]. خطر این نوع حمله به ویژه وقتی مشخص می‌شود که دقت کنیم هیچ برنامه‌ی ویروس‌کش یا دیواره‌ی آتشی وجود ندارد که بتواند از کارگزار در مقابل Bootkit‌ها محافظت کند و همچنین اولویت Bootkit‌ها بسیار بالا است به این معنی که اختیار کامل بخش‌های مختلف کارگزار را بدون مزاحمت هیچ واحد محافظی دارا است.

با توجه به خطرات بیان شده برای Bootkit امروزه کارگزارها مجهز به واحد Secure Boot هستند که جلوی این Bootkit‌ها را بگیرد. روش کار به این شکل است که Secure Boot دارای تعدادی پایگاه داده از امضاهای مجاز است که آن‌ها را درون یک تراشه روی مادربورد نگهداری می‌کند و هر برنامه‌ای که بخواهد در روند Boot اجرا گردد باید حتماً دارای امضای مجاز نزد Secure Boot باشد و در غیراینصورت اجازه‌ی اجرا نخواهد داشت.

نکته‌ی کلیدی در مورد Secure Boot این است که در حال حاضر شرکت‌های بزرگ غربی و به ویژه شرکت تولید کننده‌ی واحد Secure Boot مادربورد کنترل کاملی در بروز رسانی پایگاه‌های داده درون تراشه روی مادربورد که مخصوص نگهداری امضاها در Secure Boot است دارند و به همین دلیل این شرکت‌ها می‌توانند از راه دور برای یک سرور تعیین تکلیف کنند که چه نرم‌افزاری در فرآیند Boot فعال گردد و چه نرم‌افزاری فعال نگردد [۲۴]. به عنوان مثال شرکت خارجی مربوطه می‌تواند اجازه دهد که یک نرم‌افزار که ما در داخل کشور در مورد آن نگرانی داریم در فرآیند راه‌اندازی کارگزار ما فعال گردد و عملیاتی شود (که برای بدافزارهای تولید شده‌ی گروه Equation Group [۲۵] وابسته به NSA ظاهراً همین کار را انجام داده‌اند) و برعکس شرکت خارجی مربوطه می‌تواند جلوی اجرای نرم‌افزاری که ما می‌خواهیم و نیاز داریم (مانند نرم‌افزارهای مربوط به rescue، عیب‌یابی و تعمیر کارگزار) در فرآیند راه‌اندازی سرور فعال را بگیرد (به دلایلی مانند تحریم).

در این راستا ثابت‌افزار شرکت صنایع پیشرفته سهند دارای یک مکانیسم امنیتی Secure Boot جدید است که ما آن را در اینجا

Sahand Secure Boot می‌نامیم. لایه‌ی Sahand Secure Boot مافوق Secure Boot اصلی که آن را UEFI Secure Boot می‌نامیم قرار دارد. به این ترتیب ضمن استفاده از مزایای UEFI Secure Boot در محافظت از کامپیوتر (مزیت UEFI Secure Boot این است که پایگاه‌های داده‌ی به نسبت کاملی داشته و مرتب به روزرسانی می‌گردند) اگر کشف گردد که بروز رسانی‌های UEFI Secure Boot خلاف منافع کشور است (مثلاً می‌خواهند نرم‌افزار مخربی را وارد فرآیند Boot کارگزار کنند یا جلوی اجرای نرم‌افزارهای تولید داخل و یا مورد نیاز را در فرآیند Boot به بهانه‌ی تحریم بگیرند) Sahand Secure Boot با داشتن اولویت بالاتر می‌تواند تصمیم‌های مذکور در UEFI Secure Boot را خنثی کند و جلوی اقدامات انجام شده علیه منافع ملی کشور را در فرآیند Boot کارگزارها بگیرد.

ویژگی ۵) جلوگیری از غیرفعال‌سازی مکانیسم‌های امنیتی کارگزار

بیشتر کارگزارها برای جلوگیری از حملات امنیتی دارای سازوکارهایی همانند Secure Boot یا Boot Guard هستند. باید دقت نمود که این سازوکارها هیچ ارتباطی به سیستم‌عامل یا نرم‌افزارهای نصب شده روی کارگزار ندارند و بخشی از خود کارگزار هستند. متأسفانه معمولاً کارگزارها این اجازه را به فردی که به کارگزار دسترسی دارد می‌دهند که این سازوکارها را خاموش کند و حتی در برخی از کارگزارها به شکل پیش‌فرض خاموش هستند [۲۰]. این در حالی است که به جرأت می‌توان گفت با خاموش بودن این سازوکارها کارگزار مربوطه به حملات امنیتی شدیداً آسیب‌پذیر است. لذا وقتی امنیت اهمیت کلیدی دارد، این سازوکارها نیاز است که روشن باشند و همچنین نباید اجازه‌ی غیرفعال‌سازی آن وجود داشته باشد.

خوب است اشاره گردد دلیل اینکه برخی از مدیران کارگزارها سازوکارهای امنیتی را خاموش می‌کنند این است که خود را مجبور می‌بینند. به عنوان مثال آن دسته از مدیران که از ثابت‌افزار Crack شده استفاده می‌کنند معمولاً مجبور به خاموش کردن مثلاً Boot Guard هستند تا ثابت‌افزار آن‌ها بتواند اجرا گردد. همچنین آن دسته از کاربران که Secure Boot را خاموش می‌کنند از این نظر این کار را انجام می‌دهند که بتوانند سیستم‌های عاملی که مورد تأیید شرکت مایکروسافت یا شرکت سازنده‌ی Secure Boot نیست را نیز نصب کنند یا به شرکت مایکروسافت اجازه ندهند که در حین کارکرد سرور عملکرد آن را متوقف کند (که به راحتی می‌تواند به دستور نهادهای حاکمیتی آمریکا رخ دهد).

اما کارگزار SAHAND SR220-G1 به شکلی طراحی شده است که هیچکدام از دو مشکل مذکور را ندارد که بخواهد مجبور به خاموش کردن سازوکارهای امنیتی باشد. در واقع در ویژگی شماره‌ی ۱ دیدیم که ثابت‌افزار سهند از طریق crack نمودن یک ثابت افزار تولید خارج ایجاد نشده و اصیل است و لذا مشکلی با سازوکارهای امنیتی ندارد. همچنین در ویژگی شماره‌ی ۲ دیدیم که در ثابت‌افزار شرکت صنایع پیشرفته سهند یک لایه‌ی امنیتی مافوق Secure Boot داریم که انحصار شرکت‌های خارجی از جمله مایکروسافت برروی Secure Boot را از بین می‌برد. به این ترتیب هیچ دلیلی برای خاموش کردن سازوکارهای امنیتی در این کارگزار وجود ندارد و به این ترتیب اصولاً امکان خاموش کردن این سازوکارهای امنیتی در این کارگزار عمداً از بین برده شده است و به شخصی اجازه‌ی چنین کاری را نمی‌دهد.

ویژگی ۶) وجود واحد سخت‌افزاری SFC (Security Features Controller) و ثابت‌افزار مربوطه

یکی از ویژگی‌های منحصر به فرد کارگزار SAHAND SR220-G1 وجود واحد سخت‌افزاری SFC در درون آن است که به ابتکار شرکت صنایع پیشرفته سهند و تیم تحقیقاتی دانشگاه صنعتی شریف طراحی و تولید شده است. این واحد همانطور که از نام آن مشخص است با هدف بهبود امنیت کارگزار ایجاد شده است و اعمالی را در این راستا در کارگزار انجام می‌دهد که مشابه‌ای در کارگزار دیگری ندارد. لازم به ذکر است که این واحد تنها برای تأمین امنیت و رفع مشکلات امنیتی در سطح سخت‌افزار و ثابت‌افزار کارگزار ارائه شده است و نه برای حل مشکلات لایه‌های بالاتر مانند سیستم‌عامل و برنامه‌های کاربردی و لذا برای لایه‌های بالاتر (که خارج از بحث ما است) کماکان مدیران کارگزار نیازمند استفاده از ویروس‌کش‌ها یا دیواره‌های آتش هستند.

مزایای استفاده از واحد SFC عبارتند از: الف) اگرچه سازوکارهای امنیتی رایجی مانند Boot Guard و یا PFR در کارگزارها معرفی شده‌اند ولی بررسی‌های انجام شده توسط شرکت صنایع پیشرفته سهند و تیم تحقیقاتی دانشگاه صنعتی شریف نشان می‌دهد که این

سازوکارها در بسیاری از مادربوردها یا وجود ندارد و یا غیرفعال (بدون امکان فعال‌سازی) است. دلیل این امر این است که هردوی این سازوکارها از نظر تجاری متعلق به شرکت Intel هستند و عملاً امکان استفاده از آن‌ها روی کارگزارهایی که شرکت Intel دخالت قابل توجهی در تولید آن‌ها نداشته باشد عملیاتی نبوده و کار نمی‌کنند. واحد SFC می‌تواند کمبود این سازوکارهای امنیتی را جبران کند. البته باید دقت نمود که واحد SFC دقیقاً همان سازوکار Boot Guard و PFR را پیاده‌سازی نمی‌کند به ویژه که اصولاً این سازوکارها در مالکیت معنوی شرکت Intel قراردارند. اما روش‌های نوینی در SFC طراحی شده و به کار گرفته است که می‌تواند جای خالی Boot Guard و PFR را پر کند. ب) از آنجایی که واحد SFC بطور کامل طراحی شده و تولید شده توسط شرکت صنایع پیشرفته سهند و تیم تحقیقاتی دانشگاه صنعتی شریف است ثابت‌افزار این واحد بطور کامل در داخل وجود دارد. به همین دلیل می‌توان آن را سفارشی‌سازی نموده و همچنین در طی زمان به ویژه با بازخوردها از مدیران و کاربران کارگزارها به قابلیت‌های امنیتی آن اضافه نمود. پ) مشکلات امنیتی کارگزارها در کشور عزیز ما ایران به مراتب بیشتر از مشکلات امنیتی کارگزارهای واقع شده در کشورهای صنعتی غربی است. مشکلات مربوط به طراحی حملات امنیتی بسیار تخصصی که توسط نهادهای حاکمیتی مدیریت می‌شوند و یا مشکلات مربوط به تحریم‌ها که اجازه‌ی بروز رسانی ثابت‌افزار را نمی‌دهد یا ثابت‌افزار ممکن است به نسخه‌ی صحیح و پایدار خود بروزرسانی نگردد بسیار جدی است. لذا قرار دادن یک واحد امنیتی اضافه (در اینجا SFC) حقیقتاً یک چاره‌اندیشی قابل توجه است.

ویژگی ۷) کشف و خنثی‌سازی حملات امنیتی مربوط به تغییر محتوای تراشه‌های SPI Flash

امروز یکی از خطرناک‌ترین حملات امنیتی به کارگزارها این است که حمله‌کنندگان اقدام به تغییر محتوای واحدهای تراشه SPI Flash می‌کنند که روی مادربورد قراردارد. لازم به ذکر است که این کار امروز یک پدیده‌ی ثابت شده است که شواهد آن وجود دارد (از جمله شرکت Kaspersky اعلام نموده است که بدافزارهای Equation Drug و Gary Fish که تولید Equation Group وابسته به NSA هستند به همین شکل و بر اساس نفوذ به درون واحدهای SPI Flash عمل می‌کنند [۲۵]). خطر چنین حملاتی از آن رو است که اولاً نفوذ به واحدهای SPI Flash به معنای تغییر ثابت‌افزار است که با ایجاد تغییر در ثابت‌افزار، با توجه به سطح دسترسی و اولویت بسیار بالایی که ثابت‌افزار دارد، شخص حمله کننده اختیار کامل کارگزار را در دست می‌گیرد و می‌تواند به هر نوع عملیات اقدام کند و حتی نرم‌افزارهای امنیتی مانند دیواره‌های آتش و ویروس‌کش‌ها توان مقابله با وی را نخواهند داشت. نکته‌ی دیگر نیز این است که وقتی بدافزاری به درون واحدهای SPI Flash وارد می‌شود اکثر صاحبان و مدیران کارگزارها از پاک کردن و خلاصی یافتن از آن عاجز هستند و حتی با پاک کردن کامل سیستم‌عامل و نصب مجدد آن رهایی از بدافزار وجود نخواهد داشت.

برای اقدام به چنین حمله‌ای دو راه وجود دارد، یکی اینکه شخص حمله کننده دسترسی فیزیکی به سرور داشته و تراشه‌های SPI Flash را عوض می‌کند و یا آن را Re Flash کند. راه دیگر این است که شخص دسترسی مستقیم و فیزیکی به کارگزار نداشته ولی از طریق روش‌هایی مانند ارائه‌ی نرم‌افزارهای بروز رسانی اقدام به تغییر محتوای واحدهای SPI Flash کند.

کارگزار SAHAND SR220-G1 این قابلیت را دارد که هر نوع حمله جهت تغییر SPI Flashها را شناسایی و کشف نموده و جلوی آن را بگیرد. به جرأت ادعا می‌کنیم که تاکنون هیچ کارگزاری تا به این اندازه به سازوکارهای تخصصی جلوگیری از تغییر محتوای SPI Flashها مجهز نبوده است.

ویژگی ۸) مجهز بودن به روش‌های جلوگیری از اعمال روش‌های مهندسی معکوس

یکی از کارهایی که انجام آن تا حدی رایج است این است که برخی افراد یا مؤسسات اقدام به اعمال روش‌های مهندسی معکوس برروی کارگزار می‌کنند و با کمک این روش‌ها پاره‌ای تغییرات را در آن ایجاد می‌کنند. این تغییرات معمولاً برای از بین بردن و غیرفعال کردن برخی از قابلیت‌های کارگزار به ویژه قابلیت‌های امنیتی آن با هدف دست یافتن به برخی از توانایی‌های غیرمجاز صورت می‌گیرد.

انجام چنین کارهایی می‌تواند پیامدهای بسیار منفی برای مصرف‌کننده‌ی کارگزار به ویژه از منظر امنیت داشته باشد. در واقع کارگزارهایی که با روش‌های مهندسی معکوس دچار تغییر شده‌اند مشکلات متعدد امنیتی، رفتار ناشناخته و ناپایداری در طول زمان

دارند [۲۱] که واضح است این موارد امنیت مصرف‌کنندگان را به خطر می‌اندازد. ایجاد مخاطره برای مصرف‌کننده نیز به نوبه‌ی خود موجب خسارت برای تولیدکننده و نهادهای تأییدکننده‌ی کارگزار می‌گردد چراکه اصولاً مصرف‌کنندگان از وجود و فعالیت‌های افرادی که عملیات مهندسی معکوس انجام داده‌اند چندان مطلع نیستند و مشکلات مذکور را ناشی از تصمیمات تولیدکنندگان یا نهادهای تأییدکننده می‌دانند.

از ویژگی‌های مهم کارگزار SAHAND SR220-G1 این است که مجهز به روش‌های قدرتمند برای جلوگیری از اعمال روش‌های مهندسی معکوس است تا چنین مشکلاتی استفاده کنندگان این کارگزار را تهدید نکند و مشتریانی که کارگزار SAHAND SR220-G1 را دریافت می‌کنند بدانند که نسخه‌ی مورد استفاده اصیل است.

ویژگی ۹) مجهز به مکانیسم‌های وارسی خودکار برای بهبود قابلیت اطمینان و دسترسی‌پذیری کارگزار

در کارگزار SAHAND SR220-G1 وقتی که کارگزار روشن شده و شروع به کار می‌کند، برخی واحدهای سخت‌افزاری و حتی نرم‌افزاری کارگزار توسط خود آن (بدون اینکه نیاز باشد سیستم‌عامل یا برنامه‌های کاربردی این کار را انجام دهند) مورد صحت‌سنجی قرار می‌گیرد و در صورتی که مشکلی در آن‌ها وجود داشته باشد به مدیران کارگزار اخطارهای مربوطه داده می‌شود تا کارگزار به کار گرفته نشود. لازم است ذکر گردد که وقتی وجود یک مشکل در یک کارگزار توسط مدیران تشخیص داده شده و کارگزار وارد خدمت رسانی نگردد پیامدهای بسیار کمتری نسبت به وقتی دارد که کارگزار در حین ارائه‌ی خدمات خراب گردد و به همین دلیل وجود مکانیسم‌های وارسی اهمیت بسیار زیادی دارد که انواع متعددی از این وارسی‌ها در کارگزار SAHAND SR220-G1 تعبیه شده است. نه تنها از ویژگی‌های کارگزار SAHAND SR220-G1 این است که خود مجهز به مکانیسم‌های وارسی متعدد است، بلکه حتی امکان سفارشی‌سازی چنین مکانیسم‌هایی با توجه به نیاز مشتریان داخل کشور نیز وجود دارد.

ویژگی ۱۰) پوشش کامل خدمات پس از فروش و سفارشی‌سازی برای داخل کشور

بخش‌های مهمی از کارگزارهای داخل کشور به ویژه ثابت‌افزار آن‌ها که اهمیت کلیدی از منظر امنیت دارد، تولید شرکت‌هایی هستند که به علت وجود تحریم، با کشور عزیزمان ایران داد و ستد و ارتباطی ندارند. این مسئله موجب شده است که امکان دریافت هیچ نوع خدمات پس از فروش یا سفارشی‌سازی برای آن‌ها در دسترس نباشد. از آنجایی که کارگزار SAHAND SR220-G1 و به ویژه ثابت‌افزار مادربورد UEFI BIOS و ثابت‌افزار BMC آن بطور کامل در داخل کشور تولید شده و تیم‌فنی تولید کننده‌ی آن بطور کامل در داخل کشور مستقر است امکان ارائه‌ی انواع خدمات پس از فروش و به ویژه سفارشی‌سازی برای استفاده‌کنندگان و مشتریان داخل کشور فراهم است.

ویژگی ۱۱) ارائه‌ی بروز رسانی‌های ثابت‌افزارهای کارگزار از مراکز مطمئن داخل کشور

امروز این مطلب کاملاً شناخته شده است که از دلایل مهم آسیب‌پذیری امنیتی کارگزارها عدم بروزرسانی صحیح و به موقع ثابت‌افزار آن‌ها است [۲۶]. در حال حاضر اگر حتی مدیر یک کارگزار به این مسئله دقت نموده و بخواهد بروزرسانی‌های ثابت‌افزار را به موقع انجام دهد این کار تنها از طریق شرکت‌های تولید کننده‌ی مادربورد و همچنین شرکت‌های تولید کننده‌ی سیستم‌عامل کارگزار (مانند شرکت مایکروسافت) قابل انجام است. با توجه به سطح دسترسی بسیار بالا و اولویت بسیار بالای ثابت‌افزار واضح است که وجود این امر به معنای آن است که شرکت‌های غربی کنترل کاملی برروی تمام وجوه و امنیت کارگزارهای مورد استفاده در داخل کشور داشته باشند. از مزایای کارگزار SAHAND SR220-G1 این است که بروز رسانی ثابت‌افزار کارگزارها را می‌توان به مراکز معتبر داخلی سپرد تا با اطمینان ثابت‌افزار کارگزار با تولیدات داخل کشور بروز رسانی گردد. ویژگی‌های خاص و منحصر به فرد کارگزار SAHAND SR220-G1 که در این بخش بیان شدند بطور خلاصه در شکل ۴ آورده شده‌اند.

شکل ۴: ویژگی‌های خاص و منحصر به فرد کارگزار SAHAND SR220-G1 با رویکرد تقویت امنیت کارگزار

۴- مشخصات کارگزار SAHAND SR220-G1 از منظر امکانات محاسباتی و کارآیی

تاکنون در این نوشتار بیان نمودیم که چگونه شرکت صنایع پیشرفته سهند با همکاری تیم تحقیقاتی از دانشگاه صنعتی شریف اقدام به تولید کارگزار SAHAND SR220-G1 نموده‌اند. مشاهده نمودیم که چه ویژگی‌های خاصی بخصوص از منظر امنیت در این کارگزار ارائه شده است و چه ابتکار عمل‌هایی در تولید آن بکار گرفته شده است. حال در این بخش نگاهی داریم به قدرت پردازشی و محاسباتی این کارگزار و مشخصات آن از منظر کارآیی (Performance).

پردازنده: این کارگزار از پردازنده‌های نسل سوم Intel Xeon استفاده می‌کند و این قابلیت را دارد که دو عدد از این پردازنده‌ها برروی آن نصب گردد. لازم به ذکر است پردازنده‌های نسل سوم Intel Xeon در واقع از قدرتمندترین پردازنده‌هایی هستند که هم‌اکنون به شکل عمومی چه در داخل کشور و چه در سطح بین‌المللی مورد استفاده هستند. البته پردازنده‌های نسل چهار Intel Xeon نیز اخیراً به بازار عرضه شده است ولی به دلیل اینکه این پردازنده محصول بسیار جدیدی است هنوز استفاده‌ی وسیعی از آن در کارگزارها مشاهده نمی‌شود. البته از برنامه‌های شرکت صنایع پیشرفته سهند این است که به زودی کارگزار جدیدی که قابلیت استفاده از پردازنده‌های نسل چهارم Intel Xeon را داشته باشد نیز به بازار عرضه کند.

شکل۵: نمای از روبه رو کارگزار SAHAND SR220-G1

شکل ۶: نمای پشتی کارگزار SAHAND SR220-G1

حافظه: این کارگزار دارای دو عدد واحد کنترلر حافظه است که هر کدام از این کنترلرها دارای ۱۶ عدد شکاف (Slot) برای قراردادن واحدهای حافظه است. در هرکدام از این شکاف‌ها می‌توان واحد حافظه با حداکثر ظرفیت ۲۵۶ گیگابایت قرار داد و بنابراین در مجموع این کارگزار می‌تواند تا ۸ ترابایت حافظه‌ی RAM را با سرعت بسیار بالا مورد دسترسی قرار دهد که با توجه به استانداردهای امروزی عدد بسیار قابل‌توجهی بوده و کاملاً پاسخگوی بالاترین نیازهای کاربران است.

ابعاد: این کارگزار از نظر ابعاد و حجمی که اشغال می‌کند در رده‌ی کارگزارهای 2U قرار دارد و لذا از نظر فضای اشغالی جزء کارگزارهایی محسوب می‌شود که فضای کم و فشرده‌ای را اشغال می‌کند.

سیستم خنک کننده: دارای ۶ واحد فن است که دور آن‌ها توسط واحد BMC و با سازوکار PWM کنترل می‌شود و دارای ویژگی Hot Swap هستند که یعنی در صورت از کار افتادگی یا بروز مشکل می‌توان آن‌ها را بدون اینکه سرور را خاموش نمود یا در خدمت‌رسانی وقفه ایجاد کرد، تعویض نمود.

تغذیه: دارای دو عدد تغذیه مستقل است که هر کدام می‌تواند حداکثر تا ۱۶۰۰وات توان مصرفی تحویل دهد که کاملاً برای فعالیت واحدهای محاسباتی، ذخیره‌سازی داده و خنک‌کننده کفایت می‌کند و حتی در صورت خرابی یکی از واحدهای تغذیه سرور کماکان به عملیات خود ادامه می‌دهد و از کار نمی‌افتد. البته در صورت خرابی یکی از واحدهای تغذیه واحد BMC این مسئله را کشف نموده و به مدیر کارگزار اطلاع می‌دهد تا بتوان نسبت به تعویض واحد تغذیه‌ی خراب اقدام نمود.

واحدهای ذخیره‌سازی داده و I/O: این کارگزار قابلیت استفاده از واحدهای SSD نوع M.2 را دارد. می‌تواند اجازه‌ی استفاده تا ۲۸ عدد دیسکت (SSD، NVMe یا SAS) با سایز SFF یا ۱۴ عدد دیسک با سایز LFF را فراهم کند. همچنین از حداکثر ۸ عدد شکاف PCIe نسل سه برای اتصال کارت‌های I/O پشتیبانی می‌کند.

۵- خلاصه و جمع‌بندی

شرکت صنایع پیشرفته سهند (سهامی خاص) با همکاری محققین دانشگاه صنعتی شریف اقدام به طراحی و تولید یک کارگزار با نام SAHAND SR220-G1 نموده است. بخشی بسیار مهمی از این کارگزار مانند ثابت‌افزار UEFI BIOS، ثابت‌افزار BMC، معماری سطح بالای مادربورد، برخی بخش‌های مکانیکی و فضایابی بطور کامل در داخل کشور طراحی و تولید شده است. همچنین مجتمع‌سازی (Integration) و مونتاژ و آزمون کارگزار (چه آزمون جداگانه‌ی اجزاء و چه آزمون نهایی بعد از مجتمع‌سازی) بطور کامل در خط تولید واقع در منطقه‌ی ویژه‌ی اقتصادی فرودگاه بین‌المللی پیام انجام خواهد گرفت. لازم به ذکر است که آنچه در اینجا به عنوان مشارکت شرکت صنایع پیشرفته سهند بیان شد حقیقتاً سهم قابل توجهی از تولید یک کارگزار است و این میزان مشارکت قابل مقایسه با آنچیزی است که شرکت‌های مطرح تولیدکننده‌ی کارگزار در دنیا، مانند شرکت HP انجام می‌دهند، مثلاً شرکت HP نیز خود اقدام به تولید پردازنده نمی‌کند یا اقدام به تولید مدارچاپی مادربورد نمی‌کند ولی در تولید ثابت‌افزار BMC مشارکت جدی دارد که شرکت صنایع پیشرفته سهند نیز رویه مشابه را در پیش گرفته است.

تولید کارگزار SAHAND SR220-G1 نه تنها ارزش افزوده‌ی قابل توجهی را به همراه دارد و از خروج ارز جلوگیری کرده و موجب رونق تولید در داخل کشور می‌گردد بلکه دارای ویژگی‌های خاصی است که بسیاری از آن‌ها منحصر به فرد بوده و نمونه در کارگزارهای دیگر ندارد. این ویژگی‌ها عمدتاً در راستای بهبود امنیت و مقابله با آسیب‌پذیری‌های امنیتی است که حقیقتاً امروزه باید در تولید هر کارگزاری که قرار است در داخل کشور مورد استفاده قرار گیرد مورد توجه ویژه باشد. کارگزار SAHAND SR220-G1 دارای سازوکارهای امنیتی خاصی است که در هیچ کارگزار دیگری وجود ندارد و از جمله راه بر خطرات و حملات امنیتی در سطح ثابت‌افزار و یا خطرات ناشی از اعمال محدودیت‌ها توسط شرکت‌های بزرگ خارجی بر کارگزار را بسته است.

همچنین به علت اینکه طراحی واحدهای UEFI BIOS و BMC این کارگزار صد در صد در داخل کشور صورت گرفته است کد منبع ثابت افزار این کارگزار بطور کامل در داخل کشور موجود است و لذا این اطمینان وجود دارد که هیچ درب پشتی یا آسیب‌پذیری امنیتی عمدی توسط تولید کننده‌ی خارجی در کد باینری ثابت‌افزار سیستم قرار داده نشده است.

در پایان باید گفت کارگزار SAHAND SR220-G1 از نظر قدرت محاسباتی، پردازشی و ذخیره‌سازی داده در سطح کارگزارهای نسل سوم است که در واقع متناسب با قدرتمندترین و بروزترین کارگزارهایی است که در داخل کشور و در سطح بین‌المللی در حال استفاده هستند. البته نسل‌های بعدی کارگزارها در راه هستند که شرکت صنایع پیشرفته سهند قصد دارد بزودی کارگزار بعدی خود را مبتنی بر مدل کارگزارهای نسل چهار برای بازار داخل کشور عرضه کند.

References: مراجع :

[1] Bradley Mitchell, "What Is a Server? - The internet wouldn't exist without servers", Reviewed by Ryan Perian, June 12, 2021. Accessible through:
https://www.lifewire.com/servers-in-computer-networking-817380

[2] Wikipedia page on Server (Computing). Accessible through:
https://en.wikipedia.org/wiki/Server_%28computing%29

[3] Avast Business Team, "What Is Server Security - and Why Should You Care?", June 30, 2020. Accessible through:
https://www.avast.com/c-b-what-is-server-security

[4] Paessler company team, "Take server security seriously - and stop hackers in their tracks", July 25th, 2023. Accessible through:
https://www.paessler.com/server-security

[5] Vincent Zimmer, Michael Rothman, and Suresh Marisetty, "Beyond BIOS: Developing with the Unified Extensible Firmware Interface", 3rd Edition, Walter de Gruyter, January 23, 2017.

[6] "Intel® Server Systems Baseboard Management Controller (BMC) and BIOS Security", a white paper by Intel, 2023. Accessible through:
https://www.intel.com/content/dam/support/us/en/documents/server-products/bmc-bios-security-bestpractices.pdf

[7] Yuri Diogenes, and Erdal Ozkaya, "Cybersecurity - Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system", 3rd Edition, Packt Publishing, September 30, 2022.

[8] "The Baseboard Management Controller (BMC) in Servers" documented by Integrated Silicon Solution, Inc. Accessible through:
https://www.issi.com/US/newsletter/Issue86_June_2021/ISSI_BMC-Engangement.pdf

[9] Matt Kimball, "Do You Know Where Your Servers Come From? Here's Why Securing the Supply Chain Matters", Moor Insights and Strategy, May 19, 2020. Accessible through:

https://www.forbes.com/sites/moorinsights/2020/05/19/do-you-know-where-your-servers-come-from-heres-why-securing-the-supply-chain-matters/?sh=a8638a5e1500

[10] Patrick Kennedy, "Explaining the Baseboard Management Controller or BMC in Servers", ServeTheHome ("STH"), September 27, 2018. Accessible through: https://www.servethehome.com/explaining-the-baseboard-management-controller-or-bmc-in-servers

[11] Dell Technical Team, "Dell EMC PowerEdge R640, Technical Guide" 2021. Accessible through: https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/us/PowerEdge-R640-Technical-Guide.pdf

[12] Willem Thorbecke, "The East Asian Electronics Sector - The Roles of Exchange Rates, Technology Transfer, and Global Value Chains", Cambridge University Press: 07 February 2023.

[13] MIL-HDBK-217: Reliability Prediction of Electronic Equipment

[14] Binarly Technical Team, "Vulnerabilities in Firmware Impacting Millions of Enterprise Devices" February 1, 20200. Accessible through: https://binarly.io/news/Binarly-Presents-New-Firmware-Vulnerabilities-at-LABScon-2022/index.html

[15] TianoCore_EDK_II UEFI. Accessible through: https://en.wikipedia.org/wiki/TianoCore_EDK_II

[16] "HPE Integrated Lights-Out (iLO)". Accessible through: https://www.hpe.com/us/en/hpe-integrated-lights-out-ilo.html

[17] OpenBMC. Accessible through: https://github.com/facebook/openbmc

[18] "Server performance and benchmark testing guide". June 2015. Accessible through: https://www.techtarget.com/searchdatacenter/guide/Server-performance-and-benchmark-testing-guide

[19] " Performance Tuning Guidelines for Windows Server 2022 ", May 7, 2015. Accessible through: https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/

[20] "Intel® Hardware Shield - Below-the-OS Security", Intel White Paper, 2023. Accessible through: https://www.intel.com/content/dam/www/central-libraries/us/en/documents/below-the-os-security-white-paper.pdf

[21] Oluwademilade Afolabi, "What Is Software Cracking, and What Are the Risks of Using Cracked Software?", Make Use of, 2023. Accessible through: https://www.makeuseof.com/what-is-software-cracking-and-dangers-of-cracked-software/

[22] Sheena Vasani, "Fake SSDs with great reviews are still popping up on Amazon - The Verge", Jan 17, 2023. Accessible through: https://www.theverge.com/2023/1/16/23557569/amazon-scam-review-merging-16tb-external-ssds

[23] Alex Matrosov, Eugene Rodionov, and Sergey Bratus, "Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats", No Starch Press, May 7, 2019.

[24] Microsoft Learn, "Secure boot", August 2, 2023. Accessible through: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

[25] Kaspersky Technichal Team, "Equation Group: The Crown Creator of Cyber-Espionage", February 16, 2015. Accessible through: https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

[26] Binarly Team, "The Firmware Supply-Chain Security is broken: Can we fix it?", December 27, 2021. Accessible through: https://www.binarly.io/posts/The_Firmware_Supply_Chain_Security_is_broken_Can_we_fix_it/index.html

شرکت صنایع پیشرفته سهند (سهامی خاص)

دفتر مرکزی : تهران - خیابان خالد اسلامبولی(وزراء) - خیابان یازدهم - پلاک ۲۱ کدپستی : ۱۵۱۳۷۵۷۶۱۷ تلفن : ۸۷۹۴-۰۲۱ داخلی : ۴۴۴
کارخانه : استان البرز - مهر شهر - بلوار ارم - منطقه ویژه اقتصادی پیام - بلوار شهید بابایی - خیابان ششم - تقاطع دوم کدپستی : ۳۱۸۷۴۱۱۳۳۵ تلفن : ۳۴۰۰۸۷۶۱-۰۲۶