فصلنامه مرکز تحقیقات صنایع انفورماتیک / دوره جدید / شماره ۱۳ / زمستان ۱۳۹۱

www.rcii.ir

انفورماتیک

گزارش صنایع

RCII

حمایت از تولید
نیازمند عزم جدی
همه مسئولان

آشنایی با
مرکز توسعه تجارت الکترونیکی

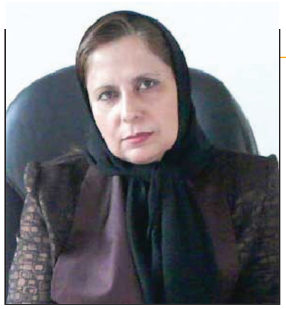
دکتر جعفر محمودی/ رییس مرکز و استاد دانشگاه تهران

آیا مایکروفرها تاثیر مخربی بر بدن انسان دارند؟

حوادثی که در واقعیت اتفاق می افتند
چگونه در استاندارد IEC60950-1
شبیه سازی می شوند؟

نگاهی به تهدیدات سخت افزاری

به نام خداوند بخشنده مهربان



یادداشت نخست

به قلم مدیر مسئول

حمایت از تولید نیازمند عزم جدی همه مسئولان کشور است.

نام گذاری سال جاری توسط مقام معظم رهبری به عنوان "تولید ملی، حمایت از کار و سرمایه ایرانی" مسئله جدی است که باید به آن توجه شود. زیر ساخت یک کشور وابسته به تولید است و فقط به منابع طبیعی بستگی ندارد. برای حفظ و صیانت از سرمایه و کار باید توجه داشت که قوانین اجرایی کشور باید حتماً دارای چشم اندازی تعیین شده و با دقت و داریت لازم و چراغ راه متولیان صنعت آن باشد و قوای سه گانه باید با قوانین ثابت و محکم، از این سرمایه ها حفظ و نگهداری کنند.

در جامعه صنعتی نمی توان با تصمیمات ناگهانی و با بخشنامه و مصوبه های غیر کارشناسانه سرمایه مردم را مورد تهاجم قرار داد. انتظار تمامی صنعت گران و سرمایه داران کشور، تامین امنیت کاری، ثبات در تصمیم گیری و مشارکت در تصمیم سازی ها است. باید با حمایت های مالیاتی، بیمه ای، تسهیلاتی و تامین ضمانت های بانکی و ... از کار آفرینان و سرمایه گذاران قدردانی و پاسداری شود. در عین حال مکانیزم هایی را جهت شفاف سازی پیاده کنیم تا کسی در لوای این گروه سوء استفاده نکند.

در خصوص توزیع عادلانه فرصت های شغلی در تمامی نقاط کشور باید با توجه به اقلیم هر منطقه، مسائل فرهنگی و اقتصادی، وضعیت جغرافیایی، کشاورزی، علمی و صنعتی و ... بررسی شود که چه نوع محصولاتی و خدماتی می توانند تولید کنند. همچنین مبارز با قاچاق و دامپینگ یکی دیگر از مسائل تولید کنندگان است و در آخر مهمترین مسئله بازاریابی داخلی و خارجی و توزیع و فروش کالاهای تولیدی است که تولید کنندگان کوچک و متوسط شاید قادر به انجام درست آن نباشند و در این خصوص ضعف دارند. دولت باید در این زمینه به شدت وارد عمل شده و توسط نهادهایی که ایجاد می کند در تحقق این امر قدم بردارد.

گزارش صنایع انفورماتیک

فصلنامه مرکز تحقیقات صنایع انفورماتیک

دوره جدید / شماره۱۳ / زمستان۱۳۹۱

صاحب امتیاز: مرکز تحقیقات صنایع انفورماتیک

مدیر مسئول: ویدا سینا

مدیر اجرایی: افسانه عبادی

مدیرفنی: رامین رضایی

روابط عمومی: سمانه کیومرثی

همکاران این شماره: آنوشا شجاعیان / حمید شریفی / ف.قادری

نشانی: تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

تلفن: ۸۸۹۲۵۹۵۰ (۱۰خط)

فکس: ۸۸۹۳۷۶۵۸

سایت : www.rcii.ir

مجری طرح فصلنامه:گروه رسانه‌ای مهرتابان/۰۹۱۲۳۰۸۹۳۰۳

[akbarkarimi40@yahoo.com]

نشانی آزمایشگاه‌ها:

آزمایشگاه مرکزی: تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

تلفن: ۸۸۹۲۵۹۵۰ (۱۰خط) **فکس**: ۸۸۹۳۷۶۵۸

آزمایشگاه بندر عباس: مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی هرمزگان مستقر در اسکله شهید رجایی

تلفن: ۰۷۶۱۴۵۱۴۲۵۹ فکس:۰۷۶۱۴۵۱۴۲۵۸

آزمایشگاه پرند: شهرک صنعتی پرند، بلوار فن آوری، خیابان گلزار، خیابان گلگشت قطعه D 44

تلفکس:۵۶۴۱۸۸۹۲-۵۶۴۱۸۸۶۴-۵۶۴۱۸۸۶۵

آشنایی با مرکز توسعه تجارت الکترونیکی

آنچه در این بخش می‌خوانید، معرفی مرکز توسعه تجارت الکترونیکی به بیان جناب آقای دکتر جعفر محمودی، رئیس این مرکز و استاد دانشگاه تهران است.

حوزه‌های اصلی فعالیت مرکز توسعه تجارت الکترونیکی

مرکز توسعه تجارت الکترونیکی متولی توسعه تجارت الکترونیکی در کشور است. وظایف تصریح شده در اساسنامه این مرکز (مصوب هیات وزیران شماره ۱۵۱۷۳۴/ت۳۲۵۶۵ه-مورخ ۸۷/۰۷/۲۹) به خوبی نشان دهنده تولی گری مرکز در حوزه تجارت الکترونیکی است. مهمترین این وظایف عبارتند از:

۱- برنامه ریزی، ارائه راهکارها، پشتیبانی و نظارت به منظور:

- بهره برداری از بسترها، راهبردها و نوآوری تجارت الکترونیکی در سطح کشور
- ارایه تسهیلات و حمایت از ایجاد و توسعه زیرساخت های فنی، سرمایه های انسانی، قانونی، حاکمیتی و امنیتی توسعه تجارت الکترونیکی
- فرهنگ سازی و آموزش جهت توسعه و ترویج استفاده از تجارت الکترونیکی در فرآیندهای کسب و کار مبتنی بر استانداردهای ملی و بین المللی
- توسعه کاربردها و نوآوری ها در جهت دست یابی به منافع تجارت الکترونیکی در اقتصاد کشور
- توسعه فعالیت های تدارکاتی و معاملاتی به صورت تجارت الکترونیکی
- استانداردسازی فعالیت های اطلاع رسانی تجاری
- حمایت از گسترش بازارهای داد و ستد الکترونیکی
- ساماندهی فعالیت ایستگاه های تجارت الکترونیکی کشور.
- فراهم سازی زمینه تعاملات ملی و بین المللی در تجارت الکترونیکی.

۲- تسهیل تجارت از طریق استفاده از ابزارها، مدل ها و استانداردهای تجارت الکترونیکی ملی و بین المللی و ایجاد پنجره واحد تجاری.

۳- تدوین مقررات، استانداردها و ضوابط مربوط به تجارت الکترونیکی و پیشنهاد به مراجع ذی صلاح جهت تصویب.

۴- ایجاد، نگهداری و پشتیبانی از مراکز داده بخش بازرگانی در چهارچوب نظام جامع فناوری اطلاعات کشور.

۵- ارائه خدمات صدور گواهی الکترونیکی کشور.

۶- سایر موارد بر اساس مفاد اساسنامه مرکز توسعه تجارت الکترونیکی

وضعیت مرکز توسعه تجارت الکترونیکی ایران، با توجه به چشم انداز ۱۴۰۴ که طبق آن ایران باید رتبه اول منطقه را داشته باشد

کمیسیون سازمان ملل در تجارت و توسعه (آنکتاد) سه مرحله اصلی برای توسعه تجارت الکترونیکی در نظر گرفته است که عبارتند از ایجاد زیرساخت ها، توسعه کاربری و آثار.

در مرحله زیرساخت، بسترهای لازم به منظور بهره برداری از تجارت الکترونیکی ایجاد می شود. پس از آن زیرساخت ها در قالب برنامه های کاربردی مورد بهره برداری قرار گرفته و پس از آن آثار تجارت الکترونیکی بر متغیرهای مختلف (اقتصادی، اجتماعی و ...) مورد بررسی قرار می گیرد. در این خصوص کشورهای توسعه یافته با توجه به عبور از مرحله اول و انتشار موفق تجارت الکترونیکی در عرصه های مختلف به اندازه گیری آثار تجارت الکترونیکی بر متغیرهایی چون رشد اشتغال، رشد تجارت، کاهش آلودگی هوا و ترافیک، رشد اقتصادی و ... می پردازند. دغدغه کشورهای در حال توسعه در مرحله ایجاد زیرساخت و توسعه کاربری است.

در خصوص وضعیت کشور ما بر اساس دسته بندی آنکتاد در حال حاضر خوشبختانه از مرحله بسترسازی عبور کرده و وارد مرحله توسعه کاربردها شده ایم.

در خصوص زیرساخت ها هم اکنون حداقل زیرساخت های لازم مخابراتی، امنیتی، قانونی و منابع انسانی جهت بهره برداری از زیرساخت ها در قالب برنامه های کاربردی تجارت الکترونیکی وجود داشته و متاسفانه از بسترهای ایجاد شده استفاده حداکثری نمی شود. بنابراین جهت اخذ رتبه اول در منطقه نیازمند برنامه ریزی دقیق جهت افزایش کیفیت زیرساخت ها و توسعه کاربردهای تجارت الکترونیکی هستیم.

راهبردهای مرکز توسعه تجارت الکترونیکی برای دستیابی به اهداف چشم انداز ۱۴۰۴

مهمترین راهبردهای این مرکز به‌منظور نیل به اهداف چشم‌انداز ۱۴۰۴ عبارتند از:

- توسعه کاربردهای تجارت و کسب و کار الکترونیکی در کشور (از قبیل کاربردهای گواهی الکترونیکی، سامانه تدارکات الکترونیکی، نماد اعتماد الکترونیکی و ...)
- تسهیل الکترونیکی تجارت با استفاده از ابزارها و استانداردهای تجارت الکترونیکی
- بهره برداری حداکثر از زیرساخت های موجود به منظور معرفی خدمات نوین کسب و کار الکترونیکی
- استفاده از پتانسیل بخش علمی کشور به منظور پیشبرد طرح های تجارت الکترونیکی و انتقال نیازمندی های فنی کشور در حوزه تجارت و کسب و کار الکترونیکی به دانشگاه ها و مراکز علمی کشور جهت تربیت نیروهای متخصص مورد نیاز

موانع گسترش مناسب دولت الکترونیکی در ایران

پیاده سازی دولت الکترونیکی مستلزم توجه به ابعاد مختلف دولت الکترونیکی است. دولت الکترونیکی طرحی وسیعی است که استقرار آن نیازمند تبعیت از یک نقشه منسجم کاری، بهره برداری از زیرساخت های فنی، حقوقی، منابع انسانی و همکاری ذی نفعان می باشد.

به‌طور کلی موانع توسعه دولت الکترونیکی در کشور را می توان در قالب موارد ذیل دسته بندی کرد:

- مشخص نبودن نقشه راه: پیاده سازی دولت الکترونیکی مانند هر طرح دیگری مستلزم وجود نقشه راه است. در حال حاضر نقشه جامع و استراتژی های هم سو و یکپارچه برای نیل به هدف توسعه دولت الکترونیکی در کشور وجود نداشته و بعضا شاهد تناقض هایی میان سیاست های عمومی کشور و سیاست های فناوری اطلاعات کشور هستیم.
- وجود نقشه راه سبب یکپارچگی فعالیت ها و خدمات الکترونیکی ارایه شده، از میان بردن تناقض ها، تعیین مشخص نقش کلیه سازمان های ذی نفع، استاندارد سازی سیستم های ارایه دهنده خدمات

گردیده و فعالیت های لازم به منظور توسعه دولت الکترونیکی را به روشنی به تصویر می کشد. عدم وجود برنامه و نقشه راه مشخص موجب به هدر رفتن تلاش ها و عدم استفاده بهینه از زیرساخت های فراهم شده می گردد. این برنامه جامع در حقیقت پازل دولت الکترونیکی محسوب می گردد که کلیه ابعاد دولت الکترونیکی از جنبه زیرساخت وکاربری را دربر می گیرد. فعالیت هایی که در کشور به منظور پیاده سازی دولت الکترونیکی صورت گرفته به صورت مجزا از یکدیگر و جزیره‌ای بوده و از یک نقشه راه واحد تبعیت نکرده ایم.

◄ایجاد زیرساخت های لازم به منظور توسعه دولت الکترونیکی: استقرار دولت الکترونیکی نیازمند وجود بسترهای لازم سیاسی، فنی، حقوقی، منابع انسانی و فرهنگ سازی است. منظور از بستر سیاسی وجود عزم و اراده حکومت و مجریان پیاده سازی دولت الکترونیکی است. زیرساخت حقوقی به قوانین و مقررات لازم جهت توسعه تجارت و دولت الکترونیکی، زیرساخت انسانی به منابع انسانی ماهر و آموزش دیده، زیرساخت های فنی به بسترهای شبکه و مخابرات ، تجهیزات فنی، استانداردها و بستر فرهنگ سازی نیز به مباحث فرهنگ سازی لازم جهت توسعه دولت الکترونیکی اشاره دارد. خوشبختانه در کشور ما نیاز به پیاده سازی دولت الکترونیکی از سال های پیش به صورت جدی توسط مسئولین کشور درک شده که منجر به پیاده‌سازی زیرساخت های توسعه تجارت الکترونیکی در سطح قابل قبولی شده است.

◄ساختار اجرایی دولت الکترونیکی: پس از تدوین نقشه راه و ایجاد زیرساخت ها وارد مرحله اجرا می شویم. در این مرحله ساختار اجرایی طرح پیاده سازی دولت الکترونیکی و رهبری کلان آن مشخص گردیده و طرح های مشخص شده در مرحله اول اجرا می شود. در هر مرحله از پیاده سازی لازم است که میزان پیشرفت طرح مورد ارزیابی قرار گرفته و گزارش پیشرفت کار به بالاترین مدیران اجرایی کشور ارایه گردد. در حال حاضر ساختار اجرایی طرح به روشنی مشخص نیست و بعضاً موازی کاری هایی میان فعالیت های مختلف سازمان های دولتی مشاهده می شود. همچنین از میزان پیشرفت طرح به صورت دقیق مطلع نیستیم.

فعالیت‌های عملیاتی مراکز میانی صدور گواهی الکترونیکی

در راستای اجرای بند الف از ماده ۴ آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی (مصوب ۱۳۸۲به شماره ۹۸۹۸۶/ت ۳۱۸۱۹ ه) عملیات اجرایی پروژه ایجاد و راه‌اندازی زیرساخت کلید عمومی کشور از سال ۱۳۸۲ آغاز گردیده است. مطابق با آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی مصوب مورخ ۱۳۸۶/۰۶/۱۱هیئت وزیران، مدل سلسله مراتبی زیرساخت کلید عمومی (PKI) جهت رسمیت بخشیدن به امضای الکترونیکی در کشور است. سلسله مراتب زیرساخت کلید عمومی کشور متشکل از شورای سیاست گذاری گواهی الکترونیکی در رأس، مرکز دولتی صدور گواهی الکترونیکی ریشه به عنوان نقطه اعتماد و مراکز صدور گواهی الکترونیکی میانی زیرین است.

مطابق با آئین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و به منظور حفظ یکپارچگی و جلوگیری از تفکیک راه کارها و استانداردهای به کار گرفته شده در مراکز صدور گواهی، شورایی به نام «شورای سیاست گذاری گواهی الکترونیکی کشور» متشکل از معاونین ذی ربط وزارتخانه ها و روسای سازمان ها تشکیل شد.

برخی از وظایف این شورا به شرح زیر است :

◄سیاست گذاری در زمینه فعالیت های مرکز دولتی صدور گواهی الکترونیکی ریشه کشور

◄به روزرسانی سیاست های گواهی زیرساخت کلید عمومی کشور

◄تایید تطابق دستورالعمل اجرایی کلیه مراکز میانی با سند سیاست های گواهی زیرساخت کلید عمومی کشور

مرکز دولتی صدور گواهی الکترونیکی ریشه، نقطه اطمینان در زیرساخت کلید عمومی کشور است. این مرکز بر اساس مفاد بند الف از ماده ۴ آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی و طی اولین جلسه شورای سیاست گذاری گواهی الکترونیکی کشور مورخ ۱۳۸۶/۰۷/۳۰ مجوز ایجاد، امضا، صدور و ابطال گواهی الکترونیکی مراکز صدور گواهی الکترونیکی میانی را دریافت کرده است.

برخی از وظایف این مرکز به شرح زیر است :

◄مسئولیت تمام ابعاد صدور و مدیریت مراکز صدور گواهی الکترونیکی میانی، شامل نظارت بر فرایندهای ثبت نام، احراز هویت، صدور گواهی های میانی، انتشار و ابطال گواهی ها و تجدید کلید

◄ تضمین تطابق تمام ابعاد خدمات و عملیات این مرکز با زیرساخت مربوط به صدور گواهی الکترونیکی تحت سیاست های گواهی الکترونیکی و مطابق با خواسته ها و ضمانت های آن سیاست ها. لازم به ذکر است وظیفه صدور گواهی موجودیت‌های نهایی برعهده مراکز صدور گواهی الکترونیکی میانی است.

درحال حاضر دو مرکز صدور گواهی الکترونیکی میانی به صورت عملیاتی در کشور فعال هستند. نخستین مرکز به نام «مرکز میانی عام» فعالیت خود را در سال ۱۳۸۶ و پس از راه اندازی مرکز دولتی صدور گواهی الکترونیکی ریشه کشور آغاز کرده و فعال است. مطابق با مصوبه «دستورالعمل اجرایی ساماندهی مراکز صدور گواهی الکترونیکی میانی» مرکز میانی عام، مرکز منحصر به فردی است که به طور عام مبادرت به صدور گواهی الکترونیکی در کاربردهای مختلف می نماید. دومین مرکز میانی، مرکز صدور گواهی الکترونیکی میانی خصوصی به نام پارس ساین در سال ۱۳۹۱ و جهت ارائه خدمات به بخش خصوصی فعال شده است. کلیه خدمات صدور گواهی الکترونیکی از آغاز فعالیت مراکز میانی تا پیش از تصویب تعرفه صدور گواهی الکترونیکی رایگان بوده است.

همچنین مراکز میانی دولتی نفت، سازمان ثبت اسناد و املاک کشور، سازمان امور مالیاتی و مرکز میانی خصوصی فناوران اعتماد راهبر پس از دریافت تائیدیه دستورالعمل اجرایی از شورای سیاست گذاری گواهی الکترونیکی، در مرحله راه‌اندازی و پیاده سازی قراردارند. مرکز میانی دولتی سازمان فناوری اطلاعات ایران و مرکز میانی خصوصی فرهنگ آزما در حال فعالیت جهت اخذ مجوز شورای سیاست گذاری گواهی الکترونیکی هستند.

در ادامه، اهم اقدامات صورت گرفته توسط مرکز دولتی صدور گواهی الکترونیکی ریشه در سال های مختلف دیده می شود.

اقدامات مرکز دولتی صدور گواهی الکترونیکی ریشه

۱۳۸۲: ◄تصویب قانون تجارت الکترونیکی

۱۳۸۶ : ◄تصویب آیین نامه اجرایی ماده ۳۲ در هیئت دولت◄تشکیل شورای سیاست گذاری گواهی الکترونیکی کشور◄ راه‌اندازی مرکز دولتی صدور گواهی الکترونیکی ریشه کشور◄ راه‌اندازی مرکز صدور گواهی الکترونیکی میانی دولتی عام

۱۳۸۷ : ◄تدوین سند نقشه راه زیرساخت کلید عمومی کشور

۱۳۸۸ : ◄تصویب طرح ساماندهی مراکز صدور گواهی الکترونیکی میانی◄ تصویب سطوح اطمینان چهارگانه در زیرساخت کلید عمومی کشور

۱۳۸۹: ◄ تهیه و تدوین نظام ارزش گذاری گواهی الکترونیکی◄ تصویب نرخ ریالی تعرفه گواهی

۱۳۹۰: ◄ تصویب سند دستورالعمل اجرایی گواهی الکترونیکی مرکز میانی خصوصی◄تدوین استانداردهای ملی زیرساخت کلید عمومی کشور◄راه اندازی آزمایشگاه‌های زیرساخت کلید عمومی

۱۳۹۱: ◄ تصویب ویرایش سوم سند سیاست های گواهی الکترونیکی زیرساخت کلید عمومی کشور منطبق با RFC ۳۶۴۷◄ تصویب سند جامع پروفایل های زیرساخت کلید عمومی کشور ◄ راه اندازی مرکزصدورگواهی الکترونیکی میانی خصوصی پارس ساین ◄ارزیابی سخت افزارهای PKE◄ارزیابی و آزمون نرم افزارهای PKE ◄ تصویب سند دستورالعمل اجرایی مرکز میانی وزارت نفت ◄تصویب سند دستورالعمل اجرایی مرکز میانی سازمان ثبت اسناد و املاک کشور ◄ تصویب سند دستورالعمل اجرایی مرکز میانی سازمان امور مالیاتی ◄تصویب سند دستورالعمل اجرایی مرکز میانی خصوصی فناوران اعتماد راهبر ◄برگزاری کارگاه های آموزشی آشنایی با زیرساخت کلید عمومی کشور

آیا مایکروفرها تاثیر مخربی بر بدن انسان دارند؟

تهیه کننده: آنوشا شجاعیان

شاید بارها این جمله را شنیده باشید که "از ایستادن در نزدیکی مایکروفری که روشن است خودداری کنید." مدت زیادی است که از حضور مایکروفرهای خانگی در خانه ها و محیط های اداری می گذرد و هنوز بسیاری از مردم از اینکه هنگام ایستادن کنار مایکروفری که روشن است، در معرض اشعه قرار گیرند، نگرانند. در حقیقت مایکروفرها هنگام کار مقداری پرتو تشعشع می کنند. در اینجا به چگونگی کار مایکروفر و میزان تشعشع و اینکه چگونه مطمئن شویم مایکروفروی که در منزل یا محیط کار از آن استفاده می شود دارای تشعشعات در محدوده ایمن است، می پردازیم.

مایکروفر چیست؟

مایکروفر نوعی از امواج الکترومغناطیسی است و در واقع امواجی رادیویی با فرکانس بسیار بالا هستند. برد چنین امواجی کوتاه بوده و در حد چند متر است، ولی میزان نفوذ آن ها نسبتا بالا است. به عبارتی هر چه فرکانس بیشتر باشد، شدت نفوذ بیشتر ولی برد امواج، کوتاه تر می شود.

این امواج دارای ۳ مشخصه اصلی هستند، ممکن است در برخورد با یک ماده منعکس، منتشر یا جذب شود. مواد فلزی این امواج را کاملا منعکس می کنند. اغلب مواد غیرفلزی مثل شیشه و پلاستیک امواج را از خود عبور می دهند و موادی که حاوی آب هستند مانند غذاها و حتی انسان، انرژی این امواج را جذب می کنند.

اجاق مایکروفر چگونه کار می کند؟

در داخل اجاق مایکروفر قطعه ای به نام مگنترون وجود دارد که این امواج را با فرکانسی حدود ۲/۴۵۰ مگاهرتز تولید می کند. امواج تولید شده وارد فضای بسته اجاق که فلزی است شده و از دیواره ها منعکس می شود تا توسط غذا یا مایع داخل آن جذب شود. امواج در غذا نفوذ کرده و ملکول های آب داخل آن را تکان می دهد و با ایجاد سایش مولکولی تولید گرما و افزایش سریع دما می کند.

اجاق مایکروفر دارای ۲ قسمت اصلی است یکی قسمت ولتاژ پایین که در واقع واحد کنترلی دستگاه را به عهده دارد مانند فن ها، موتورهای میز گردان و لامپ ها، دیگری قسمت ولتاژ بالا است که مگنترون، ترانس ولتاژ بالا و مدار doubling را شامل می شود. در واقع ترانسفورمر، برق ورودی که ۲۲۰ ولت است را به برق حدود ۴۰۰۰ ولت تبدیل کرده و سپس از طریق مداری که شامل دیود و خازن ولتاژ بالا است، آن را به ولتاژ DC تبدیل می کند.

مگنترون نیز با دریافت این ولتاژ زیاد، امواج مایکروویو را به فرکانس حدود ۲/۴۵۰ مگاهرتز تبدیل می کند. این امواج توسط آنتن و سپس از طریق لوله های خاصی به نام موج بر[1] به داخل محفظه ی فر هدایت و در آن ساطع می شود؛ موج ساطع شده در صورت برخورد با مواد غذایی جذب و تبدیل به حرارت می شود.

تشعشات امواج به بدن انسان

از آنجایی که بدن انسان نیز حاوی آب است، می تواند امواج مایکروویو را جذب کند. قرار گرفتن در معرض تابش مستقیم امواج مایکروویو می تواند موجب سوختگی های عمیق بافتی و آب مروارید شود. اگر دستگاه مایکروفر شما چند سال کار کرده باشد، یا قفل آن خراب یا ضربه دیده باشد، ممکن است در آن به خوبی بسته نشود و در حین روشن بودن دستگاه، اشعه های مایکروویو به بیرون نشت کنند که در این صورت می تواند خطرات جبران ناپذیری را به بار آورد. نشتی اشعه مایکروویو بایستی با دستگاه های مخصوص اندازه گیری شود که مقدار آن از حد استانداردهای بین المللی و ملی بیشتر نباشد. مطابق با استاندارد ملی ISIRI ۱۵۶۲-۲-۲۲۵ و استاندارد بین المللی IEC۶۰۳۳۵-۲-۲۵ مقدار نشتی در فاصله ۵۰ میلی متری یا بیشتر از سطح بیرونی فر نباید از $50 W/m^2$ بیشتر شود.

چگونه این امواج را اندازه گیری کنیم؟

به طور کلی بهتر است در فاصله های زمانی مشخص پس از یکسال کارکرد مستمر، مقدار نشتی امواج اندازه گیری شود. از آنجا که برای اندازه گیری این امواج به دستگاه اندازه گیری چگالی شار مایکروویو با مشخصات ویژه نیازاست، از این رو بهتر است این کار توسط مراکز و موسساتی صورت گیرد که توانایی این کار را داشته باشند جهت اطمینان بیشتر نیز می توان به مراکزی که از جانب اداره کل استاندارد ایران در این زمینه دارای تایید صلاحیت می باشند مراجعه نمود.

مراجع:

[۱] استاندارد ملی ایران به شماره ISIRI ۱۵۶۲-۲-۲۵

[۲]. MICRIWAVE OVEN OPERATION (WWW.ERPARTS.COM)

1.waveguide

این مقاله به سوالی در مورد رابطه بین عملکرد غیرعادی و تمهیدات حفاظت الکترونیکی اضافی، با استفاده از یک مثال واقعی که برای کامپیوتر شخصی خودم اتفاق افتاد، پاسخ می‌دهد

حوادثی که در واقعیت اتفاق می‌افتند چگونه در استاندارد IEC60950-1 شبیه سازی می‌شوند؟

تهیه کننده: حمید شریفی

خلاصه

یک کامپیوتر از اسمبل کردن چند قطعه و ماژول سخت افزاری بر روی یکدیگر تشکیل می شود و معمولاً وقتی که در جایی خارج از کارخانه تولید قطعات کامپیوتری اسمبل می شود، احتمال استفاده از کارت ها و ماژول های سخت افزاری شرکت های مختلف بیشتر می شود.

در آخر، کیفیت محصول نهایی که یک کامپیوتر اسمبل شده است، نه تنها به اقداماتی از قبیل استفاده از ماژول ها و کارت های سخت افزاری شرکت های معتبر و دارای تاییدیه های انطباق با استاندارد و نحوه انتخاب ماژول های سخت افزاری مناسب جهت نصب شدن در کنار هم، بستگی دارد که حتی رعایت این موارد می تواند به ایمنی کاربر و محیط اطراف کامپیوتر در حین استفاده از آن تاثیر گذار باشد.

اتفاقی که برای کامپیوتر من افتاد، تا اندازه ای به روشن کردن موارد زیر کمک خواهد کرد:

۱ یک منبع تغذیه کامپیوتر معتبر دارای تمهیدات حفاظت الکترونیکی اضافی، چگونه می تواند از انفجار یک آی سی رگولاتور کارت گرافیک تقلبی، جلوگیری کند؟

۲ یک مادربرد کامپیوتر معتبر دارای تاییدیه های انطباق با استاندارد، چگونه می تواند در مقابل جریان اضافی که توسط یک منبع تغذیه کامپیوتر معمولی بدون تمهیدات حفاظت الکترونیکی اضافی ایجاد شده است، مقاومت کند؟

۳ یک منبع تغذیه کامپیوتر معمولی بدون تمهیدات حفاظت الکترونیکی اضافی، چگونه می تواند به انفجار آی سی رگولاتور کارت گرافیک تقلبی، کمک کند؟

۴ شرایط عملکرد غیرعادی که ممکن است برای یک کارت گرافیک تقلبی در طول زمان استفاده از آن به وجود آیند چه شرایطی هستند؟ یک محفظه

۵ آتش (قسمتی از دستگاه که برای به حداقل رساندن گسترش آتش یا شعله از درون دستگاه به اطراف درنظر گرفته شده است.) چگونه می تواند از گسترش شعله ی حاصل از انفجار آی سی رگولاتور کارت گرافیک تقلبی، جلوگیری کند؟

به نظر می‌آید

کامپیوترم مرده است!

یک روز، می خواستم با کامپیوترم کار کنم. دکمه ی آن را فشار دادم، اما روشن نشد.

چند بار دیگر دکمه ی آن را فشار دادم، اما به فشاری که به کلیدش وارد می کردم هیچ عکس العملی نشان نمی داد.

با خودم فکر کردم، یعنی چه اتفاقی افتاده است؟

درب های کناری کیس کامپیوتر را باز کرده و کانکتورهای منبع تغذیه را از سوکت های مادربرد جدا کردم.

منبع تغذیه کامپیوتر را با وصل کردن پین های شماره

۱۴ و ۱۵ کانکتور برق منبع تغذیه به هم و اندازه گیری ولتاژ های خروجی هر کدام از ریل های ولتاژ دی سی، تست کردم.منبع تغذیه سالم به نظر می رسید و هیچ مشکلی نداشت.منبع تغذیه کامپیوترم معتبر و دارای تمهیدات حفاظت الکترونیکی اضافی بود.

بعد از تست منبع تغذیه، من با خودم فکر کردم که نکند مادربرد یا سی پی یو کامپیوترم خراب شده باشد، پس شاید با اتصال یک منبع تغذیه معمولی بدون تمهیدات حفاظت الکترونیکی اضافی که در دسترسم بود، می توانستم متوجه شوم چه اتفاقی می افتد؟ منبع تغذیه ای در دسترسم بود، دارای تمهیدات حفاظت الکترونیکی اضافی نبود.

کانکتورهای برق منبع تغذیه ای که در دسترس داشتم را به جای کانکتورهای برق منبع تغذیه کامپیوتر خودم به سوکت مادربرد کامپیوتر وصل و اقدام به روشن کردن کامپیوتر کردم.

خوشبختانه، منبع تغذیه به فشاری که به کلید پاور وارد کردم عکس العمل نشان داد و فن سی پی یو شروع به چرخش کرد، اما بلا فاصله بعد از شروع به چرخیدن از حرکت باز ایستاد.

از آنجایی که مادربرد کامپیوترم از نوع معتبر و دارای تاییدیه های انطباق با استاندارد و خیلی گران قیمت بود، شک کردم که مادربرد کامپیوترم نمی تواند خراب شده باشد.

بنابراین، چند دفعه دیگر سعی کردم که کامپیوترم را روشن کنم. بعد از فشردن دکمه پاور کامپیوتر برای سومین بار، ناگهان صدایی به گوشم رسید و ذره ای که شعله ور شده بود را در حال افتادن روی سینی فلزی زیر کیس کامپیوترم دیدم که بلافاصله بعد از افتادن آن روی سینی فلزی کیس شعله اش خاموش شد.

به سرعت دوشاخه برق کامپیوتر را از پریز برق جدا کردم و برای اینکه بفهمم ذره مذاب از چه قسمتی جدا شده؟ شروع به بررسی کردم.

ماژول های سخت افزاری کامپیوتر را جدا کردم و از آنجا که ذره مذاب درست در جایی از سینی فلزی زیر کیس افتاده بود که زیر کارت گرافیک کامپیوترم بود، بررسی دقیق تری رو کارت گرافیک کامپیوتر انجام دادم و فهمیدم که ذره مذاب تکه ای از آی سی رگولاتور روی کارت گرافیک بود که منفجر و ذوب شده بود.

بعد مشخص شد که کارت گرافیک کامپیوترم تقلبی بوده و بعد از مدتی استفاده به دلیل ورود ذرات گرد و غبار موجود در هوا به داخل فن خنک کننده کارت گرافیک باعث قفل شدنش شده بود.

معیارهای انطباق برای عملکرد غیرعادی و حالات اشکال به صورت زیر است:

الف اگر آتش سوزی رخ دهد، نباید فراتر از تجهیز منتشر شود؛

ب تجهیزات نباید فلز مذاب به بیرون پرتاب نمایند؛

ج محفظه ها نباید به گونه ای تغییر شکل دهند که با الزامات مربوطه مشخص شده در استاندارد، مغایر شوند.

نتیجه گیری

۱ منبع تغذیه معتبر دارای تمهیدات حفاظت الکترونیکی اضافی کامپیوترم از انفجار آی سی رگولاتور کارت گرافیک کامپیوتر از طریق حفاظت اضافه جریان و محدود کردن توان خروجی، جلوگیری کرده بود.

۲ مادربرد معتبر و دارای تاییدیه های انطباق با استاندارد کامپیوترم با عبور جریان اضافی که منبع تغذیه کامپیوتر معمولی بدون حفاظت الکترونیکی اضافی تولید کرده بود، خراب نشد. (این جریان اضافی باعث شده بود که آی سی رگولاتور کارت گرافیک تقلبی کامپیوترم منفجر شود.)

۳ در صورتیکه انفجار آی سی رگولاتور کارت گرافیک تقلبی کامپیوترم را به عنوان خطری که در ارتباط با بروز یک حالت تک اشکال بوجود آمده در نظر بگیریم، منبع تغذیه معمولی کامپیوتر بدون تمهیدات حفاظت الکترونیک اضافی، می تواند به آی سی رگولاتور آسیب دیده با تغذیه جریان اضافی کمک کند تا منفجر شود.

۴ با مطالعه حادثه ی واقعی که اتفاق افتاده بود، می توانیم نتیجه بگیریم که استفاده از قطعات و ماژول های معتبر و دارای تاییدیه های انطباق با استاندارد، برای اسمبل کردن یک کامپیوتر کامل بسیار حائز اهمیت است و می تواند احتمال و ریسک بروز خطرات را کاهش داده و همچنین انجام آزمون زیربند ۵-۳ از استاندارد بین المللی IEC ۶۰۹۵۰-۱ (عملکرد غیرعادی و حالات اشکال) بسیار مهم است. طبق این زیربند، عملکرد غیر عادی و حالات اشکال موتورهای به کار رفته در داخل تجهیزات تحت اضافه بار، روتور قفل شده یا سایر شرایط غیرعادی، موتورها نباید موجب ایجاد خطری ناشی از دمای بیش از حد شوند.

۵ با مطالعه حادثه ی واقعی که اتفاق افتاده بود، می توانیم نتیجه بگیریم که انجام آزمون زیربند ۲-۶-۴ از استاندارد بین المللی IEC ۶۰۹۵۰-۱ بسیار مهم است. طبق این زیربند، قسمت های پایینی محفظه های آتش باید پوشش مناسبی ایجاد کنند تا از آتش گرفتن سطح نگه دارنده در اثر افتادن مواد و فلزات مذاب احتمالی از قسمت هایی که تحت شرایط اشکال هستند، جلوگیری به عمل آورند. همچنین دهانه هایی که در سطح زیرین محفظه آتش قرار دارند باید به وسیله یک تیغه، صفحه یا وسایل دیگر به گونه ای حفاظت شوند که احتمال پخش شدن مواد و فلزات مذاب به بیرون از محفظه امکان پذیر نباشد.

انجام آزمون زیربند ۲-۶-۴ از استاندارد بین‌المللی IEC ۶۰۹۵۰-۱ بسیار مهم است. طبق این زیربند، قسمت‌های پایینی محفظه‌های آتش باید پوشش مناسبی ایجاد کنند تا از آتش گرفتن سطح نگه‌دارنده در اثر افتادن مواد و فلزات مذاب احتمالی از قسمت‌هایی که تحت شرایط اشکال هستند، جلوگیری به‌عمل آورند. همچنین دهانه‌هایی که در سطح زیرین محفظه آتش قرار دارند باید به‌وسیله یک تیغه، صفحه یا وسایل دیگر به‌گونه‌ای حفاظت شوند که احتمال پخش شدن مواد و فلزات مذاب به بیرون از محفظه امکان‌پذیر نباشد.

خبـــــــر کوتاه
گزارش انفورماتیک

مرکز RA مرکز تحقیقات صنایع انفورماتیک راه اندازی شد

طی قراردادی با مرکز صدورگواهی الکترونیکی میانی عام، نمایندگی دفتر ثبت نام برای ارائه خدمات مربوط به شناسایی و احراز هویت متقاضیان صدور گواهی از طرف مرکز صدور گواهی الکترونیکی به مرکز تحقیقات صنایع انفورماتیک اعطا شد.

نگاهی به

تهدیدات سخت‌افزاری

بخش نخست

تهیه کننده: ف. قادری
آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک

مقدمه

در دنیای تکنولوژی امروزی، بیش از هر زمانی، دیگر جایی برای فراموش کردن ICها و قطعات الکترونیکی نمانده است. از تجهیزات موبایل تا پردازنده‌های سیستم‌های کامپیوتری یا هر نوع قطعات الکترونیکی به کاررفته در صنایع پزشکی، هوافضا، ابزارهای کنترل و مانیتورینگ و ... همگی از تراشه‌هایی استفاده می‌کنند که وظیفه‌ی محاسبات و کنترل را به عهده دارند. با آن‌که طراحی تراشه‌ها در کشورهای پیشرفته صورت می‌گیرد، ولی سازندگان قطعات، غالبا پیمانکارانی هستند که از طریق کشورهای واسط مانند چین و تایوان اقدام به ساخت و تولید این گونه قطعات می‌کنند. قطعاتی که در هزاران تجهیز نظامی، غیرنظامی، مخابراتی یا پزشکی استفاده خواهد شد.

دستگاه‌هایی که از تراشه‌ها و مدارات مجتمع استفاده می‌کنند، طیف گسترده‌ای از وظایف را بر عهده دارند. وظایفی مانند یک جستجوی ساده در اینترنت، ویرایش سندی روی سیستم، برقراری تماس تلفنی، انجام یک تراکنش مالی که به ارتباط پیچیده‌ای بین نرم‌افزار و سخت‌افزار نیاز دارد. نرم‌افزار، مجموعه‌ای از دستورالعمل‌ها است که نشان می‌دهد یک عمل چطور انجام شود، درحالی که سخت‌افزار، مداراتی است که دستورالعمل‌ها را پیاده‌سازی می‌کند تا یک عمل انجام شود.

اهداف جدید

هکرها سال‌ها به دنبال کشف آسیب‌پذیری‌هایی در نرم‌افزار بوده‌اند که دسترسی غیرمجاز به سیستم‌ها را برای آن‌ها میسر سازند. ولی در سال‌های اخیر، پردازنده‌ها و قطعات الکترونیکی نیز جزء اهداف آن‌ها به شمار می‌آیند که این نوع تهدیدات، حتی در سطوح گسترده‌ی مخابراتی یا نظامی وجود دارد.

به عنوان مثال، طبق گزارشی که از سوی Sergei Skorobogatov عضو تیم تحقیقاتی دانشگاه کمبریج در ماه May سال ۲۰۱۲ منتشر شد، تراشه‌های ساخت یک شرکت چینی که در تجهیزات نیروی هوایی آمریکا استفاده می‌شود، دارای یک نقطه‌ی دسترسی مخفی است که امکان دستکاری را برای شخص سازنده فراهم کرده و نوعی Backdoor به حساب می‌آید. این تراشه مداراتی دارد که به طور پیش فرض غیرفعال بوده و در محاسبات معمول فعال نمی‌شوند.

در تحقیقی که در سال ۲۰۰۸ توسط تیم تحقیقاتی دانشگاه Illinois در Champaign-Urbana انجام شد، آن‌ها نشان دادند که چطور با تغییر تراشه توانستند با حمله‌ی Backdoor، به کامپیوتر دسترسی پیدا کنند. این متد با پیچیدگی‌های زیادی که دارد، غیرقابل کشف است. تیم تحقیقاتی برای پیاده‌سازی این حمله، از پردازنده‌ی قابل برنامه‌ریزی با سیستم عامل لینوکس استفاده کردند. تراشه طوری برنامه‌ریزی شده بود که Firmware آلوده را به تراشه حافظه تزریق کند و این اتفاق به هکر اجازه می‌دهد به سیستم وارد شود. برای برنامه‌ریزی مجدد تراشه، محققان نیازداشتند تا بخش کوچکی از مدارات پردازنده را دستکاری کنند. به این منظور، طبق اظهارات SamuelKing دستیار پروفسور در دانشکده‌ی علوم کامپیوتر، ۱۳۴۱ گیت منطقی در تراشه‌ای که بیش از ۱ میلیون دارد را تغییر دادند. بنابراین تیم تحقیقاتی این دانشگاه موفق شدند با برنامه ریزی مجدد تعداد اندکی از مدارات روی پردازنده‌ی LEON، Backdoor را به سیستم اضافه کنند. مدل این گونه تراشه‌های قابل برنامه ریزی، با طراحی مشابه Sparc که در سیستم‌های SUN استفاده می‌شوند، شباهت دارد. برای حمله به این نوع سیستم‌ها دکتر King، در ابتدا با ارسال بسته‌های مخرب در شبکه، پردازنده را مجبور می‌کند که از مدارات مخرب استفاده کرده و Firmware آلوده را فراخوانی کند. سپس با استفاده از رمز عبور خاص به سیستم عامل لینوکس دسترسی پیدا می‌کند. در حال حاضر محققان در صدد تهیه‌ی ابزارهایی هستند که بتوانند مدارات مخرب را شناسایی کنند.

مساله‌ی اساسی در دنیای واقعی دسترسی به این نوع پردازنده‌ها است. ولی با توجه به تحقیقات به عمل آمده و گستردگی تکنولوژی، یک توسعه دهنده‌ی MOLE (Military Overlay Editor) تا زمانی که روی طراحی تراشه کار می‌کند، می‌تواند کدهایی را به طراحی اضافه کند یا با زبان‌هایی مانند اسمبلی به جای استفاده از پردازنده‌ها، به نصب تراشه‌های مخرب اقدام کند. در نهایت هکر می‌تواند نسخه‌های تقلبی سیستم‌ها و مسیریاب‌ها و هرنوع قطعه‌ی الکترونیکی را با تراشه‌های آلوده وارد بازار کند.

این نوع حملات دیگر در حد یک تهدید Script Kiddie نبوده و تمامی منابع اطلاعاتی و عملیاتی را تحت تاثیر قرارمی‌دهد. منابع و محصولاتی که به‌طور عموم استفاده می‌شوند، مانند تلفن‌های همراه iPod که در سال ۲۰۰۶ به ویروس RavMonE.exe آلوده بودند تا تجهیزات نظامی مانند پردازشگر Actel/Microsemi ProASIC3 (PA3) A3P250 به کاررفته در رادارها آلوده به Backdoor و تجهیزات صنعتی آلوده به Stuxnet که به مراکز صنعتی آسیب جدی وارد ساخت، همگی حاوی اطلاعات شخصی، سازمانی و دولتی هستند که انتشار هر یک از انواع اطلاعات آن، خسارات جدی را به دنبال خواهد داشت.

بررسی مجموعه تراشه‌های ProASIC 3 / E طبق ادعای سازنده

برخلاف FPGA[1]های مبتنی بر SRAM[2]، تجهیزات ProASIC 3/E که مبتنی بر Flash هستند، طراحی‌های ایمن را در صنعت به کار برده و سطح جدیدی از امنیت را در بازار FPGAها وارد کرده‌اند. ایمن سازی این نوع تراشه‌ها در ۲ سطح اصلی رمزنگاری و استفاده از قفل است. علاوه بر به کارگیری استاندارد صنعتی الگوریتم رمزنگاری AES ۱۲۸بیتی، برنامه‌ریزی مجدد در سیستم، به طور ایمن انجام می‌شود و قابلیت کپی و در معرض خطر قرارگرفتن intellectual property به هنگام ارتقاء تراشه وجود ندارد. همچنین استفاده از FlashLock، مانع از خواندن bitstreamهای برنامه‌ریزی مجدد سیستم به عنوان یک ویژگی منحصربه فرد بوده و این اطمینان را می‌دهد که تغییر ویژگی‌ها و دستکاری توسط دسترسی افراد غیرمجاز ممکن نیست. در کنار این تدابیر، مدارات امنیتی تعبیه شده روی بورد سیستم، از دسترسی به اطلاعات برنامه نویسی درمقابل حملات غیرتهاجمی جلوگیری می‌کند. چراکه حملات تهاجمی تنها به آشکارسازی ساختار دستگاه بسنده کرده و به محتویات سلول‌های flash دسترسی ندارد.

این محصول که برای شرایط محیط‌های نظامی طراحی شده است، دمای بین -55°C تا +125°C را تحمل کرده و ظرفیت ۶۰۰۰۰۰ تا ۳ میلیون گیت را داراست. طراحان Actel با حذف مدارات با مصرف برق بالاتر و خطر شکست که اغلب در FPGA های مبتنی بر SRAM رخ می‌دهد و استفاده از flash به جای SRAM ، کارایی را در تجهیزات نظامی افزایش داده اند. به طوری که عملکرد حافظه‌های flash روی تراشه با ۱/۲ ولت تا ۱/۵ ولت تامین شده و از خطاهای ناشی از نوترون و نواسانات در امان هستند. نوترونها و ذرات آلفا که در تکنولوژی FPGA های مبتنی بر SRAM به کار می‌روند، در عناصر حافظه اختلال ایجاد می‌کنند. از آن جایی که این تراشه‌ها در سیستم‌های Avionic[3] و کنترل خودکار استفاده می‌شوند، اختلال ایجاد شده در حافظه از طریق آن‌ها، قابلیت اطمینان و در دسترس بودن سیستم را شدیدا تحت تاثیر قرار می‌دهد.

دو جدول زیر نتایج تست های مقایسه ای بین SRAM و Flash و خطاهای رخ داده در تنظیم حافظه و دسترسی به آن و خطاهای نرم افزار واسط در اثر استفاده از نوترون و ذرات آلفا را نشان می دهد.

جدول۱: خلاصه نتایج تست رخ دادن خطا در مقابل نوترون و تکنولوژی Flash.FIT به منظور تعداد وقوع خطا در زمان است.

FPGA	Technology	Equivalent FIT Rates per Device			
		Ground-level Applications		Commercial Aviation	Military Aviation
		Sea Level	5,000 ft	30,000 ft	60,000 ft
Actel AX1000 (1 M Gate)	0.15 µm Antifuse	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
Actel APA1000 (1 M Gate)	0.22 µm Flash	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
Actel A3PE600 (600 K Gate)	0.13 µm Flash	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
SRAM FPGA (Vendor 1 – 3 M Gate)	0.15 µm SRAM	1,150 FITs	3,900 FITs	170,000 FITs	540,000 FITs
SRAM FPGA (Vendor 1 – 1 M Gate)	90 nm SRAM	320 FITs	1,100 FITs	47,000 FITs	150,000 FITs
SRAM FPGA (Vendor 2 – 1 M Gate)	0.13 µm SRAM	460 FITs	1,600 FITs	67,000 FITs	220,000 FITs
SRAM FPGA (Vendor 2 – 1 M Gate)	90 nm SRAM	730 FITs	2,500 FITs	108,000 FITs	346,000 FITs
SRAM FPGA (Vendor 2 – 2 M Gate)	90 nm SRAM	1,600 FITs	5,500 FITs	236,000 FITs	751,000 FITs

جدول۲: خلاصه نتایج تست رخ دادن خطا در مقابل ذرات آلفا و تکنولوژی FIT .Flash به منظور تعداد وقوع خطا در زمان است.

FPGA	Technology	Configuration Upsets	Functional Failures	Equivalent FIT Rates (FITs)	
				Low-Alpha Mold Compound (0.001 α/cm^2-hr)	Standard Mold Compound (0.04 α/cm^2-hr)
Actel AX1000 (1 M Gate)	0.15 µm Antifuse	Not Measured *	0	No Failures Detected	No Failures Detected
Actel APA1000 (1 M Gate)	0.22 µm Flash	Not Measured *	0	No Failures Detected	No Failures Detected
SRAM FPGA (Vendor 1 – 3 M Gate)	0.15 µm SRAM	1,040	140	140	5,600
SRAM FPGA (Vendor 1 – 1 M Gate)	90 nm SRAM	940	260	260	10,400
SRAM FPGA (Vendor 2 – 1 M Gate)	0.13 µm SRAM	Could not be measured	100	100	4,000

طبق ادعای شرکت سازنده، برنامه های موجود در این سری از FPGAها از استاندارد رمزنگاری پیشرفته ی ۱۲۸ بیتی AES استفاده کرده و رمزگشایی با دستورات JTAG انجام می شود. از آنجایی که این تکنولوژی از Soft ARM پشتیبانی می کند، در صورت فعال بودن این قابلیت، رمزنگاری در برنامه نویسی به کار نمی رود. این الگوریتم تحت لایسنس شرکت .Inc , Cryptography Research (CRI) در ایالات متحده ی آمریکا در سانفرانسیسکو است که سالانه ۵ بیلیون تراشه را در سال محافظت می کند. بیشتر نگرانی ها این است که این تراشه به عنوان محصولی غیرقابل نفوذ در بازار شناخته شده که در تجهیزات و سلاح های نظامی، هدایت گرها، کنترل پرواز، سخت افزارهای شبکه و ارتباطات استفاده می شود. با توجه به گزارش Skorobogatov، کاربرد PA 3 به تجهیزات نظامی محدود نبوده و در نیروگاه های هسته ای، نیروگاه های توزیع قدرت، هوافضا، حمل و نقل و حتی در خودروها به طور عموم استفاده می شود.

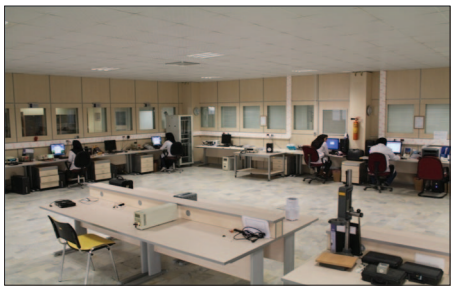
با توجه به گستره استفاده از Actel/Microsemi ProASIC 3(PA 3)A 3 P250 و استفاده ی فراگیر از آن در صنایع نظامی و بازارهای حساس، تهدیدات را در مقیاس بزرگ مانند حملاتی مشابه Stuxnet از طریق اینترنت و شبکه ممکن می سازد ، به همین دلیل، این قطعه مورد توجه قرارگرفته و به عنوان تراشه ی مورد تست از سوی پژوهشگران انتخاب شد. طبق تحقیقات پژوهشگران، آسیب‌پذیری‌های دیگری نیز روی تراشه‌های متفاوت میکروکنترلرها وجود دارد که لیست برخی از تراشه ها در زیر آمده است:

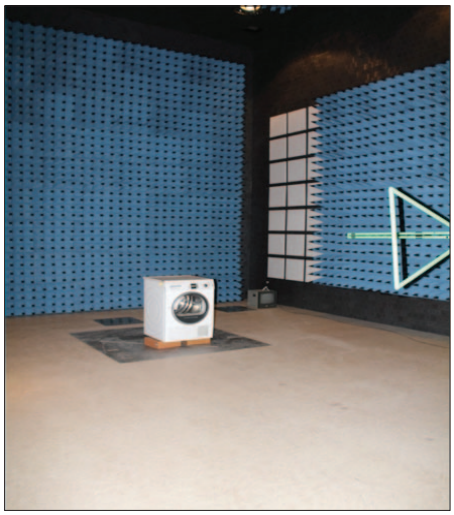
68HC05xx, 68HC705xx, 68HC08xx, 68HC908xx, 68HC11xx, PIC12Cxx, PIC12Fxx, PIC16Cxx, PIC16Fxx, PIC17Cxx, PIC18Cxx, PIC18Fxx, PIC24HJxx, dsPIC30Fxx, dsPIC33FJxx, AT89Cxx, AT89Sxx, AT90Sxx, ATtinyxx, ATmegaxx, H8/3xx, D78xx, D78Fxx, XC95xx, XCR3xx, XC2Cxx, A500Kxx, A3Pxx, CY7C6xx, Z867xx, Z86Exx, DS2432, M306xx, EPM3xx, EPM7xx, EPM9xx, MSP430Fxx, N87Cxx, SXxx, ST62Txx, ST72Fxx, W921Exx, HT48Rxx, P87LPCxx, T89Cxx, SAB-Cxx, MX10xx, EL78Pxx, LPC3xx

طبق گزارشات پژوهشگران دانشگاه کمبریج، این Backdoor دقیقا روی سیلیکون قرار دارد و نه روی میان افزارهایی که روی تراشه بارگذاری می شوند. تکنیک کشف به کارگرفته شده مربوط به آنالیز انتشار خطوط انتقال یا PEA بوده، که منجر به استخراج کلید امنیتی فعال سازی Backdoor شده است. با این راه هکر می تواند تمامی تدابیر امنیتی روی تراشه را غیرفعال ، رمزها و کلیدهای دسترسی را مجددا برنامه ریزی کند، ویژگی های سطح پایین سیلیکون را تغییر دهد، به جریان های bitstream رمزنشده دسترسی پیدا کرده و یا به طور دائم در تجهیز اختلال ایجاد کند. در سطح بالاتر می توان با متدهای مهندسی معکوس طراحی، Backdoorهای جدیدی ایجاد کرد. واضح است که هیچگونه وصله ای برای رفع این مخاطره در تراشه های سری PA وجود ندارد. لذا استفاده از آنها با مخاطراتی جدی همراه خواهد بود. با توجه به جهانی شدن تولید نیمه هادی ها و مدارات مجتمع، قراردادن مدارات مخرب، نرم افزارهای مبانی آلوده و مخفی سازی آنها در زمان ساخت دور از انتظار نیست.

در قسمت بعدی مقاله به روش های آزمایش و کشف قطعات مخرب می پردازیم.

[1] Field-Programmable Gate Array
[2] Static Random Access Memory
[3] electronic systems used on aircraft, artificial satellites and spacecraft





رعایت استاندارد ملی ایران ۱-۱۵۶۲ تحت عنوان "وسایل برقی خانگی و مشابه- ایمنی- اجباری بوده و به دلیل اهمیت رعایت الزامات سازگاری الکترومغناطیسی در ایمنی این وسایل، الزامات سازگاری الکترومغناطیسی به عنوان بخشی از الزامات ایمنی در استاندارد مذکور لحاظ شده است که به شرح زیر می باشد:

- بند ۱۹-۱۱-۴-: ۱ آزمون مصونیت در برابر تخلیه الکتریسیته ساکن طبق استاندارد ملی ایران ۲-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-:۲ آزمون مصونیت در برابر میدانهای تابش فرکانس رادیویی طبق استاندارد ملی ایران ۳-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-: ۳ آزمون مصونیت در پالسهای الکتریکی (رگباره) طبق استاندارد ملی ایران ۴-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-: ۴ آزمون مصونیت در برابر موجهای ضربه افرا تاخت طبق استاندارد ملی ایران ۵-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-: ۵ آزمون مصونیت در برابر اختلالهای هدایتی طبق استاندارد ملی ایران ۶-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-: ۶ آزمون مصونیت در برابر افتهای ولتاژ، وقفه های کوتاه و تغییرات ولتاژ طبق استاندارد ملی ایران ۱۱-۴-۷۲۶۰
- بند ۱۹-۱۱-۴-: ۷ آزمون مصونیت در برابر فرکانسهای پائین طبق استاندارد ملی ایران ۱۳-۴-۶۱۰۰۰

آزمایشگاه مجهز EMC مرکز تحقیقات صنایع انفورماتیک آماده آزمون کلیه بندهای این استاندارد می باشد

inno3D®

www.inno3d.com

شارلوت رایانه

شرکت شارلوت رایانه نمایندگی رسمی محصولات اینو تری دی در ایران می باشد یکی از محصولات
این شرکت که آمار فروش بسیار بالایی در بازار ایران داشته کارت گرافیک GeForce210DDR31GB است که این محصول تنها
دارندهٔ تاییدیه مرکز تحقیقات صنایع انفورماتیک در ایران می باشد GeForce 210 DDR3 1GB کارت گرافیک

مرکز تحقیقات صنایع انفورماتیک تائید شده RCII Certified

GeForce 210 DDR3 1GB

NVIDIA Essential Vista | NVIDIA PureVideo HD | NVIDIA GeForce CUDA | PCI EXPRESS | PhysX by NVIDIA

SHARLOOT GUARANTY

GeForce GTX 690

NVIDIA Essential Vista | NVIDIA PureVideo HD | NVIDIA GeForce CUDA | PCI EXPRESS | PhysX by NVIDIA

GPU Engine Specs

CUDA Cores :3072
Graphics Clock (MHz) : 915
Processor Clock (MHz) : 1830
Texture Fill Rate (billion/sec) : 234

Memory Specs:

Memory Clock (MHz):6Gbps
Standard Memory Config (MB):4096
Memory Interface Width:512-bit
Memory Bandwidth (GB/sec):384

Feature Support:

OpenGL:4.2
Bus Support:PCI-E3.0 X16
Supported Technologies
(3D Vision, 3D Vision Surround, CUDA, DirectX 11,PhysX, SLI)

ISO 9001:2008 Registered CCPL
NORWEGIAN ACCREDITATION MSYS 013

دارنده گواهینامه ISO 9001:2008 در کیفیت مدیریت

www.sharloot.com

انفورماتیک

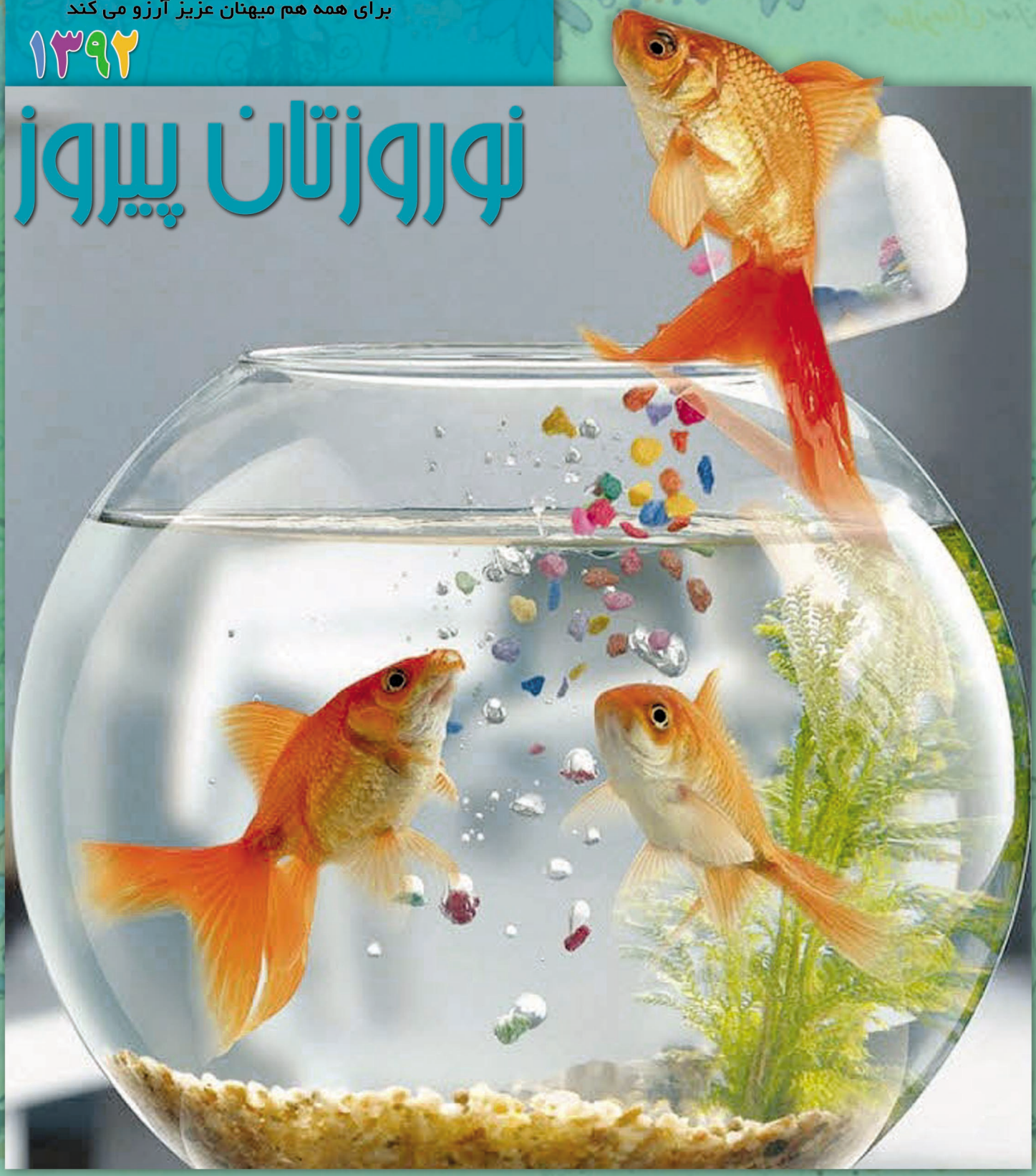
RCH

مرکز تحقیقات صنایع انفورماتیک

سال خوب و سرشار از برکت را
برای همه هم میهنان عزیز آرزو می کند

۱۳۹۲

نوروزتان پیروز



دفتر مرکزی و آزمایشگاه تهران: خیابان کریمخان زند،
خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر، پلاک ۳،
صندوق پستی:۱۵۸۷۵/۳۴۸۵
تلفن:۸۸۹۲۵۹۵(۱۰خط) فکس:۸۸۹۳۷۶۵۸

مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی
استان هرمزگان مستقر در اسکله شهید رجایی
تلفن:۴۵۱۴۲۵۹(۰۷۶۱) فاکس:۴۵۱۴۲۵۸(۰۷۶۱)

آزمایشگاه شهرک صنعتی پرند:
شهرک صنعتی پرند،بلوار فناوری، خیابان گلزار، خیابان گلگشت
قطعه D44 تلفن:۵-۵۶۴۱۸۸۶۴