فصلنامه تخصصی مرکز تحقیقات صنایع انفورماتیک

RCII

گزارش صنایع

انفورماتیک

| شماره ۲۸ | پاییز ۱۳۹۵ |

دولت الکترونیک، الزامات و زیرساخت‌ها

مراسم روز جهانی استاندارد برگزار شد

بانوی استاندارد ایران گواهی و تندیس شایستگی مدیریت زنان کارآفرین سال ۲۰۱۶ اتحادیه اروپا را در پاریس دریافت کرد

گزارش صنایع انفورماتیک
فصلنامه تخصصی
مرکز تحقیقات صنایع انفورماتیک
شماره۲۸ | پاییز ۱۳۹۵

صاحب امتیاز: مرکز تحقیقات صنایع انفورماتیک
مدیرمسئول: ویدا سینا
مدیر اجرایی: افسانه عبادی
مدیرفنی: رامین رضایی
روابط عمومی: فریبا نبی زاده
همکاران این شماره: مهرداد لطفعلیان
هادی اسکندی، بهاره هدایت، مهری یحیایی
نشانی: تهران، خیابان کریم‌خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر، پلاک ۳
تلفن: ۵۰-۸۸۹۲۵۹۴۳ (۱۰خط) **فکس:**۸۸۹۳۷۶۵۸
مجری فصلنامه:اکبر کریمی[۰۹۱۲۳۰۸۹۳۰۳]

www.rcii.ir

نشانی آزمایشگاه‌ها:

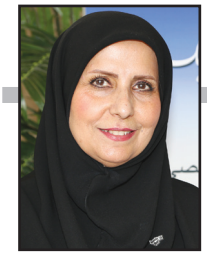
دفتر و آزمایشگاه مرکزی
تهران، خیابان کریم‌خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر، پلاک ۳
تلفن: ۸۸۹۲۵۹۵۰(۱۰خطر)
فکس:۸۸۹۳۷۶۵۸

آزمایشگاه بندرعباس
مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی هرمزگان مستقر در اسکله شهید رجایی
تلفن:۰۷۶۳۳۵۱۴۲۵۹
فکس:۰۷۶۳۳۵۱۴۲۵۸

آزمایشگاه پرند
شهرک صنعتی پرند، بلوار فن‌آوری، خیابان گلزار خیابان گلگشت، قطعه D7
تلفکس:۵۶۴۱۸۸۹۲

آزمایشگاه بندرلنگه
بندرلنگه، بلوار معلم، حسین آباد شمالی، خیابان گلایل، نبش گلایل پنجم
تلفن:۰۷۶۴۴۲۲۲۴۷۶

سرمقاله



ویدا سینا
مدیر عامل مرکز تحقیقات صنایع انفورماتیک

دولت الکترونیک، الزامات و زیرساخت‌ها

یکی از اهداف کلان کشـور که در برنامه‌های پنج‌سـاله نیز منعکس شده، حرکت به سوی دولت الکترونیک اسـت. در این راسـتا همایش‌ها و جلسات متعددی برگزار شده، اما آنچه حائز اهمیت اسـت بررسی زیرساخت ها و الزامات دولت الکترونیک است که شاید کمتر به‌صورت عملیاتی به آن توجه شده باشد.

آنچه مسـلم اسـت، هدف از راه‌انـدازی دولت الکترونیـک، افزایش سـرعت و کیفیت خدمات و جلوگیری از مسافرت‌های درون‌شهری شهروندان برای انجام امور جاری است، اما چقدر مسئولان محترم در نیل به این اهداف موفق بوده‌اند؟

اکنون در بسـیاری از سازمان‌ها، پورتال سـازمان به ظاهر پذیرش درخواست‌های ارباب رجوع را انجام می‌دهند ولی اگر درخصوص کیفیت و سـرعت خدمات از ارباب رجوع نظرسنجی شود، در بسیاری از موارد با عدم رضایت مواجه خواهیم بود. علت چیست؟

دولـت الکترونیک نیاز به زیرسـاخت‌های قدرتمند انتقال داده‌ها دارد کـه این موضوع تقریباً در دولت یازدهم مورد توجه قرار گرفته و اقدامات بسیارخوبی نیز در این حوزه درحال رخداد است. در گام بعدی استاندارد بودن نرم‌افزارهای ارائه خدمات برخط (آنلاین) در ارائه خدمات الکترونیک با کیفیت و امنیت بالا بسیار مهم خواهند بود.

متأسفانه این بخش کمتر مورد توجه تصمیم‌گیرندگان دولتی قرار گرفته است. در حوزه امنیت و کیفیت سـامانه‌ها و نرم‌افزارهای خدمات الکترونیک کمتر سازمانی را می‌توان یافت که طراحان نرم‌افزار را ملزم به دریافت اسـتانداردهای لازم برای نرم‌افزار و سـامانه کرده باشـند. بسیاری از سـامانه‌ها و نرم‌افزارهای ارائه کننده خدمات دولت الکترونیـک مانند ثبت احوال، گمرک، بانک، ثبت شـرکت‌ها و مالکیت‌های معنوی و حتی سـامانه‌های خاص مربوط به سـازمان‌ها و نهادها، اطلاعـات محرمانه‌ای را دریافت و منتقل می‌کنند که افشـاء آنها می‌تواند امنیت ملی کشـور یا امنیت اجتماعی و اقتصادی خانوارها را مورد تهدید قرار دهد.

از مسـئولان و تصمیم‌گیرنـدگان در این حوزه درخواسـت می‌شـود تا جهـت افزایش کیفیت و امنیت خدمات الکترونیک و در نتیجه افزایش اعتماد کاربران به دولت الکترونیک، رعایت امضای دیجیتال و اسـتانداردهای امنیت و کیفیت نرم‌افزار را جزو الزامات سـامانه‌های دولت الکترونیک قرار دهند.

بانوی استاندارد ایران گواهی و تندیس شایستگی مدیریت زنان کارآفرین سال ۲۰۱۶ اتحادیه اروپا را در پاریس دریافت کرد

روزنامه دنیای اقتصاد مورخ ۹۵/۹/۲ طی مصاحبه‌ای با مدیرعامل مرکز تحقیقات صنایع انفورماتیک، ویدا سینا را به عنوان بانوی استاندارد معرفی کرد و همچنین خاطرنشان کرد: این بانوی کارآفرین اخیراً گواهی و تندیس شایستگی مدیریت زنان کارآفرین سال ۲۰۱۶ اتحادیه اروپا در پاریس را دریافت کرد در زیر به شرح مصاحبه ویدا سینا با روزنامه دنیای اقتصاد می پردازیم.

مدیرعامل مرکز تحقیقات صنایع انفورماتیک، خروج از رکود اقتصادی را ایجاد اشتغال از طریق تعاونی‌های تولیدی، ولی نه بصورت تعاونی‌های فعلی می‌داند. ویدا سینا که به عنوان بانوی استاندارد، مدیر عامل مرکز تحقیقات صنایع انفورماتیک و یکی از زنان با سابقه کشور در کارآفرینی است، بر این باور است زمانی که مردم بجای دریافت یارانه، سهامدار شرکت‌های تعاونی محلی خود شوند، آنگاه شاهد اشتغال‌زایی و کاهش نرخ بیکاری، افزایش امنیت اجتماعی و سرانجام رشد و شکوفایی اقتصاد خواهیم بود.
وی می گوید: ماهانه بالغ بر ۳ هزار و ۶۰۰ میلیارد تومان یارانه به قشرهای مختلف پرداخت می‌شود در حالی که اگر این مبلغ وارد جریان تولید شود، اقتصاد کشور از رکود خارج خواهد شد. پول نفت باید صرف توسعه زیرساخت‌ها و دانش فنی شود نه مسایل روزمره و پرداخت حقوق، همین مسئله به تنهایی باعث تشدید رکود در بازار می شود.
وی بر این باور است زمانی که چرخه اقتصاد از مسیر واقعی خود خارج شود، دور زدن‌های مالیاتی و قاچاق کالا عرصه گسترده‌تری پیدا می‌کنند و صنایع قادر نخواهند بود در رقابت‌های عادلانه نیروی خود را صرف حضور در بازارهای داخلی و خارجی کنند.در این شرایط بنگاه‌های اقتصادی نیز تضعیف شده و قادر نیستند اقتصاد کشور را به حرکت درآورند. سینا که مدیر مسئول نشریه انفورماتیک نیز است، بحث استاندارد را یکی از حلقه‌های رشد اقتصادی دانست و در گفت‌وگو با دنیای اقتصاد افزود، با افزایش و تنوع در تولید کالاها، بازاری نو برای کالاهای جدید ایجاد شده که رعایت استاندارد و لزوم حمایت از مصرف کنندگان را بیش از پیش ضروری‌می‌کند.
این بانوی کارآفرین که اخیراً گواهی و تندیس شایستگی مدیریت زنان کارآفرین سال ۲۰۱۶ اتحادیه اروپا را در پاریس دریافت کرده است،درباره نقش مرکز تحقیقات صنایع انفورماتیک در استاندارد تصریح کرد: ما به عنوان بخش خصوصی در کنار استاندارد و سازمان‌های نظارتی بالادستی، کالاهای لوازم خانگی و تجهیزات پزشکی، تجهیزات ICT، دستگاه‌های صوتی و تصویری، تست EMC (تشعشعات الکترومغناطیسی) لیزر، تجهیزات امنیتی، قطعات خودرو، سرورها، نرم‌افزارها و سامانه‌هایی را که تولید یا وارد کشور می‌شوند در آزمایشگاه‌های فوق تخصصی‌مان آزمایش کرده و تقلبی یا غیر استاندارد بودن آنها را بررسی می کنیم.ویدا سینا افزود: تاکید ما به واردکنندگان و تولیدکنندگان احترام به حقوق شهروندی است، چرا که اگر کالا غیر استاندارد باشد برای مصرف کننده عوارض و لطماتی در پی خواهد داشت که گاه غیر قابل جبران است.

بی توجهی به استانداردها هدر رفت سرمایه ها

مدیرعامل مرکز تحقیقات صنایع انفورماتیک خاطرنشان کرد: بی توجهی به استانداردها باعث هدر رفتن سرمایه ها در حوزه تولید می شود و این در حالی است که توجه به استانداردها در بالا رفتن صرفه اقتصادی تولید و ارتقای جایگاه مصرف کننده به عنوان یکی از ارکان چرخه بازار بسیار حائز اهمیت است. وی بخش خصوصی را

همکار صدیق دولت دانست و گفت: همراهی و حمایت دولت در توسعه آزمایشگاه‌های همکار خصوصی در زمینه بررسی استانداردها و تخصیص اعتبارات بانکی به آنها، بسترهای مناسب و لازم را ایجاد و مسیر فعالیت‌ها را تسهیل می کند که در نهایت انگیزه بخش خصوصی برای سرمایه گذاری و توسعه بیشتر را به همراه دارد. همین امر زمینه ساز حرکت پرشتاب بازار به سمت تولید و واردات کالاهای مناسب و با کیفیت خواهد شد.

این بانوی کارآفرین که عضو هیئت رییسه سندیکای تولیدکنندگان فناوری اطلاعات نیز است، با اشاره به اینکه تولید، بدون در نظر گرفتن استانداردهای بین‌المللی محکوم به شکست خواهد بود، اظهار کرد: اگر تولیدکننده نتواند به بازارهای جهانی راه یابد، پس از اشباع بازار داخل عدم توانمندی در رقابت‌های داخلی باید به تعطیلی بنگاه خود بیاندیشد، بنابراین یکی از ارکان حمایت از تولیدکننده، تولید کالا یا خدمات منطبق با استانداردهای بین المللی است. وی فراهم کردن شرایط لازم برای ایجاد رقابت سالم در تولید را بسیار با اهمیت دانست و با اشاره به اینکه هدایت نشدن صحیح بنگاه ها باعث اتلاف سرمایه ملی می شود تصریح کرد: دادن موافقت اصولی وپروانه بهره برداری بدون بررسی اصولی، سبب شد تا وضعیت تقاضاهای بالفعل و بالقوه داخلی و خارجی در نظر گرفته نشود، بسیاری از شرکت های تولیدی را به ورشکستگی بکشاند و به تلف شدن سرمایه ملی منجر شود.

وی یادآور شد که سهامداران مجموعه مرکز تحقیقات صنایع انفوماتیک حدود ۲۵ سال است هیچ سودی دریافت نکرده ند و این در حالی است که طی این سال ها تمام سودها در قالب طرح‌های توسعه‌ای جدید به مجموعه باز گشته است. سینا با اشاره به اینکه مجموعه یاد شده از صفر و بدون هیچ حمایتی کار خود را آغاز کرده و اکنون به بزرگ‌ترین آزمایشگاه تخصصی کشور تبدیل شده و در رتبه برترین‌ها جای دارد، اظهار امیدواری کرد که این مرکز تا سال ۱۴۰۴ رتبه نخست خاورمیانه را از آن خودسازد.

تلاش مضاعف زنان در مقابل مردان

عضو فدراسیون ICT اتاق ایران در ادامه گفت‌وگو به نقش زنان در جامعه امروز و تلاش ۳ برابری آنها در مقابل مردان اشاره کرد و گفت: اگر امروز یک مرد در جامعه با توان A فعالیت دارد، یک زن در همان شرایط یکسان با توان ۳A کار می‌کند.این به معنای آن است که خانم‌ها برای دستیابی به موفقیت باید فشار بیشتری را نسبت به مردان تحمل کنند. وی افزود: در حال حاضر بانوان موفق بسیاری در کشور هستند که برای هر قدمی که در مسیر موفقیت خود برداشته‌اند زحمت بسیار کشیده‌اند. بنابراین دستیابی به موفقیت غیر ممکن نیست به شرطی که بانوان جامعه خود راباورداشته‌باشند.

ویدا سینا با اشاره به اینکه همه ما از سرمایه‌های این مرز و بوم بهره برده‌ایم و باید دین خود را به میهن مان ادا کنیم، یادآور شد، قطعاً حضور فعال تک تک ما در جامعه می‌تواند به ارتقای سطح علمی، فرهنگی و اجتماعی کمک کند.

خبر کوتاه

حضور مرکز تحقیقات صنایع انفورماتیک در نمایشگاه لیزر و صنایع وابسته

نمایشگاه لیزر و صنایع وابسته همزمان با چهارمین کنفرانس لیزر و کاربردهای آن در تاریخ ۱۱ الی ۱۳ آبان ماه سال جاری در دانشکده فیزیک دانشگاه صنعتی شریف به همت سازمان انرژی اتمی و با حضور فعالان این عرصه از جمله پژوهشکده لیزر سازمان انرژی اتمی، مرکز ملی علوم و فنون لیزر، صنایع الکترواپتیک صاایران و بخش‌های صنعتی، دانشگاهی (از جمله شهید بهشتی)، خصوصی (الکترواپتیک پارس، مهر اپتیک، نور صنعت پارس) و همچنین آزمایشگاه لیزر مرکز تحقیقات صنایع انفورماتیک برگزار شد.

خبر کوتاه

دریافت لوح سپاس مرکز تحقیقات صنایع انفورماتیک از اداره کل استاندارد استان هرمزگان

در مراسم روز جهانی استاندارد در بندرعباس، مرکز تحقیقات صنایع انفورماتیک از طرف اداره کل استاندارد استان هرمزگان لوح سپاس دریافت کرد.

مراسم روزجهانی استاندارد برگزار شد

مراسم روز جهانی استاندارد در روز دوشنبه ۲۶ مهر ماه در مرکز همایش‌های سازمان صدا و سیمای جمهوری اسلامی ایران برگزار شد. رئیس محترم سازمان ملی استاندارد ایران، سرکار خانم پیروزبخت اخذ استاندارد پیش از تولید محصولات را ضروری دانسته و تاکید کردند این مهم نباید به بعد از تولید موکول شود.

دیگر سخنران این مراسم معاون اول محترم رئیس جمهور، جناب آقای اسحاق جهانگیری بود. ایشان با بیان اینکه هدف‌گیری تولیدکنندگان داخلی باید بازارهای بین‌المللی باشد، فرمودند: استاندارد نقش تعیین‌کننده‌ای در رشد اقتصادی کشور دارد. استاندارد سخت نیست و حداقل‌ها است. باید در راستای اخذ استانداردهای بالاتر اهتمام بیشتر و ویژه‌تری صورت گیرد و باید استانداردهایی داشته باشیم که در سطوح جهانی قابل قبول باشند.

حجت‌الاسلام مصطفی پورمحمدی وزیر محترم دادگستری با تاکید بر اینکه وجود استاندارد با توجه به بازار گسترده و حجم کالاها از ضروریات جامعه امروز است، فرمودند : بدون استاندارد نباید هیچگونه کالا و خدمتی ارائه شود، استاندارد کف مقررات است.

معقله

Fog Computing or Edge Computing

رایانش ابری در اینترنت اشیاء

مهرداد لطفعلیان

مقدمه

امروزه با توجه به اینکه اینترنت اشیا یا Internet of Things (IoT) به ارائه داده‌های حجیم در طیف وسیع می‌پردازد، این تهدید وجود دارد که در زمان انتقال داده‌ها به Cloud جهت تجزیه و تحلیل، فرصت انجام هرگونه فعالیتی بر روی آنها از بین برود. قصد داریم به بررسی یک مدل جدید برای تجزیه و تحلیل و فعالیت بر روی داده‌های IoT بپردازیم که Edge Computing یا Fog Computing نامیده می‌شود و شامل اقدامات زیر می باشد:

۱) به جای ارسال حجم زیادی از داده‌های IoT به Cloud، به تحلیل داده‌های حساس به زمان یا Time-Sensitive در لبه (Edge) شبکه و در نزدیکی مکانی که اطلاعات ایجاد شده‌اند، می پردازد.

۲) بر اساس Policy های اعمال شده، در مدت زمان چند میلی‌ثانیه بر روی داده‌های IoT فعالیت می‌کند.

۳) داده‌های انتخاب شده را برای تحلیل و بررسی مبتنی بر تاریخ و ذخیره‌سازی بلندمدت به Cloud می‌فرستد.

مزایای استفاده از IoT

IoT، کسب اطلاعات در مورد رویدادها و پاسخ‌گویی به آنها را تسریع می‌نماید. زمان پاسخ‌گویی کوتاه‌تر در صنایعی نظیر صنایع تولیدی، نفت و گاز، خدمات رفاهی، حمل و نقل، معدن و بخش دولتی می‌تواند موجب بهبود خروجی کار، ارتقای سطح خدمات و افزایش امنیت شود.

زیرساخت مناسب جهت استفاده از Fog Computing

سرمایه‌گذاری روی IoT مستلزم نوع جدیدی از زیرساخت‌ها می‌باشد که مدل‌های فعلی Cloud برای حجم، تنوع و سرعت داده‌های ارائه شده توسط IoT طراحی نشده‌اند. تعداد زیادی از تجهیزاتی که قبلا به اینترنت متصل نبودند، در حال حاضر روزانه بیش از ۲ اگزابایت داده تولید می‌کنند. تا سال ۲۰۲۰، حدود ۵۰ بیلیون شیء به اینترنت متصل خواهند شد که انتقال تمامی داده‌های تولید شده توسط آنها به Cloud جهت انجام فرآیند تجزیه و تحلیل مستلزم پهنای باند بسیار زیادی است و مدل‌های کنونی Cloud، برای حجم، تنوع و سرعت داده‌هایی که IoT ایجاد می‌کند، طراحی نشده‌اند.

این حجم وسیع از اشیاء می‌توانند انواع بی‌شماری از اشیاء جدید را نیز ارائه نماید (شکل ۱). برخی از آنها شامل دستگاه‌هایی هستند که جهت اتصال به Controller از پروتکل‌های صنعتی استفاده می‌کنند نه IP، بنابراین با توجه به این موضوع، قبل از ارسال اطلاعات به Cloud برای تجزیه‌وتحلیل و یا ذخیره‌سازی باید آنها را به IP تبدیل کرد.

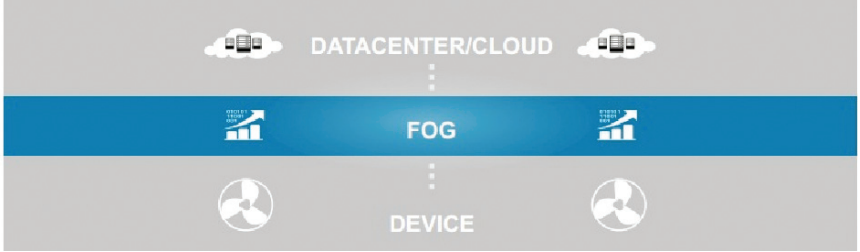
شکل۱: اتصال تعداد زیادی از اشیاء و انواع مختلف آن به Cloud با توجه به ساختار کنونی امکان پذیر نمی باشد.

Fog computing چیست؟

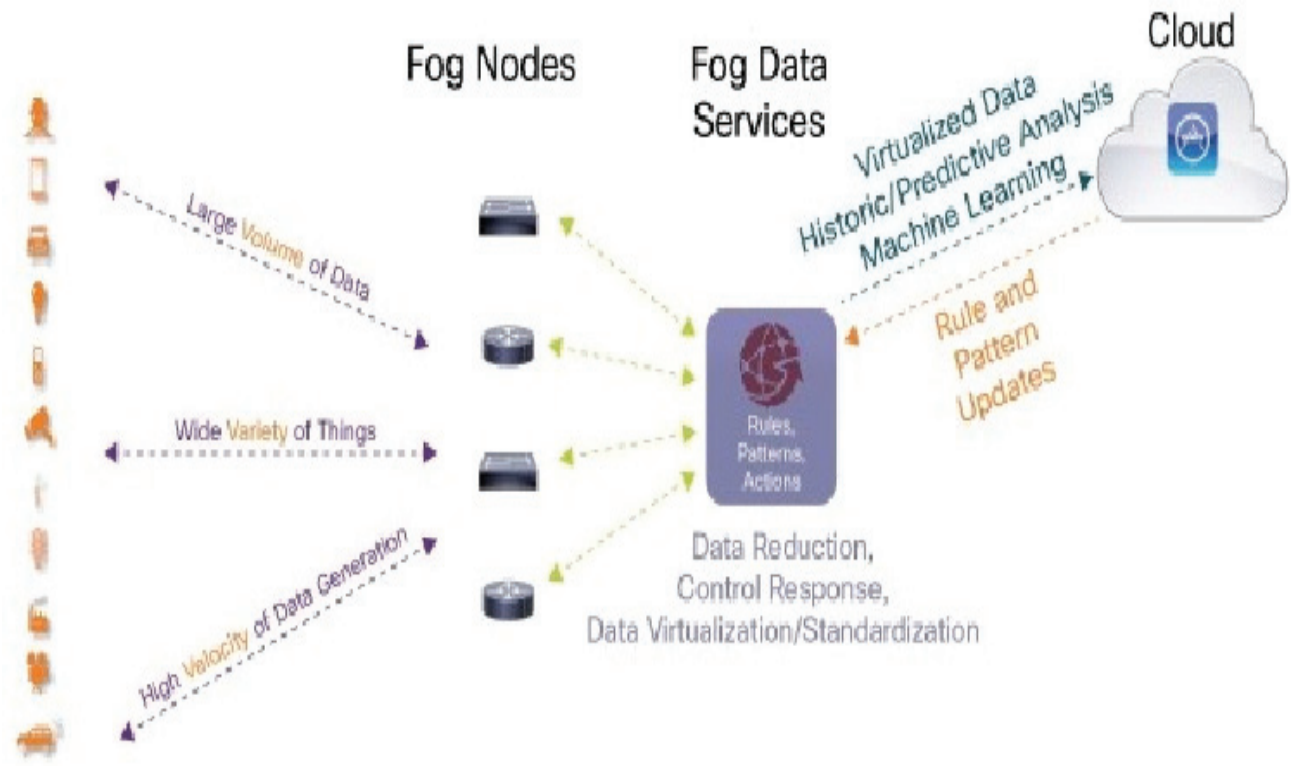
تکنولوژی Fog Computing، شرایط استقرار Cloud در نزدیکی تجهیزاتی که داده‌های IoT را تولید و روی آن فعالیت انجام می‌دهند، فراهم می‌نماید. این تجهیزات Fog Node نامیده می‌شوند و از طریق اتصال شبکه در هر جایی مانند سطح کارخانه، بالای تیرهای برق، در امتداد مسیر ریلی، در وسایل نقلیه یا روی سکوهای نفتی قابل استفاده می‌باشند. هر تجهیزی با دارا بودن اتصال Storage ، Network و Computing، می‌تواند یک Fog Node باشد. به عنوان نمونه می‌توان از Controllerها، سوییچ‌ها، روترها، سرورهای Embedشده و دوربین‌های مداربسته نام برد.

حجم داده‌های تحلیل شده در تجهیزاتی که به لحاظ فیزیکی در نزدیکی IoT قرار دارند، حدود ۴۰ درصد می‌باشد. بنابراین استدلال این است که تجزیه و تحلیل داده‌های IoT در نزدیکی جایی که ارائه می‌شوند، موجب کاهش زمان تاخیر می‌گردد.

این تکنولوژی چندین گیگابایت از ترافیک را از شبکه اصلی منتقل نموده و داده‌های حساس را در داخل شبکه نگه می‌دارد.



Fog به ایجاد Cloud در نزدیکی تجهیزات تولید کننده‌ی داده‌ها می پردازد



انواع برنامه های مربوط به Fog

برنامه‌های Fog نیز به اندازه Internet of Things از تنوع برخوردار می‌باشند. قابلیت‌های معمول این برنامه‌ها شامل مانیتورینگ و یا تجزیه و تحلیل داده‌های Real-Time مربوط به اشیای متصل به شبکه و سپس آغاز یک فعالیت است. لازم به ذکر است که این فعالیت می‌تواند شامل ارتباطات ماشین به ماشین یا M۲M و یا تعاملات انسان با ماشین یا HMI گردد. به عنوان نمونه می‌توان از قفل شدن درب، تغییر تنظیمات تجهیزات، استفاده از ترمز در قطار، زوم شدن دوربین، باز شدن دریچه در صورت ایجاد فشار، رسم نمودار میله‌ای یا ارسال هشدار به تکنسین برای انجام اقدامات پیشگیرانه نام برد؛ و البته شایان ذکر است که این امکان و احتمالات نامحدود می‌باشند.

ایجاد برنامه‌های Fog در بخش تولید، نفت و گاز، خدمات رفاهی، حمل و نقل، معدن و بخش دولتی به سرعت در حال گسترش می‌باشد.

نحوه عملکرد Fog

Developer ها، برنامه‌های IoT را برای Fog Node ها در لبه شبکه نوشته و ارائه می‌دهند. Fog Node هایی که در نزدیک‌ترین مکان به لبه شبکه قرار دارند، داده‌ها را از تجهیزات IoT دریافت می‌کنند. سپس انواع مختلفی از داده‌ها توسط برنامه‌های Fog IoT به منظور تجزیه و تحلیل به مکان مناسب هدایت می‌شوند.

بررسی فرآیند های Fog و Cloud :

Fog Node

Feed های مربوط به تجهیزات IoT را که از هر نوع پروتکلی استفاده می‌کند، به صورت Real-Time دریافت می‌کند.

برنامه‌های فعال IoT را برای تحلیل و کنترل Real-Time با مدت زمان پاسخگویی میلی‌ثانیه اجرا می‌نماید.

قابلیت ذخیره‌سازی موقت، اغلب به مدت ۱تا ۲ ساعت را ارائه می‌نماید.

یک خلاصه‌ی دوره‌ای از داده‌ها را به Cloud ارسال می‌کند.

پلتفرم Cloud

خلاصه داده‌ها را از تعداد زیادی Fog Node دریافت و جمع‌آوری می‌نماید.

روی داده‌های IoT و داده‌های حاصل از سایر منابع، تجزیه و تحلیل انجام می‌دهد تا به اطلاعات کسب‌وکار دسترسی یابد.

بر اساس این اطلاعات می‌تواند قواعد جدید برنامه را به Fog Node ها ارسال نماید.

جمع‌بندی

Fog Computing، شرایطی را برای Cloud فراهم می‌آورد که بتواند تا دو اگزابایت داده‌ی حاصل از IoT در طول روز را مدیریت نماید. علاوه بر آن می توان چالش‌های مربوط به گسترش حجم زیاد داده‌ها، تنوع و سرعت را نیز با پردازش داده‌ها در نزدیک جایی که ایجاد شده و مورد نیاز می‌باشند، حل نمود.

این تکنولوژی با حذف مسیر ارسال به Cloud جهت انجام فرآیند تجزیه و تحلیل، موجب تسریع کسب آگاهی و اطلاعات در مورد رویدادها و پاسخ‌دهی سریع به آنها می‌گردد.

همچنین با انتقال چندین گیگابایت ترافیک از شبکه اصلی، نیاز به فرآیند پرهزینه‌ی افزایش پهنای باند را از بین برده و از طریق تحلیل داده‌های IoT در داخل همان فضا از این داده‌های حساس محافظت می‌نماید. در نهایت، سازمان‌هایی که از Fog Computing استفاده می‌کنند، به اطلاعات دقیق‌تر و سریع‌تری دست می‌یابند که موجب افزایش چابکی در کسب‌وکار، ارتقای سطح سرویس‌دهی و بهبود امنیت می‌گردد.

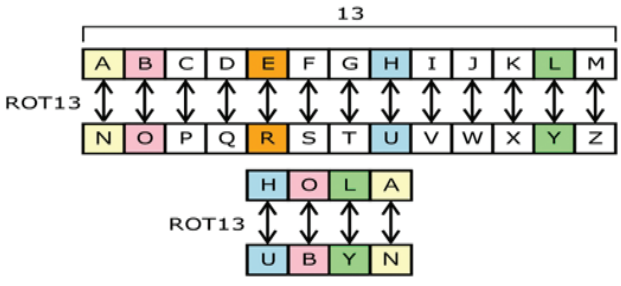
مقاله

مروری بر حملات جانبی بر روی کارت هوشمند

هادی اسکندری سبزی،بهاره هدایت، مهری یحیایی

مقدمه

رمزنگاری از دیرباز به‌عنوان یک ضرورت برای حفاظت از اطلاعات خصوصی در مقابل دسترسی‌های غیرمجاز در تجارت، سیاست و مسائل نظامی وجود داشته است. به‌طور مثال تلاش برای ارسال یک پیام سری بین دو هم‌پیمان به‌گونه‌ای که حتی اگر توسط دشمن دریافت شود نیز قابل‌درک نباشد، در تاریخ رم قدیم نیز دیده شده و یک تاریخچه و قدمت طولانی دارد. در شکل زیر یک نمونه از رمزنگاری برای ارسال محرمانه اطلاعات که با شیفت دادن کلمات بوده است نشان داده شده است.



نمونه‌ای از مدل رمزنگاری شیفت کلمات

در سالهای اخیر رمزنگاری و تحلیل رمز از یک هنر، پا را فراتر گذاشته و یک علم مستقل شده است و درواقع به‌عنوان یک وسیله عملی برای ارسال اطلاعات محرمانه روی کانال‌های غیر امن همانند اینترنت، تلفن، ماکرویو و ماهواره‌ها شناخته می‌شود. با توجه به گستردگی ارتباطات کامپیوتری، پیشرفت تکنولوژی، آسان شدن روش‌های نقل و انتقال اطلاعات دیجیتال و توسعه فناوری‌های اطلاعات، به وجود آمدن مخابرات امن و شبکه‌های دیجیتالی مانند شبکه‌های اینترنت، هرروزه بر تعداد مصرف‌کنندگان از محصولات دیجیتالی افزوده می‌شود. از طرف دیگر قابلیت کپی‌برداری راحت‌تر و بدون افت کیفیت از این محصولات باعث شده است تا همواره طراحی سامانه‌هایی که بتواند از این محصولات و حقوق صاحبان آن‌ها محافظت کند یکی از نیازهای جدی این عرصه است.

از یک دیدگاه کلی امنیت اطلاعات دارای سه هدف اصلی است که این سه هدف را می‌توان به‌صورت زیر بیان کرد:

- **محرمانگی:** اطلاعات تنها توسط افراد مجاز قابل‌خواندن باشد.
- **جامعیت:** اگر اطلاعات در حین ارسال یا پردازش دست‌کاری شود، قابل‌تشخیص نباشد.
- **در دسترس بودن:** اطلاعات و منابع سیستم در دسترس افراد مجاز باشد و افراد غیرمجاز نتوانند خللی در امکان استفاده از منابع ایجاد کنند.

در سالیان دور مکانیزم‌های امنیتی و کاربردهای آن معمولاً محدود به حوزه‌های نظامی و مراکز امنیتی بوده، اما در دهه‌های اخیر با گسترش شبکه‌های کامپیوتری و بوجود آمدن کاربردهای گوناگون الکترونیکی مانند تجارت الکترونیک، امنیت اطلاعات در سایر حوزه‌ها هم مورد توجه قرارگرفته و به یک مسئله روزمره تبدیل شده است که ما همواره در کاربردهای روزانه با آن سروکار داریم. یکی از این کاربردهای مهم روزانه، استفاده از کارت‌های هوشمند است.

گسترش کارت‌های پلاستیکی در اوایل دهه ۱۹۵۰ میلادی آغاز شد. هزینه پایین این کارت‌ها که از جنس پلیوینیل کلراید بودند، باعث شد تا به‌سرعت جایگزین کارت‌های کاغذی شوند که تحمل تنش‌های فیزیکی و تغییرات آب و هوا را ندارند.

در سال ۱۹۷۰ با پیشرفت چشمگیر در ریزپردازنده‌ها و ترکیب آن‌ها با حافظه‌های غیرفعال این امکان به وجود آمد تا از آن‌ها در کارت‌های هوشمند استفاده شود و تا به امروز ادامه دارد.کارت‌های هوشمند، امروزه در بسیاری از مواردی به‌کار می‌روند که نیاز به نگهداری و انتقال امن اطلاعات داده‌ها، کنترل دسترسی به سیستم‌های رایانه‌ای و نیز کنترل دسترسی فیزیکی به محیط‌های خاص به‌عنوان کلید الکترونیکی وجود دارند. از این نوع کارت میتوان به‌جای کارت اعتباری و کارت پول، یا در سیستم‌های امنیتی کامپیوتری، سیستم‌های تشخیص هویت و بسیاری موارد دیگر استفاده کرد. بنابراین با توجه به کاربردهای مهمی که برای کارت هوشمند اشاره شد، می‌توان گفت که رمزنگاری و امنیت در کارت‌های هوشمند نیازی غیر قابل انکار و یکی از ملزومات مهم برای پیاده‌سازی کارت هوشمند است. کارت‌های هوشمند شرایطی را برای دسترسی به اطلاعات خود اعمال می‌کنند تا از محتویات داده‌های موجود در فایل‌ها محافظت کنند. کاربران فقط در شرایطی می‌توانند به نوشتن یا خواندن اطلاعات کارت اقدام کنند که شرایط دسترسی و مجوزهای لازم را داشته باشند.

در یک سیستم رمزنگاری معمولی با استفاده از رمز کننده‌های بلوکی، رمزگشایی معمولاً با توجه و تمرکز بر ورودی اولیه و خروجی نهایی و پنهانی به‌عنوان یک منبع اطلاعات برای حمله، آغاز میشود. این موارد شامل متن ورودی، کلیدهای مخفی و خروجی متن رمز شده نهایی است.

برخی از فرضیاتی که در این رابطه اظهار میشود عبارتند از اینکه: هیچ اطلاعاتی از کلید محرمانه برای مهاجم در دسترس نیست و تابع رمزنگاری به‌عنوان یک جعبه سیاه عمل میکند. ازآنجایی‌که این تابع در تمامی دستگاه‌های دنیا اجرا می‌شود، این فرضیات ممکن است کاملاً صحیح باشد که می‌توان به نحوی به این کلید دستیابی پیدا کرد. پس برای این‌که بتوان به کلید دست یافت، باید به الگوریتم حملاتی را ارائه نمود. بر اساس اینکه حمله کننده چه کنترلی را بر عملیات رمزگذاری دارد، حملات به دو دسته تقسیم‌بندی می‌شوند:

• حملات فعال

در این نوع حملات دستگاه رمزنگاری، ورودی‌های آن یا محیطی که دستگاه در آن در حال انجام عملیات است، دست‌کاری می‌شوند تا دستگاه رمزنگاری در شرایط غیرمعمول به اجرای عملیات رمزنگاری بپردازد

• حملات غیرفعال

در این نوع حملات دستگاه رمزنگاری به کار عادی خود ادامه داده و حمله‌کننده سعی دارد با استفاده از پارامترهای فیزیکی دستگاه تحت حمله، (همچون زمان اجرا و توان مصرفی و غیره) کلید مخفی دستگاه را کشف کند. به دلیل اینکه در این نوع حملات هیچگونه محدودیتی بر روی فعالیتی که دستگاه رمزنگاری انجام میدهد وجود ندارد، این نوع حملات قویترین نوع از حملاتی هستند که به دستگاه‌های رمزنگاری اعمال میشوند. در این نوع حملات دستگاه رمزنگاری به همان شکلی که وجود دارد بدون اینکه کوچکترین آسیب فیزیکی ببیند، در حین اجرای الگوریتم رمزنگاری مورد حمله قرار می‌گیرد و هیچ خللی در شکل ظاهر و روند اجرای آن به وجود نمی‌آید، در نتیجه هیچ آثاری از حمله انجام شده بر روی دستگاه رمزنگاری باقی نخواهد ماند.

حملات جانبی بر روی کارت هوشمند

دستگاه‌های رمزنگاری دارای رابطه فیزیکی، منطقی و الکتریکی هستند. دسترسی به برخی از این رابطه‌ها ساده بوده و دسترسی به برخی نیازمند ابزار و تجهیزات خاصی است. در این نوع حملات دستگاه رمزنگاری به همان شکلی که وجود دارد مورد حمله قرار میگیرد و هیچ خللی در شکل ظاهر و روند اجرای آن به وجود نمی‌آید، در نتیجه هیچ آثاری از حمله انجام شده بر روی دستگاه رمزنگاری باقی نخواهد ماند. اغلب حملات غیر متجاوزانه با استفاده از ابزار و تجهیزات ارزان‌قیمتی انجام میپذیرد و درنتیجه تهدیدی جدی برای امنیت دستگاه‌های رمزنگاری است.

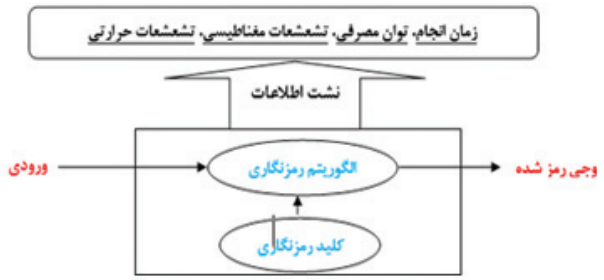
عموماً این نوع حملات را حملات جانبی کانال گویند. برای اولین بار در سال ۱۹۹۶ ایده استفاده از اطلاعات کانال جانبی برای تحلیل الگوریتم‌های رمز مدرن ارائه شد.

تاکنون چهار کانال اصلی به‌عنوان کانال جانبی تحلیل الگوریتم‌های رمزنگاری مورد استفاده قرار گرفته است که این چهار کانال عبارتند از: زمان اجرای الگوریتم، خطای محاسباتی الگوریتم، توان مصرفی در حین اجرای الگوریتم و امواج الکترومغناطیسی. البته باید ذکر کرد که عملی بودن هر یک از حملات کانال جانبی به قابل اندازه‌گیری بودن اطلاعات کانال جانبی مورد نظر بستگی دارد. برای مثال تنها در صورتی می‌توان از تحلیل توان مصرفی استفاده کرد که بتوان با دقت بالاتر و مناسبی مقدار توان مصرف شده در حین اجرای الگوریتم را به دست آورد.

در حالت کلی اینگونه می‌توان بیان کرد که هدف حملات جانبی کانال، استفاده از نشت اطلاعاتی است که یک دستگاه رمزنگاری به‌منظور دستیابی به کلید مخفی سامانه مورد استفاده قرار می‌دهد.

برای مثال یک الگوریتم رمزنگاری برای اجرای یک عملیات با کلیدهای متفاوت، دارای زمان‌های متفاوتی خواهد بود. این اختلاف زمان ممکن است قابل اندازه‌گیری بوده و برای حمله از طریق زمان مورد استفاده قرار گیرد و نشت اطلاعات از تراشه‌های الکترونیکی و کامپیوتر هنگام پردازش عملیات باعث به وجود آمدن آن شده است.

برخی از نمونه‌های نشت اطلاعات در شکل زیر نشان داده شده اند.



خروجی‌های غیرمستقیم از اجرای رمزنگاری بلوکی

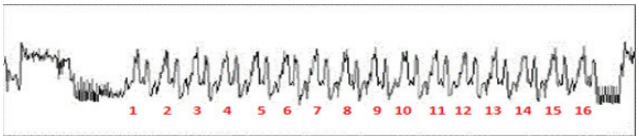
حمله بر اساس تجزیه‌وتحلیل توان

ازآنجایی‌کـه سـامانه‌های رمزنگاری نوین (کارت‌های هوشـمند) با اسـتفاده از گیت‌های منطقی پیادهسـازی میشـوند که خود ایـن گیت‌های منطقی، از تعدادی ترانزیسـتور و المان‌های دیگر تشـکیل شـده است، جریان‌های به وجود آمده در این مدارات و ترانزیسـتورها باعث به وجود آمدن تشعشـعات الکترومغناطیسی شده و باعث بروز اختلاف توان مصرفی و اتلاف توان مصرفی می‌شود. یکی از قدرتمندترین و معمولترین نوع حملات جانبی کانال استفاده از تجزیه و تحلیل توان برای حمله اسـت. این حمله از طریق نشـت اطلاعات از منبع توان که در طول اجرای الگوریتم رمزنگاری رخ می‌دهد مورد استفاده قرار می‌گیرد. در این حملات سـعی بر پیدا کردن یک راه‌حل و رابطه مناسب بین مصـرف لحظه‌ای توان و وضعیـت داخلی آن در زمان اجـرای الگوریتم رمزنگاری اسـت. چون تـوان مصرفی در یک مدار مجتمع نشـان‌دهنده بروز اجزای سـازنده مدار اسـت، پس می‌توان گفت که توان مصرفی یک قسـمت خاص از مدار و تغییرات به وجود آمده در توان مصرف آن براسـاس تغییرات اعمال شـده در روشـن و خاموش کردن مدار یا همان ترانزیستور است. برای مثال می‌توان اینگونه بیان کرد که یک پردازنده برای انجام عملیات جمع و یا هر عمل دیگر، مقداری انـرژی مصرف می‌کند که در حالات مختلف متفاوت اسـت. با توجه به اینکه میـزان توان مصرفی یک مـدار مجتمع به داده‌های پردازش شـده بسـتگی دارد، اندازه‌گیری توان مصرفـی آن، اطلاعاتی درباره عملیات اتفاق افتاده را آشکار میکند. پس هنگامی‌که سامانه در حال پردازش داده‌های یک الگوریتم رمزنگاری اسـت، توان آن می‌تواند برای استخراج کلید مورد استفاده قرار گیرد.

تجزیه و تحلیل توان برای حملات جانبی را میتوان به سه بخش تقسیم‌بندی کرد:

- پیـدا کردن یک رابطه منطقی بین اطلاعات کلیـد محرمانه و مصرف توان لحظه‌ای و همچنین نیاز به تعیین ورودی‌های مورد نیاز برای سیستم و مقادیر خروجی برای اندازه‌گیری و یادداشت کردن آن.
- اسـتخراج حالت‌های مختلف اندازه‌گیری و یادداشت آن که شامل موارد از قبل مشخص شده برای مصرف توان می‌شود.
- بررسـی رابطه بین آیتم‌های اندازه‌گیری به وسـیله پردازش کردن بر روی اطلاعات استخراج شده.

بنابراین با بررسی اثرات توان، استخراج کردن آنچه در طول عملیات رخ داده است برای ما ممکن خواهد بود. برای مثال شکل زیر نشان میدهد که مصرف تـوان لحظه‌ای برای یـک قطعه رمزنگاری بر اسـاس الگوریتم (DES) انجام شده است.



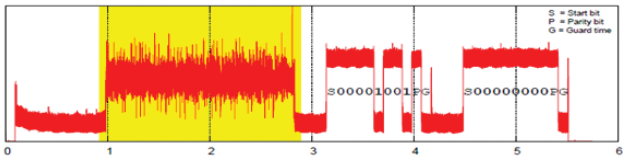
نشان دادن آثار مصرف توان در الگوریتم DES

۱۶ مرحلـه منحصربه‌فرد از رمزنگاری با اسـتفاده از الگوهای تکرار شـده در شکل قابل مشاهده اسـت. شکل بالا نشان دهنده مصرف توان لحظه‌ای برای یک قطعه رمزنگاری بر اساس الگوریتم (DES) می‌باشد.

به وسیله شناختن این نقاط در یک رمزنگاری برای حمله، میتوان آن را برای حمله قدرتمندانه‌تر مورد اسـتفاده قـرار داد. این اختلاف و تفاوت در مصرف توان لحظه‌ای نیز می‌تواند به ارزش و مقدار هر بیت که در حال دسـت‌کاری و اجرای عملیات اسـت، مربوط باشـد. در این حالت حمله‌کننده مستقیما از طریـق بررسـی مقدار توان خروجـی توان مصرفی حملـه را انجام می‌دهد و داده‌هـای به دسـت آمده از تـوان مصرفی الگوریتم در حیـن اجرای رمز، به صورت مستقیم برای پی بردن به الگوریتم رمز و بیت‌های کلید مورد استفاده قرار می‌گیرد. در این نوع روش‌ها با اسـتفاده از شکل موج خروجی و اینکه با چه الگوریتمی سیستم در حال رمز کردن است مستقیماً می‌توان پی به رابطه الگوریتم برد و مقدمات استخراج برای کلید را فراهم آورد. حملاتی که مبتنی بر این روش هستند به دو صورت انجام می‌پذیرد:

• حمله از طریق تحلیل توانی ساده (SPA)[1]

در این روش حمله کننده مسـتقیماً از طریق بررسی شکل موج بدست آمده، مقـدار توان خروجی توان مصرفی حمله را انجام می‌دهد. داده‌های به دسـت آمـده از شـکل موج توان مصرفـی الگوریتم در حین اجـرای رمز، به صورت مسـتقیم برای پی بردن به الگوریتم رمز و بیت‌های کلید مورد اسـتفاده قرار می‌گیـرد. در این روش‌ها با اسـتفاده از شـکل موج خروجـی و اینکه با چه الگوریتمی سیسـتم در حال رمز کردن اسـت، مستقیما می‌توان پی به رابطه الگوریتـم برد و مقدمات اسـتخراج کلید را فراهم آورد. اگـر الگوریتم رمز به نحوی پیاده‌سـازی شـود که مسـیر اجرای دنباله دسـتورالعمل‌ها وابسته به داده‌های مورد پردازش، مثلا بیت‌های کلید باشـد. با توجه به اینکه با SPA می‌توان دسـتورالعمل‌های در حال اجرا را آشکار کرد، در این‌صورت با روش سـاده SPA می‌توان اطلاعـات زیادی در رابطه با بیت‌های کلید به دسـت آورد. در این نوع روش، با اسـتفاده از تجزیه و تحلیل شکل موج‌های خروجی و همچین مقادیر خروجی به دست آمده، مهاجم سعی در پیداکردن الگوهایی برای مطابقت دادن با یک الگوی قالب و یک رابطه منطقی بین الگوریتم‌های به وجود آمده برای رمز کردن را دارد. شـکل زیر اسـتخراج و حدس کلید به این روش را نشان می‌دهد.



استخراج کد از طریق تجزیه و تحلیل توانی ساده

• حمله از طریق تحلیل تفاضلی توان (DPA)[2]

در اغلـب موارد، SPA به تنهایی برای اسـتخراج یـک کلید مخفی کافی نیسـت. حملـه از طریق DPA بسـیار قویتر از حملـه از طریق تجزیه و تحلیل آماری اسـت. در روش پیشـرفته‌تر تحلیل توان یعنی روش تحلیل تفاضلی توان از همبسـتگی بین مصرف توان سیستم که در هنگام اجرای الگوریتم رمز به کار می‌روند، جهت حمله به سیسـتم اسـتفاده می‌شوند. مزیت اصلی حملات DPA در مقایسـه با حملات SPA این است که در این نوع حملات هیچ دانش دقیق در مورد رمزنگاری دسـتگاه لازم نیست. در حمـلات SPA آنالیـز مصرف توان یک دسـتگاه عمدتاً در طول محور زمـان قـرار دارد و درنتیجه مهاجم سـعی میکند با پیـدا کردن یک الگو و رابطه مناسـب بین شـکل موج اصلی الگوریتم رمز و شـکل موج بدست آورده از اجـرای الگوریتم، پی به کلید و نـوع رمزنگاری ببرد. در صورتی که در حمله DPA، شکل نمونه‌ها در طول محور زمان زیاد مورد اهمیت نیسـت و از این رو در لحظـات ثابتی از زمان به داده‌های پردازش‌شـده بسـتگی دارد، همچنیـن حملات DPA منحصراً وابسـته به مصرف توان داده‌امی‌باشـد.

گام‌های اساسی برای انجام یک آزمون DPA به شرح زیر است:

- انجام تعداد زیادی از عملیات رمز یا رمزگشایی بر روی یک دستگاه رمزنگاری با مجموعه‌های مختلف از داده‌ها
- پردازش و اندازه‌گیری و ثبت مصرف توان و خروجی داده‌ها یا ورودی آن در طول هر یک از عملیات اجرایی
- تقسیم‌بندی اندازه‌گیری توان به زیرمجموعه‌هایی مطابق با ویژگی پردازش‌شده

در نهایت با پیدا کردن اختلاف آماری بین زیر مجموعه‌ها، وقتی که اختلاف مشاهده شد، نشت اطلاعات تشخیص داده شده است.

جمع بندی

امنیت در تمام دوران‌ها یکی از نگرانی‌های بزرگ در سیستم مخابراتی و محاسباتی بوده و محققان همواره در تلاش برای بالا بردن امنیت اطلاعات ذخیره شده خود هستند.

با توجه به توسعه اجتناب ناپذیر کارت هوشمند در زندگی روزمره، امنیت کارت هوشمند از اهمیت ویژه‌ای برخوردار است. هدف اصلی این تحقیق، بررسی نقاط ضعف در الگوریتم‌های رمزنگاری پیاده‌سازی شده در کارت‌های هوشمند با استفاده از تحلیل حملات جانبی بر روی آن بوده ، به همین منظور با استفاده از تحلیل‌ها می‌توان به کلید رمزنگاری پیاده‌سازی شده در کارت هوشمند پی برد و اطلاعات را استخراج کرد. اهمیت این نوع حملات به حدی بوده که به محض مطرح شدن موضوع، پیاده‌سازی روش‌هایی که اقدام به جلوگیری از تحلیل‌های مختلف بر روی کارت هوشمند باشد، الزام شده و تولیدکنندگان این قطعات باید در تکنولوژی ساخت، این موارد را در نظر داشته باشند.

پی نوشت:

1. Simple Power Analysis
2. Differential Power Analysis

منابع:

۱. باقرزاده، ج.، (۱۳۹۱) ، «تحلیل توانی کارت هوشمند»، پایان نامه کارشناسی ارشد، دانشگاه صنعتی شریف.

۲. اسکندری، ه.، (۱۳۹۳) ، «رمزنگاری تصاویر دیجیتال »، پایان نامه

۳. فرجی، آ.، (۱۳۸۷) ، «حمله تحلیل توانی روی الگوریتم رمز Serpent و بررسی تکنیک WDDL در ارتقاء امنیت آن»، پایان نامه کارشناسی ارشد، دانشگاه صنعتی امیرکبیر.

۴.ریحانی‌تبار، م.، (۱۳۸۱) ، «حمله به کارتهای هوشمند با استفاده از اطلاعات نشتی»، پایان نامه کارشناسی ارشد، دانشگاه صنعتی شریف.

کارشناسی ارشد، دانشگاه آزاد اسلامی.

5. https://fa.wikipedia.org/wiki

6. International Standard, (2006) ISO/IEC 3-7816 Third edition, Published in Switzerland.

7. Kevin, M., (2012) “Differential Power Analysis attacks on AES” Cryptography II VCSG706-, USA.

8. Pauk, K. (1999) “Differential Power Analysis” technical report, cryptography research inc.

9. Dennis, V,.(2012) “Reverse engineering of Java Card applets using power analysis” Faculty of Electrical Engineering, Mathematics and Computer Science, Mekelweg 4,2628 CD Delft.The Netherlands.

10. Artin ,P.,(2010) “Reverse engineering of Java Card Applets” Bachelor Thesis, Masaryk University Faculty Of Informatics.

11. Pauk, K. (1996) “timing attacks on implementations of diffie hellman rsa dss and other systems” in Advances in cryptography –crypto,. Vol 1109 ,pp113-104

از مطلوبیت تا مسئولیت با نشان کیفیت

نشان کیفیت

مرکز تحقیقات صنایع انفورماتیک، نشان کیفیت محصولات را در زمینه تجهیزات و قطعات فناوری اطلاعات و ارتباطات، لوازم صوتی- تصویری، تجهیزات پزشکی، باتری (لیتیم ثانویه و اسید سربی)، گیرنده‌های تلویزیونی دیجیتال، انواع لوازم خانگی و امنیت و کیفیت و زیر ساخت کلید عمومی محصولات فناوری اطلاعات، در راستای حمایت از حقوق مصرف کنندگان نهایی و حمایت و تشویق وارد کنندگان و تولید کنندگان معتبر، ارائه می‌کند.

نشان کیفیت بر اساس ویژگی‌های محصول، نماینده معتبر و خدمات حین فروش و پس از فروش آن شاخص بندی شده و بعنوان تائید کیفیت و تطابق محصول با استانداردهای ملی و بین‌المللی بر روی محصول ، یا بسته‌بندی آن نصب می‌شود.

نشان کیفیت گویای این مطلب است که محصول دارای این نشان، علاوه بر رعایت استانداردهای فنی و ایمنی، دارای نمایندگی‌های فروش و خدمات حین فروش و پس از فروش معتبر و شناخته شده است و به مصرف کننده اطمینان استفاده از این خدمات را می دهد.

جهت ارائه نشان کیفیت لازم است نمونه محصول از نظر کیفیت، کارایی، امنیت، ایمنی و سازگاری‌الکترومغناطیسی، در جریان آزمونها با استانداردهای ملی و بین‌المللی تطبیق داده شود.

همچنین محصولات در طول دوره تحت گواهی بصورت مستمر مورد پایش قرار می گیرند تا از ثبات کیفیت و تطابق با استاندارد آنها اطمینان حاصل شود.

نشان کیفیت تامین کننده را از نظر ارائه خدمات حین فروش و ارائه خدمات پس از فروش شاخصهای سازمان حمایت مصرف کنندگان و تولید کنندگان ارزیابی می‌کند.

فرایند اعطای **نشان کیفیت** به تدریج موجب خروج محصولات بی کیفیت و خدمات فروش و پس از فروش نامعتبر از بازار شده و بدین ترتیب تولیدکنندگان مشکل رقابت با محصولات ارزان قیمت ولی بدون کیفیت و با خدمات فروش و پس از فروش نامناسب را نخواهند داشت و فروش، تولید و واردات محصولات مرغوب گسترش خواهد یافت.

مزایا برای مصرف کنندگان

- اطمینان مصرف کننده از صحت ادعاها در مورد محصول و نماینده فروش، خدمات حین فروش و پس از فروش معتبر.
- سنجش صحت ادعاها توسط شخص ثالث معتبر و متخصص (جلب اعتماد مصرف کننده).
- ایجاد پایه مناسبی برای مقایسه محصولات مختلف (حق انتخاب مصرف کننده از حقوق اساسی اوست).
- کاهش خطرات ناشی از قاچاق کالا، ایجاد بازار خاکستری و ورود کالاهای بی کیفیت.

مزایا برای متولی محصول

- کمک به تولید کننده و وارد کننده در تشخیص اشکالات احتمالی و عدم تطابق محصول خود با استانداردهای ضروری.
- کمک به تولید کننده و واردکننده در جلوگیری از جعل محصولات آنان.
- افزایش سهم بازار با تکیه بر مزیت کیفیت.
- حرکت به سمت شفاف سازی بازار.
- اطلاع رسانی عمومی در سایت و معرفی شرکت‌ها و محصولات دارنده نشان کیفیت.

این حق مسلم شماست که کالای با کیفیت و با خدمات معتبر خریداری کنید

با نشان کیفیت مرکز تحقیقات صنایع انفورماتیک این اطمینان محقق می گردد.