



تحقیق رویکرد جدید DevSecOps

The infographic features a central black padlock surrounded by two large circles filled with white gears. To the left is a circle containing the word "DEV" and silhouettes of two people at a desk. To the right is a circle containing the word "OPS" and silhouettes of two people at a desk. Between the circles are various icons: a bar chart labeled "PLAN", a code bracket labeled "</CODE>", a wrench and screwdriver, a rocket launching from a desk, and three gears. At the bottom, there is a triangle containing the text: "سرقت داده‌ها بدون اتصال به شبکه", "احراز هویت ضعیف در دستگاه‌های IoT", and "قابلیت‌های پروتکل امنیتی WPA3".

DEV OPS

PLAN

</CODE>

WPA3

IoT

سرقت داده‌ها بدون اتصال به شبکه

احراز هویت ضعیف در دستگاه‌های

قابلیت‌های پروتکل امنیتی



دانشمند

روشی برای تأمین امنیت دستگاه‌های متصل به IoT به کارگیری شیوه امضای کد در نرم‌افزارها

به منظور ایجاد اعتماد و اطمینان در دنیاپری تحت سلطه نرم‌افزارها است، به فرایندی بی‌نقص برای احراز هویت کدها نیاز است؛ به همین دلیل، سازمان‌ها روزه‌روز بیشتر به شیوه امضای کد روی می‌آورند. در شیوه امضای کد، فایل‌های اجرایی و اسکریپت‌ها به صورت دیجیتالی امضا می‌شوند تا سازنده نرم‌افزار تأیید شود و ضمین گردد که کدها پس از امضا شدن، دستکاری و مخدوش نشده‌اند.

صفحه ۸

آسیب‌پذیری

بررسی یکی از مهم‌ترین تهدیدات اینترنت اشیا: احراز هویت ضعیف در دستگاه‌های IoT

یکی از مشکلات امنیتی در دستگاه‌های اینترنت اشیا (IoT)، به کارگیری شیوه‌های احراز هویت ضعیف، به خصوص استفاده از گذر واژه‌های پیش‌فرض است. از روش‌های مختلفی می‌توان برای اجتناب از کاربرد گذر واژه‌های پیش‌فرض استفاده کرد، مانند تعیین مک‌آدرس به عنوان گذر واژه، تغییر اجباری گذر واژه و تعیین گذر واژه‌های تصادفی.

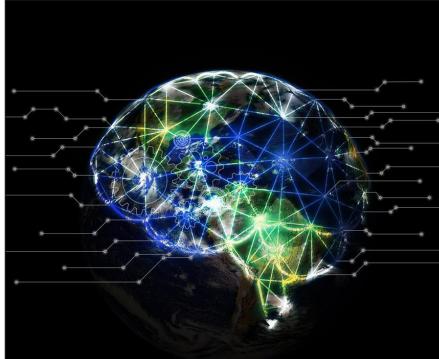
صفحه ۶

آسیب‌پذیری

چهار روش برای هک رایانه‌های دارای شکاف هوایی: سرقت داده‌ها بدون اتصال به شبکه

هکرها رایانه‌های دارای شکاف هوایی را به عنوان هدایتی بالرزش می‌شناسند. از این رو، پژوهش‌های گسترده‌ای برای کشف شیوه‌های استخراج داده‌ها از این سیستم‌ها، بدون اتصال به شبکه، صورت گرفته‌اند.

صفحه ۴



دانشمند

تأمین امنیت شبکه‌های توزیع برق: به کارگیری یادگیری ماشین و حسگرهای پیشرفته

امروزه، با افزایش حملات سایبری به شبکه‌های برق، اهمیت امنیت در این شبکه‌ها نیز افزایش یافته است. فناوری‌های جدیدی چون حسگرهای پیشرفته و یادگیری ماشین به اپراتورهای شبکه‌های توزیع برق کمک می‌کند تا شبکه‌های خود را در برابر حملات سایبری مقاوم سازند.

صفحه ۱۶

دانشمند

افزایش امنیت و سرعت شبکه‌های بی‌سیم: قابلیت‌های پروتکل امنیتی WPA3

در آینده نزدیک با به کارگیری پروتکل امنیتی جدید وای‌فای WPA3، سرعت و امنیت شبکه‌های بی‌سیم افزایش می‌یابد. WPA3 قرار است مشکلات شناخته شده WPA2 که امروزه تقریباً در تمام دستگاه‌های بی‌سیم وجود دارد را رفع کند.

صفحه ۱۴

دانشمند

بررسی آینده امنیت IoT در دستگاه‌های کوچک: تأمین امنیت اینترنت اشیا با تولید سخت‌افزارهای قابل به‌روزرسانی

نمایم آسیب‌پذیری‌های امنیتی را تنها از طریق اصلاح نرم‌افزار رفع کرد. تنها راه برای رفع چنین مشکلی، استفاده از سخت‌افزارهایی است که بتوان آن را پس از ساخت، مجدداً پیکربندی نمود.

صفحه ۱۰



دانشی

دانشی

ضرورتی در اقتصاد کسبوکارهای امروزی:

تحقیق رویکرد جدید DevSecOps

افزایش مخاطرات در فضای کسبوکار، موضوع امنیت را در صدر اولویت‌های رهبران سازمان‌ها جای داده است. در نتیجه، شمار روزافزونی از سازمان‌ها به استفاده از رویکرد DevSecOps روی آورده‌اند تا بتوانند با این مخاطرات، مقابله کنند. DevSecOps بر اساس رویکرد مشهور DevOps بنا شده است؛ اما امنیت را نیز در چرخه توسعه و آزمایش، وارد می‌کند و برنامه‌های کاربردی سریع‌تر، باکیفیت‌تر و امن‌تری را تولید می‌نماید.

صفحه ۲۱

صفحه ۱۸

معرفی یک فناوری:

زیرساخت جابجایی پذیری مبتنی بر بافتار

مفهوم زیرساخت جابجایی پذیری مبتنی بر بافتار بر اساس درخواست جهانی برای پشتیبانی بهتر از جابجایی پذیری در سیستم‌های اسکادا و مدیریت ساختمان توسعه یافت. این فناوری سبب استفاده بینهایت از موابع انسانی می‌شود. کاهش زمان مورد نیاز برای راهاندازی یک سیستم جدید را می‌توان از بهبودهای مهم در این حوزه دانست.



آلوگی سرورهای Redis به بدافزار

بنابر گزارش‌ها، ۷۵ درصد سرورهای Redis به بدافزار آلوگه شده‌اند. وبسایت در پاسخ به علت این الودگی اعلام کرد Redis برای دسترسی کلاینت‌های Redis مورد اعتماد در محیط‌های مطمئن طراحی شده است و نایاب قوّاً و مستقیماً در اینترنت یا در محیط‌هایی که کلاینت‌های نامطمئن مستقیماً آن‌ها دسترسی دارند، قرار گیرد. در اتفاقی که حداقل امنیت خدمات نیست (به عنوان مثال امنیتی Redis)، آن‌ها ممکن است از همان سرویسها برای حملات مخرب استفاده کنند.

دانشی

آسیب‌پذیری

بدافزار

خبر کوتاه

- ۱- آلوگی سرورهای Redis به بدافزار
- ۲- آسیب‌پذیری سرورهای کدباز
- ۳- آسیب‌پذیری برنامه‌های کاربردی
- ۴- بی‌اعتمادی توسعه‌دهندگان به امنیت کدهای خود
- ۵- امنیت کدهای شخص ثالث
- ۶- تهدیدات توحالی حملات فیشنینگ جدید
- ۷- وضعیت بدافزارها در سال ۲۰۱۷
- ۸- افزایش حملات DDoS
- ۹- افزایش مخاطرات سیستم‌های کنترل صنعتی به IoT
- ۱۰- تهدیدات ناشی از سیستم‌های کنترل صنعتی در سازمان‌ها
- ۱۱- مشکلات امنیتی هات‌اسپات‌های وای‌فای در جام جهانی فوتبال
- ۱۲- بی‌توجهی کسبوکارها به تدوین راهبرد امنیتی مناسب

صفحه ۲۴

سرقت داده‌ها بدون اتصال به شبکه



استخراج اطلاعات را در بر می‌گیرند؛ از شنود روى امواج ساطع شده از گذرگاه حافظه^۲ گرفته تا نشت از کابل‌ها و پورت‌های USB. کanal الکترومغناطیسی، اولین کanalی بود که به طور گستردۀ مورد بررسی و استفاده قرار گرفت و باعث رواج استفاده از محافظه‌ای امواج الکترومغناطیس به عنوان یک اقدام پیشگیرانه شد.

کanal‌های صوتی پس از پیدایش گوشی‌های هوشمند رواج یافتند. میکروفون‌های این گوشی‌ها می‌توانند طیفی از امواج صوتی را که انسان‌ها قادر به تشخیص آن از صدای همهمه پس زمینه نیستند، جدا و ضبط کنند. جدیدترین دستاوردها، استفاده از امواج فرماصوتی است که به خاطر فرکانس بالا، قابل شنیدن نیستند و همچنین پهنهای باند بیشتری دارند.

قبلًا مواردی از هک‌های حرارتی مشاهده شده است، اما پهنهای باند آن‌ها به چند ۱۰ بیت در ثانیه از فاصله کوتاه محدود می‌شود. از این رو، معلوم نیست آیا انتقال حرارتی در آینده به عنوان کanalی مخفی کاربرد خواهد داشت یا خیر.

هک‌ها رایانه‌های دارای شکاف هوایی^۱ را به عنوان اهدافی باارزش می‌شناسند. از این رو، پژوهش‌های گستردۀای برای کشف شیوه‌های استخراج داده‌ها از این سیستم‌ها، بدون اتصال به شبکه، صورت گرفته‌اند.

پژوهشگران به تازگی روش‌های جدیدی برای استخراج داده‌ها از سیستم‌های رایانه‌ای از طریق کanal‌های پنهان ایجاد کرده‌اند. این کanal‌ها به چهار دسته کلی تقسیم می‌شوند:

- کanal‌های الکترومغناطیسی (اولین نوع بردارهای حمله)
 - کanal‌های صوتی (علاوه بر بلندگوها، می‌توان از صدای فن و دیسک درایو نیز استفاده کرد)
 - کanal‌های حرارتی (در سرعت‌های بسیار پایین امکان پذیر است)
 - کanal‌های نوری (یک حوزه جدید و جذاب که سرعت آن به چهار کیلو بیت در ثانیه می‌رسد)
- کanal‌های الکترومغناطیسی، طیف گستردۀای از شیوه‌های

از شبکه‌های دارای شکاف هوایی از طریق نشانگر LED حالت ثابت^۲، نشان دادند که می‌توان از LED‌های معمولی کیبورد مانند چراغ دکمه‌های caps lock و num lock بدون اطلاع کاربر و از طریق دوربین‌های IP برای استخراج داده‌ها استفاده کرد. همانند سایر کانال‌های ارتباطی، روش کدگذاری سیگنال، کلید دستیابی به بالاترین عملکرد و اطمینان از یک پنهانی باند محدود است. در روش ساده کلیدگذاری روشن یا خاموش^۳ (OOK)، زمانی که چراغ خاموش است، معادل رقم صفر و زمانی که روشن است، نشان‌دهنده رقم یک است. مشکل اینجا است که دوربین‌های نظارتی معمولاً با سرعت ۱۵ فریم در ثانیه کار می‌کنند و این سرعت، پنهانی باند داده‌ها را محدود می‌کند. البته، کاربران نیز ممکن است مشکوک شوند که چرا LED‌های کیبوردشان بدون هیچ دلیلی روشن و خاموش می‌شوند. پژوهشگران در این رابطه توضیح دادند: «ما در رویکرد خود از روش کلیدگذاری تغییر فرکانس باینری^۴ (B-FSK) برای ایجاد سیگنال استفاده کردیم. ما می‌توانیم از یک فرکانس چشمک ۴۰ برای کدگذاری صفر منطقی (۰) و از یک فرکانس چشمک دیگر f1 برای کدگذاری یک منطقی استفاده کنیم». با این حال، یک مشکل دیگر نیز وجود دارد: وقتی LED در یکی از دو حالت روشن یا خاموش قرار دارد یا به عبارت دیگر، وقتی LED حالت ثابت دارد، چگونه می‌توان فرکانس چشمک را ایجاد کرد؟ این تیم پژوهشی متوجه شد اگر یک LED که در حالت عادی روشن است به مدت کمتر از ۵۰ میلی ثانیه خاموش شود، چشم انسان نمی‌تواند چشمک را تشخیص دهد. در نتیجه می‌توان دو الگوی چشمک متفاوت را برای یک LED که همیشه روشن است، اجرا کرد. بزرگ‌ترین نقطه ضعف این روش آن است که سرعت آن ۱۲ بیت در ثانیه است. اما اگر داده‌ها ارزش بالایی داشته باشند، مانند داده‌های مربوط به یک کلید رمزگذاری، همین سرعت نیز کافی است.

سرقت داده‌های ذخیره‌شده

سازندگان سیستم‌های ذخیره‌سازی، اغلب بر رمزگذاری داده‌های بایگانی شده تأکید دارند. از این رو، نمی‌توان درایوی را دزدید و به داده‌های روی آن دسترسی پیدا کرد. اما مشکل اصلی این نیست، به ویژه اگر داده‌ها روی چند درایو مختلف تقسیم شوند. در واقع، مشکل زمانی ایجاد می‌شود که داده‌ها در حال انتقال هستند، تایپ می‌شوند، نمایش داده می‌شوند یا پردازش می‌گردند. LED‌ها ابزارهای پرکاربردی هستند، اما ظاهراً استفاده از آن‌ها در نمایشگرهای کیبوردها، سوییچ‌ها و درایوهای رایانه‌ای باعث بروز مشکلات امنیتی می‌شود. با توجه به فرآگیری استفاده از LED‌ها، تمام تجهیزاتی که تحت نظارت دوربین‌های مداربسته قرار دارند، در معرض خطر شنود هستند.

منبع: www.zdnet.com

جدیدترین حوزه، استخراج اطلاعات از طریق انتقال نوری بوده است. پس از پیدایش دوربین‌های نظارتی که بسیار فرآگیر شده‌اند و به راحتی هم هک می‌شوند، LED‌هایی که تقریباً روی همه سیستم‌های نظارتی وجود دارند، می‌توانند حجم چشمگیری از داده‌ها را انتقال دهند. امروزه، سه نوع LED در تجهیزات رایانه‌ای مورد استفاده قرار می‌گیرند:

- LED‌های حالت ثابت^۳ که وضعیت دستگاه مانند روشن بودنش را نشان می‌دهند.

- LED‌های پالس‌دار^۴ که سطح فعالیت دستگاه را نشان می‌دهند.

- LED‌های حالت متغیر^۵ که محتوای داده‌های در حال پردازش را نشان می‌دهند.

چشم انسان به سختی می‌تواند تغییرات نوری بالای ۶۰ هرتز را تشخیص دهد. از این رو، کاربران نمی‌توانند تشخیص دهنند آیا LED به صورت پنهانی مورد سوءاستفاده قرار می‌گیرد یا خیر. البته، بسیاری از دستگاه‌های مصرفی مانند آیفون ایکس جدید به LED‌های مادون قرمز (IR) مجهز هستند که برای انتقال یا دریافت داده‌ها به صورت نامرئی طراحی شده‌اند.

LED‌های افشاکننده

بسیاری از دستگاه‌های شبکه از LED‌ها برای نشان دادن فعالیت داده‌ها استفاده می‌کنند و اگر کسی به نمونه‌های کافی برای تشخیص الگوی آن‌ها دسترسی داشته باشد، می‌تواند ترافیک در حال عبور از آن‌ها را به دست آورد. اگر دستگاهی قابل‌هک باشد، که البته امروزه تقریباً همه دستگاه‌ها قابل‌هک هستند، LED‌ها می‌توانند داده‌های بسیار خاص‌تری را افشا کنند. LED‌هایی که فعالیت درایو حافظه را نشان می‌دهند، می‌توانند با استفاده از دوربین‌های نظارتی مداربسته به عنوان گیرنده‌های نوری، داده‌ها را تا سرعت چهار کیلو بیت در ثانیه انتقال دهند. این سرعت به اندازه‌ای بالا است که می‌تواند کلیدهای رمزگذاری، الگوی فشردن کلیدهای کیبورد و فایل‌های باینری و متنی را به راحتی انتقال دهد. چراغ‌های درایو معمولاً در حین اجرای عملیات، چشمک می‌زنند، در نتیجه کاربران نمی‌توانند چشمک‌های اضافی را در حین سرقت داده‌ها تشخیص دهند. از آنجا که درایوهای دارای پردازشگرهای کوچکی هستند که در کنترلهای اینترنتی شده است، بی‌شک قابل‌هک هستند. اخیراً قابلیت کانال‌های پنهان در LED‌های چاپگرها نیز کشف شده است. در کل، تمام دستگاه‌هایی که LED و پردازشگر دارند، قابل‌هک هستند.

نشانگرهای حالت ثابت

حال این سؤال پیش می‌آید که در صورت استفاده از ابتدایی‌ترین نوع LED، یعنی نشانگرهای حالت ثابت وضعیت، چه اتفاقی می‌افتد؟ اخیراً جمعی از پژوهشگران در مقاله‌ای با عنوان «استخراج داده‌ها

unmodulated LEDs -۳

time modulated LEDs -۴

modulated LEDs -۵

-۶

Exfiltration of Data from Air-gapped Networks via Unmodulated LED Status Indicators -۶

On-Off Keying -۷

Binary Frequency Shift Keying -۸

احراز هویت ضعیف در دستگاه‌های IoT



در همایش هفته افتای اینترنت سنگاپور^۱ (SICW)، یکی از بزرگ‌ترین همایش‌های افتای در منطقه جنوب شرقی آسیا، برای نخستین بار یک بخش مجزا به موضوع اینترنت اشیا اختصاص داشت. یکی از جلسات مهم این بخش، نشستی اختصاصی بود که با دعوت از متخصصین امنیت IoT برگزار شد. این نشست به اندازه‌ای جذاب بود که چهار ساعت به طول انجامید. گروه‌هایی از یکی از مشکلات امنیتی در دستگاه‌های اینترنت اشیا (IoT)، به کارگیری شیوه‌های احراز هویت ضعیف، به خصوص استفاده از گذر واژه‌های پیش‌فرض است. از روش‌های مختلفی می‌توان برای اجتناب از کاربرد گذر واژه‌های پیش‌فرض استفاده کرد، مانند تعیین مک‌آدرس به عنوان گذر واژه، تغییر اجباری گذر واژه و تعیین گذر واژه‌های تصادفی.

گذر واژه های تصادفی

قوی ترین روش این است که سازنده برای تمام دستگاهها، یک گذر واژه تک و منحصر بفرد تعیین کند. این امن ترین روش است، اما پرهزینه ترین روش برای سازنده نیز به شمار می آید. علاوه بر این، در این روش نیز همان مشکلی وجود دارد که در دو روش اول وجود داشت: مقیاس.

در دسر مقیاس پذیری^۲

در پروژه های بزرگ، هزاران دستگاه متصل به IoT در مقیاسی گسترده به کار گرفته می شوند. برای مثال، تجهیزات دفاتر شرکت های بزرگ را در نظر بگیرید؛ یا پیمانکارانی که چنین دستگاه هایی را در یک مرکز خرید جدید تعییه می کنند. فروگاه Changi در سنگاپور بیش از ۱۰ هزار دوربین ویدئویی متصل به IoT دارد. تصور کنید باید ۱۰ هزار گذر واژه منحصر بفرد این دستگاه ها را مدیریت کنید. البته، راه حل هایی برای رفع مشکل مدیریت گذر واژه ها وجود دارند، مانند راه حل های مدیریت حساب های دارای امتیاز، اما نمی توان تمام دستگاهها را به این شکل مدیریت کرد. اگر گذر واژه های منحصر بفردی برای هر دستگاهی تعیین کرده اید و سعی دارید آن ها را مدیریت نمایید، این قضیه خیلی خوب است؛ چون شما حداقل دارید تلاشتان را می کنید.

راه حلی جدید برای IoT

برای حل این مسئله، در همایش SICW یک راه حل جدید با نام پروژه شبکه داده های نام گذاری شده^۳ (NDN) مطرح شد. NDN برای شبکه هایی مانند اینترنت اشیا طراحی شده است و امکان اتصال امن دستگاه هایی را که سطح رایانش پایینی دارند، از پهنای باند پایینی بهره می بردند و توان کمی دارند، فراهم می آورد. این پروژه، امنیت شبکه را از طریق یک الگوی نام گذاری تأمین می کند که به عنوان یک management plane و کنترل دسترسی عمل می کند و به استفاده از گذر واژه نیاز ندارد. NDN از پروتکل استاندارد اینترنت بسیار متفاوت است. از این رو، نمی توان پیش بینی کرد که آیا این پروژه می تواند در سیستم های اینترنت اشیای امروزی به خوبی کار کند یا خیر. اگر قرار است تا سال ۲۰۲۵ بیش از ۵۰ میلیارد دستگاه IoT وجود داشته باشد، بد نیست این دستگاهها از زیر ساخت امنیتی مختص خود برخوردار باشند؛ زیر ساختی که متفاوت از زیر ساخت هایی است که افراد یا حداقل لپ تاپ ها و گوشی ها را مدیریت می کنند.

اما به موضوع مدل سازی تهدیدات IoT برگردیم. پروژه اینترنت اشیای شما باید مشکل گذر واژه پیش فرض را در اولویت های بالا قرار دهد. مدیریت راه حل های حذف استفاده از گذر واژه های پیش فرض به صورت تکی، کار راحتی است، اما در مقیاس گسترده بسیار دشوار می شود. بنابراین، مقیاس پذیری را نیز در نظر بگیرید.

منبع: www.securityweek.com

برنامه ریزان شهری پروژه های Smart Nation در کشورهای آسیایی نیز در سخنرانی هایی پیرامون مدل سازی تهدیدات IoT حضور پیدا کردند. همان طور که می دانید، مدل سازی تهدیدات برای IoT دارای سه مرحله است: تهیه فهرست دارایی ها، شناسایی تهدیداتی که متوجه این دارایی ها هستند و رتبه بندی این تهدیدات. اما مهم ترین تهدیدی که میان تمام دستگاه های متصل به IoT در سطح مصرف کنندگان، مشترک است، احراز هویت ضعیف است.

به گفته یکی از پژوهشگران، IoT زیر ساختی است که از انبوهی از سازو کارهای ضعیف احراز هویت ساخته شده است. وی هزاران دستگاه متصل به IoT را به مدت یک سال پایش کرده است. در این مدت، درصد دستگاه هایی که از گذر واژه های پیش فرض استفاده می کنند، روی رقم ۶۰ درصد ثابت مانده است؛ واقعاً رقم بسیار زیادی است. برآوردهای دیگر هم رقمی بین ۱۵ تا ۵۰ درصد را نشان می دهند. مجلس سنای آمریکا سعی دارد این وضعیت را از طریق لایحه ارتقای افتتا در اینترنت اشیا بر طرف کند. بسیاری از کارشناسان امنیتی، این لایحه را اقدام بسیار خوبی می دانند که می تواند الگویی برای دیگر سیستم های حقوقی در سراسر جهان باشد. یکی از مفاد مهم این استفاده می کنند، منع می کند. سازندگان دستگاهها در حال حاضر از روش های مختلفی برای اجتناب از کاربرد گذر واژه های پیش فرض استفاده می کنند. از برخی از این روش ها در مودم های خانگی نیز استفاده شده است؛ چرا که در دهه ۲۰۰۰، همین مشکلات امنیتی در این دستگاه ها نیز وجود داشت. در ادامه به سه روش رایج برای اجتناب از کاربرد گذر واژه های پیش فرض می پردازیم.

انتخاب مک آدرس به عنوان گذر واژه

برخی از سازندگان، مک آدرس مربوط به واسطه دستگاه را به عنوان گذر واژه پیش فرض انتخاب می کنند. پژوهشگران حوزه امنیت، این روش را تأیید نمی کنند، زیرا تمام افرادی که روی یک شبکه محلی هستند، مک آدرس را می بینند. در نتیجه، نمی توان این روش را کاملاً امن دانست. با این حال، اکثر botnet هایی که در بازار وجود دارند، از پوششگرهایی استفاده می کنند که نمی توانند مک آدرس را ببینند. به هر حال این روش بهتر از استفاده از گذر واژه های پیش فرض است.

تغییر اجباری گذر واژه

یکی دیگر از روش های اجتناب از کاربرد گذر واژه های پیش فرض آن است که صاحب دستگاه را مجبور به تغییر گذر واژه در هنگام پیکربندی دستگاه کرد. اگرچه این روش نیز بهتر از استفاده از گذر واژه های پیش فرض است، اما مصرف کنندگان نیز نمی توانند گذر واژه های خوبی انتخاب کنند. فهرست گذر واژه های پر کاربرد از فهرست گذر واژه های پیش فرض دستگاه های IoT طولانی تر نیست.



روشی برای تأمین امنیت دستگاه‌های متصل به IoT:

به کارگیری شیوه امضای کد در نرم‌افزارها

از شرکا، کاربران و مصرف‌کنندگان آن‌ها نیز در برابر تهدیدات دیجیتال که روزبه‌روز بیشتر متحول می‌شوند، حفاظت می‌نماید. دستکاری کردن نرم‌افزار مخاطرات مختلفی به همراه دارد که با گسترش به کارگیری ابر و اینترنت اشیا (IoT) توسط مصرف‌کنندگان و کسبوکارها، روزبه‌روز افزایش می‌یابند. به منظور ایجاد اعتماد و اطمینان در دنیایی که دیگر احراز هویت کدها نیاز است؛ به همین دلیل، سازمان‌ها روزبه‌روز بیشتر به شیوه امضای کد^۱ روی می‌آورند. در شیوه امضای کد، فایل‌های اجرایی و اسکریپت‌های صورت دیجیتالی امضا می‌شوند تا سازنده نرم‌افزار تأیید شود و تضمین گردد که کدها پس از امضا شدن، دستکاری و مخدوش نشده‌اند.

برای احراز هویت کدها نیاز دارند.

امضای کد، در اصل روشی برای اثبات منشأ و یکپارچگی^۲ یک فایل

به منظور ایجاد اعتماد و اطمینان در دنیایی که دیگر تحت سلطه نرم‌افزارها است، به فرایندی بی‌نقص برای احراز هویت کدها نیاز است؛ به همین دلیل، سازمان‌ها روزبه‌روز بیشتر به شیوه امضای کد^۱ روی می‌آورند. در شیوه امضای کد، فایل‌های اجرایی و اسکریپت‌های صورت دیجیتالی امضا می‌شوند تا سازنده نرم‌افزار تأیید شود و تضمین گردد که کدها پس از امضا شدن، دستکاری و مخدوش نشده‌اند.

شیوه امضای کد علاوه بر این که از سازمان‌ها حفاظت می‌کند،

پژوهشگران اظهار داشته‌اند که برخی عیوب امنیتی در مدل‌های جدید وسایل نقلیه وجود دارد که به عنوان مخاطرات نوین ناشی از اتصال دائمی به شبکه شناخته می‌شوند؛ در نتیجه، این مخاطرات ممکن است خود را به شکل مخاطرات ایمنی در جاده‌ها نیز نشان دهد.

است. این فرایند مستلزم امضا کردن دیجیتالی فایل‌های اجرایی و اسکریپت‌ها است تا سازنده نرم‌افزار تأیید شود و تضمین گردد که کدها پس از امضا شدن، دستکاری یا مخدوش نشده‌اند. این فرایند، اعتبار احراز هویت کدهای جدید را تأیید می‌کند و همچنین، تضمین می‌نماید که منشأ کدها از یک تأمین‌کننده معتر و قانونی است.

اجتناب از ریسک پذیری

ترکیب اتصالات شبکه که به سرعت در حال گسترش هستند با فناوری‌های پیشرفته‌ای که توسط مجرمان سایبری به کار گرفته می‌شوند، باعث شده است مهاجمان بتوانند پس از دسترسی یافتن به یک آسیب‌پذیری، به سیستم‌های دیگر نیز نفوذ کنند.

این دستاوردها نشان می‌دهند که اگر امضای کد به درستی صورت نگیرد و از تجربیات برتر نیز استفاده نشود، این دو در کنار هم سازمان‌ها را با این خطر مواجه می‌کنند که مجرمان شکل‌های مخرب کدها را از طرف آن‌ها منتشر نمایند.

در نهایت، حفاظت از یک کلید امضای خصوصی همان چیزی است که یک سیستم امضای کد را سر پا نگه می‌دارد یا آن را به زمین می‌زند. بیشتر اوقات، این کلیدها در دست برنامه‌نویسانی است که به اندازه کافی روی امنیت تمرکز نمی‌کنند.

حفاظت از این کلیدهای امضای خصوصی در یک مازول امنیتی سخت‌افزاری^۳ (HSM) و همچنین، پیاده‌سازی کنترل‌های دسترسی مناسب و بررسی تأییدیه‌ها، باعث می‌شود حفاظتی قدرتمندتر نسبت به شیوه امضای کد مرسوم که در آن کلیدهای واقع در نرم‌افزار آسیب‌پذیرتر هستند، فراهم گردد.

مهم‌تر از همه، سازمان‌ها باید سیستم‌هایی امن برای امضای کد ایجاد کنند که برنامه‌نویسان را ملزم می‌سازد برای مدیریت کلیدهای رمزگذاری با استفاده از HSM‌ها برنامه‌ریزی کنند و تجربیات برتر حوزه رمزگاری را پیاده‌سازی نمایند.

دفع در برابر حملات و از دست داده‌ها از طریق پیروی از تجربیات برتر و به دنبال آن، ایجاد شبکه‌ای از دستگاه‌های قابل اعتماد متصل به IoT، از طرف دیگر کاهش هزینه‌های عملیاتی از طریق کنترل و پایش دستگاه‌هایی که در مناطق جغرافیایی مختلف پراکنده هستند و در نهایت، حفاظت از جریان‌های درآمدی و شهرت و اعتبار سازمان از طریق حفاظت از دستگاه‌های تولیدی، همه و همه بخش‌هایی حیاتی از یک راهبرد افتای مؤثر هستند که برای رفع مخاطرات IoT طراحی شده است.

هر روز شاهد تحقق بیشتر دگرگی‌سی دیجیتال^۴ در زندگی روزمره مصرف‌کنندگان هستیم و از همین رو، نرم‌افزارها به تدریج در همه تعاملات روزمره ما حضور پیدا می‌کنند. با این حساب، شیوه امضای کد، کلید شکوفا‌سازی پتانسیل واقعی IoT و همچنین، تضمین امنیت و ایمنی در ارتباط با دستگاه‌ها است.

اگر امضای کد به درستی اجرا شود، یکی از قدرتمندترین سلاح‌های صنعت افتتا محسوب می‌شود که برای کاهش و پیشگیری از بروز مخاطرات مورد استفاده قرار می‌گیرد. از این رو، جای تعجب ندارد که سازمان‌های سراسر جهان روزی‌روز بیشتر به شیوه امضای کد به عنوان یک رویکرد برگرفته از تجربیات برتر برای حفاظت از کسب‌وکار و برندهای خود در برابر مخاطرات نرم‌افزارهای آلوده روی می‌آورند.

سال‌ها است که بسیاری از نقش‌آفرینان بزرگ در صنعت فناوری از طرفداران علمی و پژوهشی پیاده‌سازی شیوه امضای کد هستند و شرکت‌هایی مانند مایکروسافت، اپل و گوگل همچنان شرکت‌ها را به سمت استفاده از روش‌های قدرتمندتر و قابل اتکاتر امضای کد تشویق می‌کنند؛ به ویژه به این خاطر که تقریباً تمام دستگاه‌های الکترونیکی جدید به اینترنت متصل هستند. دستگاه‌هایی مانند تلویزیون‌های هوشمند، کنسول‌های بازی و دستگاه‌های پایش تناسب اندام، همه از شیوه امضای کد به عنوان تجربیات برتر استفاده می‌کنند تا قبل از به کارگیری نرم‌افزار جدید توسط دستگاه، از اعتبار و اصالت نرم‌افزار مطمئن شوند. این سازمان‌ها با پیاده‌سازی سیاست‌های امضای کد، از نرم‌افزارها در مقابل مخدوش شدن حفاظت می‌کنند و این امکان را فراهم می‌آورند که روی فعالیت‌های انتشار نرم‌افزار، کنترل و نظارت مناسبی وجود داشته باشد.

تأثیر امضای کد روی IoT

سازمان‌ها تازه در حال کشف مزایا و فرصت‌های حاصل از IoT هستند؛ از این رو، شاهد افزایش دستگاه‌های متصل به شبکه هستیم که کارکردهای ارزشمندی را فراهم می‌آورند تا بتوانند جریان‌های جدیدی برای درآمد ایجاد نمایند و هزینه‌ها را کاهش دهند. با این حال، علی‌رغم مزایای IoT، مخاطرات امنیتی آن و خطرات مرتبط با استفاده گسترده از کدهای مخرب، حالا واقعی هستند و به همین علت، استفاده از شیوه امضای کد اجتناب‌ناپذیر است.

به گفته گارتنر، تا سال ۲۰۲۰ در سراسر جهان حدود ۲۱ میلیارد دستگاه متصل به شبکه وجود خواهد داشت و انتظار می‌رود این رقم تا سال ۲۰۲۵ به ۸۰ میلیارد دستگاه برسد. در نتیجه، همچنان هر روز سازمان‌ها را در معرض آسیب‌پذیری‌های امنیتی جدید و در حال تغییر قرار خواهد داد.

از آن گذشته، این مخاطرات به گوشی‌های همراه یا محصولاتی که در خانه‌های متصل به شبکه^۵ وجود دارند، محدود نیستند.

تأمین امنیت اینترنت اشیا با تولید سخت افزارهای قابل به روزرسانی



DDoS، حملات نسبتاً شایعی هستند. اما این حمله دو ویژگی داشت که آن را از سایرین تمایز می‌کرد. ویژگی اول این بود که باعث اختلال در خدمات یک ارائه‌دهنده بزرگ DNS شد و توanst وебسایت‌های زیادی را از دسترس خارج کند. ویژگی دوم این بود که درخواست‌های جعلی، از باتن‌های معمول روی رابطه‌های رومیزی و لپ‌تاپ‌های آلوهه ارسال نشده بودند، بلکه این حمله از طریق دهها میلیون دستگاه کوچک متصل به اینترنت اجرا شده بود؛ دستگاه‌هایی مانند مسیریاب‌های خانگی و دوربین‌های متصل به اینترنت که در واقع اجزای اینترنت اشیا (IoT) محسوب می‌شوند. در چند سال اخیر، تعداد اشیای متصل به اینترنت از جمله گوشی‌ها، ساعت‌های هوشمند، دستبند‌های تناسب اندام، ترمومترات‌های خانگی و حسگرهای مختلف، از جمعیت انسان‌ها بیشتر شده است. تا سال ۲۰۲۰، دهها میلیارد از این ابزارهای آنلاین وجود خواهد داشت. رشد روزافزون اینترنت اشیا نشان از سریع‌ترین رشد اقتصادی تاریخ تمدن انسان‌ها دارد. این پیشرفت سریع، فرصت بزرگی برای مهندسان و در کل، برای جامعه فراهم می‌آورد. اما این

متخصصین به این نتیجه رسیده‌اند که نمی‌توان تمام آسیب‌پذیری‌های امنیتی را تنها از طریق اصلاح نرم‌افزار رفع کرد. تنها راه برای رفع چنین مشکلی، استفاده از سخت افزارهایی است که بتوان آن را پس از ساخت، مجدداً پیکربندی نمود.

در ۲۱ اکتبر سال ۲۰۱۶، چند وебسایت بزرگ و معتبر از جمله توییتر، پی‌پل، اسپاتیفای، نتفلیکس، نیویورک‌تایمز و روزنامه وال استریت جورنال از دسترس خارج شدند. علت این وقفه، یک حمله DDoS بود. البته این حمله، خود وебسایت‌ها را هدف نگرفته بود و به ارائه‌دهنده سامانه نام دامنه^۱ (DNS) این وебسایت‌ها و بسیاری از وебسایت‌های دیگر حمله کرده بود. DNS، نام وебسایت‌ها را به آدرس عددی آن‌ها در اینترنت ترجمه می‌کند. ارائه‌دهنده DNS در این مورد، شرکتی به نام Dyn بود که سرورهایش با چنان حجمی از درخواست‌های جعلی برای جستجوی DNS روبرو شدند که نتوانستند به جستجوهای واقعی DNS پاسخ دهند. حملات

این تعاملات دسترسی پیدا کند، می‌تواند به برخی از شخصی‌ترین اطلاعات شما دسترسی یابد.

یکی دیگر از مسائل نگران‌کننده در مورد حمله به این دستگاه‌ها، تعامل آن‌ها با دنیای فیزیکی است. اگر یک دستگاه تواند هوشمند در خانه یا حسگرهای یک کارخانه هک شوند، می‌توانند منجر به پیامدهای فاجعه‌آمیزی شوند که روی ماشین‌های تحت کنترل نیز تأثیر می‌گذارند. سازوکارهای مرسومی که از آن‌ها برای حفظ امنیت رایانه‌ها استفاده می‌شد، دیگر کارایی نخواهد داشت. زیرا بیشتر این سازوکارهای حفاظتی که برای لپ‌تاپ‌ها، رایانه‌های رومیزی، سرورها و حتی گوشی‌ها طراحی شده‌اند، انرژی زیادی مصرف می‌کنند. در نتیجه برای دستگاه‌های کوچکی مانند یک ساعت یا یک حسگر که باید با انرژی کمی کار کنند، مناسب نیستند. علاوه بر این، سازوکارهای حفاظتی معمولاً برای آن دسته از سیستم‌های رایانشی طراحی شده‌اند که تنها برای چند سال کار می‌کنند. کاربران معمولاً رایانه‌های رومیزی و لپ‌تاپ‌های خود را هر سه تا چهار سال یک بار و گوشی‌ها و تبلت‌هایشان را حتی در فواصل کوتاه‌تر، تعویض می‌کنند. اما یک خودروی هوشمند، کنتور برق متصل به اینترنت یا چراغ راهنمایی هوشمند ممکن است عمر بسیار طولانی‌تری داشته باشد و در برخی موارد حتی تا ده سال مورد استفاده قرار بگیرد. در نتیجه نمی‌توان انتظار داشت که با جایگزین کردن دستگاه‌ها، مشکلات امنیتی دستگاه‌های قدیمی رفع شود. سازندگان دستگاه‌ها نیز نمی‌توانند پیش‌بینی کنند دستگاه‌هایشان به چه نوع منابع سخت‌افزاری خاصی نیاز خواهند داشت تا بتوانند حملاتی را که در آینده دور با آن‌ها مواجه می‌شوند، خنثی کنند.

امروزه حتی نمی‌توان تصور کرد که از این دستگاه‌ها دقیقاً چگونه استفاده خواهد شد، چه برسد به این که بتوان پیش‌بینی کرد در ۱۰ تا ۲۰ سال آینده چه تهدیداتی وجود خواهد داشت. شاید تا آن زمان، یخچال شما با خودروی بدون راننده شما به تعامل بپردازد و بتواند به صورت خودکار خواروبار مورد نیاز شما را تحويل بگیرد. اما چراغ هوشمند آشپزخانه شما که به آن نفوذ شده است نیز می‌تواند ارتباطات بین یخچال و خودرو را شنود کند و اطلاعات را دستکاری نماید. ما برای پیش‌بینی موارد کاربری انواع ابزارهای هوشمند در آینده یا پیامدهای نفوذ به آن‌ها اطلاعات کافی نداریم. از این رو، باید سعی کنیم این سیستم‌ها را طوری طراحی کنیم که از ما در برابر حملاتی که در آینده از آن‌ها مطلع خواهیم شد، حفاظت کنند.

اما مهندسین چگونه می‌توانند امنیت اینترنت اشیا را تأمین کنند؟ برای پاسخ به این سؤال و دستیابی به راه حل آن، وارد حوزه‌ای کاملاً مبهم می‌شویم که ناشناخته‌های زیادی دارد و تنها چند پاسخ قطعی در آن وجود دارد. در نتیجه، متخصصین امنیت نه تنها باید تمام سعی خود را برای توسعه سازوکارهای حفاظتی در برابر حملات شناخته‌شده به کار بینندن، بلکه باید دستگاه‌هایی نیز طراحی کنند که بتوان آن‌ها را در واکنش به نفوذها و آسیب‌پذیری‌های غیرمنتظره، پیکربندی کرد و ارتقا داد. رویکرد ما برای دستیابی به چنین دستگاه‌هایی، توسعه سخت‌افزارهایی است

فناوری بزرگ‌علی‌رغم مزایای فراوانش، جنبه تاریکی نیز دارد و آن هم تهدیداتی است که برای امنیت و حریم خصوصی ایجاد می‌کند؛ و مقیاس این تهدیدات به اندازه‌های است که تاکنون مشابه نداشته است. سیستم‌های دیجیتال کنونی ما در برابر هکرهای خرابکاری که سعی دارند به آن‌ها دسترسی غیرمجاز پیدا کنند، داده‌های شخصی و سایر اطلاعات را بدزدند، در ازای بازگرداندن اطلاعات باج بگیرند و حتی همانند حمله به Dyn، سیستم‌ها را به طور کامل از کار بیندازند، آسیب‌پذیر هستند. در نتیجه، رقابت تسلیحاتی میان هکرها و کارشناسان امنیت رایانه همچنان ادامه دارد و کاربران مجبورند دائمًا به روزرسانی‌های امنیتی را برای نرم‌افزارهای روی رایانه‌های مختلف خود انجام دهند.

الگوی فعلی یا همان بازی موش و گربه‌ای که بین به روزرسانی‌های نرم‌افزار و هک‌های پیشرفت‌به وجود آمده است، خبر از چالش بزرگی برای دستگاه‌های متصل به IoT می‌دهد. یکی از دلایل ایجاد این چالش آن است که حملات امنیتی به IoT می‌تواند پیامدهای فاجعه‌آمیزی برای زیرساخت‌های حیاتی مانند شبکه برق، منابع آب و بیمارستان‌ها داشته باشد. دلیل نگران‌کننده‌ی دیگر آن است که در دستگاه‌های هوشمند که به صورت انبوه تولید می‌شوند، نمی‌توان سخت‌افزارها را طوری طراحی کرد که بتوانند در مقابل تمام تهدیداتی که در چرخه عمرشان با آن‌ها مواجه می‌شوند، مقاومت کنند. این واقعیت‌ها ما را به شک می‌اندازند که آیا واقعاً برای پذیرش نظام گسترش و فرآگیر دستگاه‌های رایانش مدرن آماده هستیم یا خیر. در این نوشتار، به بررسی شیوه‌های احتمالی رفع این مشکل می‌پردازیم. به طور خلاصه، پیشنهاد ما این است که تمام ابزارهای تشکیل‌دهنده IoT باید طوری ساخته شوند که سخت‌افزارهایشان بتوانند خود را با تهدیدات امنیتی آینده وفق دهند. مهندسی چنین وسایلی راحت نیست، اما ما فکر می‌کنیم روشی هوشمند برای طراحی دستگاه‌های هوشمند است.

چرا دستگاه‌های متصل به IoT در برابر هک تا این اندازه آسیب‌پذیر هستند؟

یکی از دلایل آشکار این آسیب‌پذیری، تعداد بالای این دستگاه‌ها است. مطمئناً وقتی میلیارد‌ها دستگاه وجود دارد، همیشه تعداد زیادی از آن‌ها، حتی شاید میلیون‌ها دستگاه، رفتار مخرب داشته باشند یا به آن‌ها نفوذ شود؛ و هر دستگاه آلوده‌ای که به اینترنت متصل شود، ممکن است سعی کند سایر دستگاه‌ها را نیز آلود کند. از این رو، در اینترنت اشیا شاهد حملات گسترش و بی‌وقفه‌ای خواهیم بود. عامل شخصی‌سازی دلیل دیگری است که باعث می‌شود آسیب‌پذیری‌های امنیتی این دستگاه‌ها پیامدهای فاجعه‌آمیزی داشته باشند. ما امروزه سیستم‌های دیجیتال کوچکی داریم که بسیاری از فعالیت‌های روزمره ما را رهگیری و ثبت می‌کنند؛ از جمله الگوی خواب، تماس با سایر افراد، معیارهای سلامت، الگوهای مرور اینترنت و بسیاری موارد دیگر. اطلاعات به دست آمده از این دستگاه‌ها معمولاً از طریق اینترنت به سرورها و مخازن مرکزی ارسال می‌شوند تا در آنجا ذخیره شوند و مورد تجزیه و تحلیل قرار بگیرند. در نتیجه، اگر مهاجمی از هر نقطه‌ای به



پس از ساخت، مجدداً پیکربندی کرد.

دلیل دیگری که نشان می‌دهد باید سخت‌افزارها قابل‌به روزرسانی باشند، آن است که دستگاه‌های کوچک متصل به شبکه معمولاً باید با انرژی پایینی کار کنند. این در حالی است که پیاده‌سازی‌های نرم‌افزاری یک عملکرد معمولاً نسبت به پیاده‌سازی‌های سخت‌افزاری همان عملکرد، انرژی بیشتری مصرف می‌کنند. از این‌رو، اغلب اوقات مهندسین نمی‌توانند دستگاه کوچک کم‌صرفی طراحی کنند که بتواند کار مورد نظر را تنها با اجرای یک نرم‌افزار روی سخت‌افزارهای عمومی انجام دهد و این دستگاه‌ها باید از سخت‌افزارهای خاص منظوره برای چنین کاری استفاده کنند. در نتیجه، به روزرسانی نرم‌افزار احتمالاً برای ارتقاء امنیت به سطح مطلوب، کافی نیست. واضح است که یکی از الزامات طراحی سخت‌افزارهای قابل‌به روزرسانی که برای IoT مناسب باشند آن است که بتوانند با محدودیت‌های شدید انرژی همچنان کار کنند. به عنوان مثال، برخی از حسگرهای بی‌سیم تنها با مصرف چند میکروآمپر کار می‌کنند. نتیجه کار ما، طرحی است که می‌تواند با چنین محدودیت‌هایی به خوبی کار کند. یکی از راه‌های دستیابی به این امر، چیزی به نام مدار مجتمع دیجیتال قابل برنامه‌نویسی^۳ (FPGA) است؛ یعنی یک تراشه عام‌منظوره که پس از ساخت می‌توان منطق آن را پیکربندی کرد. کمکی که ما می‌توانیم به این پروژه پژوهشی بکنیم، توسعه یک مدل معماری است که بر اساس FPGA ساخته شده است و می‌تواند الزامات امنیتی، متفاوت را برآورده سازد.

برای درک نحوه کار این معماری، تراشه‌ای را در نظر بگیرید که قرار است در یک دستگاه کوچک تعییه گردد و مدتی طولانی روی IoT

که قابل به روزرسانی هستند. به روزرسانی مفهوم آشنایی در رایانش، حداقل در حوزه نرم افزار است. امروزه افراد می دانند که باید زحمت به روزرسانی نرم افزارها را متحمل شوند تا از عملکرد امن گوشی ها و رایانه های شان اطمینان یابند. ما دائماً هشدارهای دریافت می کنیم که به ما اطلاع می دهند نرم افزارهای جدید آماده نصب هستند. هر چه که این هشدارها را نادیده می گیریم، آن ها خطرناکتر می شوند تا زمانی که نرم افزار مورد نظر از کار بیفتند و مجبور شویم کوتاه بیاییم و آن را به روزرسانی کنیم.

اگل اوقات، برخی از برنامه‌های کاربردی پس از مدتی از کار می‌افتدند و باید خود را به روزرسانی کنند که معمولاً به زمان بیشتری نیاز دارد و گاهی باعث بروز اختلال‌های جدی می‌شود. به همین دلیل، اکثر کاربران با بی‌میلی با به روزرسانی‌های نرم‌افزاری موافقت می‌کنند. با این حال، این به روزرسانی‌های امنیتی ضروری هستند، زیرا یک دستگاه رایانش معمولی هر ماه در معرض دهها آسیب‌پذیری جدید قرار می‌گیرد. تا کنون به روزرسانی تنها برای نرم‌افزار و ثابت‌افزار^۲ یا همان کد سیستمی که روی دستگاه‌های کوچک اجرا می‌شود، انجام می‌شد و سخت‌افزار زیربنایی غیرقابل تغییر بود. به باور ما، مهندسین باید کاری کنند که نه تنها نرم‌افزارها بلکه سخت‌افزارهایی را که روی دستگاه‌هایی که رفع چنین مشکله استفاده از سخت‌افزاری است که بتوان آن را

هستند، رهگیری کند. در این صورت، اگر الزام امنیتی جدیدی ایجاد شود که مستلزم پایش یا واکنش نسبت به رویدادی باشد که برای اعتبارآزمایی IP حیاتی است، به روزرسانی سخت‌افزاری به موتور سیاست‌های امنیتی اجازه می‌دهد رویدادهای مرتبط را فوراً و بدون نیاز به تغییر IP‌ها رهگیری کند.

البته اگر یک الزام امنیتی جدید به رویدادهای یک IP مربوط باشد که از طریق واسط اشکال زدایی قابل دسترسی نیستند، راهی وجود نخواهد داشت. ما امیدواریم چنین شرایطی کمتر پیش بباید و سازندگان IP با گذشت زمان، واسطهای اشکال زدایی خود را توانمندتر سازند، حداقل تا زمانی که یک واسط امنیتی استاندارد برای IPها تدوین شود. در بلندمدت و همچنان که متخصصین امنیت درک بهتری از نیازها پیدا می‌کنند، سازوکارهای حفاظتی انعطاف‌پذیرتری نیز برای این دستگاههای کم‌صرف ایجاد خواهند کرد. همان‌طور که امروزه به‌روزرسانی نرم‌افزار امر رایجی است، به‌روزرسانی سخت‌افزاری نیز روزی به امری عادی در اینترنت اشیا تبدیل خواهد شد. در آینده، چالش اینترنت اشیا این خواهد بود که راهی برای به‌روزرسانی خودکار و منظم سیستم‌ها پیدا کنیم که به شیوه‌ای بی‌دردسر صورت بگیرد و دیگر اثری از ترس و گریزی که امروزه از به‌روزرسانی‌های نرم‌افزاری وجود دارد، نباشد.

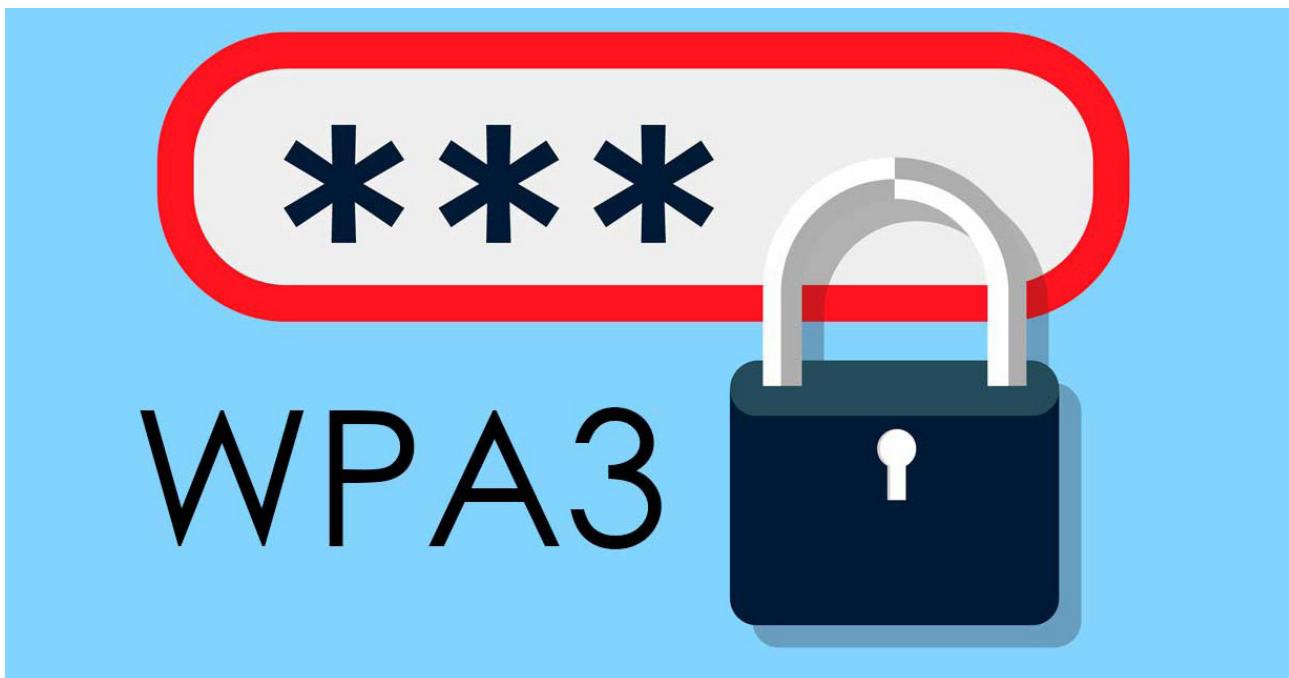
در حال حاضر، متخصصین در تلاش هستند تا به روزرسانی نرم افزار را برای انواع دستگاه های کوچک متصل به اینترنت مانند گوشی ها، خودکار کنند. این فرایند، به روزرسانی OTA⁷ نامیده می شود. چنین سازو کارهایی باید حتماً تضمین کنند که فقط به روزرسانی های معتبر نرم افزاری بارگذاری می شوند. این سازو کارها همچنین باید به اندازه ای قابل اتکا باشند که بتوانند حتی در حین قطع برق یا قطع ارتباطات هنگام به روزرسانی، این فرایند را بدون از کار انداختن دستگاه انجام دهند. چنین ملاحظاتی در مورد خودکارسازی به روزرسانی های پیکربندی سخت افزارها نیز وجود دارند. رعایت این الزامات در دستگاه های کوچک متصل به IoT که معمولاً سخت افزار یا نرم افزار لازم برای پشتیبانی از چنین وظایف پیچیده های را ندارند، دشوار است. مطمئناً حفظ امنیت اینترنت اشیا، بدون درخواست از کاربران یا مدیران سیستم ها برای به روزرسانی دستی دهنده ای شاید صدها دستگاه مختلف، کار پرچالشی خواهد بود. اما ما امیدواریم که در این زمینه پیشرفت هایی حاصل شود و تعداد سیستم های به روزرسانی خودکار نیز همراه با رشد تعداد دستگاه ها، افزایش یابد. اگر این اتفاق بیفت و مؤلفه های تشکیل دهنده اینترنت اشیا به اندازه کافی انعطاف پذیر باشند، باور داریم که سطح معقولی از امنیت به وجود می آید، حتی اگر تعداد دستگاه های متصل به IoT به تریلیون ها عدد برسد. چنین شرایطی زودتر از آنچه تصور ممکن است، اتفاقاً خواهد افتاد.

به کار گرفته شود. این تراشه ممکن است برای یک چراغ هوشمند، یک یخچال یا هر دستگاه دیگری باشد. در عمارتی مورد نظر ما، یک بلوک سختافزار مرکزی به نام «موتور سیاست امنیتی»^۴ مجموعه‌ای جامع از رویدادهای مهم امنیتی، از جمله ارتباطات میان سایر بلوک‌های طراحی در سیستم و جهان خارجی را مدیریت می‌کند. به عنوان مثال، ممکن است موتور سیاست امنیتی چنین الزام کند که کلیدهای رمزنگاری مورد استفاده برای ارتباط، تنها باید در دسترس برخی بلوک‌های خاص سختافزاری باشند. برای اجرای این قانون، موتور سیاست امنیتی باید اشتراک‌گذاری کلیدهای محروم‌انه بین بلوک‌ها را مدیریت کند و از تبادلاتی که الزامات امنیتی خاص را رعایت نمی‌کنند، جلوگیری نماید. حال اگر روزی متوجه شوید یک بلوک سختافزاری حاوی یک آسیب‌پذیری امنیتی است و دیگر نباید به کلید رمزنگاری دسترسی داشته باشد، چه انفاقی می‌افتد؟ در این صورت اگر سختافزار غیرقابل تغییر باشد، نمی‌توان کاری انجام داد.

حالاً تصور کنید که این موتور سیاست امنیتی با استفاده از یک FPGA ساخته شده است. از آنجا که FPGA قابل ارتقا است، می‌توانید آن را به روزرسانی کنید. به طور خاص، اگر لازم باشد از دستگاه در برابر یک تهدید جدید حفاظت نمایید، می‌توانید سخت‌افزار را به روزرسانی کنید تا مجموعه جدیدی از الزامات امنیتی را اجرا نماید و در عین حال، همچنان تنها چند میکروآمپر مصرف کند. به طور نظری، این معماری ساده به نظر می‌رسد. اما در عمل، جزئیات زیادی وجود دارد که باید روی آن‌ها کار شود. زیرا حتی دستگاه‌های دیجیتال کوچک نیز معمولاً دارای چند بلوک مختلف سخت‌افزاری هستند که توسط اشخاص متفاوتی طراحی شده‌اند. در زبان تجارت، این بلوک‌ها مالکیت‌های معنوی^۵ یا IP نامیده می‌شوند. یک موتور سیاست امنیتی باید ارتباطات بین IP های مختلف را دنبال کند تا بتواند الزامات امنیتی را اجرا نماید و موارد تخطی از آن‌ها را شناسایی کند.علاوه بر این، یک موتور سیاست امنیتی باید به رویدادهای مهم امنیتی که در داخل هر یک از بلوک‌های IP در جریان هستند نیز دسترسی داشته باشد تا بتواند این حوادث را به درستی شناسایی کند و نسبت به آن‌ها واکنش نشان دهد.

برای این کار به یک واسطه خاص نیاز داریم که به تمام سازندگان IP اجازه می‌دهد از سازوکار مشترکی برای بلوک‌های سخت‌افزاری خود استفاده کنند تا بتوانند با موتور سیاست امنیتی به ارتباط پیردازند. چنین واسطه‌ی در حال حاضر وجود ندارد و ممکن است تدوین استانداردهای چنین واسطه‌ی سال‌ها طول بکشد. اما خوشبختانه بیشتر IP‌ها چیزی به نام واسطه اشکال‌زادایی^۶ دارند که بررسی می‌کند آیا IP مورد نظر پس از تولید در قالب یک تراشه، آن طور که باید کار می‌کند یا خیر. اگر موتور سیاست امنیتی را به این واسطه وصل کنیم، موتور می‌تواند تعداد زیادی از رویدادهای مختلف را که داخل بلوک‌های مورد نظر در حال وقوع

قابلیت‌های پروتکل امنیتی WPA3



گسترده‌වای فای که در سال ۲۰۱۷ برای WPA2 به وجود آمد، اکنون زمان مناسبی برای ارائه آن است.

مشکلات WPA2

در اکتبر سال ۲۰۱۷ یک آسیب‌پذیری جدی به نام KRACK که مخفف حمله نصب مجدد کلید^۳ است، در WPA2 کشف شد. هکرها می‌توانستند از این آسیب‌پذیری به عنوان ابزاری برای خواندن و سرقت داده‌ها و گذر واژه‌ها استفاده کنند. این آسیب‌پذیری با دستکاری بخشی از فرایند دستدهی^۴ چهار طرفه‌ای که WPA2 از آن برای اطمینان از وارد شدن گذر واژه درست استفاده می‌کند، عمل می‌نماید. پس از این آسیب‌پذیری، بسیاری از افراد متوجه شدن شبکه‌های بی‌سیم شان آن طور هم که تصور می‌کردند، امن نیست.

تدابیر آسیب‌پذیری WPA2

آسیب‌پذیری KRACK باعث شد بسیاری از مسیریاب‌ها و دستگاه‌های در معرض آسیب باشند، اما این آسیب‌پذیری قبل از این که کسی بتواند با سوءاستفاده از آن دست به خرابکاری بزند، عیب‌یابی و رفع شد. مایکروسافت در ماه اکتبر ۲۰۱۷ ویندوز را با یک وصله امنیتی، به روزرسانی کرد. اپل به سرعت نسخه ۱۱.۱ iOS را برای رفع مشکلاتی که بر مدل‌های آیفون ۸ به بعد تأثیر می‌گذاشتند عرضه

در آینده نزدیک با به کارگیری پروتکل امنیتی جدید وای‌فای WPA3، سرعت و امنیت شبکه‌های بی‌سیم افزایش می‌یابد. WPA3 قرار است مشکلات شناخته شده WPA2 که امروزه تقریباً در تمام دستگاه‌های بی‌سیم وجود دارد را رفع کند.

WPA3 چیست؟

WPA3 یک پروتکل پیشرفته امنیتی برای شبکه‌های بی‌سیم است که هک شبکه‌های بی‌سیم را برای مجرمان دشوارتر می‌سازد. این پروتکل در نمایشگاه اخیر محصولات الکترونیکی مصرفی (CES) در لاس‌وگاس معرفی شد. طبق اعلام انجمن وای‌فای، این فناوری در مقایسه با فناوری استاندارد فعلی یعنی WPA2 چهار مزیت مهم خواهد داشت. از این رو، قرار است به زودی جایگزین پروتکل‌های فعلی شود.

مزایای هیجان‌انگیز WPA3

شاید لغت «هیجان‌انگیز» برای توصیف مزایای این پروتکل کمی اغراق باشد، اما مطمئناً چیزی است که ارزش انتظار کشیدن را دارد؛ زیرا قرار است مشکلات شناخته شده پروتکل WPA2 که امروزه تقریباً در تمام دستگاه‌های بی‌سیم وجود دارد را رفع کند. از همه مهم‌تر، پروتکل امن‌تری خواهد بود و با توجه به اکسپلوبیت

و نحوه تعامل ما با فناوری تغییر زیادی کرده است. WPA3 قصد دارد این تغییرات را منعکس کند. طبق گفته انجمن وای‌فای، اگر یک دستگاه بدون صفحه‌نمایش دارید، مانند یک Amazon Echo WPA3 معمولی، پیکربندی آن راحت‌تر و امن‌تر از قبل خواهد بود. از دستگاه‌هایی مانند گوشی‌های هوشمند نیز استفاده خواهد کرد تا گجتها را به راحتی به شبکه‌های وای‌فای وصل کند. با این حال، هنوز جزئیات آن منتشر نشده است.

سطح امنیت WPA3

WPA2 از رمزگذاری ۶۴ یا ۱۲۸ بیتی استفاده می‌کند، اما WPA3 با فناوری امنیتی ۱۹۲ بیتی که مختص دولت‌ها، صنایع و دفاع طراحی شده است، امنیت را افزایش می‌دهد. طبق گفته انجمن وای‌فای، این پروتکل از آخرین فناوری‌های تقویت رمزگذاری استفاده می‌کند. همچنین، انجمن وای‌فای اقداماتی را پیشنهاد کرده است که برای افزایش امنیت می‌توان آن‌ها را به کار گرفت، از جمله این که در حال حاضر WPA2 را فعال کنید و وقتی WPA3 ارائه شد، آن را فعال نمایید؛ تنظیمات پیش‌فرض تجهیزات خود را تغییر دهید؛ آخرین بهروزرسانی‌های امنیتی را نصب کنید؛ و تنها دستگاه‌های وای‌فایی بخرید که لوگوی Wi-Fi Certified را دارند.

تدابوم پشتیبانی از WPA2

گرچه WPA2 در سال ۲۰۰۴ معرفی شد و WPA3 بسیار امن‌تر از آن است، اما انجمن وای‌فای همچنان از فناوری WPA2 پشتیبانی خواهد کرد و آن را بهبود می‌بخشد. جدیدترین پیکربندی WPA2 به زودی ارائه می‌شود و قرار است حفاظت‌های پیشرفته‌ای ارائه دهد که شامل بررسی‌های امنیتی جدید هستند. با این حال، WPA2 باید تا زمان ارائه WPA3 فعال باشد، اما در نهایت زمانی فرا می‌رسد که باید آن را کنار گذاشت؛ همان‌طور که WPA قدیمی کنار گذاشته شد. علاوه بر این، انجمن وای‌فای اظهار داشت تمام دستگاه‌های جدیدی که می‌خواهند لوگوی Wi-Fi Certified را بگیرند، باید از WPA3 پشتیبانی کنند.

نحوه دسترسی به WPA3

برای دسترسی به WPA3 باید منتظر بمانید. احتمالاً تا پایان سال ۲۰۱۸، مسیریاب‌ها و سایر دستگاه‌های بی‌سیم با برچسب WPA3 در بازار عرضه می‌شوند. اگر سازندگان بتوانند برای فناوری‌های فعلی خود نیز مجوز WPA3 را بگیرند، ممکن است دستگاه‌های فعلی هم بهروزرسانی شوند. اما اگر می‌خواهید حتماً مسیریابی بخرید که از پروتکل جدید پشتیبانی می‌کند، به یاد داشته باشید تنها زمانی می‌توانید از ویژگی‌های جدید این پروتکل بهره ببرید که دستگاه‌هایی که به مسیریاب متصل می‌کنید نیز با این پروتکل سازگار باشند. با این حال، خبر خوب این است که اگر لازم باشد، هنوز هم می‌توانید از WPA2 استفاده کنید.

منبع: www.itpro.co.uk

کرد و گوگل نیز در هفته نخست نوامبر ۲۰۱۷، این مشکل را در دستگاه‌هاییش رفع نمود. انجمن وای‌فای همچنان در حال تست این آسیب‌پذیری است و به کاربران وای‌فای توصیه کرده است همیشه بهروزرسانی‌های ارائه شده توسط سازندگان دستگاه‌ها را نصب کنند.

نحوه عملکرد WPA3

می‌توان گفت که WPA3 تا حد زیادی بر اساس WPA2 ساخته شده است و همانند آن، وقتی یک اتصال مبتنی بر گذر واژه به یک شبکه وای‌فای بسته برقرار شود، مشخص می‌کند چه اتفاقی بیفتد. WPA3 پروتکلهای ضروری را که از مسیریاب حفاظت می‌کنند، ایجاد می‌نماید و فرایند دستدهی مذکور را بین دستگاه‌ها در سمت کاربر و شبکه‌هایی که کاربر به آن وصل می‌شود، اجرا می‌کند. این کار به تأیید گذر واژه‌ها و اطمینان از رمزگذاری قدرتمند نیاز دارد. هدف اصلی از این پروتکل آن است که بدون درگیری با جزئیات فنی، مانع هک ارتباطات بی‌سیم کاربر توسط هکرها شود. ظاهراً بسیار بهتر از پروتکلهای قبلی عمل خواهد کرد.

سایر قابلیت‌های WPA3

شاید مهم‌ترین مزیت WPA3، روش حفاظت آن از داده‌ها هنگام استفاده از اینترنت در شبکه‌های باز وای‌فای است. این هات‌اسپیت‌ها در فرودگاه‌ها، کافی‌شایپ‌ها و سایر مکان‌های عمومی، امکان دسترسی به اینترنت را فراهم می‌آورند؛ اما در واقع مخاطرات بسیاری نیز به همراه دارند، زیرا همه می‌توانند به آن‌ها متصل شوند و داده‌هایی که تبادل می‌شود، رمزگذاری نمی‌شوند. کافی است تنها کمی دانش فنی داشته باشید تا بتوانید به ترافیک این شبکه‌ها دسترسی یابید و داده‌های ارسالی و دریافتی را به صورت رمزگذاری نشده مشاهده کنید. WPA3 از چیزی به نام رمزگذاری بی‌سیم فرصت‌طلبانه^۵ برای رمزگذاری داده‌های تک‌تک کاربران استفاده می‌کند و برای متوقف کردن هکرها، الگوی ارتباط بین مسیریاب و تمام دستگاه‌های روی شبکه را به هم می‌ریزد.

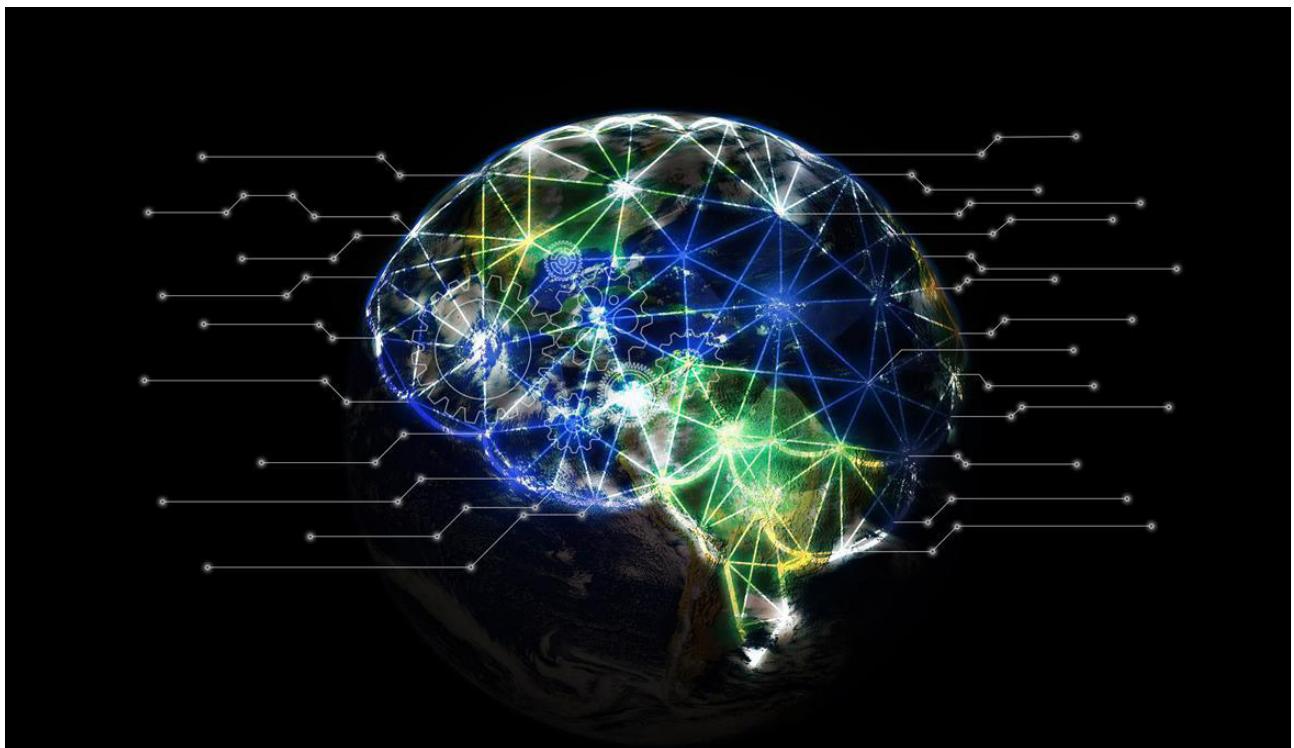
دشوارتر شدن دستیابی به گذر واژه‌ها

WPA3 از گذر واژه‌های ضعیف حفاظت می‌کند. در نتیجه، حتی وقتی چند حرف و عدد ساده را به عنوان گذر واژه انتخاب می‌کنید که به اندازه کافی پیچیده نیستند، مانند واژه password یا ۱۲۳۴۵۶ یا ۱۲۳۴۵۶ از گذر واژه شما نیز حفاظت می‌شود. زیرا در این پروتکل، اجرای حملات جستجوی فرآگیر^۶ (که در آن تعداد زیادی از ترکیب‌های احتمالی کلمات تست می‌شوند یا از یک لیست کامپایل شده استفاده می‌شود تا در نهایت گذر واژه پیدا شود) برای هکرها دشوارتر شده است و وقتی چند بار گذر واژه نادرست وارد شود، فرایند احرار هویت وای‌فای مسدود می‌شود.

تسهیل پیکربندی دستگاه‌ها

امروزه پیشرفته‌های زیادی در حوزه فناوری به دست آمده است

به کار گیری یادگیری ماشین و حسگرهای پیشرفته



- کاهش مصرف برق در زمان‌های اوج بار که باعث کاهش نرخ مصرف برق می‌شود.
- شبکه هوشمند با برقراری ارتباطات دوطرفه بین مراکز توزیع و تجهیزات هوشمند (کنترلهای هوشمند و لوازم برقی هوشمند) می‌تواند قابلیت‌های مذکور را ارائه دهد. البته بهبود ارتباطات نه تنها به کارکنان شرکت برق که به دنبال برقراری جریان برق هستند، بلکه به افرادی که در صدد آسیب رساندن به شبکه‌های برق هستند نیز کمک می‌کند.

ناکارامدی تجربیات امنیت IT برای حفاظت از شبکه‌های برق کتی کین کید در مقاله‌ای با عنوان «ترکیب فناوری‌های قدیمی و جدید برای دستیابی به ابزارهای جدید افتتا برای شبکه‌های برق» در مورد پروژه آزمایشگاه ملی لارنس برکلی^۲ (LBL) می‌گوید: «شبکه‌های توزیع برق با ملاحظات دقیقی توسعه یافته‌ند تا عملیات‌های ایمن و قابل اعتماد را تضمین کنند. با نوین سازی این شبکه‌ها برای افزایش قابلیت اعتماد، باید ویژگی‌های جدیدی برای ایجاد مقاومت سایبری طراحی گردد تا از بروز حملات سایبری از طریق شبکه‌های IP جلوگیری شود».

به گفته کین کید، رویکردهای فعلی در امنیت IT (از جمله

امروزه، با افزایش حملات سایبری به شبکه‌های برق، اهمیت امنیت در این شبکه‌ها نیز افزایش یافته است. فناوری‌های جدیدی چون حسگرهای پیشرفته و یادگیری ماشین به اپراتورهای شبکه‌های توزیع برق کمک می‌کند تا شبکه‌های خود را در برابر حملات سایبری مقاوم سازند.

شروع یوینز در مقاله‌ای با عنوان «اگر برق به مدت طولانی قطع شود، چه اتفاقی می‌افتد؟» نوشته است: «در حقیقت، بیش از آنچه تصور می‌کنیم به برق وابسته هستیم. حتی اگر شما هم همانند من سال‌ها در جایی بدون برق زندگی کنید، باز هم در جهان و جامعه‌ای حضور دارید که به شدت به برق وابسته است». همین «وابستگی عمیق» باعث شده است شرکت‌های تولیدکننده برق به زیرساخت شبکه هوشمند^۱ روی آورند؛ یک زیرساخت کارآمدتر و قابل اطمینان‌تر برای توزیع برق. شبکه هوشمند که می‌توان آن را اینترنت خطوط برق نیز نامید، قابلیت‌های بین‌نظری ارائه می‌کند، از جمله:

- اتصال سریع برق پس از قطعی.
- کاهش هزینه‌های عملیاتی و مدیریتی خدمات برق و در نهایت کاهش هزینه برق برای مصرف‌کنندگان.

به نوشته کین کید: «PMUها کوچک‌تر و ارزان‌تر هستند. از این رو، می‌توان چند PMU را به صورت همزمان در شبکه توزیع مستقر کرد که دقت بالاتری (۱۲۰ مورد اندازه‌گیری در ثانیه) در شبکه فراهم می‌کنند و حملات بالقوه به شبکه را به صورت بلادرنگ به اپراتورها اطلاع می‌دهند».

شناسایی نفوذ، فایروال‌ها و فناوری‌های رمزگذاری) برای حفاظت از شبکه‌های برق کافی نیستند. وی در این رابطه، گفت: «اگر این روش‌ها در دستگاه‌های سایبری-فیزیکی به کار گرفته شوند، امنیت آن‌ها به درستی تأمین نمی‌شود؛ چراکه اطلاعات فیزیکی دستگاهی را که از آن حفاظت می‌کنند، در نظر نمی‌گیرند».

گزارش بلادرنگ با به کارگیری الگوریتم یادگیری ماشین
پژوهشگران در این پژوهه، از یک الگوریتم یادگیری ماشین که نخستین بار در سال ۱۹۵۴ تحت عنوان CUSUM یا SUM معرفی شده بود، استفاده کردند. به گفته سیاران رابرتر، این الگوریتم باعث می‌شود نرم‌افزار با شناسایی تغییرات سریع در محیط فیزیکی، عادی یا غیرعادی بودن معیارهایی مانند میزان جریان، انرژی فعال و انرژی واکنش‌گر را مشخص کند.

نمونه آزمایشی کارامد

دانشگاه برکلی ایستگاه توزیع برق اختصاصی دارد. در نتیجه، پژوهشگران می‌توانند چارچوب پایش و تحلیل خود را آزمایش کنند. کاربردهایی که روی این شبکه مورد پژوهش قرار گرفتند، عبارتند از:

- پیش‌بینی وضعیت و افزایش پدیداری^۱ برای اپراتورهای سیستم (توضیح مترجم: پدیداری، بدان معنا است که سیستم به گونه‌ای طراحی و پیاده‌سازی شود که هیچ اقدامی در آن، دور از دید کنترل‌های امنیتی انجام نگیرد).

- تعیین مشخصات بار و تولید توزیع شده برق.
- تشخیص شرایط مشکل‌سازی مانند نوسانات یا تأخیر در بازیابی ولتاژ در اثر هر گونه جریان غیرعادی در مدار^۲ (FIDVR).
- هماهنگ‌سازی شبکه‌های کوچک.
- تأمین افتاده تجهیزات شبکه توزیع برق.

اهمیت فناوری مذکور

امروزه، حملات سایبری به شبکه‌های برق در حال تبدیل به تیتر مشترک اخبار فناوری و اخبار عادی هستند. علاوه بر این، شاهد افزایش پیش‌بینی آثار ناشی از قطع گسترشده برق به مدت طولانی هستیم. متأسفانه، پیش‌بینی‌های جرج اورول در رمان ۱۹۸۴، در مقایسه با شرایط فعلی، اصلاً هیجان‌انگیز نیست! از این رو امیدوارکننده است که کارشناسان با جدیت در حال تلاش برای حل این مشکلات هستند.

پایسرت معتقد است: «با استفاده از حسگرهای دارای دقت بالا در شبکه‌های توزیع برق و مجموعه‌ای از الگوریتم‌های یادگیری ماشین که توسط تیم ما توسعه یافته‌اند و همچنین، ترکیب آن‌ها با مدل ساده‌ای از شبکه توزیع، ارائه‌دهندگان خدمات برق می‌توانند از فناوری ما در شبکه‌های توزیع خود استفاده کنند تا بتوانند حملات سایبری و سایر خواص‌ها را شناسایی نمایند».

منبع: www.techrepublic.com

نقش یادگیری ماشین و حسگرهای دارای تأمین امنیت شبکه‌های برق

تیمی از پژوهشگران به رهبری شان پایسرت از مرکز علمی LBL، متشکل از سیاران رابرتر، آنا سگولین از دانشگاه ایالتی آریزونا، الکس مک‌ایچرن از مرکز Power Standards و چاک مک‌پارلند، بازنیشته مرکز LBL و اما استیوارت از مرکز ملی Lawrence Livermore در حال کار روی پژوههای هستند که شیوه‌های افتاده، الگوریتم‌های یادگیری ماشین و فناوری حسگرهای سیستم‌های برق را در قالب یک چارچوب پایش و تحلیل شبکه‌های برق ترکیب می‌کند.

این تیم در حال حاضر به طراحی معماری این چارچوب مشغول هستند تا حملات سایبری-فیزیکی به شبکه‌های توزیع برق را شناسایی کنند. طبق مقاله کین کید، پژوهشگران برای شناسایی این حملات، از دستگاه‌های اندازه‌گیری میکرو-فازور^۳ (PMUs) استفاده می‌کنند تا اطلاعات مربوط به وضعیت فیزیکی شبکه توزیع برق را به دست آورند. سپس، این داده‌ها با اطلاعات اسکادا^۴ ترکیب می‌شود تا بازخورد بلادرنگی درباره عملکرد سیستم فراهم آید.

هدف از این پژوهه، پایش رفتار فیزیکی مؤلفه‌های درون شبکه برق است تا هم حملات سایبری و هم تغییرات غیرعادی دستگاه‌ها مشخص شود. پایسرت در این رابطه توضیح داد: «این دستگاه‌ها معیارهای بیشتری را اندازه‌گیری می‌کنند تا فرایندهای شبکه توزیع برق با دقت بیشتری ردگیری شوند».

پایسرت با تأکید بر ارزش اندازه‌گیری معیارهای بیشتر در هنگام استفاده از دستگاه‌های اسکادا و PMU، گفت: «مهاجم می‌تواند شخصاً اطلاعات ارائه شده توسط تک‌تک حسگرهای یا منبع اطلاعات را دست‌کاری کند که منجر به آسیب شبکه برق خواهد شد. در نتیجه، اپراتورهای شبکه برق با استفاده از این رویکرد، اطلاعات بیشتری را مشاهده می‌کنند و نسبت به حملات مقاوم می‌شوند».

علاوه بر این، افزونگی سیستم^۵ باعث می‌شود بتوان نتیجه اندازه‌گیری PMU را با اطلاعات گزارش شده توسط تجهیزات مقایسه کرد و بدین ترتیب، امکان تشخیص حملات واقعی از غیرواقعی فراهم می‌گردد.

ماهیت PMU و اهمیت کاربرد آن

دستگاه اندازه‌گیری فازور^۶ (PMU) و ضعیت الکتریکی شبکه برق را با استفاده از محاسبات فازور ولتاژ و فازور جریان تعیین می‌کند. با این حال، PMU‌ها بزرگ و گران هستند. در نتیجه، استقرار آن‌ها روی نودهای^۷ توزیع مرکزی محدود می‌شود؛ اینجا است که از PMU‌ها استفاده می‌گردد.

زیرساخت جابجایی‌پذیری مبتنی بر بافتار



سیستم‌های اسکادا و سیستم‌های مدیریت ساختمان^۳ (BMS) نوعی واسط ماشین و انسان^۴ (HMI) را با سطح بالای پدیداری^۵ به کارگنان بخش عملیات و نگهداری^۶ (O&M) ارائه می‌کنند تا از سلامت دارایی‌های صنعتی، الکتریکی و تجهیزات ساختمانی حفاظت شود. این سیستم‌های نظری گاهی اوقات از اتفاق‌های کنترل مرکزی فراتر می‌روند و به پلتفرم‌های از راه دور مانند

مفهوم زیرساخت جابجایی‌پذیری مبتنی بر بافتار^۱ بر اساس درخواست جهانی برای پشتیبانی بهتر از جابجایی‌پذیری در سیستم‌های اسکادا^۲ و مدیریت ساختمان توسعه یافت. این فناوری سبب استفاده بهینه‌تر از منابع انسانی می‌شود. کاهش زمان نیاز برای راهاندازی یک سیستم جدید را می‌توان از بیوبدهای مهم در این حوزه دانست.

Human Machine Interface -۴

visibility -۵

Operations and Maintenance -۶

contextual mobility infrastructure -۱

SCADA -۲

Building Management Systems -۳

کاربر و یک سرور جابجایی‌پذیری مبتنی بر بافتار که مسئول ارزیابی و پاسخ به نیازهای اطلاعاتی و کنترلی کاربران در مکان فعلی آن‌ها است، می‌شود. این سرور به یک سیستم نظارتی اسکادا BMS متصل است که ارتباطات را برای پایش و کنترل تجهیزات یا دیگر دارایی‌ها مدیریت می‌کند. دستگاه‌های همراه نیز با استفاده از شبکه‌های بی‌سیم استاندارد به سرور مبتنی بر بافتار متصل می‌شوند.

برنامه کاربردی HMI مبتنی بر بافتار

به لحاظ عملی، در C-HMI به طور معمول ابتدا کارکنان به یک برنامه کاربردی روی دستگاه همراه وارد می‌شوند. با قرار گرفتن دستگاه در یک منطقه جغرافیایی، برنامه کاربردی برچسب‌های اعلان بلوتوث^۹ و اکسپوینت‌های وای‌فای را شناسایی می‌کند. البته ممکن است کارکنان برای تعریف بافتار محیط، یک برچسب NFC یا کد QR را اسکن کنند.

سرور جابجایی‌پذیری مبتنی بر بافتار پایگاهداده‌ای ایجاد می‌کند که مناطق جغرافیایی و پروفایل‌های کاربران را با اطلاعات، کنترل‌های تجهیزات، اقدامات و رویدادها مرتبط می‌سازد. با بهره‌گیری از بافتار محیطی و اطلاعات حساب کاربری که توسط برنامه کاربردی دستگاه همراه ارسال می‌شود، سرور می‌تواند با توجه به بافتار کاربر و مکان، به اطلاعات مورد نیاز دسترسی یابد و سپس، اطلاعات و کنترل‌های مربوطه را به صورت خودکار به دستگاه همراه ارسال نماید.

استفاده از C-HMI می‌تواند تمام داده‌ها و کنترل‌های بلادرنگ مورد نیاز برای کنترل نظارتی، مکان بلادرنگ دستگاه‌های همراه و برچسب‌های جغرافیایی دارایی‌ها و همچنین پیام‌رسانی که در صورت نیاز گزارش‌های الکترونیکی ارائه می‌کند را به سیستم‌های اسکادا یا BMS بیفزاید. این سیستم همچنین از اطلاعات ضروری برای اجرای گام‌های خودکار بر اساس رویدادها برخوردار است. برای مثال، در مورد یک رویداد مرتبط با امنیت یا اینمنی، باید به صورت خودکار هشداری به کارکنان حاضر در مناطق تحت تأثیر ارسال شود. به علاوه، C-HMI با نظارت بر مناطق، اقدامات مناسب را به سیستم نظارتی ارسال می‌کند. برای مثال، زمانی که آخرین نفر منطقه را ترک می‌کند، چراغ‌ها به صورت خودکار خاموش شوند.

تأثیر یک فناوری ساختارشکن

مفهوم زیرساخت جابجایی‌پذیری مبتنی بر بافتار بر اساس درخواست جهانی برای پشتیبانی بهتر از جابجایی‌پذیری در سیستم‌های اسکادا و BMS توسعه یافت. در طول دو سال گذشته، تحقیقات بازار گستره‌ای از طریق جلسات خصوصی، نمایشگاه‌های تجاری، سمینارها و گروه‌های پژوهشی صورت گرفت. این تحقیقات برای فهم ارزش درکشده C-HMI و چگونگی تغییر نقش کارکنان با استفاده از فناوری C-HMI انجام شده‌اند.

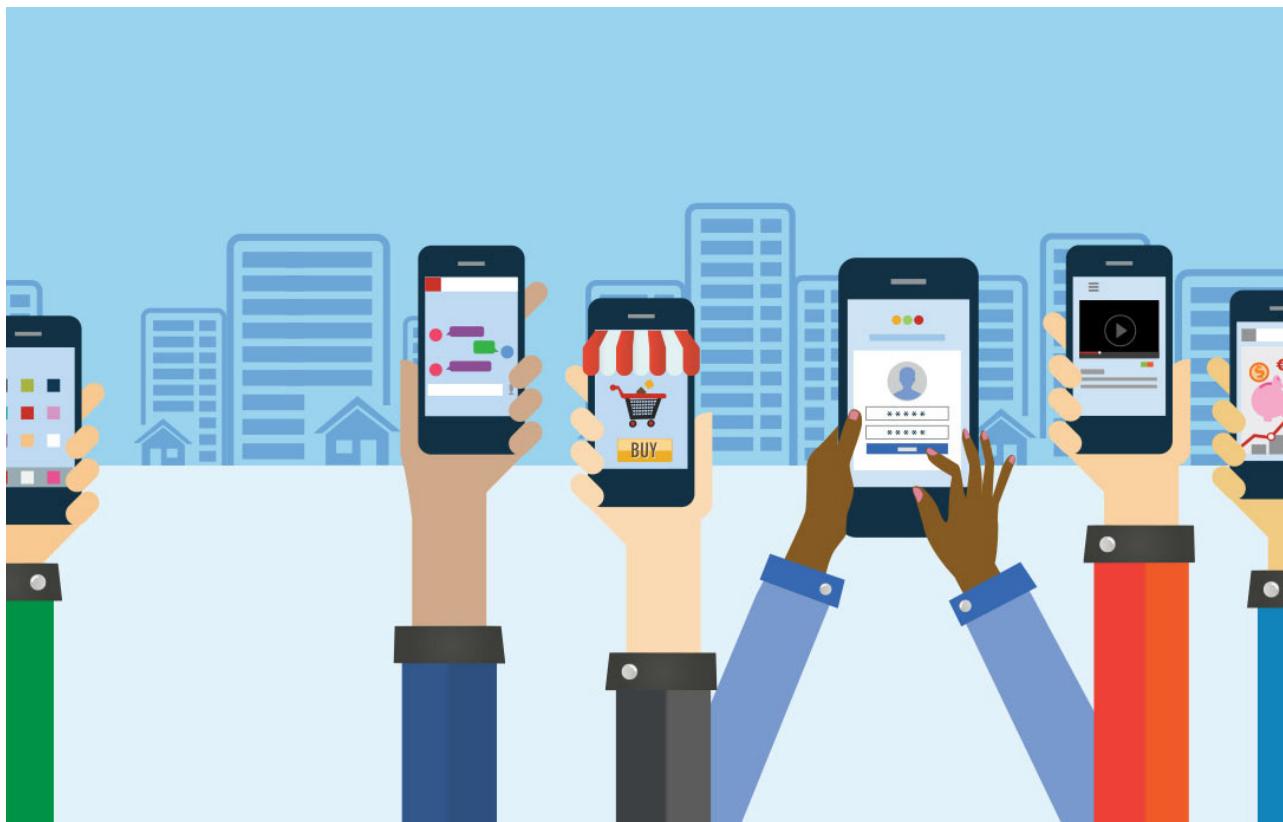
موضوع امنیت یکی از دغدغه‌های مشترک است که در پذیرش سیستم C-HMI نیز حیاتی به نظر می‌رسد. این مسئله شامل امنیت ارتباطات از C-HMI به سیستم نظارتی است تا از حملات سایبری با استفاده از سرور جابجایی‌پذیری به عنوان دروازه اسکادا یا BMS جلوگیری شود. به علاوه، باید اطمینان حاصل گردد کاربری که وارد حساب کاربری در دستگاه همراه می‌شود، همان کسی باشد که اعلام کرده است و نه فرد دیگری که از اطلاعات حساب کاربری برای دسترسی به کنترل تجهیزات سوءاستفاده می‌کند.

لپتاپ‌ها گسترش می‌یابند. به این ترتیب، کارکنان بخش عملیات و نگهداری می‌توانند شرایط تجهیزات را از هر مکانی مشاهده کنند. کارکنان جابجایی‌پذیر^۷ همواره از تکامل سیستم‌های مخابرات، به ویژه در دستگاه‌های نهایی بهره برده‌اند. امروزه، جابجایی‌پذیری به دستگاه‌های هوشمند خصوصاً گوشی‌ها و تبلت‌ها وابسته است. در واقع، افراد روزبه‌روز بیشتر به استفاده از دستگاه‌های هوشمند به جای لپتاپ‌ها برای کار از راه دور روی می‌آورند. البته نحوه کار افراد با دستگاه‌های همراه نسبت به نحوه کار آن‌ها با رایانه‌های لپتاپ متفاوت است. از این رو، رویکردهای قبلی برای نظارت، عیب‌یابی، نگهداری و کنترل دارایی‌های صنعتی و ساختمانی باید مورد بازبینی قرار گیرند و معماری جدیدی ارائه شود که برای کاربران دستگاه‌های همراه در سیستم‌های اسکادا و BMS بهینه‌سازی شده باشد.

زیرساخت جابجایی‌پذیری مبتنی بر بافتار

زیرساخت جابجایی‌پذیری مبتنی بر بافتار حول محور ارتقای ارزش و بهره‌وری سیستم بر پایه دستگاه‌های همراه هوشمند متمرکز است. این زیرساخت از فناوری‌های مکان‌یابی^۸ داخلی و خارجی برای ارائه HMI مبتنی بر بافتار (C-HMI) بر اساس نزدیکی کارکنان جابجایی‌پذیر به تجهیزات استفاده می‌کند. کارکنان عملیات و نگهداری اینک می‌توانند به کنترل‌ها و اطلاعات مرتبطی که بر اساس موقعیت فعلی و پروفایل کاربر به صورت خودکار بر روی دستگاه‌ها دانلود می‌شود، دسترسی یابند. این امر وابستگی به مسیریابی در رایانه‌های استاندارد را در زمان استفاده از دستگاه‌های همراه با صفحات نمایش کوچک از میان می‌برد. نوآوری ساختارشکن حاضر ضمن بهبود اینمی، عملکرد و کارایی عملیاتی را ارتقا می‌دهد.

زیرساخت C-HMI شامل مجموعه‌ای از برچسب‌های مکانی که برای مناطق جغرافیایی تحت کنترل (geo-zone) به کار می‌روند، یک برنامه کاربردی بر روی دستگاه همراه مبتنی بر میزان نزدیکی



امنیت ارتباطات از C-HMI به سیستم نظارتی است تا از حملات افتاده استفاده از سرور جابجایی‌پذیری به عنوان دروازه اسکادا یا BMS جلوگیری شود. به علاوه، باید اطمینان حاصل گردد کاربری که وارد حساب کاربری در دستگاه همراه می‌شود، همان کسی باشد که اعلام کرده است و نه فرد دیگری که از اطلاعات حساب کاربری برای دسترسی به کنترل تجهیزات سوءاستفاده می‌کند.

دسترسی‌پذیری اطلاعات جامع اسکادا و BMS یکی از مهم‌ترین ویژگی‌های شناخته شده در این زمینه است. توانایی دسترسی به اطلاعات از هر مکان تنها با استفاده از یک اتصال را می‌توان یک مزیت محسوب نمود. این ویژگی به شکل قابل توجهی باعث صرفه‌جویی در زمان می‌شود. هنگامی که فرایند یا امکانات نظارتی به لحاظ جغرافیایی پراکنده هستند، ارزش صرفه‌جویی در زمان بسیار بیشتر خواهد شد.

در نهایت، باید گفت که راه حل‌های جابجایی‌پذیری مبتنی بر بافتار با بهره‌گیری از C-HMI می‌توانند بهره‌وری، راحتی و قابلیت استفاده سیستم‌های نظارتی را بهبود بخشنند. نظرارت بر مکان استقرار منابع جابجایی‌پذیر و خودکارسازی کنترل‌ها و اطلاعات مبتنی بر بافتار، بهره‌وری و کارایی نیروها را ارتقا می‌دهد. در واقع، با این کار تمام بخش‌های سازمان از ایمنی، امنیت، راحتی و کارایی بیشتر بهره‌مند خواهند شد.

منبع: www.automation.com

دو نکته مهم در تحقیقات مشخص شد. نخست آن که این فناوری سبب استفاده بهینه‌تر از منابع انسانی می‌شود. کاهش زمان مورد نیاز برای راهاندازی یک سیستم را می‌توان یکی از بهبودهای اصلی در این حوزه دانست. از جمله رویه‌های متداول این است که حين مراحل راهاندازی یک نفر در محل مورد نظر مشغول به کار باشد و دیگری در اتاق کنترل مستقر گردد. یکی از مشتریان این فناوری، برای مدیریت انرژی در ساختمان‌های هوشمند، پرده‌های خودکار را ارائه می‌دهد. با بهره‌گیری از C-HMI، تنها یک نفر به تنها یافر خواهد بود فرایند راهاندازی را از راه دور و با کنترل BMS به انجام رساند. این امر چه در هزینه و چه در زمان موجب صرفه‌جویی می‌شود.

نکته دیگر، اعزام کارکنان به صورت بهینه در واکنش به رویدادها است. با استفاده از پروفایل کارکنان جابجایی‌پذیر و در اختیار داشتن گواهینامه‌ها و آموزش‌های آن‌ها، می‌توان نزدیک‌ترین نیروی مورد تأیید را در واکنش به مشکلات به محل اعزام نمود. در یکی از نمونه‌ها، سازمانی حدود ۵۰۰ نیرو در بخش نگهداری داشت که در مکان‌های مختلفی مستقر بودند. ردیابی و مکان‌یابی نیروهای مورد تأیید در چنین سازمانی موجب افزایش قابل توجه کارایی خواهد شد. با آن که گروه‌های نگهداری اغلب تا این اندازه بزرگ نیستند، گروه‌های کوچک‌تر نیز از دریافت اطلاعات درست برای رفع مشکلات موجود منتفع خواهند شد. به طور مشخص، این نکته می‌تواند در مورد موضوعات حساس و نیازمند اقدام سریع بسیار سودمند باشد.

موضوع امنیت یکی از دغدغه‌های مشترک است که در پذیرش سیستم C-HMI نیز حیاتی به نظر می‌رسد. این مسئله شامل



ضرورتی در اقتصاد کسب و کارهای امروزی:

تحقیق رویکرد جدید DevSecOps

است. در نتیجه، شمار روزافزونی از سازمان‌ها به استفاده از رویکرد DevSecOps روی آورده‌اند تا بتوانند با این تغییرات مواجه شوند. نتیجه، شمار روزافزونی از سازمان‌ها به استفاده از رویکرد DevSecOps بر اساس رویکرد مشهور DevOps بنا شده است و امنیت را نیز در چرخه توسعه و آزمایش وارد می‌کند و برنامه‌های کاربردی سریع‌تر، باکیفیت‌تر و امن‌تری را تولید می‌نماید. این تحولات، نقش تیم‌های توسعه را به طور بنیادین تغییر می‌دهند. آن روزها که وظیفه توسعه‌دهندگان تنها تضمین عملکرد مطلوب کدها بود و تیم امنیت مسئول تضمین امن بودن برنامه‌های کاربردی پس از پایان مرحله ساخت آن‌ها به شمار می‌رفت، سپری شده‌اند. امروزه تیم‌های امنیت، توسعه و عملیات باید در تمام مراحل توسعه با یکدیگر همکاری کنند تا برنامه‌های کاربردی با سرعت و امنیت بیشتری نسبت به گذشته تولید، آزمایش و مستقر شوند.

شکاف مهارت‌های امنیتی و تأثیر آن بر کسب و کار
برای رقابت در اقتصادِ روبرشد برنامه‌های کاربردی، سازمان‌ها در تلاشند تا بر سرعت توسعه نرم‌افزارهای خود بیفزایند. بر اساس نتایج نظرسنجی Veracode و DevOps.com، حدود ۴۰ درصد از سازمان‌ها اعلام کرده‌اند که یافتن کارکنان متخصص و جامع در حوزه DevOps که از دانش کافی در زمینه تست امنیتی برخوردار باشند، دشوارتر از یافتن سایر مهارت‌ها است. در زمینه عملیات IT

افزایش مخاطرات در فضای کسب و کار، موضوع امنیت را در صدر اولویت‌های رهبران سازمان‌ها جای داده است. در نتیجه، شمار روزافزونی از سازمان‌ها به استفاده از رویکرد DevSecOps روی آورده‌اند تا بتوانند با این مخاطرات، مقابله کنند. DevSecOps بر اساس رویکرد مشهور DevOps بنا شده است؛ اما امنیت را نیز در چرخه توسعه و آزمایش، وارد می‌کند و برنامه‌های کاربردی سریع‌تر، باکیفیت‌تر و امن‌تری را تولید می‌نماید.

انقلاب دیجیتال، کسب و کارها را وادار ساخته است تا شیوه عرضه محصولات و خدمات خود را تغییر دهند. تا پیش از این، توسعه نرم‌افزار اغلب جزو وظایف بک‌آفیس قلمداد می‌شد، در حالی که امروزه در خطوط مقدم کسب و کار قرار گرفته است و هر تأخیر یا ایراد عملکردی در آن، بر کل کسب و کار تأثیر می‌گذارد و ممکن است میزان درآمد سازمان یا سطح رضایت مشتریان را تحت تأثیر قرار دهد. مسائل امنیتی نیز چالش‌های دیگری را پیش روی کسب و کارها قرار می‌دهند. تنها در سال گذشته میلادی از هر ده سازمان، هفت سازمان تحت تأثیر حملات سایبری یا رخنه به داده‌ها قرار گرفته‌اند. این افزایش مخاطرات، موضوع امنیت را در صدر فهرست اولویت‌های رهبران ارشد سازمان‌ها جای داده

امروزی هماهنگ نشده‌اند. به طور معمول، تنها یک تا دو ساعت از کلاس‌های دانشگاهی به مقوله طراحی امن، یک تا دو ساعت به برنامه‌نویسی دفاعی، دو ساعت آموزش اختیاری برای امنیت شبکه و یک ساعت نیز برای تهدیدات و حملات اختصاص داده می‌شود. به گفته یکی از استادی دانشگاهی: «به جای این که منتظر کسی باشیم تا کلاسی با موضوع امنیت برگزار کند، این آموزش‌ها باید از ابتدا در برنامه آموزشی جای داده شوند».

اما ارتقای کیفیت برنامه‌ها، تنها بر عهده دانشگاه‌ها و مراکز آموزشی نیست، بلکه صنعت هم باید وارد عمل شود. برنامه‌های آموزشی کنونی فاقد آموزش‌های واقعی نظریه کدنویسی ورودی و خروجی هستند (که بسیاری از آسیب‌پذیری‌ها در آن نهفته است) و تأکیدی روی آموزش‌های امنیتی عملی که در حال حاضر حداقل زمان ممکن صرف آن‌ها می‌شود، ندارند. در نظرسنجی DevSecOps، نظرات ۴۰۰ کارشناس IT در سراسر جهان گردآوری شده است. ۶۴ درصد از این کارشناسان اظهار داشته‌اند که ارزشمندترین مهارت‌های خود را در کار آموخته‌اند، در حالی که تنها سه درصد از آن‌ها مهارت‌های ویژه شغلی خود را از طریق تحصیل به دست آورده‌اند. این فاصله زیاد به خوبی نشان می‌دهد که مدیران IT و رهبران این حوزه باید برای اصلاح برنامه‌های آموزش دانشگاهی وارد عمل شوند. در مجموع، راه درازی در پیش است تا بتوان اطمینان یافته که نسل آتی، با برخورداری از مهارت‌های مناسب وارد بازار کار می‌شود؛ به ویژه که اقتصاد برنامه‌های کاربردی هیچ نشانه‌ای از کاهش رشد را نشان نمی‌دهد.

آینده امنیت DevOps

رفع این شکاف مهارتی در زمینه DevSecOps نیازمند آن است که تمام کسب‌وکارها، ذهنیت خود را تغییر دهند. گرچه رویکردهای پیاده‌سازی در هر سازمانی متفاوت از دیگری است، اما همه سازمان‌ها باید این را درک کنند که مشکل کمبود استعدادها، یک اولویت است و کلیت کسب‌وکار را تحت تأثیر قرار می‌دهد. این تغییر فرهنگی باید از سطوح بالای سازمان سرچشمه بگیرد؛ یعنی مدیران IT باید تیم مدیریت ارشد را در خصوص ضرورت آموزش کارکنان، آگاه سازند. در این صورت، این ذهنیت در تمام سازمان جریان می‌پابد. البته تمرکز تنها روی توسعه‌دهندگان نیست، بلکه باید تیم‌های امنیت و عملیات را نیز شامل شود. هر یک از نقش‌آفرینان در محیط DevSecOps باید درک دقیقی از اصول امنیت و DevOps داشته باشند تا راهبرد جدید به خوبی کار کند. مدیران IT می‌توانند از این چهار شیوه برای به جریان انداختن روند تغییرات بنیادین در سازمان استفاده کنند:

آموزش امنیت در هر فرصتی: همان طور که در آموزش عالی نیز می‌بینیم، امنیت نمی‌تواند یک واحد درسی جداگانه و مستقل باشد و باید در تمامی واحدهای آموزشی گنجانده شود. اگر سازمان‌ها اصول امنیتی را در تمامی فرصت‌های آموزشی خود بگنجانند، کارکنان می‌توانند این اصول را بهتر بیاموزند، نحوه استفاده از آن‌ها

نیز دو مهارت مهم که یافتن آن‌ها در افراد بسیار دشوار است به مدیریت آسیب‌پذیری و مهارت‌های محفظه‌بندی^۱ مربوط می‌شود. این شکاف مهارتی می‌تواند بسیاری از سازمان‌ها را از دستیابی به اهداف خود در عرضه برنامه‌های کاربردی باز دارد. تنها بخش کوچکی از پاسخ‌دهندگان به این نظرسنجی (در حدود یک‌دهم از آن‌ها) به استفاده از رویه‌های DevOps در کل فرایند سازمانی، از توسعه تا تولید، اشاره کرده‌اند. اکثر آن‌ها از DevOps در تیم‌های محدود یا به صورت مجلزاً از کسب‌وکار استفاده نموده‌اند، در حالی که دیگر سازمان‌ها هنوز کار را شروع نکرده‌اند و بنا دارند مسیر حرکت خود را به سوی DevOps در طول سال آینده آغاز کنند.

گرچه آموزش درون‌سازمانی می‌تواند سهم بزرگی در کاهش این شکاف مهارتی داشته باشد، ۷۰ درصد از توسعه‌دهندگان عنوان کرده‌اند که سازمانشان آموزش کافی را در زمینه امنیت برنامه‌های کاربردی به آن‌ها ارائه نکرده است؛ حتی بسیاری از متخصصان امنیتی نیز چنین نظری داشته‌اند. یکی از مهم‌ترین موانع سازمان‌ها در مسیر سرمایه‌گذاری آموزشی، هزینه‌های این فرایند و تأثیرات آن بر منابع سازمانی است. اکثر دوره‌های شناخته‌شده‌ی آموزش امنیتی برنامه‌های کاربردی، نیازمند صرف هزینه‌های گراف هستند و چند روز از زمان توسعه‌دهنده را اشغال می‌کنند. البته روش‌های آموزشی دیگری نیز وجود دارند و لازم نیست آموزش کارمندان چنین متمرکز و یکباره باشد.

برنامه‌های آموزش مجازی یا خودآموز، شیوه‌های مؤثری برای کسب مهارت‌های مورد نیاز این مشاغل هستند. این برنامه‌ها به اعضای تیم اجازه می‌دهند تا با سرعت مناسب خود حرکت کنند و فرایند آموزش را با زمان‌بندی کاری خود هماهنگ سازند. متأسفانه، تنها نیمی از پاسخ‌دهندگان به نظرسنجی گفته‌اند که سازمانشان تمام هزینه آموزش آن‌ها را پرداخت می‌کند. امروزه، سرمایه‌گذاری در آموزش ضمن کار می‌تواند تضمین کند که سازمان، آمادگی بهتری برای مواجهه با تقاضاهای آتی دارد. تکیه صرف روی مهارت‌های تحصیلی دانش‌آموختگان دانشگاهی، ممکن است سازمان را با شکست مواجه سازد.

كمبودهای آموزش عالی

توسعه‌دهندگان جدید یا دانش‌آموختگان حوزه IT، مهارت‌های مورد نیاز برای موفقیت در محیط امروزی که تماماً مبتنی بر برنامه‌های کاربردی است را ندارند. متأسفانه این امر ناشی از نواقص موجود در سیستم‌های آموزش رسمی کنونی است. اکثر قریب به اتفاق پاسخ‌دهندگان به نظرسنجی جهانی مهارت‌های DevSecOps در سال ۲۰۱۷ اظهار داشتند که برای اخذ مدرک دانشگاهی خود الزامی به گذراندن هیچ دوره آموزشی خاصی که روی مسائل امنیتی تمرکز داشته باشد، نداشتند. با توجه به اهمیت روزافزون امنیت برای بقای کسب‌وکارها، چنین چیزی بسیار تعجب‌آور است. بسیاری از متخصصان در این نظرسنجی عنوان کرده‌اند که برنامه‌های مرسوم آموزش علوم رایانه، با نیازهای امنیتی سازمان‌های پرستاب

را در موارد واقعی مشاهده کنند و در نهایت، خروجی بهتری برای کسبوکار داشته باشند.

بر اساس نتایج نظرسنجی Veracode و DevOps.com حدود ۴۰ درصد از سازمان‌ها اعلام کرده‌اند که یافتن کارکنان متخصص و جامع در حوزه DevOps که از دانش کافی در زمینه تست امنیتی برخوردار باشند، دشوارتر از یافتن سایر مهارت‌ها است. در زمینه عملیات IT نیز دو مهارت مهم که یافتن آن‌ها در افراد بسیار دشوار است به مدیریت آسیب‌پذیری و مهارت‌های محفظه‌بندی^۱ مربوط می‌شود.

containerization-۱

حال، چنین اقداماتی در بلندمدت تضمین می‌کنند که نسل آتی دانش‌آموختگان، برای حضور موفق در کسبوکارهای مبتنی بر برنامه‌های کاربردی، مجهز‌تر خواهند بود.

بر طرف نوden شکاف موجود در حوزه DevSecOps در کوتاه‌مدت ممکن نیست. سازمان‌ها باید همین امروز اقدامات لازم برای ارتقای مهارت توسعه‌دهندگان، آموزش تیم‌های امنیتی و ایفای نقشی فعالانه در پرورش توسعه‌دهندگان آتی را آغاز کنند. این تنها مسیری است که می‌توان رشد کسبوکار را تضمین کرد و اقتصاد برنامه‌های کاربردی را نیز برای امروز و فردا، امن ساخت.

منبع: www.itproportal.com

افزایش ارزش از طریق کاربردپذیری: صرف نظر از این که برنامه آموزشی برای توسعه‌دهندگان تدوین شده است یا تیم‌های عملیات و امنیت، این برنامه باید هدفمند باشد و برای هر یک از مشاغل و نقش‌ها، طراحی شود. گرچه هر نقش باید از دانش DevOps یا اصول امنیتی برخوردار باشد، اما بر حسب جایگاه شغلی و مجموعه مهارت‌های مورد نیاز برای آن جایگاه، سطح این دانش می‌تواند متفاوت باشد. ارزشیابی سطح دانش اولیه اعضای هر تیم و ارائه آموزش بر مبنای آن، تصمین خواهد کرد که سازمان، بودجه خود را در آموزش‌های غیرضروری صرف نکرده است و کارکنان بیشترین ارزش ممکن را از آموزش به دست آورده‌اند.

سرمایه‌گذاری در آموزش مستمر: آموزش مستمر، امری ضروری برای عرضه مستمر و امن نرم‌افزارها است. اگر اعزام توسعه‌دهندگان به کلاس‌های آموزشی بیرون از سازمان دشوار است، می‌توان کارشناسان امنیت برنامه‌های کاربردی را برای آموزش کارکنان به سازمان دعوت کرد و دوره‌ها را ضمن کار برگزار نمود.

مشارکت و ارتباط با جامعه امنیت: تشویق تیم ارشد مدیریت یا توسعه‌دهندگان و رهبران امنیتی به حضور در فضای آموزش عالی یا ارائه مشاوره گرچه ممکن است فواید فوری و کوتاه‌مدتی برای سازمان نداشته باشد، اما ارزش انجام آن را دارد. این فعالیت‌ها می‌توانند در قالب برگزاری دوره‌های آشنایی با فضای کار سازمان، برنامه پذیرش کارآموز یا ارائه مشاوره در خصوص برنامه‌های آموزشی و مهارت‌های موردنیاز برای نیروی کار باشد. به هر



أخبار کوتاه

آلودگی سرورهای Redis به بدافزار

بنا بر گزارش‌ها، ۷۵ درصد سرورهای Redis به بدافزار آلوده شده‌اند. وبسایت Redis در پاسخ به علت این آلودگی اعلام کرد Redis برای دسترسی کلاینت‌های مورداعتماد در محیط‌های مطمئن طراحی شده است و نباید مستقیماً در اینترنت یا در محیط‌هایی که کلاینت‌های نامطمئن مستقیماً به آن‌ها دسترسی دارند، قرار بگیرد. در واقع، Redis از حداکثر امنیت برخوردار نیست (به عبارتی از رمزگذاری پشتیبانی نمی‌کند، کنترل دسترسی ندارد و داده‌ها را در متن‌های ساده ذخیره می‌کند)، بلکه از حداکثر کارابی و سادگی بهره‌مند است و به همین جهت، نباید در خارج از شبکه داخلی در دسترس باشد.

آسیب‌پذیری سرورهای کدباز

گزارش‌هانشان می‌دهند سه‌چهارم سرورهای کدبازی که مورد بررسی قرار گرفته‌اند دارای آسیب‌پذیری‌های هستند که رفع نشده‌اند.

آسیب‌پذیری برنامه‌های کاربردی

براساس نتایج گزارش‌ها، با این که ۸۴ درصد از مهاجمان سایبری به جای شبکه‌ها به برنامه‌های کاربردی حمله می‌کنند، اما متأسفانه، امنیت ۸۰ درصد از برنامه‌های کاربردی توسعه‌یافته برای اینترنت اشیا (IoT) حتی تست هم نشده است تا آسیب‌پذیری‌های آن‌ها شناسایی شود.

بی‌اعتمادی توسعه‌دهندگان به امنیت کدهای خود

طبق گزارش سال ۲۰۱۷ وبسایت TechRepublic، حدود ۶۰ درصد توسعه‌دهندگان به امنیت کدهای خود اطمینان ندارند؛ اما برای تأمین امنیت آن‌ها هم کاری نمی‌کنند. به گفته شرکت‌های Sqreen و NodeSource، بخشی از این مشکل ناشی از عدم تست برنامه کاربردی است؛ چرا که بسیاری از توسعه‌دهندگان برنامه کاربردی را تست نمی‌کنند.

امنیت کدهای شخص ثالث

بنابر گزارش مشترک شرکت‌های Sqreen و NodeSource، تنها ۱۶ درصد توسعه‌دهندگان به کدهای شخص ثالثی که به کار می‌گیرند، اعتماد دارند. با این حال، ۴۰ درصد توسعه‌دهندگان این مؤلفه‌های شخص ثالث را بازبینی نمی‌کنند. از این رو، متخصصان توصیه می‌کنند که تمام مأذول‌های شخص ثالث را با دقیق بررسی کنید تا مطمئن شوید امنیت دارند.

تهدیدات توخالی حملات فیشینگ جدید

اخيراً، حملات فیشینگ جدیدی به راه افتاده است که مهاجمان آن‌ها ادعا می‌کنند سیستم‌ها را به باجافزاری (ransomware) به نام WannaCry آلوده می‌سازند و داده‌ها را رمزگذاری می‌کنند. در نهایت هم، اقدام به درخواست بیت‌کوین (bitcoin) می‌نمایند. اما پژوهشگران به این نتیجه رسیدند که این ادعا تهدیدی توخالی و صرفاً برای ترساندن قربانیان است.

وضعیت بدافزارها در سال ۲۰۱۷

طبق گزارش سالانه وضعیت بدافزارها، حملات باجافزاری (ransomware) مخرب در کل دنیا در سال گذشته تا ۷۰۰ درصد افزایش یافت.

افزایش حملات DDoS

نتایج گزارش Akamai نشان می‌دهد تعداد حملات DDoS ثبت‌شده از سال گذشته تا کنون ۱۶ درصد، حملات در سطح برنامه کاربردی نظریه تزریق SQL حدود ۳۸ درصد و حملات در سطح زیرساخت حدود ۱۶ درصد افزایش یافته است.

افزایش مخاطرات سیستم‌های کنترل صنعتی به دلیل استفاده از IoT

طبق گزارش کاسپرسکی، بسیاری از سازمان‌های فعال در حوزه صنعت در حال روی آوردن به استفاده از اینترنت اشیا (IoT) هستند، اما توجه ندارند که این امر در کنار مزایایی که به ارمنان می‌آورد، مخاطراتی هم به همراه دارد. در واقع، آن‌ها اقدامات حفاظتی را به اندازه کافی رعایت نمی‌کنند و بدین ترتیب، دسترسی مجرمان سایبری به این سیستم‌ها را آسان‌تر می‌سازند. حدود ۶۵ درصد سازمان‌ها بر این باورند که احتمال به خطر افتادن امنیت سیستم‌های کنترل صنعتی (ICS) از طریق اینترنت اشیا زیاد است.

تهدیدات ناشی از سیستم‌های کنترل صنعتی در سازمان‌ها

نتایج گزارش جدید کاسپرسکی حاکی از آن است که بیش از ۷۷ درصد سازمان‌ها معتقدند این احتمال وجود دارد که سازمانشان از طریق سیستم‌های کنترل صنعتی (ICS)، هدف مجرمان سایبری قرار بگیرد.

مشکلات امنیتی هات‌اسپات‌های وای‌فای در جام جهانی فوتبال

بررسی‌های شرکت کاسپرسکی نشان داد پیش از ۲۰ درصد هات‌اسپات‌های وای‌فای در شهرهای میزبان جام جهانی فوتبال دارای مشکل امنیتی هستند. از بین ۳۲ هزار شبکه وای‌فای عمومی در این شهرها، ترافیک حدود ۷۲۰۰ مورد رمزگذاری نشده است. از این‌رو، متخصصان این شرکت توصیه می‌کنند کاربران در استفاده از این شبکه‌ها دقت داشته باشند و برای اینکه هدف مجرمان سایبری قرار نگیرند، گزینه Always use a secure connection را در دستگاه‌های خود فعال سازند.

بی‌توجهی کسب‌وکارها به تدوین راهبرد امنیتی مناسب

بنابریک نظرسنجی، ۶۲ درصد از کسب‌وکارهای کوچک و بزرگ، به صورت جدی راهبرد مناسبی در حوزه افتاده اند. این در حالی است که به گفته شرکت سیمانک، رخنه به داده‌ها نه تنها هزینه بالایی را به سازمان‌ها تحویل می‌کند، بلکه تأثیرات منفی زیادی در بهره‌وری، زمان کارکنان و کاهش اعتبار برنده کسب‌وکارها دارد و در بدترین حالت، می‌تواند باعث از دست دادن کامل کسب‌وکار شود.