یادداشت

جنگ و خطا در تشخیص نبودن آن

ادامه از صفحه اول

به باور بسیاری از کارشناسان، دشواری و سختی مأموریت دستگاه دیپلماسی کمتر از نیروهای نظامی کشور نیست. پیروزی و موفقیت سیاست خارجی کشور می‌تواند زمینه‌ساز پایان جنگ و برگشت صلح و آرامش به کشور باشد. در این وضعیت عده‌ای با ترور دیپلماسی، موانعی را برای دیپلمات‌های ایرانی در عرصه نبرد سیاسی فراهم می‌آورند. فراموش نکنیم دیپلماسی همواره در طول تاریخی ابزاری قوی برای ایجاد مصالحه بوده است. طبق شواهد تاریخی و طبق گفته آقای سیدحسین موسویان در کتاب «ایران، آمریکا، تعامل یا تقابل»، در طول جنگ ایران و عراق و در اوج بی‌اعتمادی، دو کشور میز مذاکره را ترک نکردند. همچنین شوروی و آمریکا در زمان جنگ سرد و با وجود خصومت‌ها و بی‌اعتمادی‌ای که به یکدیگر داشتند، مذاکرات سیاسی را حفظ کردند و... . آنچه مسجل است، اینکه هیچ جنگی تا ابد ادامه نیافته و جنگ‌ها بالاخره روزی پایان می‌یابند؛ زیرا نمی‌شود انتظار داشت کشورها در یک جنگ ابدی و بی‌پایان برای گرفتن انتقام باقی بمانند. به گفته گاندی، با رعایت قاعده چشم در مقابل چشم همه کور می‌شوند. سخن آخر اینکه به‌گواه تاریخ، جنگ‌ها جز ویرانی، مرگ، آوارگی و فروپاشی اقتصاد، ارمغان دیگری همراه خود ندارند. همان‌طور که ذکر شد، تشخیص نبودن جنگ کار سخت و دشواری است. اگر چند سال قبل به هریک از ما وقوع جنگ را در آینده گوشزد می‌کردند، برای اکثر ما باورپذیر نبود. شاید امنیت، صلح و آرامش مانند یک دارایی نامشهود در نگاه ما فاقد ارزش و جایگاه ممتازی بود. از آنجایی که این دارایی ناآگاهانه و غیراکتسابی در اختیارمان قرار داشت، اهمیت چندانی برای بودن آن قائل نبودیم. زمانی ارزش دارایی‌های غیراکتسابی و اهمیت آنها را در کیفیت زندگی درک می‌کنیم که وجود و تداوم آنها دچار تردید شود. ازاین‌رو ضروری است با وجود تحمیل جنگ ناجوانمردانه توسط نیروهای بیگانه، با حمایت از مسئولان سیاسی کشور، زمینه را برای موفقیت دیپلماسی برای کشور فراهم آوریم تا از این طریق بار دیگر صلح و آرامش به کشور بازگردد و زیر سایه امنیت، مصائب و مشکلات کشور فروکش کنند.

ایران و آمریکا؛ جنگ و ناجنگ در ۳ سناریو

ادامه از صفحه اول

جنگ پرشدت فراگیر، زمانی برای تسویه‌حساب خونین پنج دهه خصومت نهادینه‌شده پیدا و پنهان میان ایران و آمریکاست و طرفین تمامی داشته‌ها، ابزار و دارایی‌های تاکتیکی و استراتژیک خود را به صحنه خواهند آورد و به کار خواهند گرفت. در سناریوی سوم به دلیل آنکه در یک سو بقای جمهوری اسلامی و از سوی دیگر اعتبار و تداوم هژمونی آمریکا بر روی میز قرار می‌گیرد، در آن حدود و ثغور جغرافیایی، جنگی، حقوقی و اخلاقی، وجود نخواهد داشت و طرفین صد از صد خود را برای هزیمت و هلاکت طرف مقابل به کار خواهند گرفت. بنابراین در سناریوی سوم، جنگ بدون مرز در تمامی سطوح و اشکال شامل جنگ هوایی، موشکی، دریایی، زمینی، فضایی، ترور و اشغال سرزمین وجود خواهد داشت و همچنین احتمال استفاده از بمب هسته‌ای تاکتیکی، بمب کثیف و بمب هسته‌ای در آن متصور خواهد بود. در سناریوی سوم، طرفین از ائتلاف‌های خود در بالاترین سطح بهره خواهند برد. به نظر می‌رسد تا پیش از وقوع جنگ پرشدت فراگیر، نیروهای نیابتی ایران در معرض فرسایش و ریزش قرار بگیرند ولی در صورت تداوم قدرت عملیاتی، نیروهای نیابتی ایران شامل حزب‌الله، حماس، حشدالشعبی، حوثی‌ها و سلول‌های خفته ایران در منطقه و جهان در بالاترین سطح ممکن خود به کنشگری خواهند پرداخت. در طرف آمریکا نیز اسرائیل با شدت و حدت وارد ماجرا خواهد شد و کشورهای جنوب خلیج فارس با اجباری رضایتمندانه وارد جنگ خواهند شد و ائتلاف عربی-عبری شکل خواهد گرفت. احتمال همکاری سطح بالا و غیرمستقیم ناتو با آمریکا بسیار بالا خواهد بود و در صورت به مشکل افتادن آمریکا، دخالت مستقیم انگلستان و فرانسه و احتمالا آلمان و در ادامه ناتو دور از ذهن نیست، به ویژه آنکه اگر یکی از اعضای ناتو مورد حمله قرار گرفته باشد. همچنین حضور مستقیم و غیرمستقیم متحدین آمریکا در شرق آسیا یعنی ژاپن، کره جنوبی و استرالیا را نباید نادیده گرفت. از ترکیه در چارچوب ناتو و پاکستان در چارچوب پیمان مکه، می‌توان انتظار اقدامات غیرمستقیم علیه ایران را داشت. از منظر جغرافیایی، در صورت وقوع جنگ پرشدت فراگیر، جنگ در محدوده خلیج فارس و دریای عمان و کشورهای پیرامون آغاز خواهد شد و با تشدید نردبانی جنگ، در ادامه جنگ فراگیر به محدوده دریای سرخ، دریای مدیترانه، دریای سیاه، اقیانوس هند، شرق اروپا و احتمالا منطقه قفقاز تسری خواهد یافت. در سناریوی سوم، زیرساخت‌های انرژی و صنعتی کشورهای درگیر در معرض تهاجم و نابودی خواهد بود و دارایی‌های کشورهای منطقه که ماحصل فروش نفت در صد سال اخیر است، دود خواهد شد تا این کشورها برای بازسازی آن دوباره، چند هزار میلیارد ثروت انباشته‌شده و آتی را به شرکت‌های نفتی آمریکایی و غربی بپردازند. و سخن پایانی با این پرسش که کدام سناریو در واقعیت محقق خواهد شد؛ پاسخ اینکه آن سناریویی که پس از خواندن این مطلب، خود شما دلواپسانه انتظار تحقق آن را دارید. حال، دستان و چشمان خود را به آسمان بدوزید؛ تنها یاریگر ما آنجاست. جایی بسیار دور اما نزدیک؛ از او یاری بجویید.

گزارش «شرق» از بحران تمدید گواهی امنیتی بانک‌ها و راه‌حلی که خود می‌تواند بحران تازه‌ای بسازد

بانکداری آنلاین در لبه ناامنی

سونیتا سراب‌پور

حتما در یک ماه گذشته با مراجعه به وب‌سایت بانک‌های کشور با این پیام روبه‌رو شده‌اید که «ارتباطات شما امن نیست، و اگر بخواهید به کار با این وب‌سایت ادامه دهید، اطلاعات شما در خطر قرار می‌گیرد». از سوی دیگر، بانک‌های کشور از جمله ملی و ملت با ارسال پیامک‌هایی به مشتریانشان به آنها می‌گویند برای دسترسی پایدارتر به خدمات بانکی، آدرس برخی خدمات آنها به‌روزرسانی شده است. این بانک‌ها لینک‌های مختلفی در اختیار کاربران می‌گذارند که اگر با هشدار امنیتی مواجه شدند، از آنها استفاده کنند. این اتفاق از اثرات شدت‌گرفتن تحریم‌های آمریکاست که حالا در فضای وب دامن بانک‌ها و مؤسسات مالی را گرفته است. تغییر آدرس بانک‌ها برای دورزدن گواهی امنیتی یک راه‌حل موقت است و در آخر باعث می‌شود (اگر همچنان تحریم‌ها ادامه پیدا کند) بانک‌ها به سمت استفاده از ظرفیت داخلی صدور گواهی بروند که اتفاقا این راه هم از نظر بسیاری از کارشناسان فناوری پیامدهای امنیتی دارد. کارشناسان در گفت‌وگو با «شرق» اعلام می‌کنند تحمیل گواهی‌های ریشه ملی فاقد اعتبارسنجی جهانی بر دستگاه‌های کاربران، بستری پرمخاطره برای امنیت سایبری و تضعیف اعتماد به خدمات پرداخت الکترونیک به وجود خواهد آورد. حتی برخی دیگر این شرایط را مناسب برای بازگشت پروژه «فیلترینگ هوشمند» می‌دانند؛ چراکه دیگر خبری از سیستم رمزگذاری پیچیده و قابل اعتماد در فضای وب نیست. به نظر می‌رسد بحران جدید در تجارت الکترونیک ایران این‌بار جایی ریشه‌ای را هدف گرفته که بی‌توجهی به آن ما را یک قدم دیگر به یک جزیره دورافتاده ناامن نزدیک‌تر می‌کند.

گواهی‌نامه‌ها چطور کار می‌کنند؟

بانکداری الکترونیک و سامانه‌های تبادل مالی آنلاین بر پایه‌ای از پروتکل‌های رمزنگاری و سازوکارهای اعتبارسنجی بین‌المللی استوار است. پروتکل امنیت لایه انتقال (TLS)، ستون فقرات محرمانگی، جامعیت داده‌ها و احراز هویت در وب مدرن به شمار می‌روند. بروز اختلال در تمدید، صدور و در مواردی ابطال ناگهانی گواهی‌های امنیتی ارائه‌شده به شرکت شبکه الکترونیکی پرداخت کارت (شاپرک)، بانک مرکزی و مؤسسات مالی بزرگ کشور، یک مسئله بنیادین فنی را به کانون کشمکش‌های ژئوپلیتیکی و حقوقی بدل کرده است.

پروتکل TLS تضمین می‌کند داده‌های مبادله‌شده میان مرورگر کاربر و کارگزار وب، از گزند استراق سمع و دستکاری در طول مسیر (تمامیت داده) در امان بمانند. با این حال، مهم‌ترین کارکرد این پروتکل که زیربنای دو اصل پیشین محسوب می‌شود، احراز اصالت هویت طرفین ارتباط، به‌ویژه هویت کارگزار است. این احراز هویت بر بستر زیرساخت کلید عمومی (PKI) بر پایه استاندارد X.509 شکل می‌گیرد. در این معماری، اعتماد به صورت یک زنجیره پیوسته (Chain of Trust) از بالا به پایین تعریف می‌شود. در رأس این هرم، مرجع صدور گواهی ریشه (Root CA) قرار دارد که گواهی خود را به شکل خودامضا (Self-Signed) صادر می‌کند. کلید خصوصی این مرجع به عنوان یک دارایی به‌شدت محافظت‌شده در ماژول‌های امنیت سخت‌افزاری ایزوله (HSM) نگهداری می‌شود. برای کاهش ریسک افشای کلید ریشه، مراجع ریشه اقدام به امضای گواهی برای مراجع صدور میانی (Intermediate CA) می‌کنند. این مراجع میانی، وظیفه بررسی هویت متقاضیان و صدور گواهی‌های نهایی (Leaf/End-Entity Certificates) را برای دامنه‌های مشخص برعهده دارند. فرایند اعتبارسنجی در سمت مشتری (مرورگر یا سیستم‌عامل) وابسته به «مخزن گواهی‌های ریشه مورد اعتماد» (Trusted Root Store) است. شرکت‌های توسعه‌دهنده سیستم‌عامل و مرورگر نظیر مایکروسافت، گوگل، اپل و موزیلا مجموعه‌ای محدود و به‌شدت غربال‌شده از گواهی‌های ریشه بین‌المللی را درون بسته‌های نرم‌افزاری خود بارگذاری می‌کنند. هنگامی که کاربری قصد دسترسی به یک پایگاه بانکی را دارد، کارگزار وب گواهی دامنه خود و زنجیره مراجع میانی را برای مرورگر ارسال می‌کند. مرورگر با بررسی امضاهای ریاضی به سمت بالا، صحت اتصال این زنجیره را به یکی از مراجع ریشه مستقر در مخزن محلی خود بررسی می‌کند. همچنین از طریق فهرست‌های ابطال گواهی (CRL) و پروتکل بررسی برخط وضعیت گواهی (OCSP)، بررسی می‌شود آیا گواهی مذکور توسط صادرکننده لغو شده است یا خیر. در صورت عدم تطابق زنجیره، انقضای تاریخ یا ثبت ابطال گواهی، مرورگر بلافاصله ارتباط را ناامن اعلام کرده و از تبادل اطلاعات جلوگیری می‌کند.

کنترل نهایی مخازن اعتماد، ریشه در انحصار شمار اندکی از ابرشرکت‌های فناوری مستقر در کشورهای غربی است. هرگونه تصمیم مبنی بر افزودن، تعلیق یا حذف یک مرجع ریشه، تحت تدابیر تنظیمی موسوم به «انجمن مراجع صدور گواهی و مرورگرها» (CA/Browser Forum) اتخاذ می‌شود و شرکت‌ها صلاحیت نهایی اعطای اعتماد را در اختیار خود نگه داشته‌اند.

افتادن در چاله بی‌امنیتی

قطع‌شدن دسترسی وب‌سایت‌ها و بانک‌های ایرانی به گواهی‌نامه‌های امنیتی معتبر داستان تازه‌ای نیست و از سال‌ها پیش و با وجود تحریم‌های همیشگی بین‌المللی وجود داشته است، اما وب‌سایت‌های ایرانی همیشه از طریق واسطه‌هایی توانسته‌اند این تحریم‌ها را دور بزنند و امنیت اطلاعات وب‌سایت خود و کاربرانشان را فراهم کنند. با این حال داستان تمدیدنشدن گواهی امنیت وب‌سایت‌های ایرانی با تشدید تحریم‌های آمریکا از ابتدای شهریورماه جدی‌تر و سخت‌گیرانه‌تر شده است.

نیما امیرشکاری، کارشناس حوزه اقتصاد دیجیتال و مشاور بانکی، در گفت‌وگو با «شرق» درباره وضعیت گواهی‌های امنیتی وب‌سایت‌های بانکی می‌گوید ایران در سال‌های گذشته نیز به‌دلیل تحریم‌ها امکان دریافت مستقیم بسیاری از گواهی‌های امنیتی را نداشته و عمدتا از طریق واسطه‌ها این گواهی‌ها را دریافت می‌کرده است. به گفته او، در سال‌های اخیر نیز بخش قابل توجهی از گواهی‌های دریافت‌شده برای سرویس‌های ایرانی، از طریق واسطه‌ها تهیه می‌شده، اما اکنون با افزایش فشارها، شناسایی و محدودکردن این واسطه‌ها نیز آغاز شده است. او توضیح می‌دهد شرکت‌های صادرکننده گواهی امنیتی، به دلیل محدودیت‌های جدید، ارائه یا تمدید گواهی برای سایت‌های ایرانی را دشوارتر کرده‌اند و در نتیجه برخی گواهی‌های قبلی نیز تمدید نشده یا اعتبارشان از بین رفته است. به گفته امیرشکاری، تغییر مداوم آدرس وب‌سایت‌های بانکی نیز در همین چارچوب قابل بررسی است. او می‌گوید تیم‌های امنیتی بانک‌ها تلاش می‌کنند با استفاده از واسطه‌ها و آدرس‌های جدید، دامنه‌هایی دریافت کنند که در فهرست‌های محدودشده قرار نداشته باشند؛ به همین دلیل ممکن است کاربران شاهد ارسال مکرر آدرس‌های جدید برای دسترسی به خدمات بانکی باشند.

او درباره تبعات عملی ازدست‌رفتن این گواهی‌ها می‌گوید کاربر ممکن است همچنان بتواند با پذیرش هشدار امنیتی مرورگر وارد سایت شود و عملیات بانکی خود را انجام دهد، اما این به معنی امن‌بودن ارتباط نیست. به گفته امیرشکاری، در چنین شرایطی دیگر نمی‌توان تضمین کرد اطلاعات در مسیر ارتباط به شکل امن و رمزگذاری‌شده منتقل می‌شود و کانال ارتباطی، از منظر امنیتی، دیگر وضعیت سابق را ندارد. او تأکید می‌کند این موضوع به معنای شنود قطعی اطلاعات نیست، اما سطح امنیت ارتباط را کاهش می‌دهد و امکان قرارگرفتن اطلاعات در معرض شنود یا دستکاری را ایجاد می‌کند.امیرشکاری معتقد است در چنین شرایطی، اگر تحریم‌ها برداشته نشود، شرکت‌ها ناچار خواهند بود بار دیگر به سراغ واسطه‌ها بروند و از مسیرهای غیرمستقیم برای دریافت گواهی‌های جدید استفاده کنند. به گفته او، حتی ممکن است شرکت‌هایی با نام‌ها و آدرس‌هایی که هیچ ارتباط آشکاری با بانکداری ندارند، به عنوان واسطه وارد این زنجیره شوند؛ برای مثال یک شرکت ایرانی با نامی غیرمرتبط، در کشوری دیگر ثبت و از طریق آن برای دریافت گواهی اقدام شود. او اما نسبت به این راه‌حل غیرمستقیم هشدار می‌دهد؛ چراکه به گفته او، تغییر دامنه‌های رسمی بانک‌ها و استفاده از آدرس‌هایی که ارتباط مشخصی با نام بانک ندارند، می‌تواند زمینه سوءاستفاده و فیشینگ را افزایش دهد. امیرشکاری توضیح می‌دهد وقتی کاربر دیگر با دامنه‌ای مواجه نیست که نام بانک در آن مشخص باشد و به او گفته می‌شود برای ورود به اینترنت‌بانک یا موبایل‌بانک به یک آدرس ناشناس مراجعه کند، تشخیص سایت واقعی از نسخه جعلی دشوارتر می‌شود. به گفته او، همین وضعیت می‌تواند فرصت بیشتری برای کلاهبرداران ایجاد کند: «ممکن است یک پیامک از یک آدرس ناشناس برای کاربر ارسال شود، کاربر روی لینک کلیک کند و وارد سایتی شود که ظاهرا شبیه سایت بانک است و اطلاعات کاربری و رمز عبور خود را وارد کند. در چنین شرایطی، مسیر برای فیشینگ و سوءاستفاده هموارتر می‌شود».

راهی برای شنود و درز اطلاعات

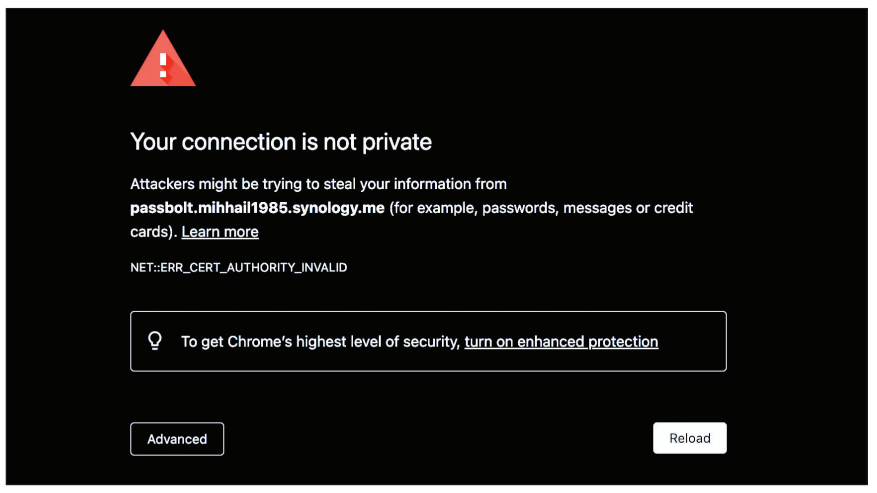
آنچه بیشتر از همه در داستان گواهی امنیتی برای کاربران عادی پررنگ است، مسئله «اعتماد» است. مسئله‌ای که دقیقا آرین اقبال، کارشناس نرم‌افزار و شبکه، به آن اشاره و قطع‌شدن دسترسی به تمدید این گواهی‌نامه‌های امنیتی را از سمتی دیگر نگاه می‌کند. اقبال در گفت‌وگو با «شرق» با اشاره به اهمیت گواهی‌های امنیتی در حفظ امنیت ارتباطات اینترنتی، می‌گوید مسئله اصلی در ماجرای گواهی‌های SSL، صرفا بازنشدن یک وب‌سایت یا نمایش یک هشدار در مرورگر نیست، بلکه موضوع به «اعتماد» در فضای اینترنت برمی‌گردد. به گفته او، TLS و گواهی‌های امنیتی برای این ایجاد شده‌اند که ارتباط میان کاربر و سرویس رمزگذاری شود و افراد یا سیستم‌های واسط در شبکه نتوانند محتوای این ارتباط را مشاهده کنند. در نبود این سازوکار، از شبکه وای‌فای خانگی یا یک کافه و دانشگاه تا سطح اپراتور، امکان شنود ترافیک و سرقت اطلاعات می‌تواند ایجاد شود؛ اطلاعاتی که می‌تواند از نام کاربری و رمز عبور تا اطلاعات بانکی و محتوای تراکنش‌ها را شامل شود. اقبال توضیح می‌دهد شکل‌گیری HTTPS و عمومی‌شدن استفاده از TLS، نتیجه تلاش‌هایی بود که باعث شد رمزگذاری ارتباطات وب به یک استاندارد فراگیر تبدیل شود. پیش از آن، ارتباطات HTTP به‌صورت متن ساده منتقل می‌شد و هر فردی که به شبکه دسترسی داشت، می‌توانست محتوای جابه‌جاشده را ببیند. بعدها با گسترش سرویس‌هایی مانند Lets Encrypt، دریافت گواهی برای وب‌سایت‌ها بسیار ساده‌تر شد و تقریبا همه وب به سمت استفاده از ارتباطات رمزگذاری‌شده رفت. به گفته او، نتیجه این روند افزایش سطح امنیت عمومی اینترنت بود. او درباره تفاوت گواهی‌های صادرشده از سوی مراجع معتبر با گواهی‌های خودامضاشده نیز می‌گوید: «مشکل اصلی در گواهی Self-Signed، شکل‌نگرفتن «زنجیره اعتماد» است. در مدل متعارف، یک مرجع صادرکننده گواهی (CA) هویت و مالکیت دامنه را تأیید و گواهی را امضا می‌کند. مرورگر نیز این زنجیره را تا یک مرجع ریشه بررسی می‌کند و اگر مرجع نهایی در فهرست مراجع مورد اعتماد سیستم‌عامل قرار داشته باشد، ارتباط معتبر شناخته می‌شود». به گفته او اما در گواهی خودامضا، کاربر نمی‌تواند مطمئن باشد گواهی واقعا متعلق به همان سرویس است یا فرد یا نهاد دیگری آن را جعل کرده است؛ به همین دلیل این مدل، جز در موارد خاص، جایگزین مناسبی برای زنجیره اعتماد عمومی نیست. او این وضعیت را از منظر امنیتی بسیار نگران‌کننده می‌داند، چراکه خطر اصلی زمانی ایجاد می‌شود که کاربران به دیدن این خطاها عادت کنند. اقبال توضیح می‌دهد: «اگر کاربر یک یا دو بار با خطای گواهی مواجه شود و مرورگر به او امکان دهد با پذیرفتن ریسک وارد سایت شود، ممکن است به‌تدریج این رفتار برایش عادی شود؛ یعنی هر بار که این هشدار را می‌بیند، آن را رد کند و وارد سایت شود. در این شرایط، اساسا فلسفه امنیت TLS زیر سؤال می‌رود».

به گفته این کارشناس، عادی‌شدن چنین هشدارهایی می‌تواند زمینه را برای حملات مرد میانی (Man-in-the-Middle) فراهم کند. در این حالت، مهاجم می‌تواند خود را میان کاربر و سرویس مورد استفاده قرار دهد و با ارائه یک گواهی نامعتبر، ارتباط را تحت کنترل بگیرد. اقبال تأکید می‌کند در چنین شرایطی، اطلاعات کاربر می‌تواند در معرض شنود قرار بگیرد و این خطر صرفا به هکرها محدود نمی‌شود و می‌تواند برای کلاهبرداران و حتی سامانه‌های نظارتی و فیلترینگ نیز اهمیت پیدا کند.

آیا استفاده از گواهی داخلی امن است؟

در مقابل این وضعیت، بانک مرکزی مسیر دیگری را پیش‌روی شبکه بانکی گذاشته است: استفاده از ظرفیت داخلی برای صدور گواهی‌های امنیتی. بانک مرکزی این موضوع را به بانک‌ها ابلاغ کرده و حالا نخستین بانک‌ها وارد فرایند دریافت گواهی از زیرساخت داخلی شده‌اند. تاکنون دست‌کم ۱۱ بانک این فرایند را آغاز کرده‌اند و با توجه به ابلاغ صورت‌گرفته به بانک‌های عامل، انتظار می‌رود تعداد بانک‌های متقاضی افزایش پیدا کند.

گزارش کامل را در سایت شرق بخوانید



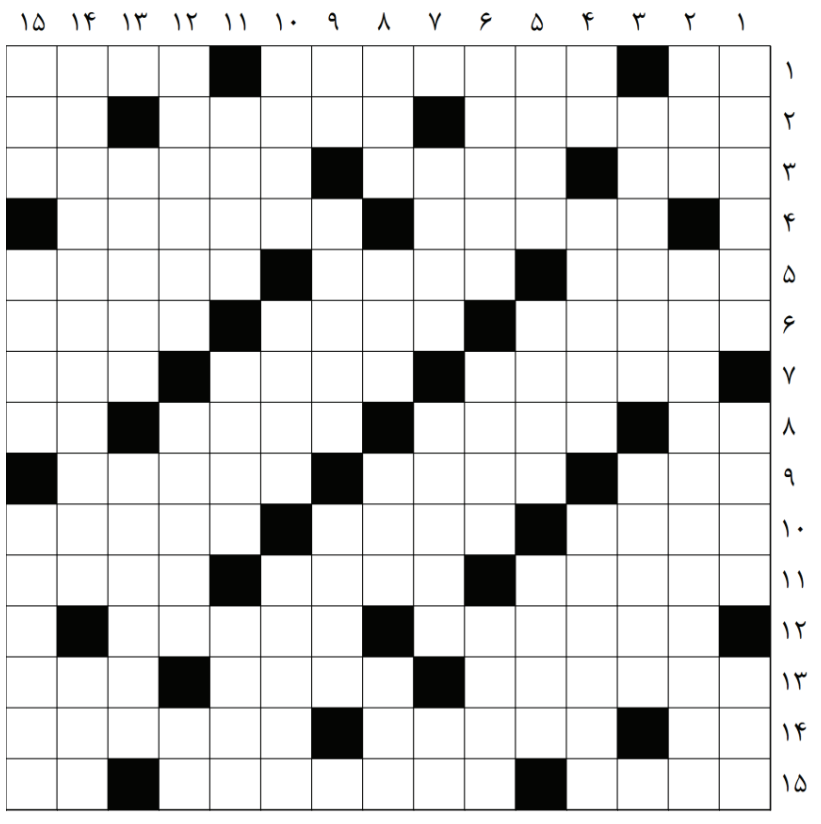
جدول ۵۴۰۴ طراح: بیژن گورانی

افقی:

۱- کشنده بی‌صدا- مرتکب معصیت- مهم‌ترین عامل دیابت ۲- دزدیده گوش‌کردن- آسودگی- عدد قرن ۳- چین‌وچروک پوست- حالت گازی آب- هنر و علم طراحی ساختمان ۴- دایره‌المعارف فرانسوی- عنکبوت ۵- چاردیواری مسقف- پردازش عکس- تکنسین ۶- رمان مشهور پائولو کوئیلو- مهم‌ترین محصول کشاورزی رفسنجان- اشک‌ریختن ۷- فرزند کیومرث در شاهنامه- شهری در عربستان- درخت تسبیح ۸- مکان- تشویق‌کننده- از اجزای دوچرخه- انتها ۹- نیروی جاذبه‌ای که زمین به یک جسم وارد می‌کند- کبیر- گلی آپارتمانی ۱۰- گازی قابل اشتعال- ماشین‌نویسی- طلای کثیف ۱۱- ماده اصلی گلوله- بخش انتهایی پرچم گل- فلزی جامد که با آب و اکسیژن به‌شدت واکنش می‌دهد ۱۲- کپی- از طرح‌های شناخته‌شده فرش دستباف ایرانی ۱۳- پزشک دربار فراعنه مصر- آهسته- پدران ۱۴- سیخونک- مغفرت- غذای اصیل بندر ترکمن ۱۵- آگهی تلویزیونی- آشپز نیکوکار ضحاک- پیشوند سلب

عمودی:

۱- از هفت‌قلم آرایش قدیم بانوان- پاسخ- بدون استحکام ۲- حیوانی که نماد سلامتی است- نوعی فوبیای رایج ۳- نوای آرام‌بخش مادر برای خواب کودک- درختی برگ، ریز و زیبا ۴- تکرار حرفی- دست به کاری زدن- لباس تازه دوخته‌شده ۵- میوه تازه به بازار آمده- شب پیش‌رو- تصور و خیال ۶- عنوانی برای سرباز آموزشی- دختر رنج‌کشیده رمان بینوایان- مجموعه مسکونی بزرگ ۷- جلگه پهناور در نواحی نیمه‌خشک- خویشاوندی- طلا ۸- سرمایه جاودانی است- میان- موی بلند- سنگ سبز قیمتی ۹- مخفف اگر- قتل‌عام- شاگرد مغازه ۱۰- خدای هندو- جثه، اندام- بندری در پاکستان ۱۱- شناساننده- رستگار- مقابل دریا ۱۲- بخیل- کوچه‌ای که فقط از یک طرف گذرگاه دارد- سرای محبت ۱۳- قصیده‌سرای ایرانی قرن ششم- قاضی تحقیق ۱۴- تابلوی نقاشی رنگ روغن اثر هنرمندانه ایران درودی- پرتابه جنگی ۱۵- دستی- جرئت- مشایعت



حل سودوکو ۴۳۹۹

۴	۳	۵	۶	۷	۱	۲	۹	۸
۷	۲	۱	۹	۴	۸	۳	۶	۵
۶	۹	۸	۲	۳	۵	۱	۷	۴
۸	۶	۹	۱	۲	۴	۷	۵	۳
۳	۱	۴	۵	۸	۷	۶	۲	۹
۵	۷	۲	۳	۶	۹	۴	۸	۱
۱	۴	۷	۸	۹	۶	۵	۳	۲
۹	۵	۳	۷	۱	۲	۸	۴	۶
۲	۸	۶	۴	۵	۳	۹	۱	۷

۲	۶	۸	۵	۴	۹	۱	۷	۳
۱	۹	۳	۲	۶	۷	۵	۸	۴
۵	۷	۴	۳	۸	۱	۶	۲	۹
۷	۸	۹	۴	۲	۵	۳	۱	۶
۴	۵	۲	۶	۱	۳	۸	۹	۷
۳	۱	۶	۷	۹	۸	۲	۴	۵
۹	۴	۱	۸	۵	۶	۷	۳	۲
۸	۳	۵	۹	۷	۲	۴	۶	۱
۶	۲	۷	۱	۳	۴	۹	۵	۸

حل جدول ۵۴۰۳

۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	
■	ی	ن	و	گ	ر	گ	د	■	ن	ا	ر	و	ا	خ	۱
ا	س	و	ر	■	د	ر	ا	م	ا	■	ه	ب	ز	ا	۲
ن	ن	س	■	ا	ی	م	ی	ر	■	ت	ب	ا	ب	ط	۳
ج	ا	ن	ف	س	ا	■	ن	ا	ت	ر	ا	■	ک	ر	۴
م	■	گ	ن	ر	ب	ا	■	ر	ب	و	ن	ص	■	ا	۵
ن	ا	ی	د	ا	■	ب	ه	ت	ل	م	■	ی	ر	ت	۶
ش	ع	■	ق	ر	و	ر	ز	■	ر	ا	گ	د	ا	ی	۷
ی	ر	ا	ل	■	ا	ی	ا	و	ز	■	م	ا	د	ک	۸
م	ا	ن	و	ک	ن	■	و	ر	ه	ا	ر	■	ی	د	۹
ی	ب	د	■	ن	م	ر	ه	ا	■	ف	ا	ل	و	ی	۱۰
ا	■	ر	ا	ک	و	ن	■	م	ا	ر	ه	ب	■	و	۱۱
ی	س	■	ن	ا	د	ج	و	■	و	ن	ی	ن	ل	ا	۱۲
ر	و	پ	ی	ش	■	و	د	ن	ا	گ	■	ی	ا	ن	۱۳
ا	ی	ا	و	■	ت	ر	ا	س	خ	■	ت	ا	ی	ه	۱۴
■	ن	و	گ	ر	گ	د	■	ن	ا	ر	و	ا	خ	۱۵	

سودوکو سخت ۴۴۰۰

زمان پیشنهادی: ۴۰ دقیقه

قانون‌های حل جدول سودوکو

۱- در هر سطر و ستون باید اعداد یک تا ۹ نوشته شود. بدیهی است که هیچ عددی نباید تکرار شود.

۲- در هر مربع ۳×۳ اعداد یک تا ۹ باید نوشته شود و در نتیجه هیچ عددی نباید تکرار شود.

۹	۷			۴	۸			
	۲		۱					
	۵	۱	۳					
	۳	۸				۷		
۵				۲				۳
		۷				۸	۴	
					۳	۲	۱	
					۴		۶	
			۹	۶			۸	۵

سودوکو ساده ۴۴۰۰

زمان پیشنهادی: ۲۰ دقیقه

سودوکو

سودوکو Sudoku یک واژه ترکیبی ژاپنی به معنای عددهای بی‌تکرار است و امروزه به جدولی از اعداد گفته می‌شود که به عنوان یک سرگرمی رایج در نشریات کشورهای مختلف به چاپ می‌رسد.

	۸							
			۹	۷			۱	۸
	۱	۷	۵		۸	۲		
		۲	۱	۴	۹			
۸		۶				۷		۱
			۶	۸	۷	۳		
		۹	۸		۳	۶	۲	
۵	۶			۲	۱			
							۵	