اینترنت آدم‌ها (۱۰)

عصر الکترونیک و جنگ بزرگ رمزنگاری

□ نوشته علیرضا محمدی‌فر

همچنان که در مقاله اول از این سلسله از مقالات گفتیم با وجود دستاوردهای بسیار بزرگ و شگفت‌انگیز در عصر اطلاعات، به دلیل توانی که فناوری‌های اطلاعات و ارتباطات در محدودکردن حریم خصوصی انسان دارند می‌توانند دورانی را بیافرینند که شاید آیندگان آن را دوران تاریک یا قرون وسطی در عصر اطلاعات نام بگذارند. از سوی دیگر، گفتیم که کنارگذاشتن و نادیده‌گرفتن فناوری‌های اطلاعات و ارتباطات برای انسان این روزگار به دلیل منافع بی‌شماری که دارد ناممکن است و نمی‌تواند به عنوان یک راه حل مطرح شود. در این مقاله به مهم‌ترین فناوری حافظ حریم خصوصی انسان در عصر الکترونیک پرداخته‌ایم: رمزنگاری.

دو فناوری مهم که در کنار هم می‌توانند در فضای مجازی برای انسان حریم خصوصی بیافرینند **رمزنگاری** و **اینترنت** هستند. **اینترنت** در اصل یک شبکه کامپیوتری بسیار بزرگ است که تعداد **گره‌های** آن در حال حاضر بیش از ۱۵میلیارد است و گفته می‌شود که تا سال ۲۰۲۰ به بیش از ۵۰ میلیارد برسد (به هر وسیله متصل به شبکه یک **گره** گفته می‌شود. هر گره می‌تواند کامپیوتر یک کاربر یا یک وسیله **اینترنت چیزها**[1] باشد). اینترنت در اصل این امکان را فراهم می‌کند که هر دو گره در دو نقطه مختلف جهان بتوانند اطلاعات را با یکدیگر مبادله کنند. فناوری دوم، یعنی **رمزنگاری داده‌ها**، به این دو گره امکان می‌دهد که هیچ‌کس نتواند اطلاعات مبادله‌شده را دستیابی کند. فناوری اول **حریم** را به وجود می‌آورد و فناوری دوم آن را **خصوصی** می‌کند.

در یک سال اخیر کمپینی از طرف رئیس FBI، **جیمز کامی**[2]، با هدف تعبیه‌کردن یک **در پشتی**[3] در نرم‌افزارهای رمزنگاری (یا به‌دست‌آوردن یک **شاه‌کلید** بازکننده قفل پیام‌های رمزنگاری‌شده) به راه افتاده است که بحث‌های فراوانی را درباره درستی یا نادرستی این اقدام به پا کرده است. بین دولت آمریکا و دره سیلیکان این بحث در گرفته است که آیا شرکت‌های دست‌اندرکار ارتباط داده‌ها و پیامک‌های دیجیتال، به ویژه گوگل و اَپل، باید برای کاربران امکان رمزنگاری داده‌های‌شان را _ که به زندگی خصوصی آنها مربوط است _ فراهم کنند یا نه، به گونه‌ای که هیچ‌کس، حتی دولت نتواند داده‌های آنها را رمزگشایی کند.

رئیس FBI تقریباً یک سال است که به شدت تلاش می‌کند به بهانه مقابله با تبهکاران یک **شاه‌کلید** یا **در پشتی** یا **در جلویی**[4] برای بازکردن پیام‌های دیجیتال رمزنگاری‌شده به دست بیاورد، و در حال حاضر بهانه خوبی پیدا کرده است: گروه تروریستی داعش. او معتقد است که بدون امکانات رمزشکنی نمی‌تواند جلوی اقدامات داعش در جذب اعضای جدید و حملات برنامه‌ریزی‌شده را بگیرد.

اعضای گروه‌های تروریستی می‌توانند با برنامک‌های ارتباطی گوشی‌های هوشمند که اطلاعات دو طرف ارتباط را رمزنگاری می‌کنند به طور مخفیانه با یکدیگر ارتباط برقرار کنند. از همین روی، مجریان قانون در آمریکا شرکت‌های بزرگ ارائه‌دهنده خدمات پیام‌رسانی را تحت فشار قرار داده‌اند تا شاه‌کلیدی برای رمزگشایی پیام‌ها به آنها ارائه بدهند.

اما متخصصان رمزشناسی، متخصصان امنیت داده‌ها، و متخصصان حریم خصوصی با دادن یک شاه‌کلید به FBI یا فراهم‌کردن یک در پشتی برای FBI به شدت مخالفند و معتقدند که بناکردن یک روزنه در نرم‌افزار رمزنگاری می‌تواند یک روزنه را برای تبهکاران، تروریست‌ها، و جاسوسان خارجی نیز باز کند. این روزنه به ویژه در ارتباطات بانکی می‌تواند هکرها را به یافتن شاه‌کلید یا بانک داده‌های کلیدهای شهروندان مختلف ترغیب کند. سیاست‌هایی که فناوری‌های رمزنگاری را ضعیف کنند حریم خصوصی را نیز کوچک می‌کنند و آزادی اینترنت را از بین می‌برند.

گفته می‌شود که اَپل و گوگل توانایی خود در رمزگشایی اطلاعات ذخیره‌شده در گوشی‌ها را غیرفعال کرده‌اند. برنامک WhatsApp در سال گذشته استفاده از رمزنگاری را آغاز کرد.

در قانون اساسی اکثر کشورها شنود تلفنی قانونی وجود دارد. قاضی با چنین قانونی می‌تواند به منظور کشف بزه یا مقابله با بزه‌کاران دستور موردی شنود تلفنی صادر کند. مجریان قانون با بهره‌گیری از چنین قانونی و تعمیم‌دادن آن سعی می‌کنند از امکانات گسترده فناوری‌های اطلاعات برای نظارت گسترده شهروندان سود بجویند. مجریان قانون میل دارند که از ترکیب هوش مصنوعی و امکان رمزگشایی پیام‌ها برای پیداکردن تبهکاران و تروریست‌ها بهره بگیرند.

[1] Internet of Things (IoT)
[2] James Comey
[3] backdoor access
[4] front door access

به عنوان مثال، آنها می‌خواهند پیام‌هایی را که در آنها از کلمه «بمب» استفاده شده است بررسی کنند و به این ترتیب بتوانند برنامه‌های تروریست‌ها را پیش از هر اقدامی خنثی کنند.

اما راهی برای تعبیه‌کردن **در پشتی** در سیستم‌های امنیتی وجود ندارد. مانند آن است که برای حفظ امنیت به جای قفل آهنی از یک قفل کاغذی بهره بگیریم. همان گونه که دولت‌ها از شهروندان نمی‌خواهند که قفل درهای خانه‌شان را ضعیف کنند نمی‌توان انتظار داشت که قفل درهای صندوقچه‌های اطلاعات آنها ضعیف شود.

ورود به عصر جدید با جدالی بزرگ همراه خواهد بود. از یک سو دولت‌ها با اشتهای سیری‌ناپذیر خود در بهره‌گیری از فناوری‌های اطلاعات و هوش مصنوعی برای نظارت گسترده بر روی فعالیت‌های شهروندان _ به منظور حفظ امنیت، مقابله با تبهکاران، و جلوگیری از فرار مالیاتی _ قرار دارند، و از سوی دیگر، شهروندان و کوچک‌شدن فزاینده حریم خصوصی‌شان. هم‌اکنون شورش‌ها آغاز شده است. **ادوارد اسنودن** و **جولین آسانژ** نخستین شورشی‌های نامدار این روند هستند. برای آنها انسان فاقد حریم خصوصی قابل قبول نیست. آنها **انسانیت** را در خطر می‌بینند. در این میان، چنانچه کمپین رئیس FBI پیروز شود، و به سمت آینده‌ای برویم که **پاتریک تاکر**[5] آن را **آینده عریان** نام نهاده است، نطفه‌های یک انقلاب بزرگ برای حریم خصوصی بسته خواهد شد، و به ویژه غرب با چالشی بزرگ روبه‌رو خواهد شد. آیا می‌توان حریم خصوصی را از انسان گرفت _ بی آن که مقاومت کند؟ بسیاری از حیوانات برای خودشان حریم خصوصی دارند، ورود به حریم خصوصی حیوانات با نزاع همراه است. جامعه در برابر این وضعیت مقاومت خواهد کرد. پیروزی مقطعی کمپین رئیس FBI و ادامه این روند نتیجه عکس به بار خواهد آورد. سطح امنیت دست‌کم تا مشخص‌شدن پیروز واقعی این میدان کاهش خواهد یافت.

عصر الکترونیک و تکامل انسان

همان گونه که در در دومین بخش از این سلسله از مقالات گفتیم وسایل همراه هوشمند را می‌توان بخشی از **تکامل بیولوژیک** انسان در نظر گرفت، که عضوهایی هستند که به صورت اکسترنال (بیرونی) مورد استفاده انسان‌ها قرار می‌گیرند، هر چند انواع پوشیدنی آنها اجتماع بیشتری با بدن برقرار می‌کنند (و انواع **بیونیک** آنها در داخل بدن قرار می‌گیرند). آنها به جز حواس پنج‌گانه حواس جدید دیگری مانند حس تعیین اندازه نور ماوراء بنفش، یا حس تعیین دقیق موقعیت مکانی را برای انسان اضافه می‌کنند. و گفتیم که پدیده رو به گسترش **خودافزارآوری**[6] (**BYOD**) به خوبی می‌تواند این نظریه مضحک را توضیح بدهد.

دوران باستان بر اساس جنس ابزارهای انسان به عصرهای مختلف سنگ، مفرغ، و آهن تقسیم‌بندی شده است. عصر جدید با ابزارهای الکترونیکی **عصر الکترونیک** است. همان گونه که ابزارهای سنگی یا برنزی یا آهنی در زندگی انسان باستان تحول آفریدند ابزارهای الکترونیک، به ویژه گوشی‌های هوشمندِ همیشه همراه انسان نیز تحولی ژرف در زندگی انسان به وجود آورده‌اند و همچنان تحول‌آفرین هستند.

هرگاه ما کارت حافظه Micro SD، حافظه اصلی گوشی، دیسک سخت «**کامپیوتر شخصی**»[7]، حتی **ابر شخصی**[8] _ که مقر آن ممکن است هزاران کیلومتر دورتر از صاحب آن باشد _ و مانند آن را بخش جدیدی از مغز و جزئی از طبیعت انسان بدانیم که به طور اکسترنال در اختیار ماست و از آن حفاظت می‌کنیم، رفتارمان با آنها **طبیعی** می‌شود. رفتار مجریان قانون با این **ابزارهای خصوصی** نیز می‌تواند همچون رفتار آنها با دانسته‌های مغز و حافظه و طبیعت انسان باشد. همان‌گونه‌که تفتیش عقاید و شکنجه برای گرفتن اعتراف در بسیاری از قوانین اساسی کشورهای مختلف ممنوع است تفتیش داده‌های شخصی نیز باید ممنوع باشد. عصر حجر با عصر الکترونیک فرق می‌کند. در عصر جدید باید قوانین عصر گذشته مورد بازنگری قرار بگیرند و با مقتضیات عصر جدید منطبق شوند.

دولت‌های آینده‌نگر انسان عصر الکترونیک و طبیعت جدید او را به رسمیت خواهند شناخت. مجریان قانون در این دولت‌ها به جای آن که قوانینی مانند قانون شنود تلفنی را _ که به گذشته تعلق دارند _ تعمیم بدهند کنار خواهند گذاشت و در عوض با امکانات و ابزارهای جدیدی که فناوری‌های اطلاعات فراهم می‌کنند به جدال با تبهکاری خواهند پرداخت. به عنوان مثال، فناوری‌های اطلاعات می‌توانند به طور کامل پول نقد (اسکناس) را از بازار حذف کنند و عملاً به جرائمی مانند کیف‌زنی، جیب‌بری، و دزدی پول نقد (از خانه‌ها، صندوق فروشگاه‌ها و بانک‌ها، متصدیان پمپ بنزین، و مانند آنها) خاتمه بدهند. خودروهای بدون راننده (خودران‌ها) انسان را از رانندگی معاف خواهند کرد و چنان می‌توانند ساخته شوند که دیگر تخلف و جریمه رانندگی موضوعی مربوط به گذشته تلقی شود.□

[5] http://patricktucker.com/

[6] Bring Your Own Device
[7] Personal Computer (PC)
[8] Personal cloud (Pc)

رمزنگاری چیست؟

واقعیت آن است که لپ‌تاپ‌ها و گوشی‌های هوشمند با انبوهی از اطلاعات خصوصی همه‌روزه توسط کاربران بی‌آن‌که داده‌های آنها رمزنگاری شده باشد جابه‌جا می‌شود. هر گاه لپ‌تاپ و گوشی هوشمند شما گم یا دزدیده شود دربارهٔ انواع اطلاعاتی که در دیسک‌سخت کامپیوترتان ذخیره کرده‌اید فکر می‌کنید. آیا عکس‌ها و ویدئوهای خانوادگی داشته‌اید؟ آلبوم‌های موسیقی محبوب‌تان؟ اطلاعات مالی، گذرواژه‌ها، و سایر داده‌های حساس؟ **رمزنگاری**[9] **اطلاعات** نه‌تنها از اطلاعات مهم شما در زمانی حفاظت می‌کند که کامپیوترتان گم می‌شود یا به سرقت می‌رود، بلکه در زمان ارتباط اینترنتی با دیگران جلوی فاش‌شدن اطلاعات شخصی شما را می‌گیرد و یک حریم خصوصی برای داده‌های شما به وجود می‌آورد.

نرم‌افزارهای **رمزنگاری داده‌ها** از الگوریتم‌های پیشرفته برای رمزی‌کردن محتویات یک فایل به گونه‌ای بهره می‌گیرند که هیچ کسی _ به جز کسانی که **کلید** درست را برای رمزگشایی دارند _ نتواند آنها را بخواند. الگوریتم‌های رمزنگاری یا الگوریتم‌های ریاضی هستند یا قواعد دیگری را روی فایل‌ها به کار می‌بندند، که به طور سیستمی محتویات آن فایل‌ها را تغییر می‌دهد.

وقتی کودکان در کلاس درس می‌خواهند یک پیام رمزی را به هم بدهند، ممکن است از **روش جایگزینی الفبایی** بهره بگیرند، مثلاً به جای «الف» از «ب» ، و به جای «ب» از «پ» ، و مانند آن استفاده کنند. الگوریتم این نوع رمزنگاری جابه‌جاکردن حروف است، و اگر کسی نداند که چند حرف جابه‌جا شده است یا چگونه حروف جابه‌جا شده‌اند نخواهد توانست که رمزگشایی کند. **رمزنگاری داده‌ها** ـ از هر نوع که باشد ـ به عمل پردازش یک پیام به وسیله الگوریتمی گفته می‌شود که آن پیام را درهم می‌ریزد، و برای بازگردانی پیام اولیه باید الگوریتم معکوس را به کار بست.

البته، الگوریتم‌های ساده، مانند جایگزینی الفبایی، امنیت زیادی به دست نمی‌دهند. کشف رمز چنین الگوریتم‌هایی بسیار ساده است. کامپیوترها بهترین ابزار رمزنگاری هستند. نظر به این که ریاضیات تنها زبان کامپیوترهاست، آنها می‌توانند فرمول‌هایی طولانی و پیچیده را روی داده‌ها به اجرا در بیاورند. آدم‌ها نمی‌توانند این فرمول‌ها را حدس بزنند. حتی سریع‌ترین و پیچیده‌ترین کامپیوترهای روی زمین برای کشف رمز فناوری‌های پیچیده رمزنگاری مجبورند سال‌ها کار کنند. آنها به دانستن الگوریتم استفاده‌شده نیاز دارند و اگر کلیدهای درست را داشته باشند (که بعداً در این باره توضیح خواهیم داد) به سرعت می‌توانند فایل رمزنگاری‌شده را باز کنند.

بدون این اطلاعات، تعداد ترکیب‌ها چنان زیاد است که کامپیوترهای بسیار قدرتمند هم نمی‌توانند به سرعت آنها را کشف رمز کنند. در حقیقت، دولت آمریکا صادرات بهترین ابزار رمزنگاری را ممنوع اعلام کرده است، فناوری‌ای که چنان خطرناک در نظر گرفته می‌شود که در فهرست صادرات ممنوع قرار می‌گیرد.

کلیدها و الگوریتم‌ها

فناوری رمزنگاری مدرن به داده‌هایی مشهور به **کلید** (key) اتکا دارد. در روزگار باستان، یک نوار کاغذی را روی یک لوله بلند می‌پیچاندند و پیام خود را روی آن می‌نوشتند. پس از نوشتن پیام، نوار کاغذی را باز می‌کردند و به مقصد ارسال می‌کردند. نوار کاغذی در خارج از لوله، حاوی یک رشته حروفی تصادفی بود. گیرنده فقط وقتی می‌توانست پیام را بخواند که لوله‌ای دقیقاً به قطر لوله استفاده‌شده برای نوشتن پیام می‌داشت. رمزنگاران امروز از **مقادیر کلیدی** به عنوان معادل لوله‌های رمزنگاری باستان بهره می‌گیرند. آنها از این کلیدها برای رمزنگاری و رمزگشایی بهره می‌گیرند.

لوله‌ای را تصور کنید که طول آن از زمین تا ماه باشد و قطر آن در نقاط بسیار زیادی از این طول تغییر کند، از اندازه تنه یک درخت تا قطر یک مداد. حالا می‌توانید دریابید که پیداکردن کلیدهای امروزی چقدر دشوار است.

در **رمزنگاری کلید عمومی** (public key)، دو کلید متفاوت برای رمزنگاری و رمزگشایی اطلاعات به کار می‌رود. **کلید خصوصی** (private key) کلیدی است که فقط در اختیار صاحب آن است، در

[9] encryption

حالی که **کلید عمومی** مکمل آن را می‌توان در اختیار کامپیوترهای دیگر شبکه، کاربران دیگر، و سرویس‌های گوناگون قرار داد.

هرگاه مشخصات یک استاندارد رمزنگاری‌ای را بخوانید که از کلید بهره می‌گیرد، ابتدا به تعداد بیت‌هایی توجه می‌کنید که آن استاندارد به کار می‌گیرد. برای ساخت یک بایت به ۸ بیت نیاز است. تعداد بیت‌های کلید هرچه بیشتر باشد رمزنگاری پیچیده‌تر و کشف رمز دشوارتر است. زیرا تعداد ترکیب‌های ممکن معادل دو به توان تعداد بیت کلید است.

به عنوان مثال، یک استاندارد رمزنگاری ۸ بیتی ساده حاوی 2^8 ترکیب ممکن است، بدین معنی که هر کسی که بخواهد کد رمزنگاری را بشکند مجبور خواهد بود که ۲۵۶ کلید را جستجو کند تا بتواند کلید اصلی را بیابد. حتی کودکان هم می‌توانند چنین رمزی را کشف کنند، و کامپیوتر در یک آن می‌تواند این کد را بیابد.

نظر به این که مقادیر بیتی نمایی هستند، هرچه تعداد بیت‌ها بیشتر شود تعداد ترکیب‌ها چنان زیاد می‌شود که کامپیوترهای سریع نیز به زحمت می‌توانند کلید را کشف کنند. به عنوان مثال، ۳۲ بیت تعداد ۴ میلیارد ترکیب را به وجود می‌آورد، و بهترین روش‌های رمزنگاری امروزی از کلیدهای ۱۲۸ بیتی تا ۲۵۶ بیتی بهره می‌گیرند، که تعداد ترکیب‌ها چنان زیاد می‌شود که ما جا برای چاپ‌کردن آن نداریم. هرچه تعداد بیت بیشتر باشد امنیت بهتر است. در حقیقت، فناوری «رمزنگاری قدرتمند» امروزی از کلیدهای ۱۲۸ بیتی به بالا استفاده می‌کنند و کلیدهای ۴۰ تا ۵۰ بیتی به گذشته تعلق دارند.

PGP

PGP[10] یک سیستم رمزنگاری کلید عمومی است که در سال ۱۹۹۱ توسط «فیلیپ زیمرمان» ساخته شده است. PGP را می‌توانید در بازار بیابید، اما گونه رایگان آن باید برای اکثر کاربران کافی باشد. از این برنامه اغلب برای امضاکردن، رمزنگاری، و رمزگشایی متون، ایمیل، فایل، پوشه، و کل یک پارتیشن دیسک استفاده می‌شود.

نگارش‌های جدید PGP به طور مستمر انتشار می‌یابد و در هر نگارش جدید اشکالات نگارش پیشین برطرف می‌گردد. شکستن رمز فایل‌های رمزنگاری‌شده با PGP چنان دشوار است که رمزشکنان ترجیح می‌دهند از روش‌هایی مانند **شکنجه**، کارگذاری یک **برنامه اسب تروا** در کامپیوتر هدف، یا استفاده از **ثبت‌کننده‌های کلیدزنی** نرم‌افزاری و سخت‌افزاری یا **دوربین‌های عکاسی** مخفی برای ربودن کلیدها و گذرواژه‌ها بهره بگیرند.

گفته می‌شود که در پاره‌ای از جرائم اتفاق‌افتاده در آمریکا و انگلستان پلیس نتوانسته است فایل‌های رمزنگاری‌شده با PGP را با نرم‌افزار رمزشکنی کند، و در بعضی از موارد از روش‌هایی مانند کارگذاری یک برنامه اسب تروا در کامپیوتر هدف، یا استفاده از ثبت‌کننده‌های کلیدزنی نرم‌افزاری و سخت‌افزاری بهره گرفته است.

افسانه ناشناس‌ماندن در اینترنت

زمانی بود که کاربران اینترنت تقریباً می‌توانستند به طور کاملاً ناشناس در اینترنت ارتباط برقرار کنند. این وضع برای بعضی از کاربران رضایت‌بخش بود و برای بعضی دیگر یک مسئله. حقیقت هر چه که باشد، این ناشناس‌ماندن به معنای آن بود که هر کس می‌توانست هر چیزی بنویسد، و مسئولیتی در برابر آن نوشته‌ها نداشته باشد. در عوض، برای کسانی که حرف مهمی برای گفتن داشتند گونه‌ای حفاظت به وجود می‌آورد. بحث دربارهٔ اهمیت گمنام‌گویی همچنان ادامه دارد، اما در حال حاضر می‌دانیم که اینترنت _ آن گونه که می‌پنداشتیم _ گمنامی را فراهم نمی‌سازد. انتظار نداشته باشید که مدتی طولانی در اینترنت ناشناس بمانید، مگر این که اقدامات احتیاطی را انجام بدهید. حقیقت آن است که اینترنت هیچ‌گاه واقعاً حریم خصوصی را حفظ نکرده است. در هر لحظه می‌توان کاربر یک کامپیوتر را شناسایی کرد، چون هر کامپیوتر متصل به اینترنت از یک **نشانی IP**[11] منحصر به فرد برای ارتباط با دیگران بهره می‌گیرد.

با وجود این، یک روش مؤثر برای محرمانه‌ماندن اطلاعات به هنگام ارتباط با اینترنت وجود دارد: استفاده از نرم‌افزار **رمزنگاری**.□

[10] Pretty Good Privacy

[11] IP (Internet Protocol) address