طراحی یک سامانه ضدنفوذ

رمزنگاری کوانتومی چالش نفوذ داده‌ای را درهم می‌شکند

در یک سال گذشته چند مرتبه در ارتباط با نقض‌های داده‌ای و اطلاعاتی که از سوی سرویس‌های مختلف شنود شده‌اند در رسانه‌ها شنیده یا در سایت‌ها خوانده‌اید؟ شرکت‌ها و همچنین دست‌اندرکاران شبکه‌های اجتماعی در تلاش هستند تا از اطلاعات ما با اتکا بر الگوریتم‌های رمزنگار محافظت به عمل آورند، اما هرچه فناوری به‌سمت جلو حرکت می‌کند، به همان نسبت الگوریتم‌های رمزنگار ضعیف‌تر می‌شوند و در بعضی موارد رخنه‌های جدی در آن‌ها شناسایی می‌شود. اما به نظر می‌رسد رمزنگاری کوانتومی قادر است ما را از این کابوس شبانه نجات دهد.

پژوهشگران دانشگاه دوک، پژوهشگران آزمایش ملی Oak Ridge و پژوهشگران دانشگاه اوهایو در تعامل با یکدیگر موفق به طراحی سامانه ضدنفوذ جدیدی شده‌اند که با الهام از محاسبات کوانتومی قادر است داده‌های ما را رمزنگاری کند. سامانه طراحی شده این پژوهشگران این توانایی را دارد تا کدهای رمزنگاری را با توان مگابیت بر ثانیه ایجاد و سپس توزیع کند. این سرعت انتقال چیزی حدود 5 تا 10 برابر سریع‌تر از راهکارهایی است که امروزه از سوی سامانه‌های رایج مورد استفاده قرار می‌گیرد. پژوهشگران این پروژه اعلام داشته‌اند که اگر الگوریتم فوق به‌شکل موازی روی چند سامانه اجرا شود، سرعت آن با سرعت فعلی اینترنت برابری می‌کند. این الگوریتم نشان داده است که در برابر بسیاری از حملات رایج و مرسوم امروزی مقاوم بوده و حتی زمانی که تجهیزات و سامانه‌های فیزیکی مورد نفوذ قرار می‌گیرند و این احتمال وجود دارد که با افشای داده‌ها روبه‌رو شویم، باز هم الگوریتم رمزنگاری کوانتومی این قابلیت را دارد تا مانع دسترسی نفوذگران به داده‌هایی شود که با استفاده از این الگوریتم رمزنگاری شده‌اند. دانیل گوتیر استاد فیزیک دانشگاه OSU در این ارتباط گفته است: «در حال حاضر یک کامپیوتر کوانتومی که قادر به انجام محاسبات است در اختیار داریم. سامانه فوق به‌اندازه‌ای پرتوان است که در آینده نزدیک ممکن است به‌منظور رمزگشایی داده‌های رمزنگاری شده مورد استفاده قرار گیرد. بر همین اساس، ضروری است به‌دنبال راهکارهای جدید و نوینی باشیم تا بتوانیم از طریق آن بستر اینترنت را ایمن سازیم.»

فعالیت‌های آنلاینی همچون خریدهای آنلاین، تعاملات بانکی، پرونده‌های پزشکی، گزارش‌های مرتبط با سازمان‌های بیمه‌گر جزء آن گروه از اطلاعات حساسی به شمار می‌روند که با استفاده از کلیدهای رمزنگار محافظت می‌شوند. اطلاعات شخصی که در بستر اینترنت روزانه مبادله می‌شوند، در اولین گام از طریق یکی از کلیدهای رمزنگار ایمن کدگذاری خواهند شد. زمانی که اطلاعات به دست گیرنده می‌رسد، از طریق کلید مربوط رمزگشایی می‌شود. همه این فرآیندها بدون آنکه کلاینت (کاربر یا سامانه کامپیوتری) دخالتی در این زمینه داشته باشد انجام می‌گیرد. اما این سامانه‌ها تنها زمانی به‌درستی کار می‌کنند که هر دو طرف کلید یکسانی در اختیار داشته باشند و این کلید نیز مخفی نگه داشته شود. اگر اتفاقی همچون حمله مرد میانی رخ دهد، همه‌چیز خراب می‌شود. رویکردی که رمزنگاری کوانتومی ارائه می‌کند این است که بر مبنای توزیع کلید کوانتومی (QKD سرنام Quantum Key Distribution) کار می‌کند. راهکار فوق یکی از قابلیت‌های زیربنایی مکانیک کوانتوم به شمار می‌رود تا فرآیند نقل و انتقال کلیدها را به‌شکلی مدیریت کند تا در زمان نفوذ امنیتی هر دو طرف گیرنده و ارسال‌کننده از به سرقت رفتن کلید یا شنود

ارتباط مطلع شوند. برای شناسایی این نفوذ پژوهشگران وضعیت ماده بسیار کوچکی همچون الکترون‌ها یا پروتون‌ها را مورد ارزیابی قرار می‌دهند. با متمرکز شدن روی فعل و انفعالات این مواد، دانشمندان آگاه می‌شوند که الکترون‌ها یا پروتون‌ها بر مبنای چه پارامتری به‌شکل خودکار قادر هستند ویژگی‌های خود را تغییر دهند.

مطلب پیشنهادی

محاسبات کوانتومی از تئوری تا واقعیت
رایانش کوانتومی چیست و اساس کار آن چگونه است؟

نظریه QKD

قدمت تئوری QKD به دهه 80 میلادی بازمی‌گردد. زمانی که تئوری فوق مطرح شد، در اندک زمانی (سال 1984) به‌شکل عملی مورد آزمایش قرار گرفت و پیاده‌سازی شد. امروزه فناوری‌ها و سرویس‌های مختلفی برای پشتیبانی از تئوری فوق در فضای مجازی عرضه شده‌اند که با کمی جست‌وجو می‌توانید این فناوری‌ها را پیدا کنید. در مقطع فعلی شرکت‌های مختلف مستقر در اروپا اقدام به فروش سامانه‌های مبتنی بر لیزری کرده‌اند که با اتکا بر تئوری QKD کار می‌کند. تقریباً 6 ماه پیش بود که دولت چین نیز خبر از پرتاب ماهواره‌ای به فضا داد که قادر است یک کلید کوانتومی را از فضای بالای جو برای دو ایستگاه زمینی که در فاصله‌ای نزدیک به 1200 کیلومتر قرار داشتند ارسال کند. مشکلی که امروزه اغلب سامانه‌های مبتنی بر QKD با آن روبه‌رو هستند، به نرخ نسبتاً پایین انتقال کلیدهای آن‌ها که بین ده‌ها تا صدها کیلوبیت بر ثانیه می‌رسد بازمی‌گردد. این نرخ انتقال پایین این شانس را ندارد تا برای اغلب عملیات‌هایی که در بستر اینترنت انجام می‌شود، مورد استفاده قرار گیرد، به‌واسطه آنکه بیش از اندازه کند است. به‌شکلی که اگر در نظر داشته باشید از سامانه‌های رمزنگار مبتنی بر مکانیسم کوانتوم به‌شکل روزانه و آن هم برای عملیاتی همچون برقراری یک تماس تلفنی رمزنگاری یا برگزاری یک ویدئو کنفرانس استفاده کنید، باید چند ساعتی به انتظار بنشینید تا فرآیند رمزنگاری اطلاعات کامل شود.

مطلب پیشنهادی

شماره 189 ماهنامه شبکه با پرونده ویژه «کامپیوترهای کوانتومی» منتشر شد

پروژه طراحی شده از سوی این تیم تحقیقاتی چگونه کار می‌کند؟

سامانه QKD مبتنی بر لیزر ضعیف بر مبنای فوتون‌های منحصر به فردی از نور برای رمزنگاری اطلاعات استفاده می‌کند که این رویکرد باعث شده است تا سرعت این سامانه به‌شکل قابل توجهی افزایش پیدا کند. الگویی که این سامانه بر مبنای آن کار می‌کند به این شکل عمل می‌کند که زمان را بر مبنای فوتونی که قرار است آزاد شود تنظیم کرده و در ادامه از یکی از ویژگی‌های فوتون که به‌نام فاز شناخته می‌شود به‌منظور رمزنگاری دو بیت از داده‌ها به‌جای یک بیت استفاده می‌کند. این تکنیک در تعامل با آشکارسازهای سرعت بالا که از سوی کلینتون کاهال دانشجوی رشته مهندسی برق و کامپیوتر و همچنین جونگسانگ کیم، استاد دپارتمان برق و کامپیوتر دانشگاه دوک طراحی و توسعه پیدا کرده است کار می‌کند. ترکیب این فناوری‌ها با یکدیگر باعث شده است تا نرخ تبادل کلیدها بین 5 تا 10 برابر سریع‌تر از روش‌های رایج امروزی شود. سامانه طراحی شده از سوی این گروه تحقیقاتی از آن جهت حائز اهمیت است که آن‌ها موفق شده‌اند ویژگی‌های فرعی فوتون‌ها را تغییر دهند و به این شکل امنیت کلیدهای رمزنگار را دو برابر بیشتر کنند. امنیت دو برابر کلیدها به این معنا است که QKD این پتانسیل را دارد تا مکانیسمی کاملاً ایمن را در اختیار ما قرار دهد، به این معنا که هرگونه کوششی برای به دست آوردن یا نفوذ به یک کلید در حالت انتقال، باعث پدید آمدن خطایی در فرآیند انتقال اطلاعات می‌شود که دریافت‌کننده به‌راحتی از این

موضوع مطلع خواهد شد. اما مشکلی که در این بین وجود دارد این است که برای پیاده‌سازی این سامانه در دنیای ملموس از دستگاه‌ها و تجهیزاتی استفاده می‌شود که کاستی‌هایی دارند. در نتیجه به‌کارگیری این دستگاه‌ها باعث پدید آمدن آسیب‌پذیری‌هایی می‌شود که درنهایت به هکرها اجازه می‌دهد از آن‌ها برای نفوذ استفاده کنند. برای حل این مشکل پژوهشگران این پروژه تحقیقاتی تجهیزاتی که در بخش‌های مختلف مورد استفاده قرار می‌گیرد را ارزیابی کرده‌اند تا نواقص هریک را پیدا کنند. در ادامه با همراهی چارلز لیم، استاد مهندسی برق و کامپیوتر دانشگاه دولتی سنگاپور سعی کردند آسیب‌پذیری‌های فوق را به‌شکلی برطرف کنند که این سامانه بدون نقص کار کند. نورال تیمور ایسلام فارغ‌التحصیل رشته فیزیک دانشگاه دوک در این ارتباط گفته است: «زمانی که موفق شوید آسیب‌پذیری‌های تجربی در سامانه خود را شناسایی و در ادامه با تئوری خود ترکیب کنید، این شانس را به دست خواهید آورد تا سامانه‌ای ایمن طراحی کنید، به‌شکلی که هیچ‌گونه عامل تهدیدکننده‌ای باعث نشود ساز و کار آن به خطر افتد.»
فرستنده طراحی شده از سوی این پژوهشگران به مؤلفه‌های تخصصی خاصی نیاز دارد، اما مؤلفه‌هایی که این سامانه به آن‌ها نیاز دارد در بازار پیدا می‌شوند. مزیت بزرگی که این سامانه دارد در ارتباط با کلیدهای رمزگشایی است که در فوتون‌های نوری رمزنگار قرار می‌گیرند. آن‌ها می‌توانند با استفاده از فیبر نوری که امروزه در هر نقطه‌ای از جهان مورد استفاده قرار می‌گیرند انتقال پیدا کنند. در نتیجه فرآیند ادغام و یکپارچگی فرستنده/دریافت‌کننده با بستر اینترنت به ساده‌ترین شکل امکان‌پذیر است. نورال تیمور ایسلام در این ارتباط گفته است: «ما تقریباً همه مؤلفه‌هایی که در حوزه ارتباطات از راه دور به آن‌ها نیاز داریم را می‌توانیم از بازار تهیه کنیم. تنها مؤلفه‌ای که در بازار وجود ندارد آشکارسازهای تک فوتونی هستند. با وجود این از طریق فرآیندهای مهندسی این شانس را داریم تا فرستنده و گیرنده را درون جعبه‌ای به‌اندازه یک پردازنده مرکزی کامپیوتری قرار دهیم.»
اوفو مائور از مدیران ارشد شرکت سینوپسیس در این ارتباط گفته است: «ما در اغلب موارد می‌شنویم که راهکار جدیدی ابداع شده که قادر است یک مکانیسم ضدنفوذ را ارائه کند. درست است که این فناوری جالب توجه به نظر می‌رسد، اما کمی زود است که از عبارت ضدنفوذ برای آن استفاده کنیم. تاکنون به دفعات افراد مختلف مدعی شده‌اند که فناوری‌های کاملاً ضدنفوذ را طراحی کرده‌اند که پس از آنکه در دنیای واقعی عملیاتی شده‌اند، به‌راحتی مورد نفوذ قرار گرفته‌اند. تاریخ نشان داده است زمانی که فرضیه‌ای در ارتباط با ضدنفوذ ارائه و در قالب یک محصول تجاری به بازار عرضه شده، آن موقع مشکلات امنیتی آن کشف شده است. زمانی که هکرها توانسته‌اند باگ‌های موجود در زیرساخت‌ها را شناسایی کنند و بر ادعای نفوذناپذیر بودن سامانه خط بطلان بکشند.»

منبع:

Infosecurity-Magazine
تاریخ انتشار:
13 فروردین 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/11927/%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C-%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C-%DA%86%D8%A7%D9%84%D8%B4-%D9%86%D9%81%D9%88%D8%B0-%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D8%A7%DB%8C-%D8%B1%D8%A7-%D8%AF%D8%B1%D9%87%D9%85-

%D9%85%DB%8C%E2%80%8C%D8%B4%DA%A9%D9%86%D8%AF