تولید امن‌ترین مین‌فریم‌ها تجاری

مین‌فریم‌های آی‌بی‌ام به رمزنگاری فراگیر تجهیز شدند

نسل بعدی مین‌فریم‌های سری Z آی‌بی‌ام قادر هستند به‌طور کامل فرآیند رمزنگاری را روی برنامه‌های کاربردی، سرویس‌های کلاود یا بانک‌های اطلاعاتی اعمال کنند. به عبارت دقیق‌تر این مین‌فریم‌ها قادر هستند داده‌ها را به‌طور کامل رمزنگاری کنند. این رویکرد به منظور مقابله با جاسوسی‌های صنعتی و حملات هکری به مرحله اجرا در آمده است.

امروزه فرآیند رمزنگاری داده‌ها به‌طور جدی از سوی بسیاری از شرکت‌ها مورد توجه قرار گرفته است. با این وجود فرآیند رمزنگاری تنها در لایه‌های خاص و همچنین روی جریان‌های مشخصی از داده‌ها به مرحله اجرا در می‌آید.
امروزه مین‌فریم‌ها در حوزه‌هایی که با حجم بالایی از تراکنش‌ها روبرو هستند همچون صنایع مالی، بیمه و شرکت‌های مسافرتی مورد استفاده قرار می‌گیرند. در ساخت سری جدید مین‌فریم‌های آی‌بی‌ام کارشناسانی از 150 سازمان مختلف حضور داشتند که ADP و Highmark Healthcare از معروف‌ترین آن‌ها به شمار می‌روند.

کالیب بارلو، معاون بخش تهدیدات هوشمند دپارتمان امنیتی آی‌بی‌ام می‌گوید: «چالشی که امروزه همه کاربران با آن روبرو هستند این است که برای رمزنگاری داده‌ها باید هزینه‌های زیادی را متقبل شوند. زمانی که در مورد هزینه صحبت می‌کنم منظورمان تنها پول نیست، بلکه زمانی است که برای رمزنگاری داده‌ها سپری می‌شود. به همین دلیل است که در اغلب موارد مشاهده می‌کنیم رمزنگاری تنها میان مرورگر و سرور یک برنامه کاربردی یا منبعی که داده‌ها روی آن ذخیره‌سازی شده‌اند انجام می‌شود. زمانی که در حال انتقال پول هستید یا به یک سایت تجارت الکترونیک مراجعه می‌کنید، فرآیند رمزگذاری و رمزگشایی به شکل کاملا محسوسی عملیات پردازشی را کند می‌سازند.»

اما در سامانه‌های سری Z که آی‌بی‌ام طراحی کرده است، داده‌ها به محض عبور از لایه شبکه روی تراشه‌ها و بوردها به حالت رمزنگاری شده قرار می‌گیرند که این ویژگی را کارشناسان رمزنگاری فراگیر (pervasive encryption) نام‌گذاری کرده‌اند. بارلو می‌گوید: «برای انجام این رمزنگاری از 6 میلیارد ترانزیستور روی پردازنده

استفاده شده است. به همین دلیل هر زمان ماشین فرآیند رمزگشایی و رمزنگاری را انجام می‌دهد هیچ افت سرعتی مشاهده نمی‌شود. داده‌ها تنها زمانی رمزگشایی می‌شوند که باید پردازشی روی آن‌ها انجام شود.»

این مین‌فریم‌ها از الگوریتم‌های رمزنگاری متقارن و غیر متقارن AES, DES, TDES, RSA, DSA, ECC, and ECDSA و همچنین CMAC و HMAC برای احراز هویت پیام‌ها و الگوریتم‌های هشینگ SHA2 و SHA3 استفاده می‌کنند. آی‌بی‌ام می‌گوید این مین‌فریم‌های جدید که به ویژگی دیگری به نام پاسخ به دستکاری تجهیز شده‌اند قادر هستند روزانه نزدیک به 12 میلیارد تراکنش را رمزنگاری کنند. ویژگی پاسخ به دستکاری هر زمان احساس کند حمله‌ای رخ داده است همه کلیدهای رمزنگاری را نابود می‌سازد و به این شکل مانع از سرقت اطلاعات می‌شود. آی‌بی‌ام در نظر دارد مین‌فریم‌های خود را در سه ماهه جاری و به قیمت 500 هزار دلار به فروش برساند. در حالی که مین‌فریم‌ها این روزها کمتر مورد استفاده قرار می‌گیرند اما هنوز هم اصلی‌ترین هدف هکرها به شمار می‌روند به واسطه آن‌که مین‌فریم‌ها در معرض حملات آلودگی فرآیندهای تجاری قرار دارند که به هکرها اجازه می‌دهند پردازه‌های آن‌ها را به شکل مخفیانه دستکاری کرده و در ادامه به سرقت اطلاعات و پول از آن‌ها بپردازند.

تاریخ انتشار:
28 تیر 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/world/8778/%D9%85%DB%8C%D9%86%E2%80%8C%D9%81%D8%B1%DB%8C%D9%85%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A2%DB%8C%E2%80%8C%D8%A8%DB%8C%E2%80%8C%D8%A7%D9%85-%D8%A8%D9%87-%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C-%D9%81%D8%B1%D8%A7%DA%AF%DB%8C%D8%B1-%D8%AA%D8%AC%D9%87%DB%8C%D8%B2-%D8%B4%D8%AF%D9%86%D8%AF