禪

مورفئوس: راهی بهسوی کامپیوترهای غیرقابل نفوذ . . . .

گروهی از محققان دانشگاه میشیگان، تصمیم دارند با تبدیل کردن مدارهای کامپیوتری به معماهای حلنشدنی، کامپیوترهایی غیرقابل نفوذ بسازند . این پروژه موسوم به مورفئوس (MORPHEUS) از حمایت مالی ۳.۶میلیون دلاری دارپا برخوردار است .

امروزه روشهای رفع آسیبپذیریهای سختافزاری بیشتر متکی بر وصلههای نرمافزاری هستند که عموماً از سوی مهاجمان دور زده میشوند. اما به عقیده تاد آستین (Todd Austin) استاد کامپیوتر دانشگاه میشیگان و مسؤول پروژه مورفئوس، چنین روشهایی کارآیی ندارند . امسال دارپا تحقیقاتی ۵۰ میلیون دلاری را به منظور یافتن راهکارهای امنیت سایبری مبتنی بر سختافزار آغاز کرد و پروژه مورفئوس بخشی از این تلاش است. علاوه بر گروه دانشگاه میشیگان، ۸ گروه دیگر نیز با این برنامه موسوم به SSITH همکاری میکنند . لینتون سالمون (Linton Salmon) مدیر برنامه « امنیت مبتنی بر سختافزار و ثابتافزار (Firmware) » دارپا یا به اختصار SSITH میگوید : « بجای اینکه برای رفع مشکلات امنیتی سختافزارها، از وصلههای نرمافزاری استفاده کنیم، در تلاش هستیم تا با رفع آسیبپذیریهای سختافزاری، بسیاری از حملات نرمافزاری فعلی را بیاثر کنیم .»

در پروژه مورفئوس راهی جدید برای طراحی سختافزار پیشنهاد شده است که بر اساس آن اطلاعات به سرعت و بطور تصادفی در تراشه جابجا شده و دوباره رمزگذاری میشوند . با این روش مهاجمان به اطلاعات مهمی که برای انجام یک حمله موفقیتآمیز نیاز دارند دسترسی نخواهند داشت . آستین در مورد این روش میگوید : « ما کامپیوتر را به یک معمای غیرقابل حل تبدیل میکنیم . شبیه این است که شما بخواهید یک مکعب روبیک را حل کنید اما هر بار که پلک میزنید، من ترتیب خانهها را به هم بریزم ». این محققان معتقد هستند که با این روش، میتوان سختافزار را در مقابل حملات ناشناخته آینده موسوم به حملات روز صفر هم محافظت کرد . به اعتقاد آستین، این روش در مقابل نقص هارتبلید (Heartbleed) که در سال ۲۰۱۴ شناسایی شد مقاوم است و در آن زمان میتوانست جلوی حملات را بگیرد . هارتبلید به مهاجمان اجازه میداد رمز عبور

یا سایر اطلاعات حیاتی کامپیوترها را بخوانند . در حالت معمول، محل چنین دادههایی تغییر نمیکند و به گفته آستین : « به محض اینکه مهاجم بفهمد نقص (باگ) در کجا است و در کجا میتواند دادهها را بیابد، دیگر بازی تمام است !». اما در روش جدید، محل باگ و نیز رمزهای عبور بطور مداوم تغییر میکنند : « امروزه چنین سطحی از محافظت در دسترس نیست زیرا پیادهسازی نرمافزاری آن بسیار پرهزینه است. »

بنا بر اعلام دارپا اگر محققان بتوانند هفت نوع آسیبپذیری سختافزاری را رفع کنند، میتوان بیش از ۴۰ درصد منافذ نرمافزاری که امروز در دسترس مهاجمان است را مسدود کرد . آسیبپذیریهایی نظیر خطاهای بافر، مدیریت منابع، نشت اطلاعات و تزریق خطا از این جملهاند .

نویسنده :
مهدی صنعتجو
منبع :
دانشگاه میشیگان
دسته بندی:
اخبار
اخبار جهان
امنیت
شاهراه اطلاعات
تاریخ انتشار :
14:20 - 07/10/1396
برچسب:
امنیت سختافزاری - تراشه غیرقابل نفوذ - پروژه مورفئوس - پروژه دانشگاه میشیگان - تحقیقات دارپا - امنیت تراشه

نشانی
https://www.shabakeh-mag.com/news/11182/%D9%85%D9%88%D8%B1%D9%81%D8%A6%D9%88%D8%B3-%D8%B1%D8%A7%D9%87%DB%8C-%D8%A8%D9%87%E2%80%8C%D8%B3%D9%88%DB%8C-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%D9%87%D8%A7%DB%8C-%D8%BA%DB%8C%D8%B1%D9%82%D8%A7%D8%A8%D9%84-%D9%86%D9%81%D9%88%D8%B0:□□□□