العلماء يستخدمون الفوضى لحماية الأجهزة من المخترقين

حقوق الصورة: CC0 Public Domain

وجد الباحثون طريقة لاستخدام الشواش أو الفوضى للمساعدة في تطوير بصمات رقمية للأجهزة الإلكترونية التي قد تكون فريدةً بما يكفي لإحباط حتى أكثر محاولات المتسللين تعقيدًا.

ما مدى تميُّز هذه البصمات؟ يعتقد الباحثون أن الأمر سيستغرق وقتًا أطول من عمر الكون لاختبار كلّ مزيج ممكن متاح.

قال دانيال غاوتييه **Daniel Gauthier**، كبير المشاركين في الدراسة وأستاذ الفيزياء في جامعة ولاية أوهايو: "في نظامنا، الفوضى جيدة

جدًا".

وقد نُشرت الدراسة مؤخرًا على الإنترنت في مجلة **IEEE Access**، إذ ابتكر الباحثون نسخةً جديدةً من تقنيةٍ ناشئةٍ تسمى الوظائف غير القابلة للاستنساخ ماديًا والمعروفة اختصارًا بـ **PUFs**، المُضمنة في رقائق الحاسوب.

قال غاوتييه إنه من المحتمل استخدام التقنية الجديدة لإنشاء بطاقات هوية آمنة، لتتبع البضائع في سلاسل التوريد وكجزء من تطبيقات التحقق، إذ أنه من الضروري معرفة أنك لا تتواصل مع محتال.

قال غاوتييه: "مشروع اختراق **SolarWinds** الذي استهدف الحكومة الأمريكية جعل الناس يفكرون حقًا في كيفية قيامنا بعمليات التحقق والتشفير، نأمل أن يكون هذا جزءًا من الحل".

يستخدم الحل الجديد تقنية **PUFs** التي تستفيد من اختلافات التصنيع الصغيرة الموجودة في كل شريحة حاسوب، اختلافات صغيرة جدًا بحيث لا يمكن ملاحظتها للمستخدم، كما قال نيلويكو شارلوت **Noeloikeau Charlot**، المشارك الرئيسي في الدراسة وطالب الدكتوراه في الفيزياء في جامعة ولاية أوهايو.

قال شارلوت: "هناك ثروة من المعلومات حتى في أصغر الاختلافات الموجودة على رقائق الحاسوب التي يمكننا استغلالها لإنشاء **PUFs**".

تُستخدم هذه الاختلافات الطفيفة ـ التي تُرى أحيانًا على المستوى الذري فقط ـ لإنشاء تسلسلات فريدة من 0 و1 يطلق عليها الباحثون في المجال، بشكل مناسب بما فيه الكفاية، "أسرار".

طورت مجموعاتٌ بحثيةٌ أخرى ما اعتقدوا أنه تقنية **PUFs** قوية، لكن أظهرت الأبحاث أن المتسللين يمكنهم مهاجمتها بنجاح. قال غاوتييه إن المشكلة هي أن **PUFs** الحالية تحتوي فقط على عدد محدود من الأسرار.

غاوتييه: "إذا كان لديك **PUF** حيث يبلغ عدد أسرارها 1,000 أو 10,000 أو حتى مليون، فيمكن للمتسلل الذي يمتلك التكنولوجيا المناسبة ووقتًا كافيًا أن يعرف كل الأسرار الموجودة على الشريحة، نعتقد أننا وجدنا طريقة لإنتاج عدد كبير لا يحصى من الأسرار لاستخدامها، ما يجعل من المستحيل على المتسللين اكتشافها، حتى لو كان لديهم وصول مباشر إلى شريحة الحاسوب".

مفتاح إنشاء **PUF** المحسّن هو الفوضى أو الشواش، وهو موضوع درسه غاوتييه لعقود. قال إنه لم يستخدم الشواش بالطريقة الموضحة في هذه الدراسة من قبل.

أنشأ الباحثون شبكةً معقدةً في **PUFs** الخاصة بهم باستخدام شبكة من البوابات المنطقية المترابطة بشكل عشوائي. تأخذ البوابات المنطقية إشارتين كهربائيتين وتستخدمهما لإنشاء إشارة جديدة.

قال غاوتييه: "نحن نستخدم البوابات المنطقية بطريقةٍ غير قياسية تخلق سلوكًا غير موثوق به. ولكن هذا ما نريده. نحن نستغل هذا السلوك غير الموثوق به لخلق نوع من الفوضى الحتمية".

تضخم الفوضى الاختلافات الصغيرة في التصنيع والموجودة على الرقاقة. حتى أصغر الاختلافات، عند تضخيمها بالفوضى العشوائية،

يمكن أن تغير فئة النتائج المحتملة بأكملها، وفي هذه الحالة فهي الأسرار التي أنتجت، وفقًا لشارلوت.

قال شارلوت: "تؤدي العشوائية حقًا إلى زيادة عدد الأسرار المتوفرة في الشريحة، ومن المحتمل أن يؤدي هذا إلى إرباك أي محاولات للتنبؤ بالأسرار".

أحد مفاتيح هذه العملية هو تركها تعمل لفترة طويلة على الرقاقة، إذا تركتها تعمل لفترة كافية، فإنها تصبح فوضوية للغاية، وفقًا لغاويتيه.

يقول غاويتيه: "نريد أن تستمر العملية لفترة طويلة بما يكفي لإنشاء أنماط معقدة للغاية بحيث يتعذر على المتسللين مهاجمتها وتخمينها، ولكن يجب أن يكون النمط قابلًا للتكرار حتى نتمكن من استخدامه في مهام المصادقة والتحقق".

حسب الباحثون فإن **PUF** الخاص بهم يمكن أن يخلق 1,077 سرًا. ما هو حجم هذا الرقم؟ تخيل لو استطاع المتسلل تخمين سر واحد كل ميكروثانية أو مليون سر في الثانية. يقول غاويتيه إن الأمر سيستغرق المتسلل وقتًا أطول من عمر الكون، نحو 20 مليار سنة لتخمين كل سر متوفر في تلك الرقاقة الدقيقة.

كجزء من الدراسة، هاجم الباحثون **PUF** الخاص بهم لمعرفة ما إذا كان يمكن اختراقه بنجاح. لقد حاولوا شن هجمات على التعلم الآلي، بما في ذلك الأساليب المستندة إلى التعلم العميق والهجمات المستندة إلى النماذج، والتي فشلت جميعها. إنهم يعرضون الآن بياناتهم على مجموعاتٍ بحثيةٍ أخرى لمعرفة ما إذا كان بإمكانهم إيجاد طريقة لاختراقها.

يقول غاويتيه إن الأمل هو أن تساعد مثل هذه التقنية في تعزيز الأمن ضد حتى هجمات القرصنة التي ترعاها الدولة، والتي تكون بشكل عام معقدةً للغاية ومدعومةً بالكثير من موارد الحاسوب.

على سبيل المثال، يُشتبه في أن روسيا تدعم اختراق **SolarWinds** الذي كُشِف عنه في ديسمبر/كانون الأول الماضي. وبحسب ما ورد، تمكن هذا الاختراق من الوصول إلى حسابات البريد الإلكتروني لمسؤولين في وزارة الأمن الداخلي الأميركية وموظفي الأمن السيبراني بالوزارة.

غاويتيه: "إنها معركة مستمرة لابتكار تكنولوجيا يمكنها أن تسبق بخطوة المتسللين. نحاول ابتكار تقنية لا يستطيع أي متسلل اختراقها، بغض النظر عن مواردك، وبغض النظر عن الحاسوب العملاق الذي تستخدمه".

وتقدم الباحثون بطلب للحصول على براءة اختراع دولية للجهاز الخاص بهم.

هدف الفريق هو تجاوز البحث والتحرك بسرعة لتسويق التكنولوجيا. أسس غاويتيه وشركاؤه مؤخرًا شركة **Verilock** بهدف طرح المنتج في السوق في غضون عام.

قال جيم نورثوب **Jim Northup**، الرئيس التنفيذي لشركة **Verilock**: "نرى هذه التكنولوجيا على أنها مغيّر حقيقي للعبة في مجال الأمن السيبراني. قد يثبت هذا النهج الجديد والقوي أنه غير قابل للاختراق فعليًا".

- التاريخ: 2021-06-11
- التصنيف: تكنولوجيا

#الامن الالكتروني #الهاكرز #الاختراقات الالكترونية

المصادر

- techxplore.com

المساهمون

- ترجمة
  - محمد السيد عبده
- مُراجعة
  - هبة العيوطي
- تحرير
  - رأفت فياض
- تصميم
  - روان زيدان
- نشر
  - احمد صلاح