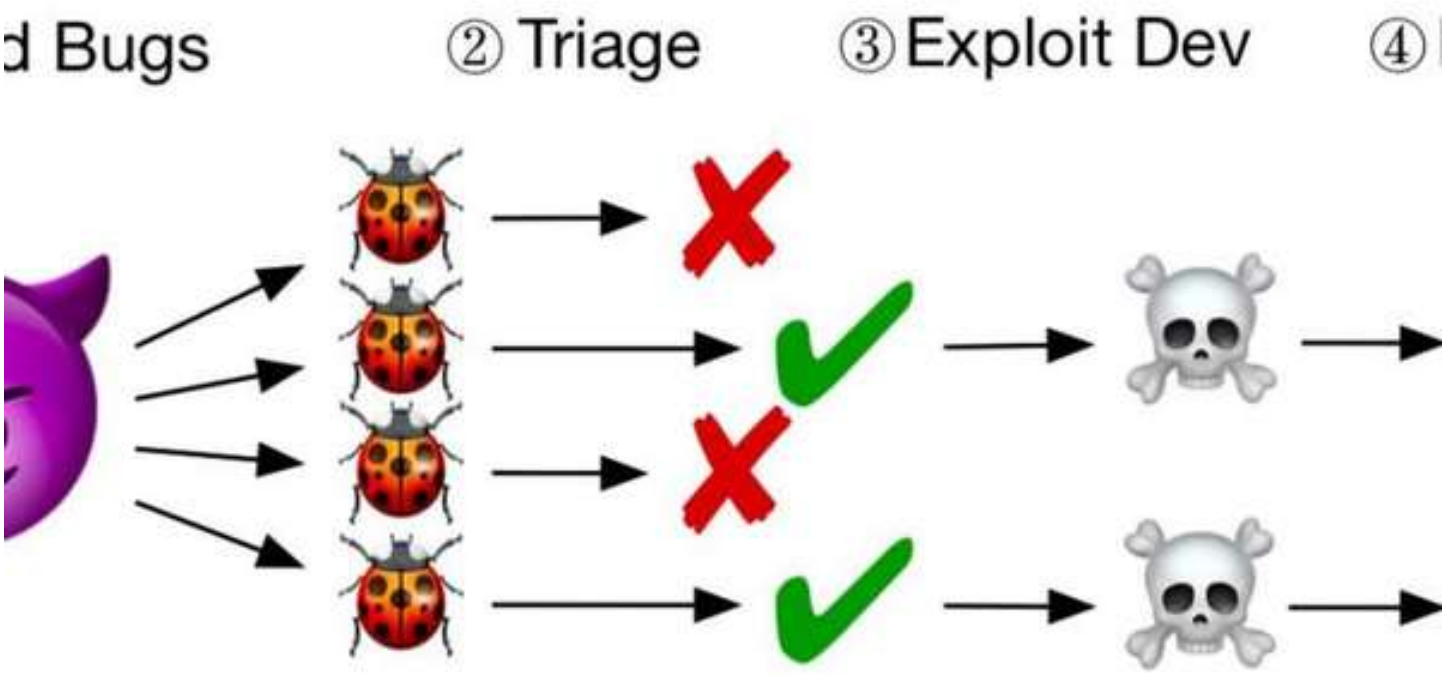
حماية البرامج من الاختراق بإضافة المزيد من الثغرات

ابتكر باحثون في جامعة نيويورك New York University تقنية دفاع إلكتروني جديدة، والتي تعمل بإضافة ما سُمي بالثغرات القشرية Chaff Bugs وهي عبارة عن ثغرة برمجية مصطنعة غير قابلة للاستغلال، وذلك عوضاً عن إزالة الثغرات الموجودة مسبقاً.



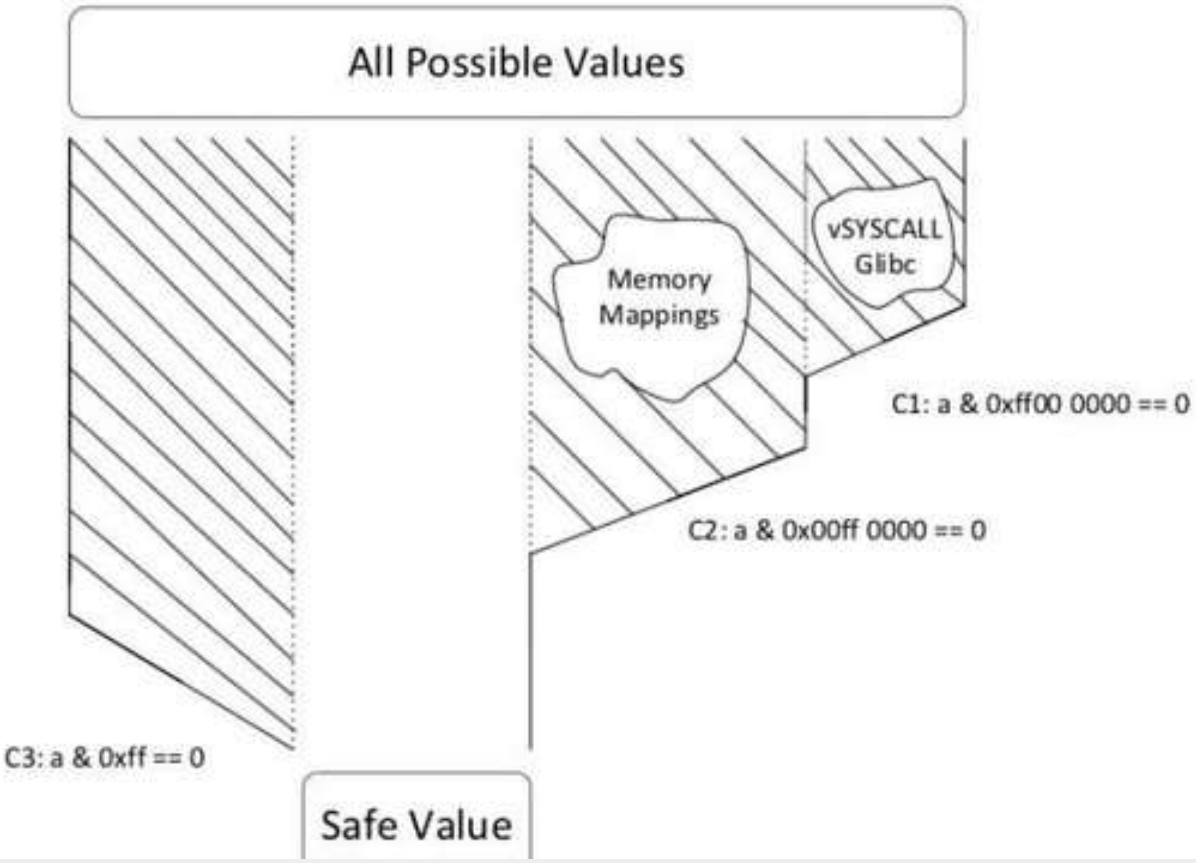
: نموذج العمل المبسط للمخترقين: يجد المخترقون الثغرات، يختبرونهم لتحديد قابلية استغلالهم، ثم يطورون برامج مهاجمة ويفعلونها في أهدافهم. حقوق الصورة: Hu, Hu & Dolan-Gavitt.

كل يوم، تزداد قدرة المخترقين المحترفين على إيجاد الثغرات في الأنظمة الحاسوبية وتقييم قابلية استغلالها وتطوير طرق لتحقيق ذلك. معظم التقنيات الدفاعية تهدف إلى التخلص من هذه الثغرات، أو الحد منها، أو إضافة عقبات تجعل استغلال الثغرات أكثر صعوبة.

بريندان دولان-غافيت **Brendan Dolan-Gavitt** هو أحد الباحثين في هذه الدراسة، يقول: "نفذنا مشروعنا بناءً على عملٍ سابق قمنا به بالتعاون مع مخبر لينكولن في جامعة ماساتشوستس للتكنولوجيا **MIT Lincoln Lab** وجامعة نورث إيسترن **Northeastern University** والذي هدف إلى تقييم استراتيجيات مختلفة لإيجاد الثغرات في البرمجيات. لتحقيق ذلك، قمنا ببناء نظام يمكنه وضع آلاف الثغرات في برنامج ما، لنتمكن بعدها من قياس مدى فعالية كل من استراتيجيات إيجاد الثغرات في إيجادها للثغرات التي قمنا بوضعها".

بعد تطوريهم لهذا النظام، بدأ الباحثون بالبحث في تطبيقاته الممكنة في سياق تحسين أمن المعلومات، واستنتجوا أن هناك طريقة موحدة لكيفية إيجاد المخترقين للثغرات في البرامج عادةً واستغلالهم لها.

يقول دولان-غافيت: "إن الأمر يتطلب الكثير من الوقت لمعرفة الثغرات القابلة للاستغلال وتطوير طريقة لاستغلالها، لذا فكرنا أنه إذا استطعنا بطريقة ما جعل جميع الثغرات التي صنعناها غير قابلة للاستغلال سنتمكن من تشويش المخترقين وإغراقهم في بحر من الثغرات التي تبدو واعدة إلا أنها في الحقيقة غير مفيدة لهم على الإطلاق".



ثغرة من نوع overconstrained value (قيمة شديدة القيود). من خلال إضافة قيود على الطريق المؤدي إلى الثغرة فإننا نلغي القيم الغير آمنة تدريجياً. حقوق الصورة: Hu, Hu & Dolam-Gavitt

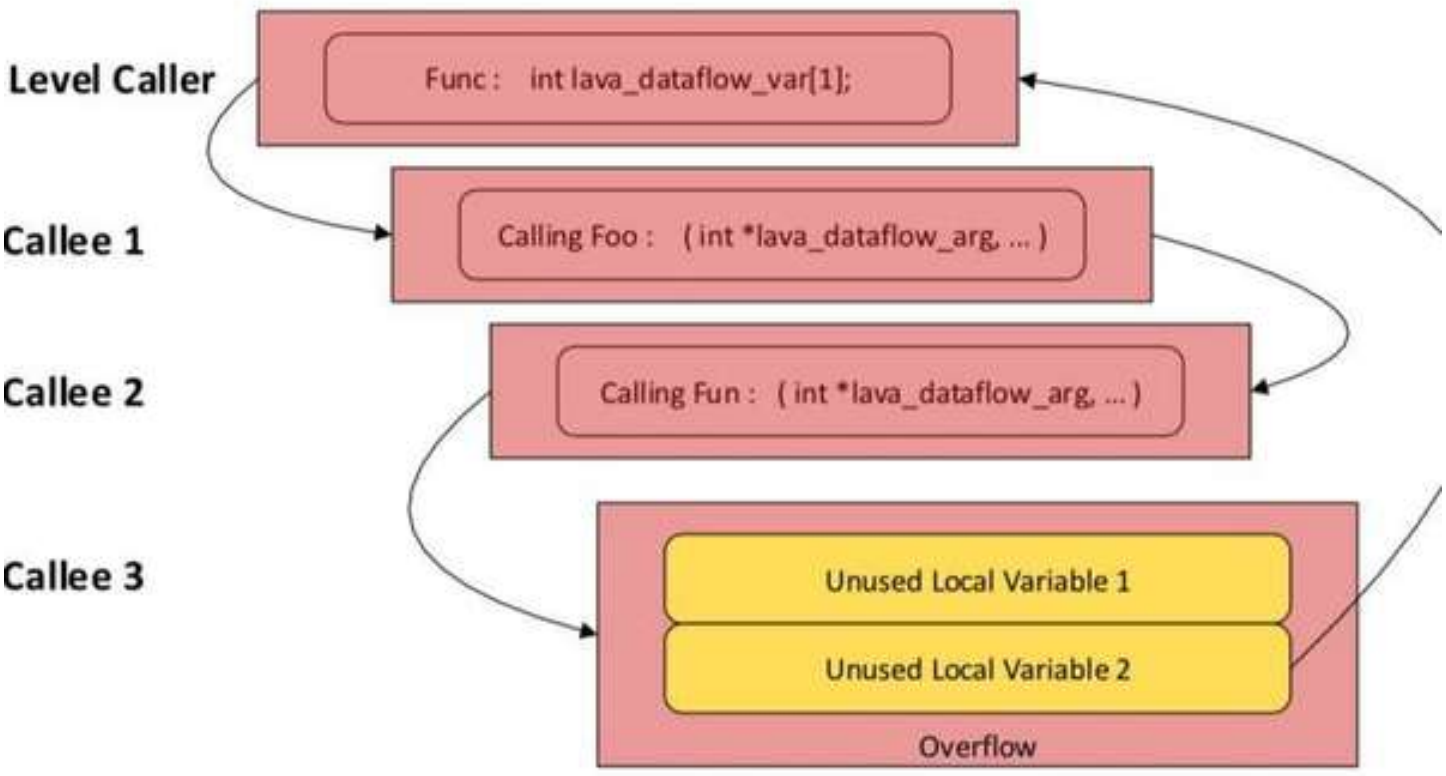
إن إضافة أعداد هائلة من الثغرات التي تبدو قابلة للاستغلال لكنها في الحقيقة ليست كذلك يمكن أن يربك المخترقين، مما يجعلهم يهدرون وقتهم وجهدهم في البحث عن طرق لاستغلال لتلك الثغرات الموضوعة عن قصد، وقد سمّى الباحثون هذه الطريقة الجديدة في مجابهة المخترقين بالثغرات القشرية.

يقول دولان-غافيت: "نظامنا الذي يقوم بإضافة الثغرات القشرية بشكل أوتوماتيكي من المفترض استخدامه أثناء بناء المطورين للبرمجيات". ويضيف: "لقد استخدمنا استراتيجيتين للحرص على كون ثغراتنا آمنة بالنسبة للبرنامج: إما من خلال تأكيد أن المخترق يمكنه إفساد البيانات التي لا يستخدمها البرنامج فقط، أو من خلال تحديد المجال للقيم التي يمكن للمخترق إضافتها بحيث يكون مجالاً من القيم الآمنة".

استخدم الباحثون هاتين الاستراتيجيتين في دراستهم لإضافة آلاف الثغرات غير القابلة للاستغلال بشكل أوتوماتيكي لبرمجيات مستخدمة في العالم الحقيقي، بما فيها مخدم الوب إنجينكس **NGINX** ومكتبة الترميز وفك الترميز ليبفلاك **libFLAC**. وجد الباحثون أن عمل البرمجيات لم يتضرر وأن الثغرات القشرية كانت ذات مظهر قابل للاستغلال من قبل أدوات اختبار الثغرات الموجودة حالياً.

يقول دولان-غافيت: "من أكثر الاكتشافات المثيرة للاهتمام أنّه من الممكن صنع هذه الثغرات غير القابلة للاختراق بشكل أوتوماتيكي بطريقة تبدو واضحة لنا بأنها غير قابلة للاستغلال، ولكن لا يراها المخترق. في بداية العمل لم يكن ذلك واضحاً لنا، كما أننا نعتقد أن هذه الطريقة في تطبيق منطق اقتصادي نوعاً ما (إيجاد المحدودية في أدوات المخترقين ومحاولة استغلالها) هي مفهوم واعد يمكّن البحث في

مجال أمن البرمجيات".



: ثغرة من نوع Unused variable (متغير غير مُستخدم). نُضيف مخطط عمل لتوسيع مجال القيمة غير المستخدمة خارج مجال الرؤية الابتدائي لإخفاء حقيقة أنها غير مستخدمة. حقوق الصورة: Hu, Hu & Dolan-Gavitt

مع أن هذه الدراسة كان لها نتائج جيدة إلا أن هناك بعض المشاكل التي يجب التخلص منها حتى تصبح هذه المنهجية أكثر قابلية للتطبيق عملياً. أهم هذه المشاكل، وجوب إيجاد طريقة لجعل هذه الثغرات غير القابلة للاستغلال مطابقة بالشكل تماماً للثغرات الحقيقية.

يقول دولان-غافيت: "حالياً، الثغرات التي نضيفها تبدو مصطنعة بعض الشيء، لذا يمكن للمخترقين تجاهلها أثناء بحثهم عن ثغرات قابلة للاستغلال. تركيزنا الأساسي الآن هو إيجاد طرق لجعل الثغرات التي نضيفها تبدو كثغرات تظهر بشكل طبيعي ومن ثم إجراء اختبارات للتأكد من أن المخترقين ينخدعون حقاً بثغراتنا القشرية".

- التاريخ: 2019-01-14
- التصنيف: تكنولوجيا

#بالثغرات القشرية #المخترقين #الثغرات

المصادر

- techxplore
- الصورة

المساهمون

- ترجمة
  - يمان علاء الدين
- مُراجعة
  - فرح درويش
- تحرير
  - زين صالح
- تصميم
  - عمرو سليمان
- نشر
  - أمل أحمد