الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbes

Graduation Thesis

To obtain the diploma of **Engineering Degree**

Field of Study: **Computer Science**

Specialization: **Computer Systems Engineering (ISI)**

Theme

Bypassing Kernel Control Flow Integrity

Presented by
Abdelouahab 'habs' Benchikh

Defended on: **07 October, 2024**
In front of the jury composed of

Mr. Amrane Abdelkader	President of the Jury
Mr. Sidi Mohammed BENSLIMANE	Thesis Supervisor
Mr. Yan Shoshitaishvili	Co-Supervisor
Ms. Baba-Ahmed Manel	Examiner

Academic Year: 2023/2024

ABSTRACT (ENGLISH)

The Linux operating system is the backbone of countless devices, personal or otherwise, servers, etc. Making its security a paramount concern. Given the open source nature of the Linux Kernel, attackers and researchers alike have access to the very core of the Linux operating system, allowing them to dive deep into its internals and find and/or patch flaws therein.

This work dives into the kernel, how it is debugged and broken by attackers, as well as common attack patterns and defenses.

With impenetrability in mind, CFI is introduced to the kernel, putting an end to a large portion of attacks that rely on control flow hijacking primitives, that have previously caused infinite damage to infrastructures, working environments, personal lives, etc. We discuss this protection and how it works in defending against the aforementioned fashion of attacks.

We also demonstrate how CFI is triggered and how it works under the hood, as well as how it is bypassed simply by adhering to its policies with data only attacks and overwriting the right pointers with the right locations.

We look at the way to bypass this protection, as a way to showcase the need for more protection, as ending the cycle of attack and defense here would only lead to more potential damage.

ABSTRACT (FRENCH)

Le système d'exploitation Linux est la colonne vertébrale d'innombrables appareils, qu'ils soient personnels ou non, de serveurs, etc., rendant sa sécurité d'une importance capitale. Étant donné la nature open source du noyau Linux, les attaquants comme les chercheurs ont accès au cœur même du système d'exploitation, leur permettant d'explorer ses entrailles et de découvrir et/ou de corriger les failles qu'il contient.

Ce travail s'intéresse au noyau, à la manière dont il est débogué et compromis par les attaquants, ainsi qu'aux schémas d'attaque courants et aux défenses associées. Avec l'inviolabilité en tête, CFI est introduite dans le noyau, mettant fin à une grande partie des attaques qui reposent sur des primitives de détournement de flux de contrôle, ayant auparavant causé d'innombrables dégâts aux infrastructures, aux environnements de travail, à la vie privée, etc. Nous discutons de cette protection et de son fonctionnement pour se défendre contre les types d'attaques mentionnés ci-dessus.

Nous montrons également comment CFI est déclenchée et comment elle fonctionne en interne, ainsi que comment elle peut être contournée simplement en respectant ses politiques, par des attaques basées uniquement sur les données et en écrasant les bons pointeurs avec les bonnes valeurs.

Nous analysons enfin les moyens de contourner cette protection, afin de souligner la nécessité d'une protection accrue, car mettre fin au cycle d'attaque et de défense à ce stade ne ferait que conduire à des dégâts potentiels encore plus importants.

ABSTRACT (ARABIC)

يعتبر نظام التشغيل لينكس العمود الفقري لعدد لا يحصى من الأجهزة، سواء كانت شخصية أو غير ذلك، والخوادم، وما إلى ذلك، مما يجعل أمنه مسألة ذات أهمية قصوى. نظرًا للطبيعة مفتوحة المصدر لنواة لينكس، فإن المهاجمين والباحثين على حد سواء لديهم وصول إلى جوهر نظام التشغيل لينكس، مما يسمح لهم بالتعمق في داخليته والعثور على العيوب وتصحيحها.

يتعمق هذا العمل في النواة، وكيف يتم تصحيحها وتحطيمها من قبل المهاجمين، بالإضافة إلى أنماط الهجمات الشائعة والدفاعات.

مع وضع عدم الاختراق في الاعتبار، يتم تقديم ثذي إلى النواة، مما يضع حدًا لجزء كبير من الهجمات التي تعتمد على اختطاف تدفق التحكم، والتي تسببت سابقًا في أضرار لا حصر لها للبنى التحتية، وبيئات العمل، والحياة الشخصية، وما إلى ذلك. نناقش هذه الحماية وكيفية عملها في الدفاع ضد نمط الهجمات المذكور أعلاه.

نحن نعرض أيضًا كيف يتم تفعيل ثذي وكيف يعمل خلف الكواليس، وكذلك كيف يتم تجاوزه ببساطة من خلال الالتزام بسياساته بهجمات تعتمد فقط على البيانات واستبدال المؤشرات الصحيحة بالمواقع الصحيحة.

ننظر في طريقة لتجاوز هذه الحماية، كوسيلة لإظهار الحاجة إلى مزيد من الحماية، حيث أن إنهاء دورة الهجوم والدفاع هنا سيؤدي فقط إلى مزيد من الأضرار المحتملة.