Hacker-Lexikon: Was ist Fuzzing?

Autor: Andy Greenberg.Andy Green Sicherheit

WIRED | 2016.06.02

Hacker manchmal ihre Arbeit als präzise Prozess darzustellen jedes Detail eines system sogar besser als ihre Designer-dann das Lernen zu erreichen tief in sie geheime Mängel zu nutzen. Aber wie oft, es ist praktisch das Gegenteil, ein grundlegend Zufallsprozess bei einer Maschine des Stoßens und beobachten, was passiert. Weiterzubilden, dass zufällige Stossen einer sorgfältigen Handwerk von Versuch und Irrtum, und es wird, was Hacker "Fuzzing" -a leistungsfähiges Werkzeug für sowohl Computer Ausbeutung und Verteidigung nennen.

TL; DR: Fuzzing ist die meist automatisierten Prozess Zufallsdaten in ein Programm zur Eingabe und der Analyse der Ergebnisse möglicherweise ausnutzbaren Fehler zu finden.

In der Welt der Sicherheit im Internet, ist ein Zerfasern der Regel automatisierten Prozess hackbare Software-Fehler zu finden, nach dem Zufallsprinzip verschiedene Permutationen von Daten in ein Zielprogramm, bis einer dieser Permutationen zeigt eine Schwachstelle zugeführt wird. Es ist eine alte, aber immer häufiger Prozess sowohl für Hacker Schwachstellen versuchen, zu nutzen und Verteidiger versuchen, sie zuerst zu finden, um zu beheben. Und in einer Zeit, als jeder kann leistungsstarke Computing-Ressourcen drehen, um eine Opfer-Anwendung mit Datenmüll auf der Suche nach einem Bug zu bombardieren, ist es ein wesentlicher Front im Zero-Day-Wettrüsten werden.

Im Vergleich zu herkömmlichen Reverse Engineering ", es ist eine Art stummen Wissenschaft", sagt Pedram Amini, Chief Technology Officer der Firma Cyber InQuest und Co-Autor des Buches Fuzzing: Brute Force Vulnerability Entdeckung. "Du bist in einem Programm eine ganze Menge Daten zu werfen, es schnell mutiert und sich auf Ihre Überwachung der Software zu finden, wenn etwas Schlimmes den Datenfluss, anstatt peinlich genau abbildet und passiert ist, einen Fehler zu finden ... Es ist ein Weg des Tötens off sehr schnell eine Reihe von Fehlern. "

Ein Hacker Fuzzing Internet Explorer, zum Beispiel könnte Microsofts Browser in einem Debugger-Tool ausführen, so dass sie jeden Befehl das Programm ausgeführt wird in den Speicher des Computers verfolgen können. Dann würden sie den Browser auf ihren eigenen Web-Server verweisen, ein entworfen ihre Fuzzing Programm auszuführen. Das fuzzer würde Tausende oder sogar Millionen von verschiedenen Web-Seiten zu erstellen und sie in seinem Browser Ziel laden, Variation nach Variation von HTML versuchen und Javascript, um zu sehen, wie der Browser reagiert. Nach Tagen oder sogar Wochen oder Monate dieser automatisierten Tests würde der Hacker Protokolle der tausende Male der Browser als Reaktion auf einen der Eingänge abgestürzt.

Diese Abstürze selbst stellen keine nützlichen Angriffe so viel wie Belästigungen; das eigentliche Ziel von Fuzzing ist nicht nur ein Programm zum Absturz zu bringen, aber es zu kapern. So wird ein Hacker ihre Flaum Eingänge scheuern, die zu Abstürzen führte, um zu sehen, welche Art von Fehler, die sie verursacht. In einigen kleinen Satz von Fällen haben diese Abstürze können für einen interessanten Grund, zum Beispiel geschehen, weil der Eingang, das Programm auszuführen Befehle verursacht wird, die an der falschen Stelle im Speicher abgelegt werden. Und in diesen Fällen könnte der Hacker gelegentlich in der Lage sein, ihre eigenen Befehle an dieser Speicherstelle zu schreiben, das Programm austricksen in ihre Gebote-den heiligen Gral zu tun, als die Codeausführung von Hacking bekannt. "Sie schütteln einen Baum wirklich hart, und Sie verwenden eine Reihe von Filtern", sagt Amini. "Schließlich Frucht kommt heraus."

Fuzzing-Methode von Zufallsdaten zwickt mit Bugs zu graben war selbst ein Unfall. Im Jahre 1987 wurde versucht, University of Wisconsin in Madison Professor Barton Miller den Desktop-VAX Computer in seinem Büro über ein Terminal in seinem Haus zu verwenden. Aber er war eine Verbindung zu dieser UNIX-Rechner über eine Telefonleitung mit einem altmodischen Modem ohne Fehlerkorrektur und ein Gewitter gehalten Lärm Einführung in die Kommandos er tippte. Programme, die auf der VAX gehalten abstürzt. "Es schien seltsam, und es löste die Idee, die wir sie studieren sollte", sagt er.

Mit einer Gruppe von Studenten, erstellt Miller das erste speziell gebaute Fuzzing-Tool, um zu versuchen, dass die Methode der wahllos Fehler stolpert in Sicherheit zu nutzen, und sie legte ein Papier darauf zu Konferenzen. "Die Software-Gemeinschaft geschlachtet mich. »Wo ist Ihr formales Modell?«, Hatte sie sagen. Ich würde sagen: "Ich bin einfach nur Fehler zu finden versuchen." Ich habe mich über die Kohlen geharkt ", erinnert er sich. „Heute, wenn Sie ein Hacker sind versucht, ein System zu knacken, das erste, was Sie tun, ist Flaum Test es."

In der Tat, Fuzzing hat sich von einer Low-Budget-Technik, die von einzelnen Hackern zu einer Art Tisch-Stakes-Sicherheits-Audit durchgeführt von großen Unternehmen auf ihren eigenen Code verwendet gewachsen. Lone Hacker können Dienste wie Amazon verwenden Armeen von Hunderten von Computern zu spin up, das ein Programm parallel Fuzz-Test. Und jetzt Unternehmen wie Google widmen auch ihre eigenen bedeutenden Server-Ressourcen zu Random-Code auf Programme werfen ihre Fehler zu finden, zuletzt Lernen mit Maschine, den Prozess zu verfeinern. Firmen wie Peach Fuzzer und Codenomicon haben sogar gebaut Unternehmen rund um den Prozess.

All das, argumentiert Amini, hat Fuzzing aktueller denn je. "Software-Shops sind, diese Arbeit als Standardteil ihres Entwicklungszyklus zu tun", sagt er. "Es ist eine große Investition, und sie helfen der Welt zur Verbesserung der Sicherheit von Software-Zyklen für jeden zu verbrennen."

lesen: https: //www.wired.com/2016/06/hacker-lexicon-fuzzing/