Projektgruppe Sicherheit in verteilten Systemen

BA-INF 051

Anmeldung

Um ein Thema zu erhalten, musst du dein Expose bis zum 08.10.2019 eingereicht haben. Sende es bitte an den Betreuer des jeweileigen Themas. Du wirst bis zum 15.10.2019 informiert, ob du dein gewünschtes Thema erhalten/nicht erhalten hast.

Deadline für das Exposé: 08.10.2019

Deadline für die Registrierung in BASIS: 31.10.2019

Getting the most out of fuzzing

Betreuer

Klaus Tulbure
tulburek@iai.uni-bonn.de

Getting the most out of fuzzing

Coverage-based fuzzing ist eine der gängigsten Fehler- und Schwachstellen-Analysen für Software. Man kann es vereinfacht als eine "intelligente" Brute-Force-Analyse beschreiben, die ein Program solange mit Eingaben bombardiert, bis es abstürzt. Die Eingaben sind dabei nicht zufällig, sondern werden mittels eines evolutionären Algorithmus mit Code-Abdeckung als Fitness-Funktion generiert.

Allerdings hat die Code-Abdeckung als alleiniges Kriterium sein Grenzen, so sagt sie zum Beispiel nichts über den Einfluss einer Eingabe aus. Daher ist es das Ziel, durch Sammeln weiterer Informtionen tiefere Einblicke in das Program zu erhalten.

Getting the most out of fuzzing

Deine Aufgabe wird es sein, diese weiteren Informationen, z.B. den Program- und Datenfluss, Code-Abdeckung, Speicherverbrauch, Fehlermeldungen, Multi-Threding, aus dem Fuzzing Prozess zu extrahieren und zu evaluieren.

Anschließend müssen die Daten verarbeitet und gespeichert werden. Dafür lassen sich auch Techniken aus de Bereichen Algorithmik, Machine Learning und Künstlicher Intelligenz nutzen.

Anforderungen sind Programmierkenntnisse in

- C/C++ für das Extrahieren der Daten und
- eine beliebige Sprache für die Evaluierung.

Getting the most out of fuzzing

Literature

Klees et al. erklären die allgemeinen Konzepte von Coverage-based fuzzing sehr verständlich. Sie haben Fuzzer der letzten Jahre evaluiert, die Techniken verglichen und außerdem einige Schwächen der codeabdeckungsbasierten Ansätze genannt.

Klees, George, et al. "Evaluating fuzz testing." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018.

Usability of fuzzers

Betreuer

Stephan Plöger
ploegers@cs.uni-bonn.de

Usability of fuzzers

The idea is to conduct a study where participants solve different fuzzing tasks with different fuzzers to determine the usability of those fuzzers.

Tasks to solve are and are not limited to: Which fuzzers to use - which programs/tasks to use - type of participants - type of study.

A key problem is to find appropriate tasks and participants.

Requirements are programming skills in

- C/C++ to be able to work with the most common fuzzers
- Knowledge about study design (USECAP lecture)
- Knowing what a fuzzer is is helpful

Usability study about fixing bugs (fuzzing)

Betreuer

Stephan Plöger
ploegers@cs.uni-bonn.de

Usability study about fixing bugs (fuzzing)

The idea is to conduct a study where participants are confronted with the output of different fuzzers and asked to find and fix the corresponding bug to determine the usability of the output.

Tasks to solve are and are not limited to: Which fuzzers to use - which programs/tasks to use - type of participants - type of study.

A key problem is to find appropriate tasks and participants.

Requirements are programming skills in

- C/C++ to be able to work with the most common fuzzers
- Knowledge about study design (USECAP lecture)
- Knowing what a fuzzer is is helpful

CTF Tasks

Betreuer

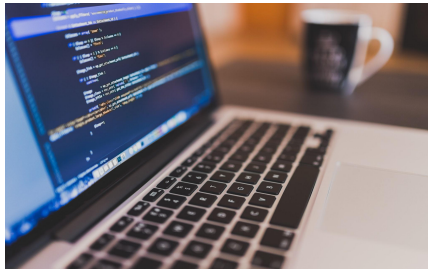
Mischa Meier
meierm@cs.uni-bonn.de

CTF Tasks

The idea is to create tasks which can be used in a Capture the Flag(CTF) event. CTFs are information security competitions which can also be used in education.

Tasks could be and are not limited to: Web-security, binary exploitation, cryptography, reversing

The key problem is to find appropriate tasks, implement them and verify the attacks.



Requirements:

- Participated in CTFs before
- Knowledge about security

Eigene Ideen?

Betreuer

jeder von uns

Email an
Klaus Tulbure
tulburek@iai.uni-bonn.de

Eigene Ideen?

Du hast ein paar eigene Ideen für ein Projekt im Bereich Usable Security and Privacy?

GROßARTIG!

Wir würden uns freuen, mit euch zusammenzuarbeiten!