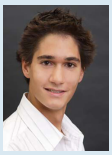


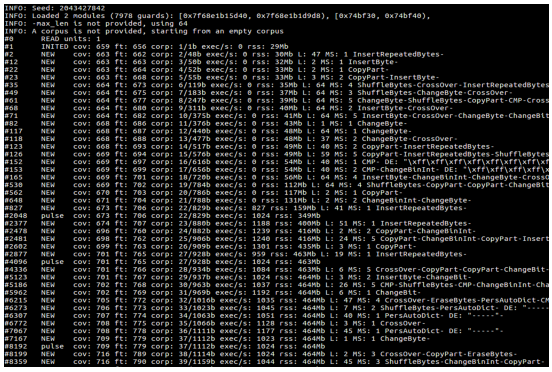
Sven
Defatsch

Studenten/-innen	Sven Defatsch
Dozenten/-innen	Prof. Dr. Andreas Steffen
Co-Betreuer/-innen	Tobias Brunner
Themengebiet	Sicherheit

Google OSS-Fuzz

Security Testing des strongSwan Codes

strongSwan



Aktiver Fuzzing Prozess

Fuzzing Ergebnisse bei in OSS mit Stack Trace

Ausgangslage: Im Jahr 2016 hat Google das sogenannte OSS-Fuzz Programm angekündigt, welches sich zum Ziel gemacht hat, ausgewählte Open Source Projekte sicherer zu machen. Dafür wird die Möglichkeit geboten, die enorme Rechenleistung der Google Infrastruktur für kontinuierliches Fuzzing, inklusive übersichtlichem Reporting zu nutzen. Die IPsec-basierte strongSwan Open Source VPN Lösung wird an der HSR entwickelt und weltweit eingesetzt. Für eine Software im Sicherheitsbereich ist es besonders wichtig, die Anzahl Fehler im Code so gering wie möglich zu halten. Dabei bietet Fuzzing eine gute Möglichkeit, latente Fehler zu entdecken und somit die Codequalität zu steigern.

Vorgehen/Technologien: Für das Fuzzing wurde libFuzzer eingesetzt, die zu diesem Zeitpunkt einzige von Google unterstütze Fuzzing Engine. Als vielversprechendes und relativ leicht umzusetzendes Fuzz Target bot sich der in strongSwan eingebaute X.509 Zertifikatsparser an. Die Fuzzing Umgebung wurde zuerst lokal getestet, um Erfahrungen im Umgang mit der Nutzung von libFuzzer zu sammeln und die notwendigen Änpassungen im strongSwan Build-Prozess zu bestimmen. Anschliessend wurde das Fuzzing auf die mächtige Google Infrastruktur verlagert, um den Code auf Herz und Nieren zu testen.

Ergebnis: Als Hauptresultat dieser Arbeit wurden Erkenntnisse über die Integration von strongSwan in das Google OSS-Fuzz Projekt gewonnen, insbesondere welche Stolpersteine beachtet werden müssen. Erfreulicherweise wurden beim intensiven Fuzzing schon nach kurzer Zeit mehrere Fehler unterschiedlicher Tragweite im strongSwan Code gefunden, die sofort behoben wurden und in Form von Security Patches in strongSwan eingeflossen sind. Somit ist das Hauptziel des Fuzzings, die strongSwan Codequalität zu verbessern, klar erreicht worden.