PNG-Fuzzing with JQF

Paul Kalz, Marwin Linke, and Sebastian Schatz

Humboldt University of Berlin, Germany

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.

Keywords: First keyword · Second keyword · Another keyword.

1 Background on the File Format PNG

1.1 Overview

TODO: Overview: Gebt einen kurzen Überblick über das ausgewählte Datenformat (Historie, Verwendungszweck,...)

History

Use Case

1.2 Input Specification

TODO: Input Specification: Beschreibt im Detail die Spezifikation des Dateiformats. Wie sind Dateien dieses Formats aufgebaut? Existiert eine formale Spezifikation? Wie ist eine Beispieldatei aufgebaut?

Specifications

Structure

1.3 Security

TODO: Security: Beschreibt mögliche Sicherheitslücken im Zusammenhang mit dem Datenformat. Geht dabei näher auf bereits existierende Fälle ein (case study), ggf. auch im Zusammenhang mit den von euch ausgewählten Tools (Bug-Tracker).

2 Implementation

2.1 Tools

TODO: Tools: Gebt einen kurzen Überblick über die von euch verwendeten Libraries. Beschreibt wie diese Libraries verwendet werden können um Dateien eures Datenformats zu generieren bzw. zu verarbeiten.

2.2 Generator

TODO: Generator: Beschreibt im Detail die Implementation eures Generators. Begründet dabei Design-Entscheidungen sowie von euch verwendete Heuristiken.

2.3 Fuzz Driver

TODO: Fuzz Driver: Beschreibt grob, wie ihr bei der Implementation der Test-Treibers vorgegangen seid und welche Funktionalitäten der Library mit eurem Treiber getestet werden.

2.4 Guidance

TODO: Guidance: Beschreibt eure Änderungen an der Suchstrategie von JQF. Geht dabei insbesondere auf die Motivation/Intuition eurer Ideen ein, d.h. weshalb ihr diese Änderungen für sinnvoll haltet.

3 Evaluation

TODO: Beschreibt die durchgeführten Experimente und deren Ergebnisse. Wie hoch war die erreichte Coverage? Konnten Bugs/Crashes gefunden werden? Wenn ja, welche?

3.1 Experiments

3.2 Results

4 Result Discussion

TODO: Versucht die Ergebnisse der Experimente zu interpretieren und zu erklären (discussion). Zieht Sie Folgerungen aus den Ergebnissen (conclusion). Beschreibt die nächsten Schritte, die durchgeführt werden müssten/könnten/sollten (future work).

4.1 Discussion

4.2 Conclusion

4.3 Future Work

References

1. Author, F.: Article title. Journal **2**(5), 99–110 (2016)
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016). https://doi.org/10.10007/1234567890
3. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999)
4. Author, A.-B.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)
5. LNCS Homepage, http://www.springer.com/lncs. Last accessed 4 Oct 2017