Automated Discovery of DNS Resolver Vulnerabilities with Stateful Fuzzing

Authors: Qifan Zhang, Xuesong Bai, Xiang Li, Haixin Duan, Qi Li and Zhou Li

Presenter: Zhou Li, UC Irvine

Domain Name System (DNS) is a critical component of the Internet. DNS resolvers, which act as the cache between DNS clients and DNS nameservers, are the centerpiece of the DNS infrastructure, essential to the scalability of DNS. Many security vulnerabilities of DNS resolvers have been discovered and acknowledged with Common Vulnerabilities and Exposures (CVE) numbers. However, finding the resolver vulnerabilities is still non-trivial, and this problem is not well addressed by the existing tools, in particular software fuzzers. To list a few reasons, first, most of the known resolver vulnerabilities are non-crash bugs that cannot be directly detected by the existing oracles (or sanitizers). Second, there lacks rigorous specifications to be used as references to classify a test case as a resolver bug. Third, DNS resolvers are stateful, and stateful fuzzing is still challenging due to the large input space.

In this talk, we'll present a new fuzzing system termed ResolverFuzz [1] to address the aforementioned challenges related to DNS resolvers, with a suite of new techniques being developed. First, we'll give a background description of the software fuzzing and present a study of the published DNS CVEs. Then, we will describe the framework of ResolverFuzz that is mainly based on stateful fuzzing. In particular, we consider the sequence of DNS queries and responses as one test input to adjust resolvers to different cache states, and we combine probabilistic context-free grammar (PCFG) based input generation with byte-level mutation for both queries and responses, so the generated test inputs are more likely to trigger bugs. To detect the non-crash, semantic bugs, we leverage differential testing and clustering to identify bugs like cache poisoning bugs.

We evaluated ResolverFuzz against 6 mainstream DNS software under 4 resolver modes. Overall, we identify 23 vulnerabilities that can result in cache poisoning, resource consumption, and crash attacks. After responsible disclosure, 19 of them have been confirmed or fixed, and 15 CVE numbers have been assigned.

Finally, I'll talk about the potential next steps of this work, like considering a broader set of states which are based on customized configurations. Through this work, we hope to advance the security of DNS resolvers by detecting and fixing the vulnerabilities more timely.

References:

[1] Qifan Zhang, Xuesong Bai, Xiang Li, Haixin Duan, Qi Li and Zhou Li. "ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing". In The 33rd USENIX Security Symposium, August, 2024.