Nyx-Net 2.0 Beta

Songyuan Bo
Miftahul Huq

What is Nyx-Net?

Nyx-Net is a novel snapshot-based fuzzing approach designed for efficient testing of complex, stateful network services.

Key Features:

- Uses incremental snapshots for efficiency.
- Supports fuzzing a wide range of targets including servers, clients, games, and IPC interfaces.
- Builds on the capabilities of Nyx, enhancing it for network fuzzing.

Achievements:

- Improved test throughput by up to 300x and coverage by up to 70% compared to state-of-the-art methods.
- Discovered previously unknown bugs in major software like Lighttpd and Firefox.

Core Design of Nyx-Net

Key Components:

- Hypervisor-Based Snapshot Fuzzing: Ensures noise-free testing and quick resets.
- Selective Emulation of Network Traffic: Avoids the heavy cost of handling real network traffic.

Incremental Snapshots:

- Reduce repeated processing of identical prefixes in test cases.
- Improve test throughput by 10x to 30x in complex scenarios.

Flexibility: Compatible with POSIX-compliant systems and supports both network and IPC fuzzing.

Advantage and Impacts

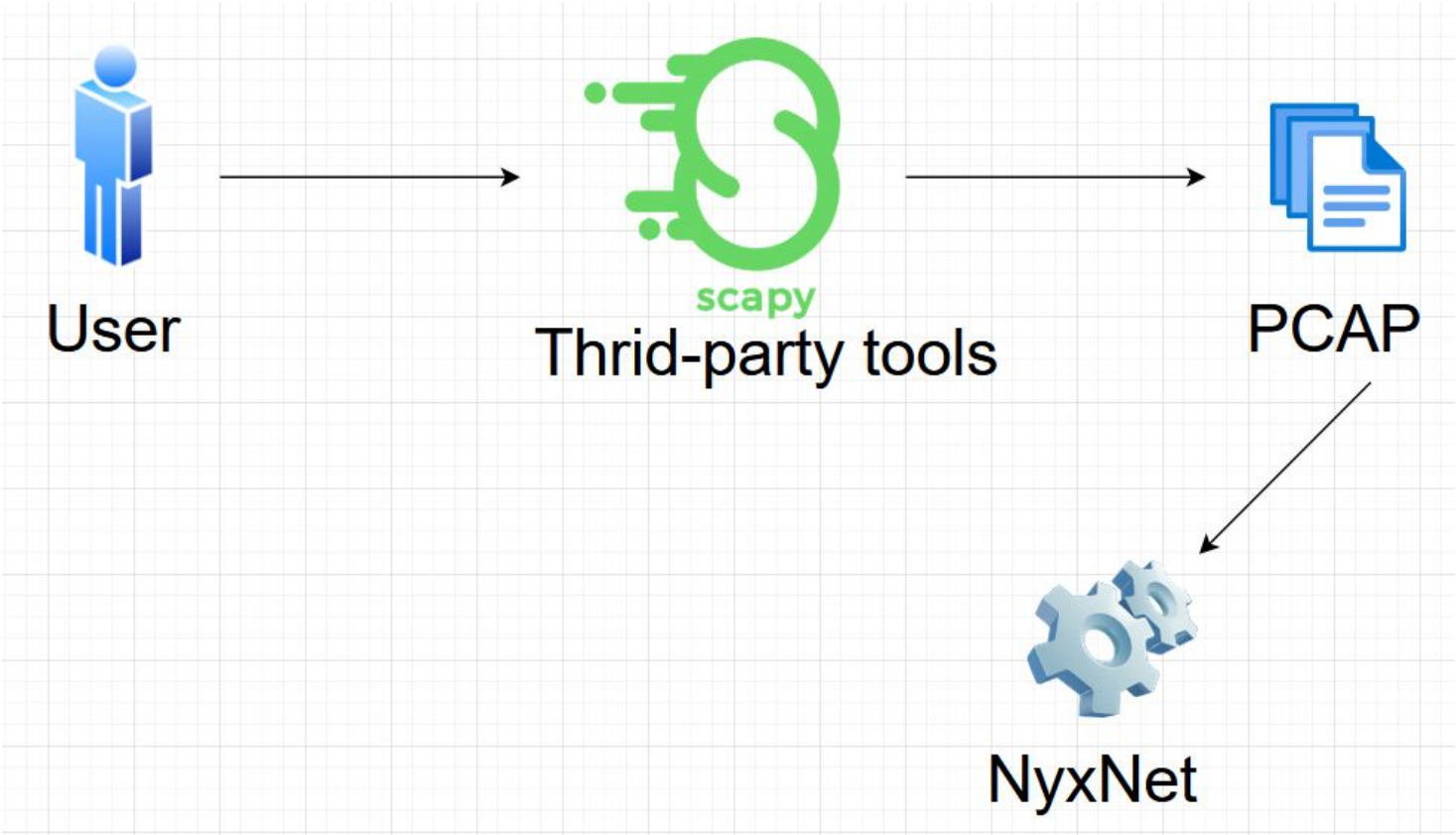
Performance:

- Handles complex, stateful message-based systems with ease.
- Outperforms AFLnet and other tools in most benchmarks, including ProFuzzBench.

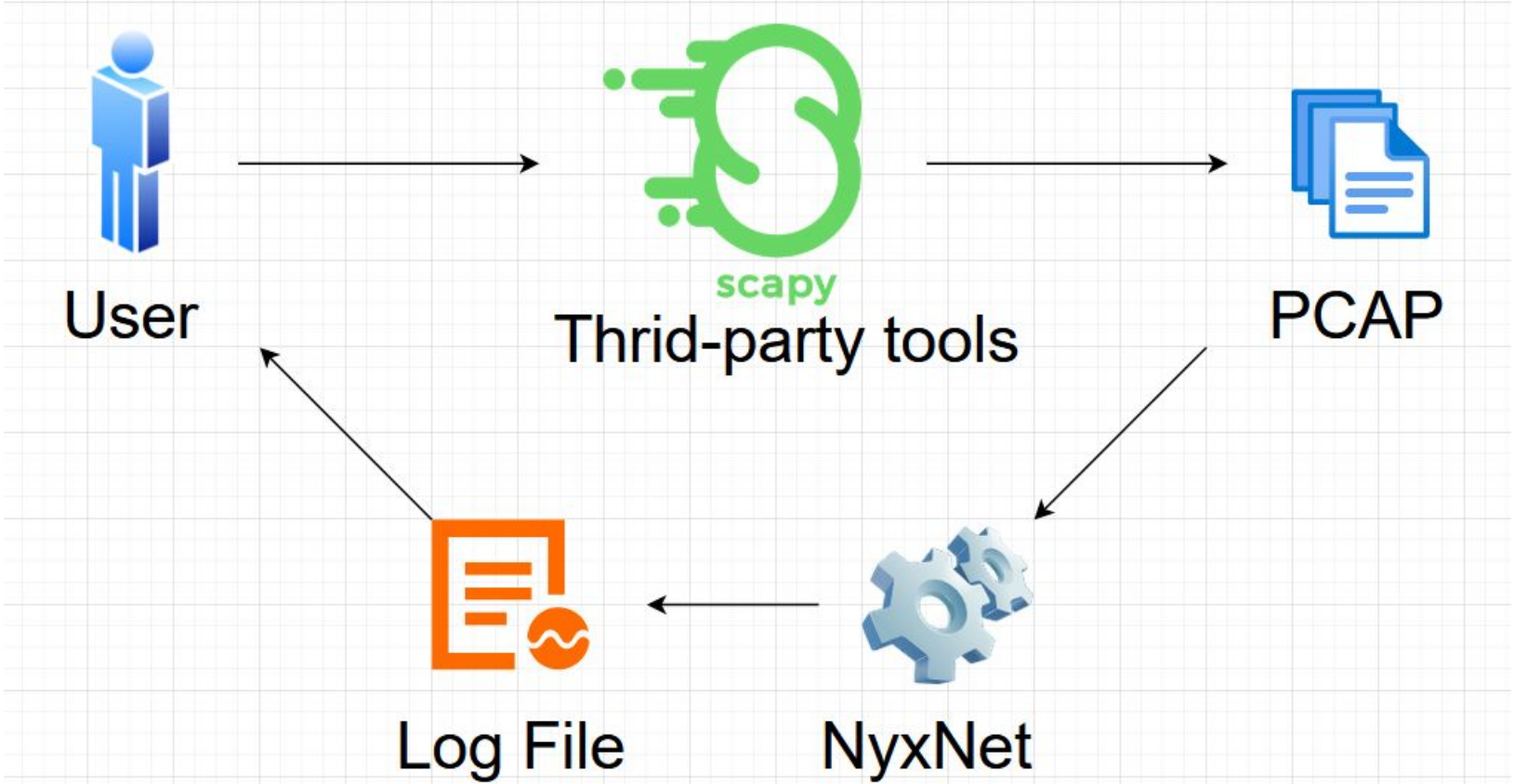
Found bugs in:

- Servers: Lighttpd.
- Clients: MySQL client.
- Games: Super Mario (10x–30x faster level-solving).
- IPC Interfaces: Firefox sandbox processes.

What it was



What it was



Grammar based fuzzing

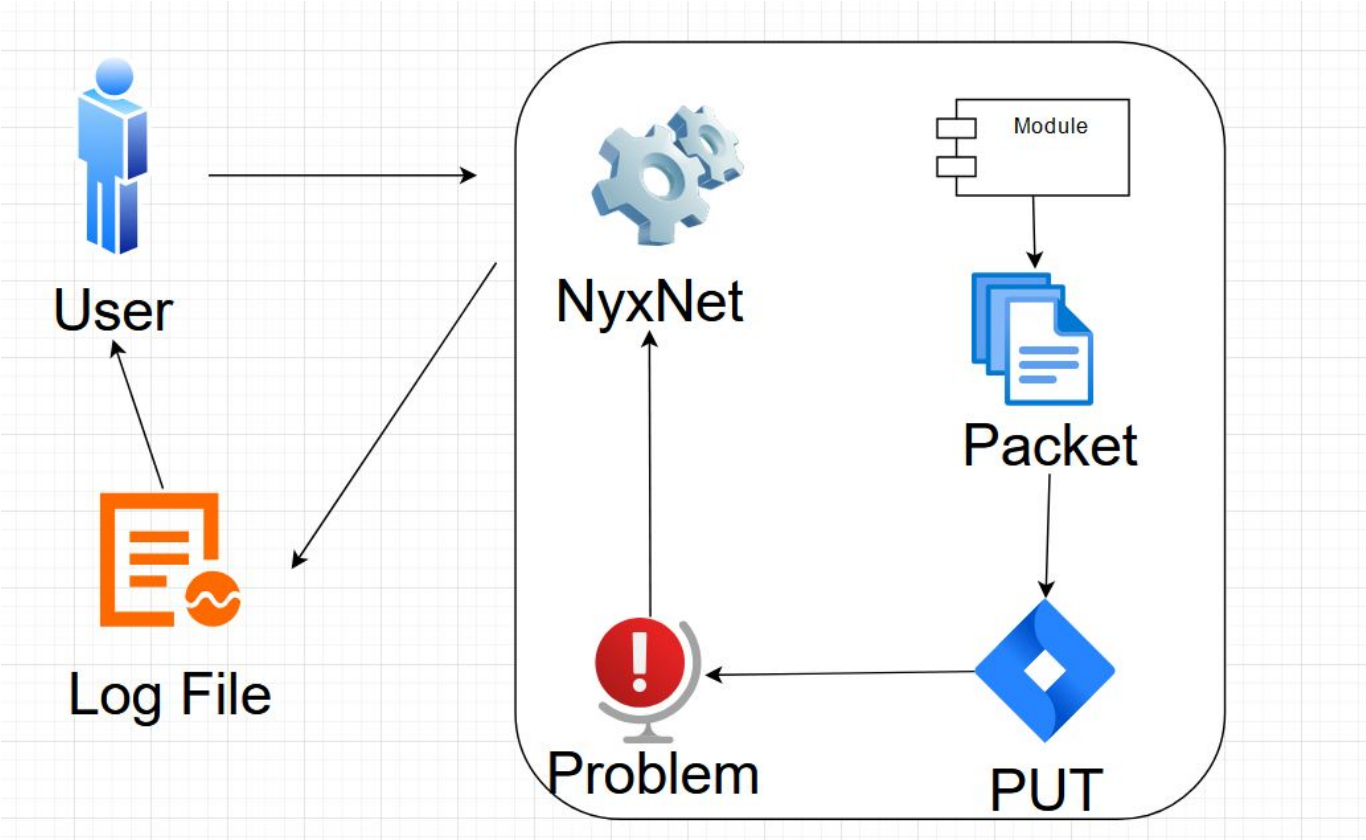
Dynamic packets generation

Automation

Improves efficiency and accuracy of fuzzing

Improves potential chance of finding vulnerability and instability of the PUT

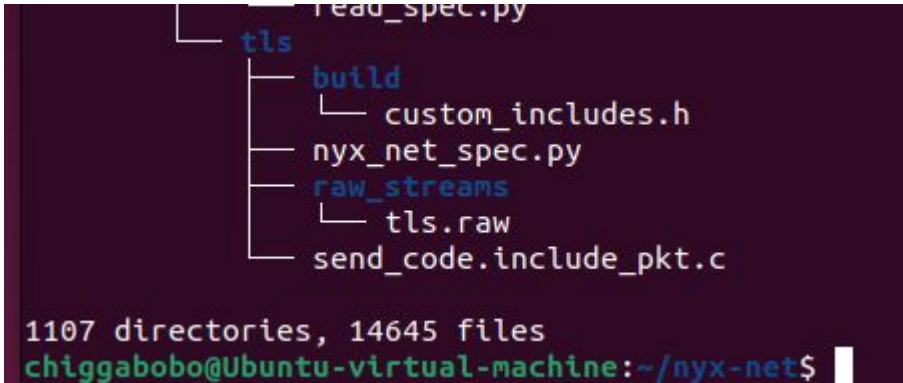
Our improvement



Problem

The source code of NyxNet 1.0 would not compile

Insufficient time given to exam all source code (586MP)



Project plan (Altered)

1. Create a standalone Grammar-based fuzzing module/program
2. Mimic NyxNet
3. Intergrate the module into NyxNet after we have it working

Live Demo!

Resources

- Schumilo, S., Aschermann, C., Jemmett, A., Abbasi, A., & Holz, T. (2022). Nyx-Net: Network Fuzzing with Incremental Snapshots. In Seventeenth European Conference on Computer Systems (EuroSys '22), April 5–8, 2022, Rennes, France. ACM. https://doi.org/10.1145/3492321.3519591
- Van-Thuan Pham, Marcel Böhme, and Abhik Roychoudhury. AFLNET: A Greybox Fuzzer for Network Protocols. In IEEE International Conference on Software Testing, 2020.
- Dokyung Song, Felicitas Hetzelt, Jonghwan Kim, Brent Byunghoon Kang, Jean-Pierre Seifert, and Michael Franz. Agamotto: Accelerating kernel driver fuzzing with lightweight virtual machine checkpoints. In USENIX Security Symposium, 2020.
- “Welcome to Scapy’s Documentation!.” Welcome to Scapy’s Documentation! - Scapy 2.6.0 Documentation, scapy.readthedocs.io/en/latest/. Accessed 21 Nov. 2024.

Questions?