Evolution of Peach: From Project to Product

Primer

This paper discusses and contrasts two distinct pieces of software: Peach Fuzzer® Community Edition and Peach Premier. Peach Fuzzer Community is a derivative of the original Peach Fuzzer that exists today as a project. Current Peach commercial offerings, Peach Professional and Peach Enterprise solutions, also include a derivative of the original Peach fuzzer. For clarity and exclusive to this writing, the current commercial Peach core system is named Peach Premier.

Peach Fuzzer Community edition is an open source project that focuses on the individual hobbyist or researcher. As an open source project, changes largely consist of bug fixes. Release cycles are lengthy.

Peach Premier is the most recent version of Peach Fuzzer, and is offered through our Peach Professional and Peach Enterprise solutions. Peach Premier includes extensive retooling of the core engine, rewriting of all mutators, and rewriting of most of the fuzzing definitions. These changes alone set Peach Premier apart from the Peach Community Edition.

In addition, Peach Premier has the support of a development team to provide direction for consistency, bug fixes, enhancements, and timely product releases. Nearly every feature found in Peach Community is present and augmented in Peach Premier. The following highlights of Peach Premier identify features and functionality not present in Peach Community:

Ease of Use

- A new web-based interface - The Peach web interface is a graphical user interface (GUI) that facilitates configuration, testing, and viewing status and findings. Reports from both current and past fuzzing sessions are available for review.
- A new command line interface – The command-line has several switches. For a list of commands available through the command-line interface, run “peach.exe –help”. You can also view a quick reference guide of the Peach DOM by running “peach.exe –showenv”.
- Documentation - The documentation includes a user guide that offers guidance in daily tasks using the web-based interface.
- The developer guide provides instructional and reference material with over 250 examples. Sections range from Setup and Getting Started to sections on using Peach.
- Fuzzing definitions (Peach Pits) from previous versions of Peach and from Peach Community are compatible with Peach Premier.
- Professional support and exclusive user forums are included with all Peach Professional and Peach Enterprise solutions. Training is available as well.

Functionality

The functionality of Peach Premier overshadows that of Peach Community, as evidenced by the extensive collection of available Peach Pits, modeling components, state modeling capabilities, and logging.

Peach Pits™

Peach Fuzzer, LLC, provides many Pits for fuzzing protocols and file types, including the following:

- **Network protocols**
  - ISO Layer protocols (UDP, Link Layer Discovery, TCP)
  - Internet protocols (ICMP, IGMP, IP)
  - Hardware (Cisco Discovery, Ethernet, Modbus)
  - File and file system (FTP, LDAP)
- **Image video file formats**:
  - BMP, GIF, JPEG, PNG, AVI

Modeling Components

- **Mutators** fuzz items that include blobs, numbers, strings, data sizes, character types, and arrays.
- **Analyzers** produce full or partial Peach data models from binary data, regular expressions, XML files, and zip archives. ASN.1 is a new analyzer.
- **Fixups** compensate for fuzzing variations to data by recalculating items such as checksums, hashes, and sequencing adjustments.
- **Transformers** encrypt and decrypt data using algorithms such as AES, Base64, HTML, and MD5.
- **Publishers** perform input/output (I/O) operations and include interfaces such as Raw Ethernet, IPv4, Serial, TCP, WebService, WebSocket, and Zip.
- **Monitors** watch for faults, memory usage, and attach debugger. Monitors include Android, Linux debugger, Windows debugger, SSH, Ping, Serial, and Socket.
- **Data types** provide atomic and container elements such as Number, String, Stream, and Block.

State Modeling

- **Gödel state-aware extensions** (patent pending) allow fuzzing of the state model that includes testing state transitions, both valid and invalid.
- **Gödel state-aware extensions** permit fuzzing on a condition, a test iteration, or a test session.
- **Mutation scope** is defined for state model coverage.

Logging

- Logging can now use **SQLite databases** to collect metrics.

Optimizing Test Efforts

The test effort over a project is a major endeavor. Peach Premier includes the following components to help keep the effort both efficient and effective:

- Predefined fuzzing definitions called Peach Pits, available as individual Pits or groups of related Pits called Pit Packs. Apart from setup for the test environment, the predefined Pits are ready "out of the box."
- Test passes can weight mutators to perform more test cases using those mutators with higher weights. Typically these have more variations and expose more vulnerabilities.
- Minset helps pare down the file count for test case coverage.

Extensibility

Peach Premier is designed for extensibility, and can expand with your fuzzing demands. The following areas are designed to extend Peach for your testing needs—today and tomorrow.

- **Python script support** provides an extension portal for fuzzing.
- **Custom Peach Agents** can be written in C, C++, C#, and Python
- **SDK** includes API documentation and extended examples
- **Custom Fixups, Mutators, Transformers**

Contact Us

Peach Fuzzer, LLC, is a leader in application security, embedded security, and security fuzz testing, having provided the *Peach Professional and Peach Enterprise* to some of the largest organizations in the world.

Visit our website
Peachfuzzer.com

Talk to a representative
Call toll free 1 (844) 55-PEACH

Email us
sales@peachfuzzer.com