Peach Fuzzer Monitors

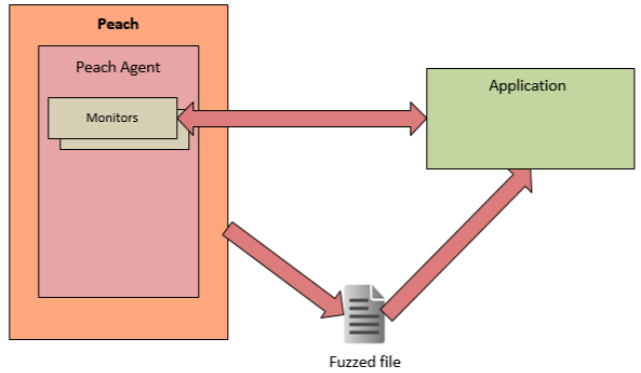
Peach Fuzzer has powerful monitoring capabilities that allow you to:

- Detect faults in the test target
- Collect detailed data about faults
- Automate the test environment

Peach's comprehensive user guide provides detailed monitor recipes

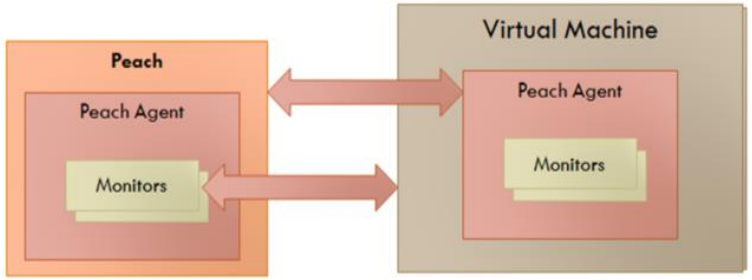
Peach Fuzzer Monitoring: File Fuzzing

- Three major steps performed by Peach
  1. Tells a file consumer to open and access data from malformed files
  2. Monitors file consumer for faults in application and captures fault data
  3. Restarts application after fault
- Simple monitoring setup
  - Window's Debugger monitor provides fault detection, data collection, and automation
  - PageHeap monitor enhances chances of finding faults



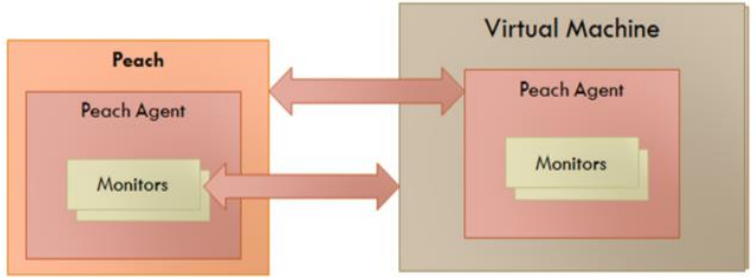
Peach Fuzzer Monitoring: Linux Network Service Client

- Three major steps performed by Peach:
  1. Initiates a network client that sends request to server
  2. Impersonates the server, sending back fuzzed data
  3. Monitors for faults in the client and captures fault data
- Simple monitoring setup
  - Within local agents residing in Peach
    - VMWare monitor watches and restarts the VM environment upon fault
    - NetworkCapture monitor captures network packets that cause faults
  - Within agents running on remote machine
    - GDB monitors for faults Linux service client
    - Save File monitor forwards log files after fault



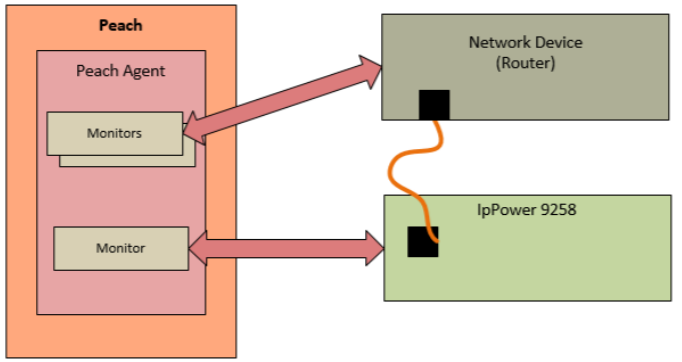
Peach Fuzzer Monitoring: Linux Network Service

- Four major steps performed by Peach:
  1. Initiates a network service on a VM
  2. Sends fuzzed data to this server
  3. Monitors for faults in the server and captures fault data
  4. Restarts service upon fault
- Simple monitoring setup
  - Within local agents residing in Peach
    - VMWare monitor watches and restarts the VM environment upon fault
    - NetworkCapture monitor captures network packets that cause faults
  - Within agents running on virtual machine
    - GDB monitor starts the Linux service and monitors for faults
    - Save File monitor forwards log files after fault



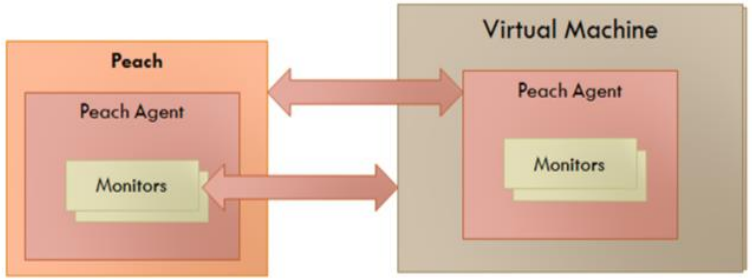
Peach Fuzzer Monitoring: Network Device

- Four major steps performed by Peach:
  1. Power-up device using programmable power supply
  2. Sends fuzzed data to device
  3. Monitors for faults in the device and captures fault data
  4. Power-cycles device upon fault
- Simple monitoring setup
  - Within local agents residing in Peach
    - IpPower9258 monitor power-cycles device
    - SerialPort monitor ensures device has properly and completely power-cycled and provides fault detection
    - TcpPort monitor identifies faults by checking the state of the TCP port on the target
    - NetworkCapture monitor captures network packets that cause faults



Peach Fuzzer Monitoring: Windows Network Service Client

- Three major steps performed by Peach:
  1. Initiates a network client that sends request to server
  2. Impersonates the server, sending back fuzzed data
  3. Monitors for faults in the client and captures fault data
- Simple monitoring setup
  - Within local agents residing in Peach
    - VMWare monitor watches and restarts the VM environment upon fault
    - NetworkCapture monitor captures network packets that cause faults
  - Within agents running on remote machine
    - WindowsDebugger monitor launches client service and detects faults in client
    - PageHeap monitor enhances chances of finding faults



Peach Fuzzer Monitoring: Windows Network Service

- Four major steps performed by Peach:
  1. Initiates a network service on a VM
  2. Sends fuzzed data to this server
  3. Monitors for faults in the server and captures fault data
  4. Restarts service upon fault
- Simple monitoring setup
  - Within local agents residing in Peach
    - VMWare monitor watches and restarts the VM environment upon fault
    - NetworkCapture monitor captures network packets that cause faults
  - Within agents running on virtual machine
    - WindowsDebugger monitor detects faults in service
    - PageHeap monitor enhances chances of finding faults
    - WindowsService monitor restarts service upon fault