Open Source Incident Response

Linux Security Summit 2015

Summary

- What is GRR?
- GRR Features & Use Cases
- GRR Architecture & Operations
- Install & Operational Demo
- Additional Configuration & Modification
- Contribute!

What is GRR?

- State Capture Based Live Response Platform
- Open Source (Python)
- Cross-Platform
- Scalable
- Scriptable
- Client/Server Model

GRR Features

- Knowledge Base Collection
- Forensic Artifact Collection
- File Acquisition
- File/Registry Search
- Live Remote Memory Analysis
- Network Connections & Information

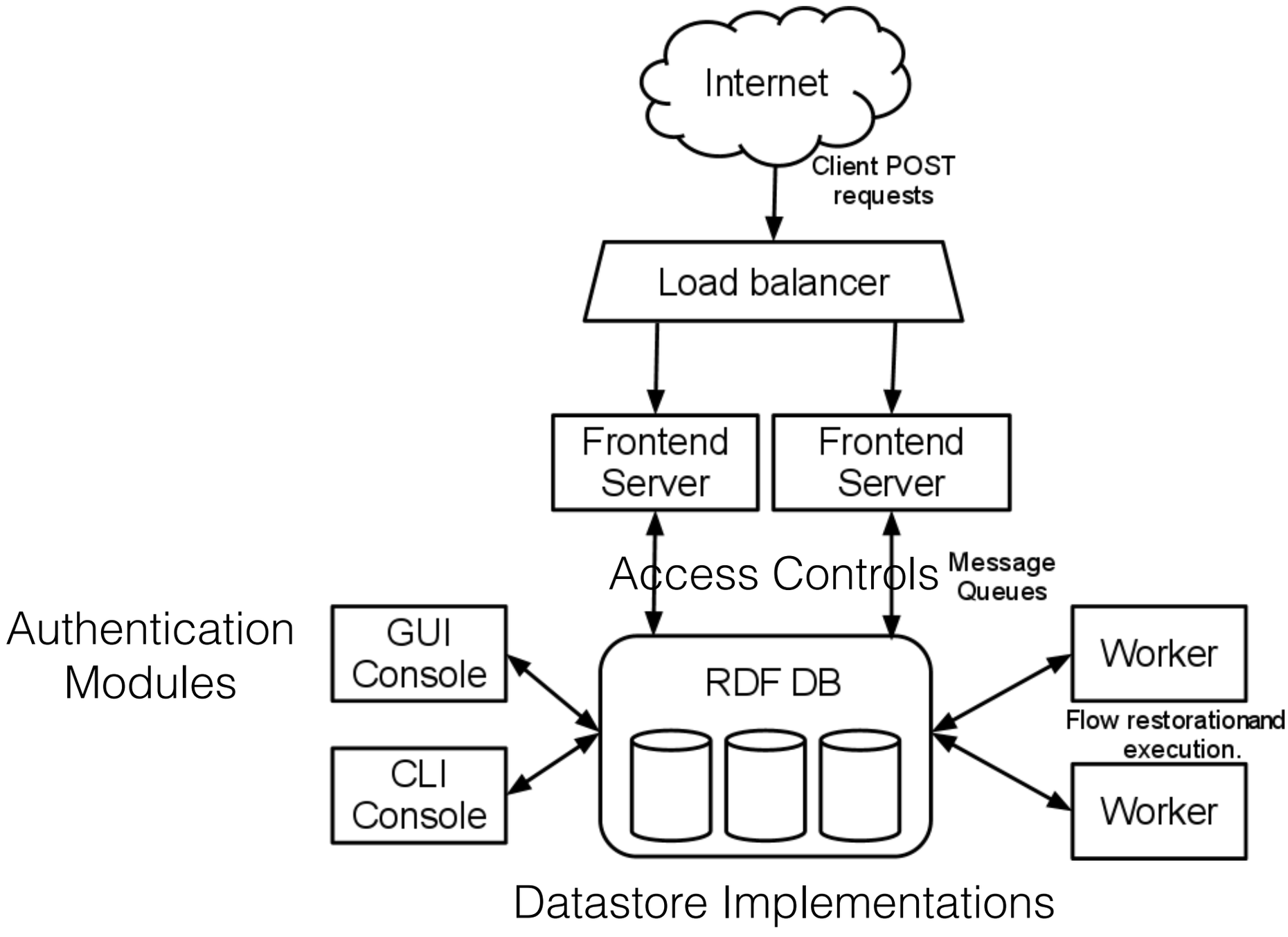
GRR
RAPID RESPONSE

GRR Use Cases

- Proactive detection
- Gather forensic evidence
- Scope compromise across fleet

GRR
RAPID RESPONSE

GRR Architecture



GRR
RAPID RESPONSE

GRR Operations

- Flow – The unit of work for GRR. Flows can call a sequence of client actions, processes results, perform server maintenance, or reporting tasks. Flows are written in python and stored on the server.

- Hunts – Mechanism for running a Flow across a fleet of clients. When a client checks it will be evaluated against the criteria of the Hunt. Scheduling is determined by rules, client rate, client limit, and hunt expiration.

- Artifact – Yaml defined “point of interest” for forensic collection.

GRR
RAPID RESPONSE

Demo Time!

GRR
RAPID RESPONSE

Additional Options

- Authentication Modules
- Access Controls
- Run as Non-root User
- Stats Store
- Datastore Tuning
- Load NSRL

GRR
RAPID RESPONSE

Common Modifications

- Authentication Modules
- Access Controls
- Parsers
- Datastores
- Flows
- Client Actions

GRR
RAPID RESPONSE

Contribute

- GRR - https://github.com/google/grr
- Rekall - https://github.com/google/rekall
- Rekall Profiles - https://github.com/google/rekall-profiles
- Artifacts - https://github.com/ForensicArtifacts/artifacts
- Google Groups - GRR Users/Developers

Summary

- What is GRR?
- GRR Features & Use Cases
- GRR Architecture & Operations
- Install & Operational Demo
- Additional Configuration & Modification
- Contribute!

Q&A

Sean Gillespie
@pidydx