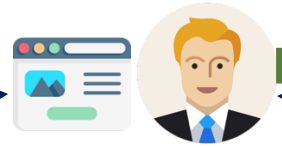
PacketScope

eBPF based general-purpose analysis and debugging tool for protocol stacks

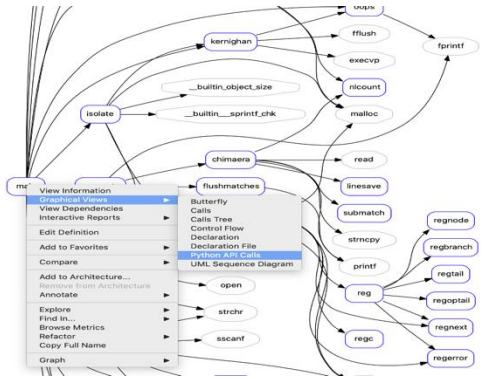
IETF 123 hackathon

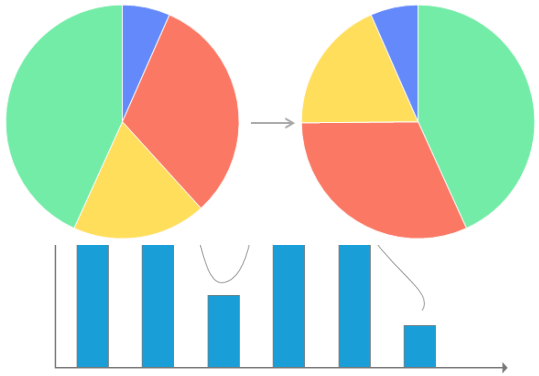
PacketScope: See Every Packet, Secure Every Host

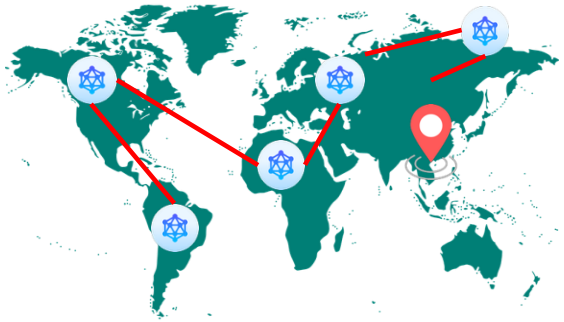


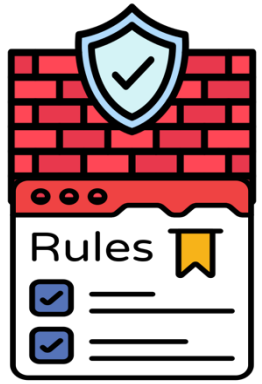
User Interface

In-depth Analysis of Packet Interaction	Flexible Packet Information Statistics	Global Tracking with Latency Markers	Kernel-Level Malicious Packet Filtering



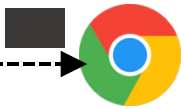






TCP/IP stack

IP → **Tracer** → **Analyzer** → **Locator** → **Guarder**



Tracer	Analyzer	Locator	Guarder
Trace the interaction of connections/packets within the protocol stack and generate detailed visual path diagrams	Multi-dimensional statistics on packet data flow within the protocol stack	Mapping and displaying the path and latency from the host to any IP address.	Filtering and control of abnormal packets, providing contextual information based on LLM.

Based on eBPF technology as the underlying support, develop four functional modules and provide good user interfaces for integration to achieve overall protocol stack security analysis capabilities.

Tracer: Packet Interaction Analysis and Visualization

- **Connection/Socket Identification:**

  Identify active sockets on the host and show their information at the connection level

- **Deep Packet Tracing**:
  - Use eBPF to capture packets at the kernel level and trace their path through the TCP/IP stack.
  - Support for **IP, TCP, UDP, ICMP**, and other common protocols.
  - Track packet flow across layers (e.g., from the network interface to the application layer).

- **Visualization**:
  - **Time-axis view**: Show packet flow over time, highlighting delays, retransmissions, and out-of-order packets.
  - **Topology view**: Map packet paths across network stack and protocol layers.
  - **Interactive interface**: Allow users to click on packets to view details.

Analyzer: Flexible and Customizable Packet Statistics

- **Multi-dimensional Metrics:**
  - ✓ Packet counts: Track the number of packets processed at each layer.
  - ✓ Latency analysis: Measure delays between layers (e.g., NIC to IP layer, TCP to application layer).
  - ✓ Cross-layer interactions: Analyze how often packets move between layers (e.g., IP to TCP).
  - ✓ Loss and retransmission rates: Identify packet drops and retransmissions.

- **Customizable Dashboards:**
  - ✓ Allow users to define custom metrics and visualizations based on their specific needs.
  - ✓ Export statistics in formats like CSV, JSON, or PDF for further analysis.

Locator: Internet Path Analysis and Visualization

- **Internet Path Identify:**
  - ✓ Trace the path from PacketScope to the specified destination, showing the complete route with each hop. This helps identify network bottlenecks and potential failure points.
  - ✓ Display the AS set label for each hop, showing which AS the packet traverses. This provides insight into the inter-domain traffic flow and routing mechanisms.

- **Latency Label on Each Hop:**
  - ✓ Show latency data for each hop, indicating the time taken between routers. This helps pinpoint high-latency areas for optimization.

- **Show on World Map:**
  - ✓ Visualize the entire path on a world map, with each hop marked geographically. This enhances the understanding of global routing and traffic flow patterns.

Guarder: Kernel-level Malicious Packet Detection and Filtering

- **Threat Detection:**
  - ✓ Detect off-path attacks, spoofed packets, malicious injections, and other threats.
  - ✓ Use LLM to provide contextual threat information (e.g., attack type, severity, recommended actions).

- **Realtime Filter Rule Engine:**
  - ✓ Intercept and block the detected malicious packets based on predefined or custom rules.
  - ✓ Support custom rules for different network environments (e.g., data centers, IoT networks).
  - ✓ Use LLM to generate filter rules for identified threat.

Thank You!

Fork us on GitHub： Internet-Architecture-and-Security/PacketScope: A general-purpose protocol stack analysis and debugging tool based on eBPF

PRs Welcome!