

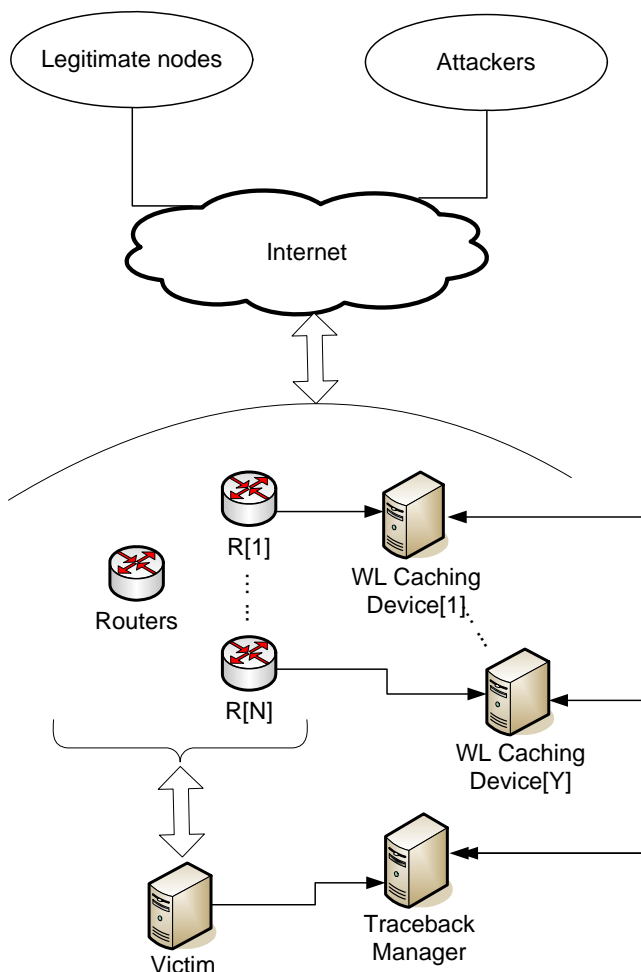
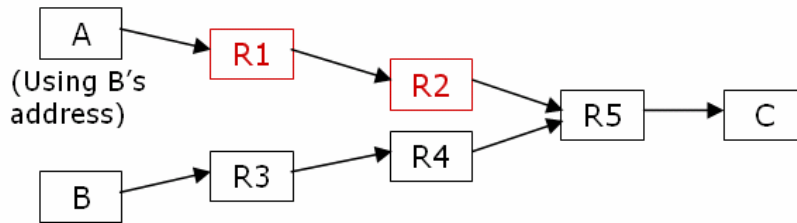


Problem: Locate ingress point nearest to the attackers

- Attackers often use spoofed source addresses to hide identity and location
- Existing techniques require changes to Internet routers making deployment difficult

Idea: Collect traffic flow information to detect route anomalies

- Internet traffic follows designated paths based on routing information
- E.g. Traffic from Node B to C traverses R3 -> R4 -> R5 while Node A (spoofing B's address) to C traverses through R1 -> R2 -> R5
- By detecting route anomalies, ingress point closest to the attacker could be located



Traceback Method

- R[1...N]: Routers sample incoming traffic and send them at regular intervals to White List Caching Devices for learning legitimate routes for src-dest pairs
- White List (WL) Caching Device[1...Y]: Nodes which receive sampled traffic flow information from Routers and perform white list generation and updates
- Traceback Manager: Queries for information from WL caching devices for analysis and generates attack graph, when triggered by victim's network during an attack

Results

- Achieved faster traceback
- Does not require changes to be made to Internet routers, therefore non-intrusive
- Allow traceback in the event of attacks with seemingly legitimate traffic contents