Denial-of-Service (DoS) attack has become an increasing threat to the reliability of the Internet. One can prevent DoS attacks by blocking attack traffic with filters or authorizing desired traffic with capabilities, but both are complicated by source spoofing: filters may block legitimate sources, and capability requests are subject to Denial-of-Capability attacks. Existing source authentication mechanisms either rely on transitive trust (ingress filtering and path identifiers), or have high computational and header overhead (digital signatures).

Our Approach to Combat DoS
- As a first step, we design Passport, a network architecture that prevents source spoofing. We then design various DoS defense systems with Passport, including a filter-based and capability-based DoS defense system.

### How Passport Works

**Secure Filtering**

\[ MAC_2 = MAC_{K_{AS_1 AS_2 AS_3}}(src, dst, len, IPID, payload[0:7]) \]

\[ MAC_3 = MAC_{K_{AS_1 AS_2 AS_3}}(src, dst, len, IPID, payload[0:7], AS_1) \]

**Per-Network Fairness to Mitigate Denial-of-Capability Attacks**

\[ d_x = g^{e_x} \mod p \quad d_y = g^{e_y} \mod p \]

\[ K(X, Y) = d_x^{e_y} \mod p = d_y^{e_x} \mod p \]

**Passport: Secure Source Authentication**

- **Effective**
  - Prevents source spoofing without relying on transitive trust
  - Eliminate reflector attacks
- **Secure and light-weighted**
  - Resilient to a wide range of attacks
  - High throughput on routers
- **Incrementally deployable**
- **Incentive compatible**
  - Provide immediate security benefit for early adopters

**Approach and Impact**

<table>
<thead>
<tr>
<th>New Approach</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source authentication with efficient symmetric key cryptography</td>
<td>Passport, a powerful building block for combating DoS attacks</td>
</tr>
<tr>
<td>Key distribution within the inter-domain routing system</td>
<td>StopIt, a filtering system that can prevent DoS attacks from multimillion-node botnets</td>
</tr>
<tr>
<td>Secure filtering protocols resilient to a wide range of attacks</td>
<td>Protects the request channel of capability-based systems</td>
</tr>
</tbody>
</table>

**NSF Cyber Trust Principal Investigators Meeting**

March 16-18, 2008
New Haven, CT