Detecting Network Denial of Service

Carla Brodley
Clay Shields
Karthik Jaganathan

Problem

- No effective mechanism exists to detect a denial–of–service attack
- Most attacks detected only after investigation of network performance problems
- Even then, the type of attack must be identified to determine the appropriate response

Project Goals

- To develop effective detection techniques for network denial of service
- Support understanding of denial of service
- To determine bottlenecks in the network
- Provide information for traceback of attacks
- Provide statistics for effective filtering

Setup and signature development

- **Implement a network test bed – *Done***
- **Collect and evaluate DoS tools – *In progress***
- **Develop signatures for each attack**

Data collection and anomaly detection

- **Collect traces of normal and attack traffic – *In progress***
- **Train machine learning algorithms to recognize attacks**
- **Evaluate and improve the algorithms**

Bottleneck determination

- **Routers**
- **End hosts**
- **Medium access**

Support for filtering

- **Rate limiting can limit effectiveness of attacks**
- **Need to find out “normal” traffic patterns**
- **Once attack is detected and identified, appropriate filter can be installed to stop attack**

Concerns

- Getting access to good training data
- Production network data required for “normal data
  - User privacy concerns
  - Cannot perform attacks against production equipment
- Test−bed used for DoS network traces

Related Documents

- **http://www.cs.purdue.edu/homes/jk/dos.html**