

How to Test DoS Defenses:

Towards Scientific Methodologies for Testing Cyber Defense Technologies

Dr. Jelena Mirkovic



Prof. Sonia Fahmy



Prof. Peter Reiher



Dr. Roshan K. Thomas



Outline

- The problem of DoS testing
- Evaluating and testing DoS defenses
- Benchmarks and metrics
- Conclusions and next steps

The Problem of Testing DDoS Defenses



■ Problem and Need

- (D)DoS continues to be an important and dynamic problem
- More of an art than science
- Wrong conclusions emerge from wrong testing

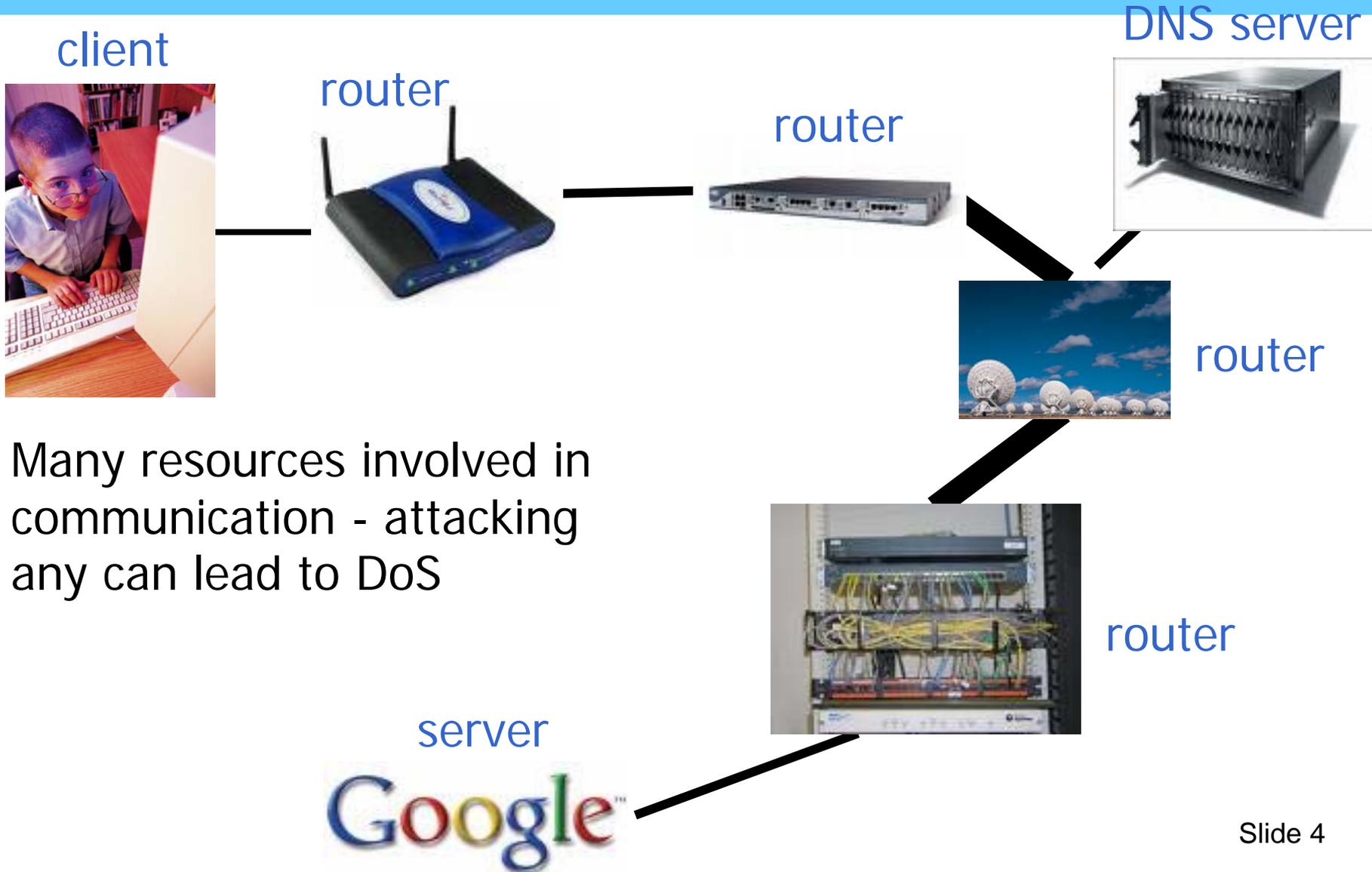
■ Our Work and Approach

- DHS-sponsored work on DoS benchmarks and metrics
- Integrated with the DETER testbed
- **User-perceptible** measures of quality of service
- Recommendations for better testing strategies

■ Benefits

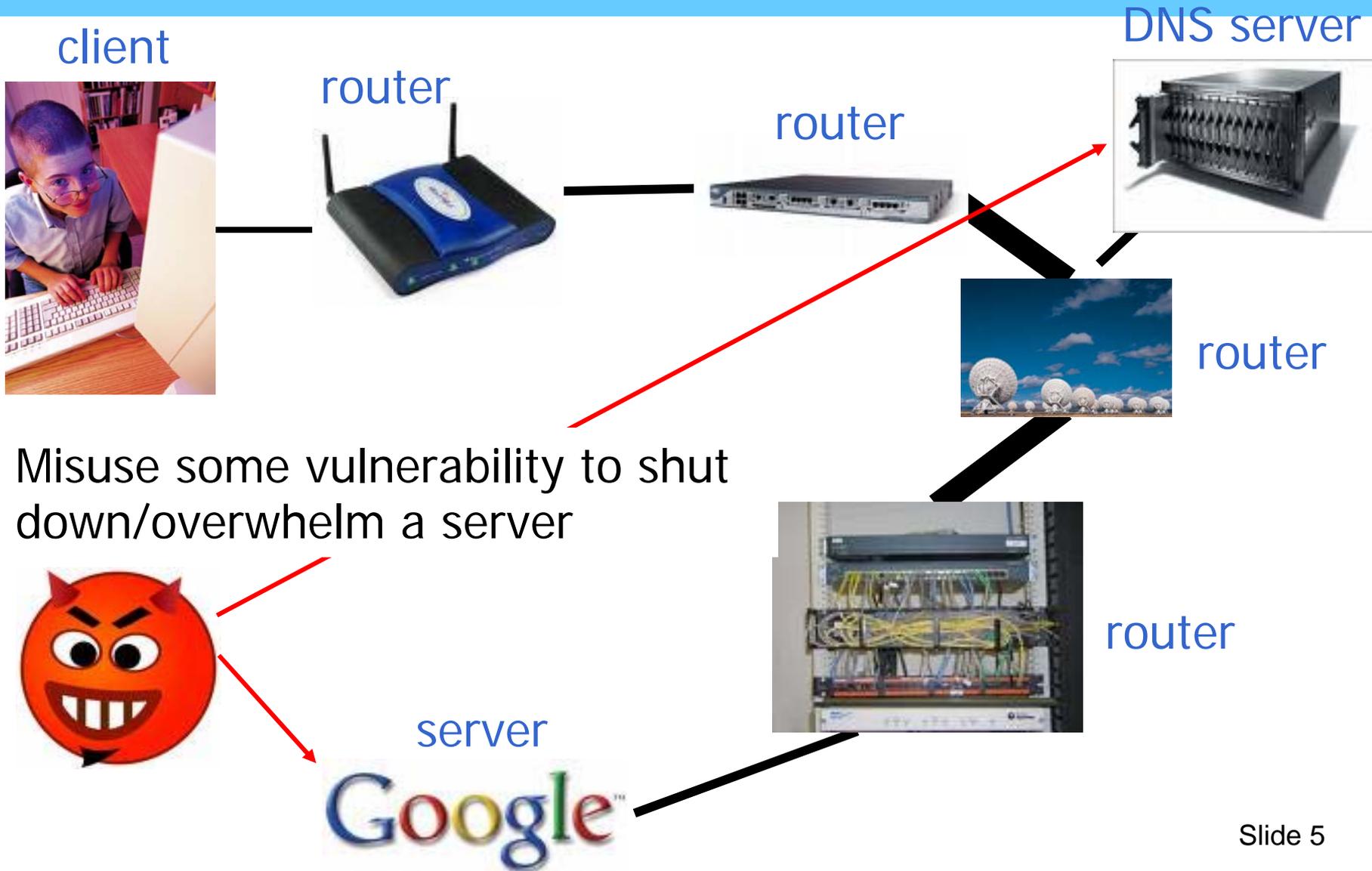
- **Enable standardized, realistic and systematic testing**
- Faster and more efficient stress-testing of networks
- More sound science and faster progress !

Denial-of-Service

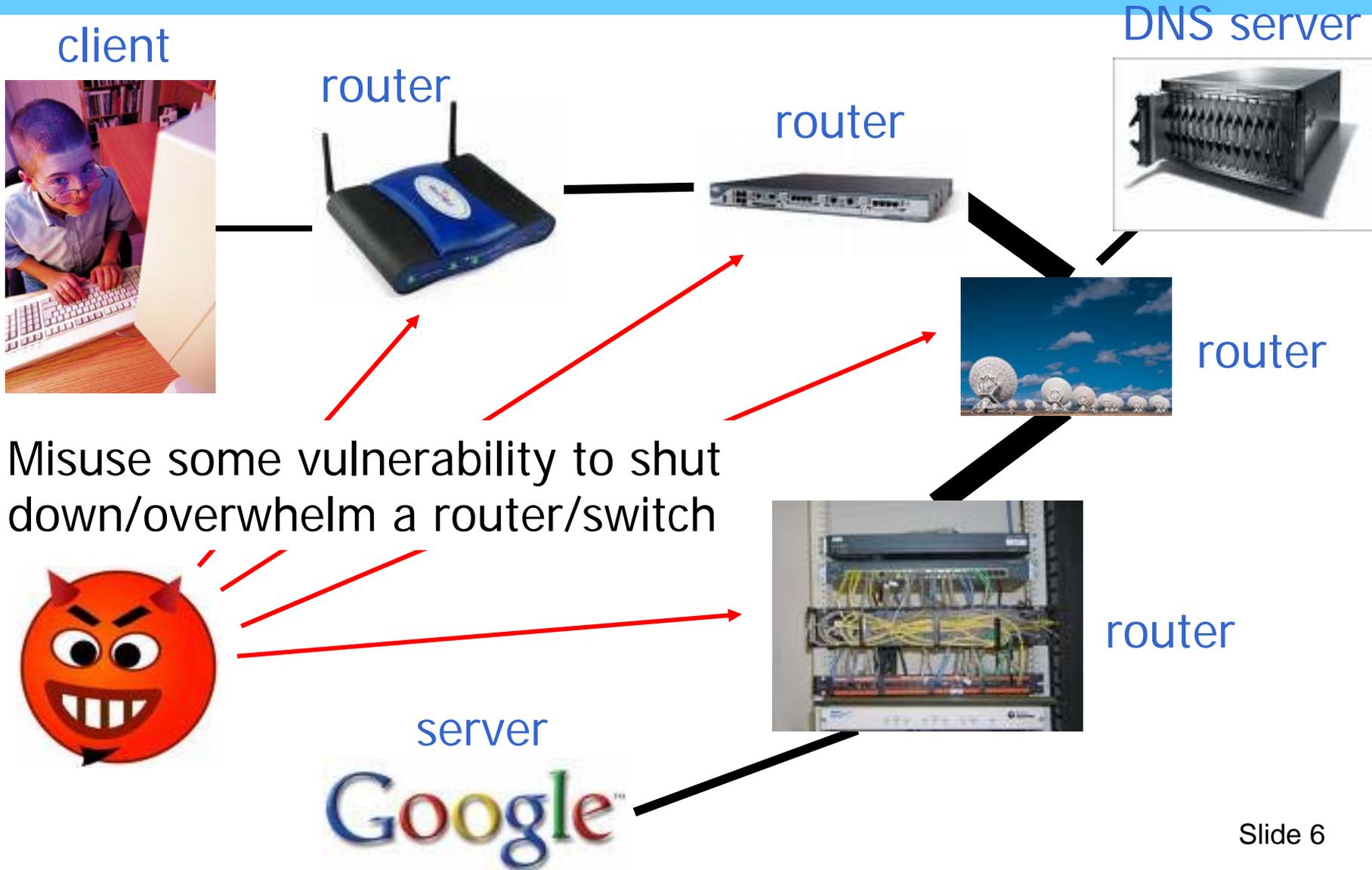


Many resources involved in communication - attacking any can lead to DoS

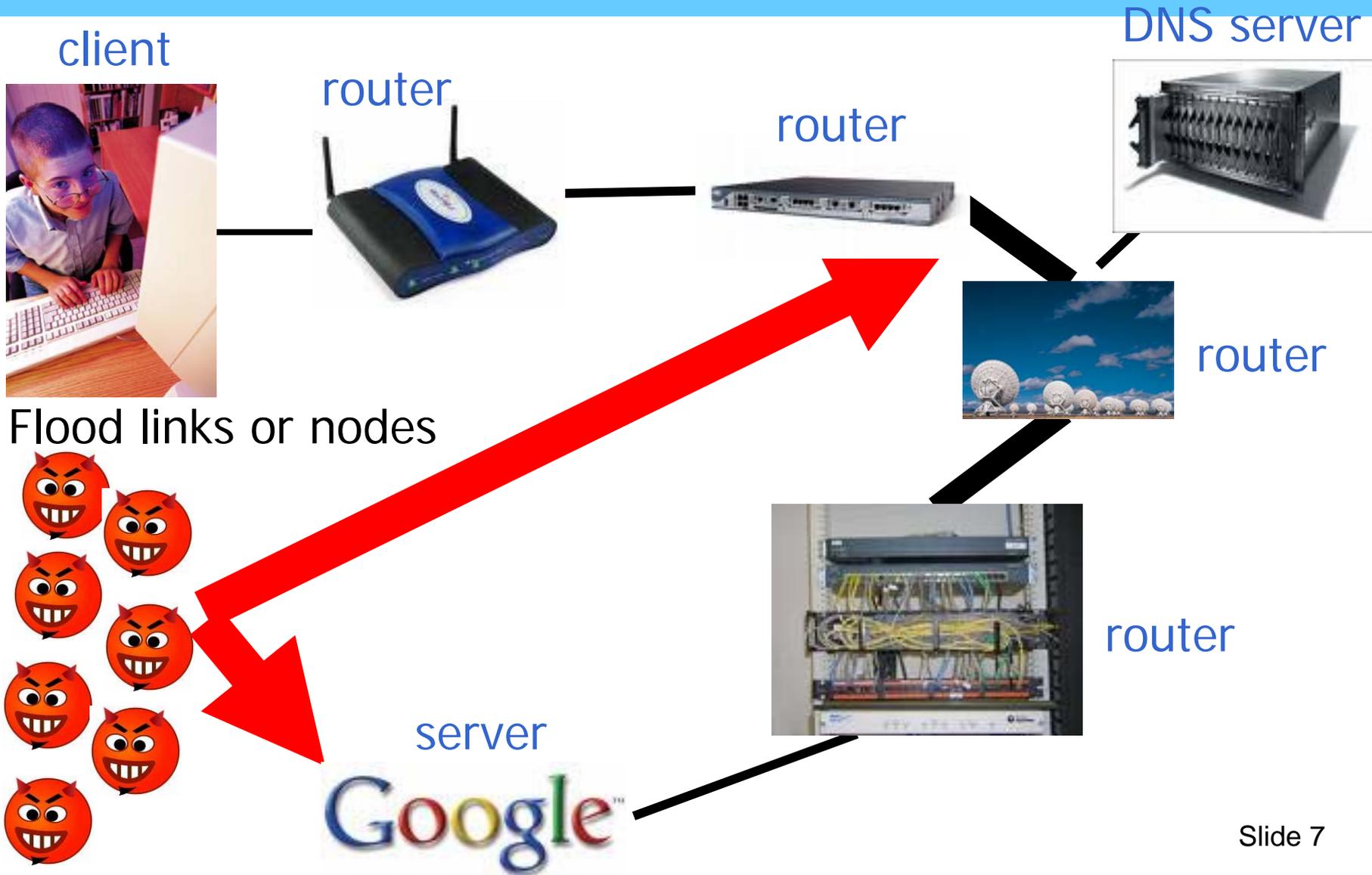
Denial-of-Service



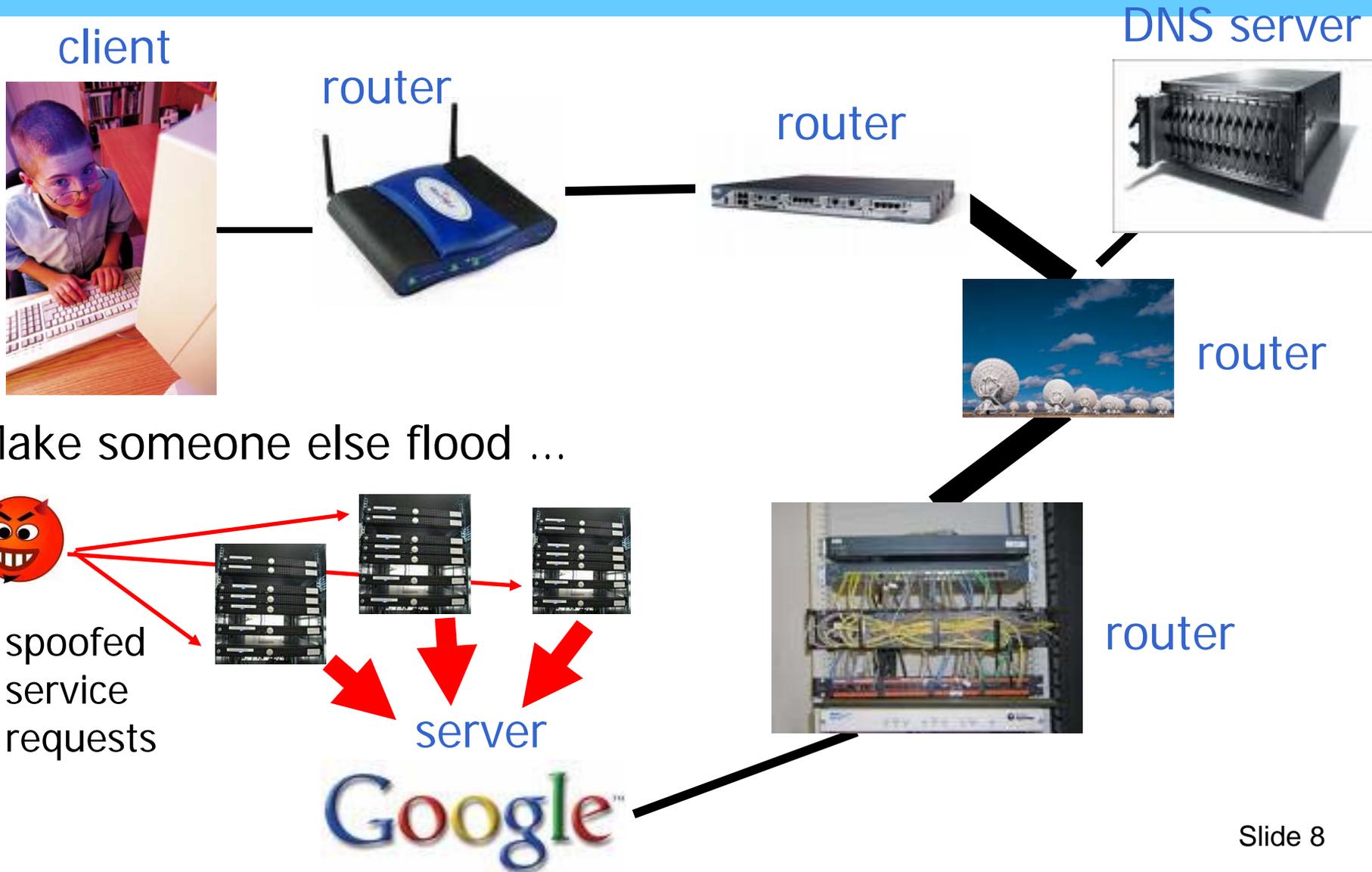
Denial-of-Service



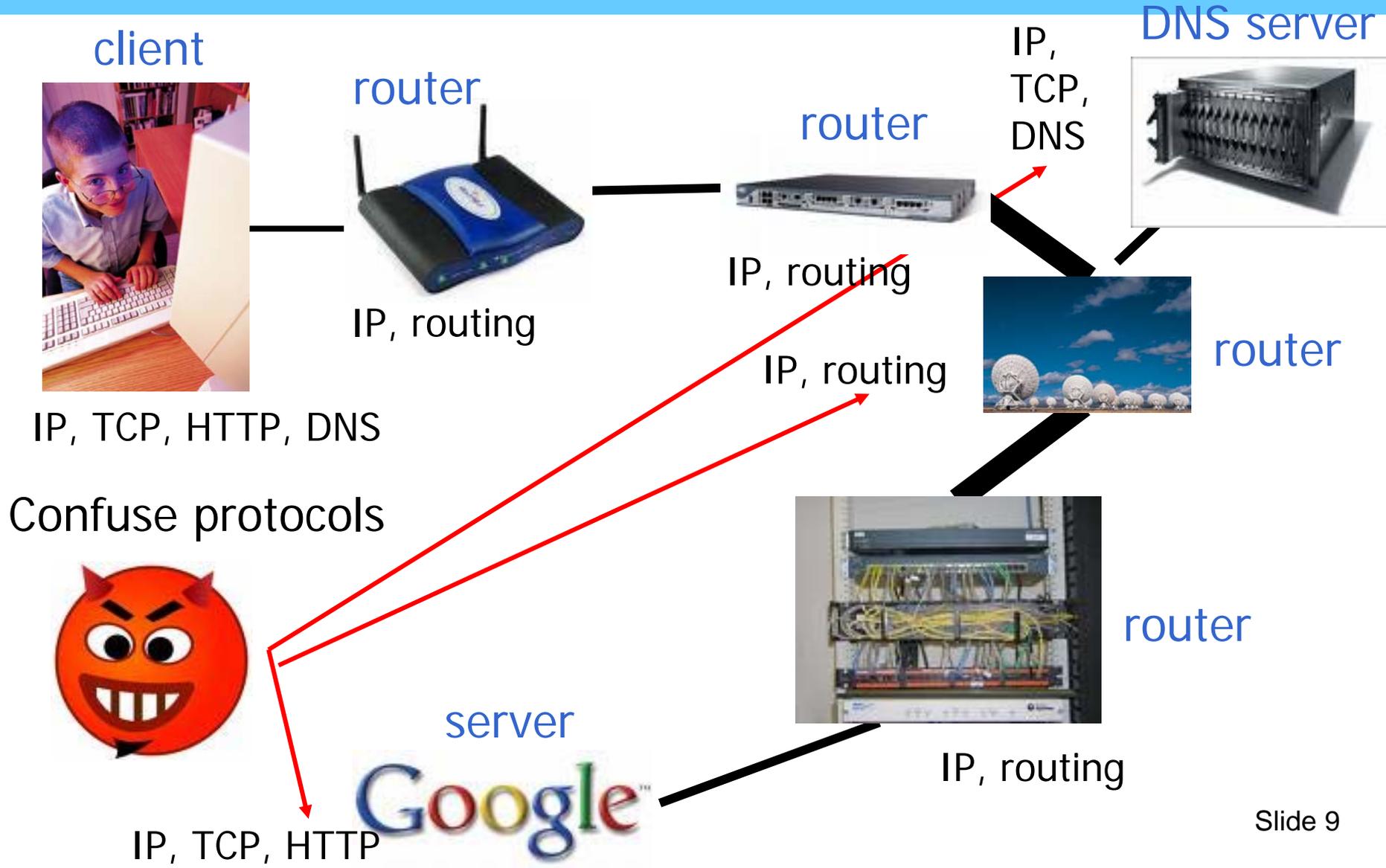
Denial-of-Service



Denial-of-Service



Denial-of-Service



Outline

- The problem of DoS testing
- ➔ ■ Evaluating and testing DoS defenses
- Benchmarks and metrics
- Conclusions and next steps

Evaluation Goals

- Assess effectiveness (does the defense work?)
- Assess collateral damage to legitimate traffic
- Time taken to minimize attack effect
- What are the memory and CPU costs (operational)
- Can it work in partial deployment?
- How scalable is a defense?
- How resilient is it to attacks?

**These goals apply broadly to
any set of cyber defense technologies**

Evaluation Components

- Testing approach
 - Theory, simulation, emulation or deployment
- Test scenarios
 - Legitimate and attack traffic, topology, events of interest
- Success metrics
 - Prove that a defense works
 - We cannot assess what we cannot measure

Evaluation Components: Approaches to Testing



■ Theory

- Good alternate when existing models work (e.g. M/M/1 queues, state diagrams, probabilistic models etc.)
- Poor choice for effectiveness evaluation

■ Simulation

- Most packages have simple router models (e.g. NS-2)
- Difficult to set values in hardware models (OPNET, OMNet ++)
- Abstractions in simulators and emulators greatly change test outcomes when compared with real hardware
- Some may overestimate attack impact (simple buffering), some may underestimate it (ignore packet handling overhead)

Evaluation Components: Approaches to Testing..2



■ Emulation

- Testing in a mini-network, e.g. testbed
- Emulab, DETER, Planetlab (SOS), own lab (TVA)
- Advantages over simulation (real OS, applications, hardware, real routers, live traffic and attacks)
- Challenges: lack of hardware diversity, lengthy setup, difficulty in internal diagnosing failures)

■ Deployment

- Most realistic but difficult to reproduce
- Cannot control events and discover ground truth
- Hard to argue tests are representative
- Not a possibility for many researchers

Evaluation Components: Which Testing Strategy to Use?



- Emulation
 - Amenable to experimentation and repeatable
 - Must be set up carefully
- Robustness and scalability
 - Theory may be a good choice
- Simulation
 - Approach with caution - often misleading
- Deployment
 - Does not enable controlled testing

Test Scenarios - Legitimate Traffic

- DoS leads to lack of resources and traffic drops
- Vulnerability to DoS is influenced by the following features of legitimate traffic:
 - Packet sizes (smaller is better)
 - Transport protocol mix (TCP is most sensitive)
 - RTT values (large values more sensitive)
 - TCP connection dynamics and application mix
 - TCP connection arrivals
 - IP address diversity and turnover

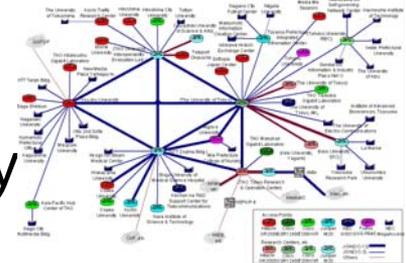
Test Scenarios - Attack Traffic

- Defenses must be stress-tested based on the technique(s) employed:
 - Path isolation - filter/fair share among paths
 - Resource accounting - per source or per destination
 - Privileged customer - issue passes to good old customers
 - Behavior learning - learn how legitimate clients behave
 - Resource multiplication - more resources on demand
 - Legitimate traffic inflation - ask leg. clients to send more
 - Collaborative defenses test for insider attacks

Evaluation Components:

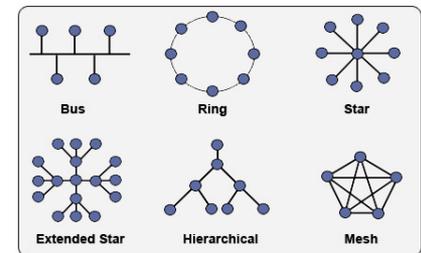
Test Scenarios - Topologies

- Topology is not critical for single-point defenses
 - But IP and traffic diversity still do
- Other defenses need realistic topologies
 - ISP topology, full or in part - realistic but only representative of ISP topologies
 - Downscaled ISP topology - need good argument that scaling down does not impact fidelity



- Best approach

- Understand what topological features influence tests
- Vary tests in realistic ranges to explore solution space



Limitations in State of the Art Metrics

- DoS is a subjective phenomenon
 - Human users perceive reduction in QoS
 - How to measure impact of any attack and defense?
- Limitations of state of the art metrics
 - **Loss** - congestion-responsive traffic and congestion-producing attacks; some packets more important
 - **Throughput/goodput** - congestion responsive traffic
 - **Request/response delay** - interactive and two-way traffic
 - **Transaction duration** - congestion-responsive traffic
 - **Allocation of resources** - flooding and exhaustion attacks

But these do not measure user-perceptible degradations in quality-of-service

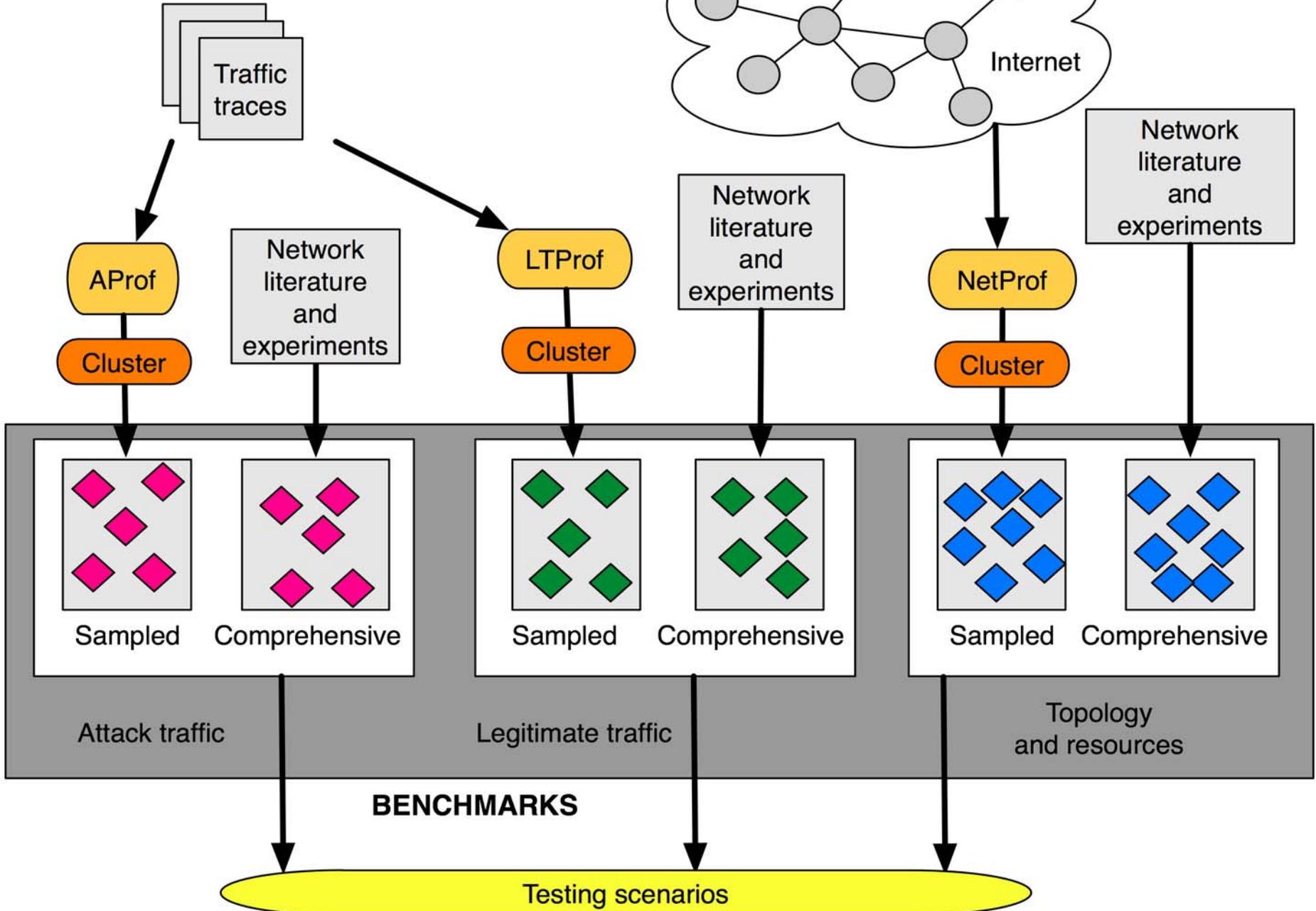
Outline

- The problem of DoS testing
- Evaluating and testing DoS defenses
- ➔ ■ Benchmarks and metrics
- Conclusions and next steps

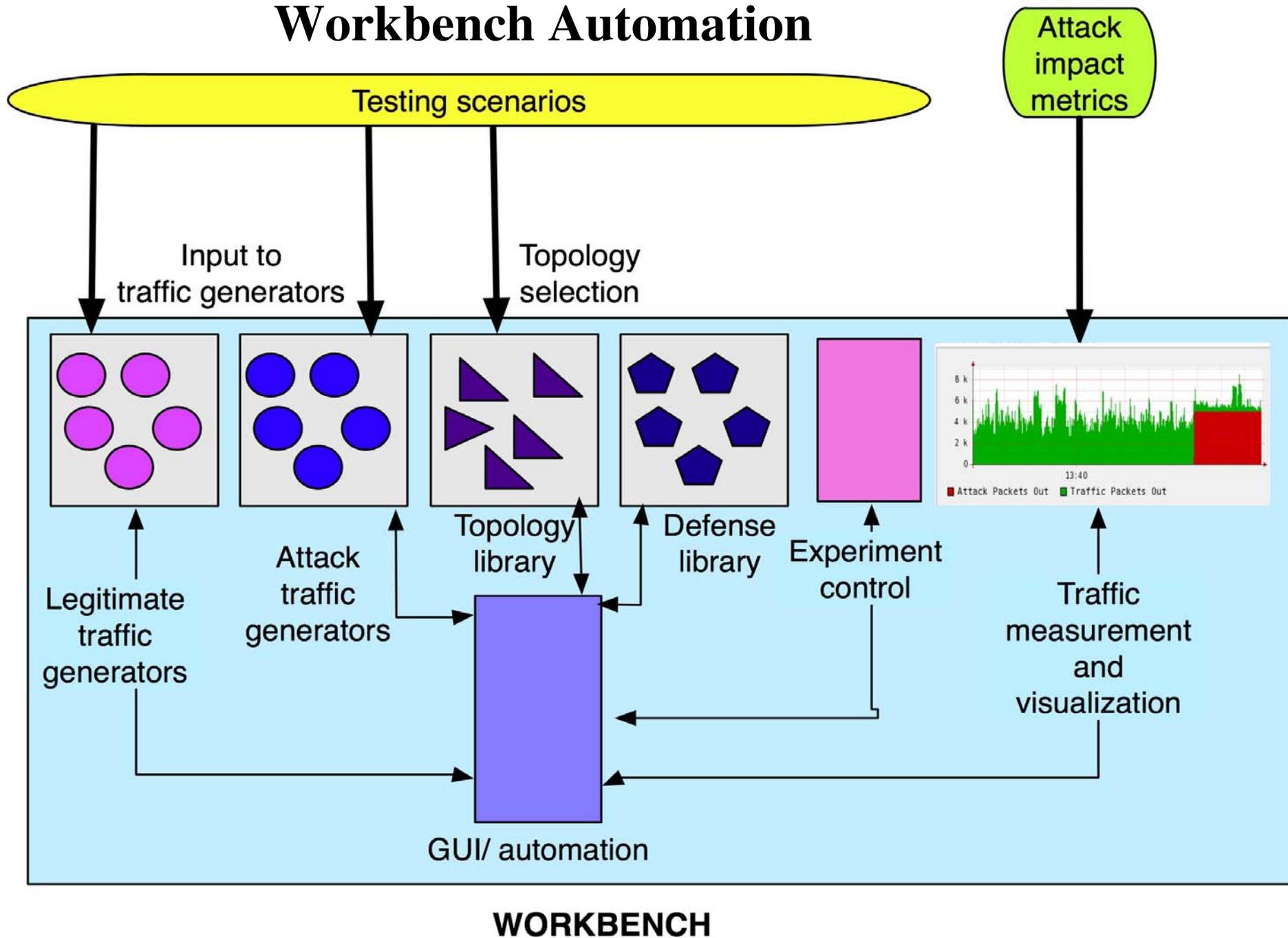
Our Work on DDoS Benchmarks

- DHS-funded work to develop a benchmarking and evaluation framework for DoS
- Built a number of tool suites for defense testing
- Use of realistic traffic traces and Internet topologies
- Comprehensive
 - Understand what matters and how to vary those features
- Focus on usability and technology transfer
 - Integrate with DETER testbed and SEER graphical tool for experiment control

Developing Benchmarks



Workbench Automation



WORKBENCH

DoS Attack Categories

■ Packet floods

- Exhaust some key resource (memory, CPU, bw)

■ Unexpected header values

■ Invalid app inputs

■ Invalid fragments

■ Large packets

■ Congestion control exploits

- Pulsing attacks

■ Impersonation attacks

- Use spoofing to blackhole or kill traffic

Crash some device
OS or application
because the input is
unexpected

DoS Attack Types

Attack type	DoS Mechanism
UDP/ICMP/TCP data packet flood	Large packets consume bandwidth, small packets consume CPU
TCP SYN flood	Consume end host's connection table
HTTP flood	Consume Web server's resources
DNS flood	Consume DNS server's resources
Random fragment flood	Consume end host's fragment table
TCP ECE flood	Invoke congestion control response
ICMP source quench flood	Invoke congestion control response

DoS Attack Feature Variations

Feature	Variation
Attack rate	Low, moderate and severe. Increase rate until the defense fails to handle it.
Attack dynamics	Continuous vs pulsing. Synchronous vs interleaved senders.
Legitimate traffic rate	5%, 30% and 90% of capacity
Path sharing	Uniform vs log-normal attacker distribution, uniform distribution of legitimate clients.
TCP traffic mix	Various mixes of data transfers, telnet-like communications and request/response exchanges.
Application traffic mix	Several applications are mixed to explore application isolation or cross effects

Scenario Feature Variations

Defense	Feature	Variation
Path isolation and res.multi.	Path sharing	Uniform vs log-normal attacker distribution, constant vs pulsing and interleaved attackers
Privileged customer	Access pattern	Distributed, small rate attack. Attacker behaves well prior to attack
Traffic baselining	Legitimate traffic pattern	Randomized attack. Distributed, small rate attack. Slow-growing attack.
Traffic inflation	Resource distribution	Vary client bandwidth
All	Attacker distrib.	Vary number of attackers.
All	Attacker dyn.	Engage new attackers, retire old ones
All	Leg. client dyn.	Engage new clients, retire old ones

Our Work on DoS Metrics

- DHS-funded work
- Wanted to capture human perception of QoS
- Observe and model traffic as set of **transactions** - tasks meaningful to users
 - Application-specific criteria for transaction success/failure
 - Map this into objective, traffic-related measurements
 - Allow multiple criteria transactions
 - Measure client-side perspective
 - Work with tcpdump traces to infer transactions
- **Full table with success criteria in paper**
 - Chat, ftp, email, RTS games, videophone

Our Work on DoS Metrics

- Percentage of failed transactions (pft)
- DoS-hist
 - A histogram of pft measures across applications
- DoS-level
 - Weighted average of the pft
- QoS
 - How good is QoS of successful transactions when compared to thresholds $(0,1]$

Metrics ...2

■ QoS-degrade

- How much worse is QoS of failed transactions when compared to thresholds $[0, +\infty)$

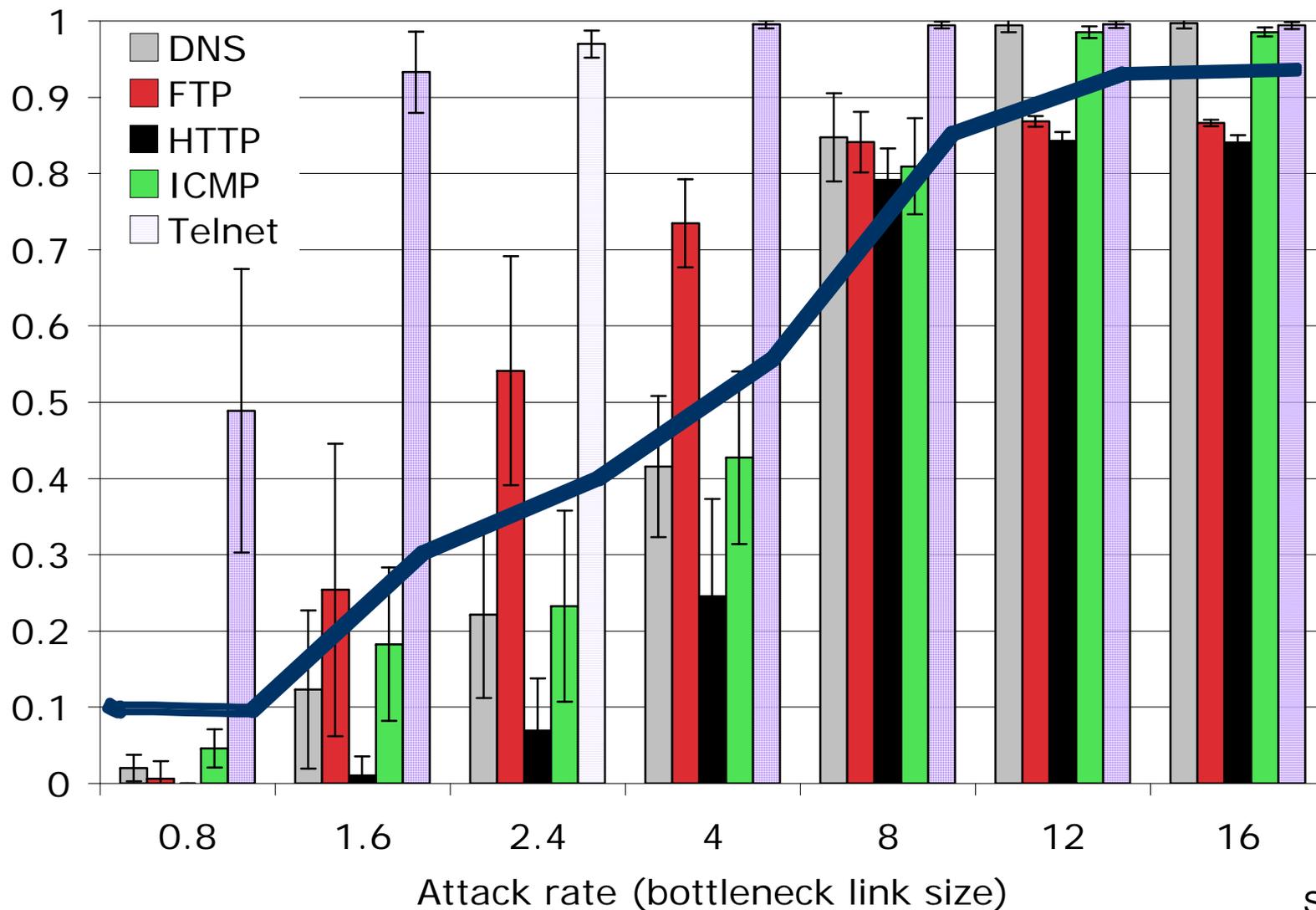
■ Life diagram

- Of successful and failed transactions
- Helps researchers detect regularities

■ Failure ratio

- Percentage of live transactions that will fail in the future
- Useful for capturing the timeliness of a defense's response

DoS-hist and DoS-level



Outline

- The problem of DoS testing
- Evaluating and testing DoS defenses
- Benchmarks and metrics
- ➔ ■ Conclusions and next steps

Conclusions and Next Steps

- Our work enables scientific testing of cyber defenses
- Tools available on DETER testbed
- Sharing of test scenarios and easy reuse are the key to advancing state of the art in cyber defense testing
- Next Steps
 - Enrichment of testbeds with automated test scenarios of high realism and fidelity
 - Development of repositories of realistic traffic/topology sources and generators to reproduce in testbeds
 - Share test setup/scenarios publicly
 - Validation and refinement by engaging the user community

For More Info ...

- Dr. Roshan Thomas
 - Roshan.Thomas@sparta.com
- Dr. Jelena Mirkovic
 - mirkovic@isi.edu
- DETER testbed
 - <http://www.deterlab.net>
- DDoS Benchmarks Web page
 - <http://www.isi.edu/~mirkovic/bench/>
- DDoS Metrics Web page
 - <http://www.isi.edu/~mirkovic/bench/>

PLEASE CONTACTS US