# Evaluating Network Defenses
# CS 239
# Advanced Topics in Network Security
# Peter Reiher
# May 10, 2006



## The Core Problem

- People have proposed many responses to:
  - Worms
  - DDoS
  - IP spoofing
  - Spam
  - Botnets
  - Many other types of attacks
- How can we tell which ones work?



## Challenges for Evaluation

- What does "works" mean?
- How does one test properly?
  - Topology
  - Attack characteristics
  - Defense locations
  - Background activity
- Where does one test properly?
- How much testing is necessary?



## Another Challenge

- Not all important information is available
  - Actual BGP policies
  - Internal topologies of ASes
  - Size, location, and character of attack networks
  - Traces of network activity during real attacks



## One More Important Challenge

- Attackers are clever and adaptive
- How do you consider that factor when performing tests?
- Do you:
  - Test only what we currently see?
  - Try to foresee and test future problems?



## Issues of Metrics

- What is the proper metric for the effectiveness of defenses against:
  - Spoofing?
  - DDoS?
  - Worms?
  - Spam?

## Topology Issues

- Most of the attacks in question are at Internet scale
- Generally not feasible to test on the Internet
  - Nor on a network of comparable size
- How to configure a 200 node test network?
- What if you don't have real routers available?
- What about network delays?
- How realistic is your routing?
  - Would it be affected by the attack or defense?



## Attack Characteristics

- Many types of attacks can vary widely in several ways
- E.g., DDoS attacks
  - How many sources?
  - How stable are identities of the sources?
  - Where are they located?
  - What kinds of traffic do they send?
  - Is the traffic mix constant?
  - How long does the attack last?
  - Does the attack respond to success by the defense?
  - If so, how? Just sending more? Altering what gets sent? Altering where it comes from?



## Defense Locations

- Which locations do you test?
- Which partial deployment patterns?
- How many different patterns?
- Do you "search" for the best?
- Or use analysis to identify the best?
- What deployment patterns are "fair" to test?



## Background Activity

- What is the normal mix of Internet traffic?
- How important to capture that in your tests?
- How important is cross-traffic?
  - To/from sites not involved in attack
- How accurate must this be?
  - Trace based vs. synthetic



## Where Does One Test?

- In one's own lab?
- On the Internet?
- On an existing testbed?
  - Emulab, Planetlab, …?
- On a specialized security testbed?



## How Much Testing?

- General issues of experiment design
  - Obtaining statistical significance
  - Covering the test space
  - While being realistic
- Do you test for particularly bad cases?
- Or just for the most likely cases?

## The DETER Testbed

- A partial response to these challenges
- A special testbed for security research
- With dedicated machines
  - Several hundred
- And special configuration capabilities
- Usable by all legitimate researchers



## But DETER Doesn't Solve Everything

- DETER is just a testbed
- It doesn't specify how to test
- Or provide tools to help design tests
- The EMIST project is intended to handle that
- Developing traffic generators, benchmarks, topology generators, etc.



## And EMIST Doesn't Solve All Problems, Either

- Doesn't provide that hard-to-get data
  - Which is mostly trade-secret stuff
  - Or too sensitive to give to all
- PREDICT is the solution
  - Repository of traces, topologies, etc.
  - Made available only to qualified researchers
  - Under restrictive conditions
- Many legal and social issues involved here
- Not quite up and running, yet



## A Different Measurement Challenge

- What's actually going on in the real world?
- Are existing defenses coping?
  - If not, where are they failing?
- What are real costs of defenses?
- What are the new trends in attacks?



## Approaches to This Problem

- Honeypots and honeynets
  - Designed to attract attackers
  - Then you observe what they do
- Network telescopes
  - Otherwise unused portions of IP address space
  - They capture automated attack traffic
    - Worms, DDoS backscatter, scanning, etc.