Spoofstat : How Easily can Network Attackers Hide their Location?

Clay Shields
Thomas E. Daniels
Greg Ellis
Benjamin Kuperman
Manu Pathak
Motivation

• Network security is going to be critical for future applications like e-commerce
• Recent Denial of Service (DoS) attacks show the difficulty in tracing source of the attacks
• Attackers hide their location by IP spoofing, and by loose source routing
• Edge filtering makes this more difficult, and is recommended. But how commonly is it done?
Goals of Spoofstat

• Evaluate the number of domains useable by attackers by testing a large number of networks

• Spoofstat goals include:
  – *Estimating percentage of hosts which can send spoofed packets*
  – *Determining percentage of these networks which disallow source routing*
Design of Spoofstat

• Simple client-server system with client publicly distributed
• When run, client connects to the server running outside our firewall
• Client then sends several types of spoofed packets
• Server measures which packets arrive
Spoofstat – Key Features

- TCP used for establishing connection
- UDP used for encapsulating nonce
- Cryptographically random nonce uniquely identifies each client
- Different types of UDP packets used to test common vulnerabilities
Spoofed Packets

• Different kinds of packets to be used:
  – Real source address of the client (normal case)
  – An unused IP address from the CERIAS domain
  – An address from unassigned address space (10.X.X.X X subnet)
  – A loose source routed packet
Basic Spoofstat Configuration

Client → Router

UDP Packets from client to server (no LSR)

Router → Server

Packets with LSR through R

Packets with LSR through R
The Spoofstat Protocol

- Client opens a TCP connection to port 80 of Server
- Server replies on the connection with cryptographically random 128 bit nonce and UDP port to be used
- Client replies on the TCP connection with an acknowledgement of receiving N and P
Details of Spoofstat

- Client sends a number of UDP packets with a spoofed source address. Each UDP packet has N as payload.
- If the Server receives a UDP packet and the nonce matches, it sends a control message and Client moves to next phase.
Details of Spoofstat

• If Server does not receive UDP packets within timeout, filtering is assumed to be in place.
• Repeat steps above for each different packet type
• Client reports to user what kind of filtering is being done
• Server logs connections results for each client
Implementation Notes

• Open Source software
• Implementation in C
• Tested on Linux, Open BSD, FreeBSD, Solaris
• Windows port planned
• Logging to a cryptographic file system for security
Execution

• Goal is to get client to be run from many domains
• Distribute to Corporate Partners for their own information
• Distribute to “geek” community via popular web forums