

Spoofer Project Updates

Matthew Luckie
mjl@wand.net.nz

Ken Keys, Ryan Koga,
Robert Beverly, kc claffy

In the beginning...

- There was the spoofer project (2005)
- A hack put together during grad school at MIT lead by Robert Beverly (w/ Steven Bauer)
 - Can a host send packets with spoofed source IP addresses? RFC 1918 addresses?
 - How far do they get?
- Did not receive external funding, held together with duct tape

Papers

- USENIX SRUTI 2005: Spoofer
- USENIX Security 2007 (poster): Tracefilter
- IMC 2009: Analysis of spoofer data
- ISOC 2013 (blog): Long term analysis

Recent News

- May 2015: CAIDA takes over stewardship of spoofer project
- August 2015: DHS funded 3-year project commences

New Spoofer Client Features

- New Client+Server to be released before 1 May 2016 (DHS deliverable)
- Intuitive GUI
 - Cross-platform: same GUI on Linux, MacOS, and Windows
- Runs in background
 - Performs measurement once a week, and whenever attached to a new network
- Explicit opt-in to publicly share results

Public reports

- We will start sharing test results marked “sharable” shortly, with some anonymisation
- Break results down by
 - Country
 - Network Types
 - Provider
- We will provide customer cone prefixes for each AS, to bootstrap ingress access list configuration