SRUTI - Bots and Spoofed Sources

- Evan Cooke
- Steve Bauer
- Mark Allman

Summary

- Botnet detection/disruption
  - Use is more important than attacking
  - Financial motivation to keep botnets running
  - Arms race between detectors/operators
  - More holistic view required, smarter/cheaper/easier detection/disruption systems required

Summary

- Spoofer Project
  - Lack of consistent RFC2827 filtering, still...
  - Measurement infrastructure for project useful to determine filter deployment (biased population tested?)
  - Spoofing not required any longer (see presentation 1)

Summary

- Behavioral History Proposal
  - Find a method to ‘know’ good from bad sources
  - Make that method trustworthy
  - Make that method feasible
  - Lots of work and thought about model/use still required

State-of-the-Art

- Home-grown
  - Flow tools
  - route-server(s)
  - rbl-like solutions
- Lots of repeated tech
- Little sharing of tech

Future

- Capitalize on communications ability
  - Working groups
  - Shared meetings
  - Mail lists/blogs/portals
- Share tech/tools/decision process
  - Simple, deployable, usable solutions for ‘everyone’
- Miscreants share by default, why don’t we?
  - pch/cymru/dhs?

Questions for Speakers?