GENI as an Infrastructure to Study Malicious Overlay Networks

Wenke Lee

Georgia Institute of Technology

Goals

- Use GENI as a large-scale distributed test-bed for security research
  - The best we can get if we can't experiment on the real Internet
- Leapfrog our ability to understand large-scale malicious networks (botnets) and predict their future trends
  - Essential properties of botnets, how botnets must rely on core network services, trade-offs of botnet design considerations, etc.
- Evaluate botnet detection and removal technologies

A New Look at Botnets

- Analyze essential properties of botnet lifecycle
  - E.g., botnets are valuable, long-term resources
- Derive *axioms* that directly follow from the properties
  - E.g., botnets need to have *agility* to evade detection and removal
- Derive *theories* from the axioms
  - E.g., a particular kind of botnet structure has better *network agility* than the others
  - E.g., by detecting and neutralizing the sources of *network agility*, we can limit botnets' evasion capabilities and thus make botnets easier to detect and remove
- Apply the theories to *practice*
  - E.g., what are the ways that network agility can be realized?
  - E.g., an on-line detection of naming (DNS) based agility.

An Experimental Approach

- Experiment with design and deployment, as well as detection and removal of botnets on GENI, e.g.,
  - design various types of botnets – topology structures, characteristics/values of essential properties, etc.
  - deploy these botnets – measure their propagation speed, size, aggregate attack power, etc.
  - evaluate detection and removal techniques