**Introduction**

- **Problems**
  - Malware spread on complex networks difficult to predict
  - Effect of proposed security policies is unclear

- **Approach**
  - Model malware spread and intervention policies
  - Mathematical analysis and simulations

**Modeling Platform: ASIM**

ASIM is an agent-based model that mimics the growth and topology of the internet at the autonomous systems level using the following information:

- **Geography**
- **Economics**
- **Traffic**

By combining ASIM with models of malware spread, we end up with a reasonable approximation of real world malware distributions on the internet.

**Graduated Response and Drive by Downloads**

To model the effect that search providers can have on infection rates, we created an epidemiological model of drive by downloads and search providers.

- **Intervention policies**
  - Blacklisting (removal from search results)
  - Graduated Response (reduction of search rank)

**Data Sources**

- **BGP Dumps (AS topology over time)**
  - RIPE [http://ripe.net](http://ripe.net)
- **Malware Data**
  - SANS ISC (Internet Storm Center) [http://isc.sans.org](http://isc.sans.org)
  - FIRE [http://maliciousnetworks.org](http://maliciousnetworks.org)

**Results: ASIM**

Filtering ingress traffic (including transit) is more than twice as effective as filtering egress traffic alone.

**Results: Graduated Response and Drive by Downloads**

The solution to the steady state client infection rate is

\[ P_c = P_s \frac{\beta_c}{\gamma_c + \beta_c} \]

For realistic distributions, high variance in client infection rates obscures the steady state solution.

**Conclusions**

- Agent based models are a powerful tool for modeling interventions in complex networks
- Real world distributions and networks give rise to noisy, unpredictable results, requiring multiple runs to understand steady state dynamics