



U.S. ARMY  
RDECOM

# Metrics and method for efficient post-infection network triage

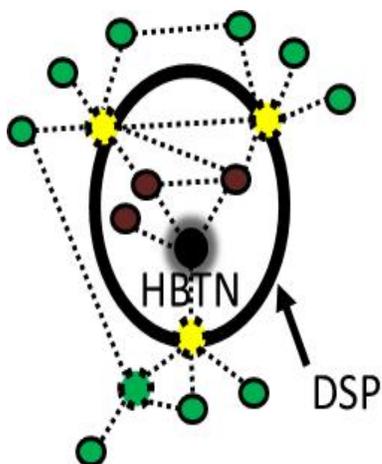


## S&T Campaign: Information Sciences Cybersecurity

Rich Harang, (301) 394-2444  
richard.e.harang.civ@mail.mil

### Research Objective

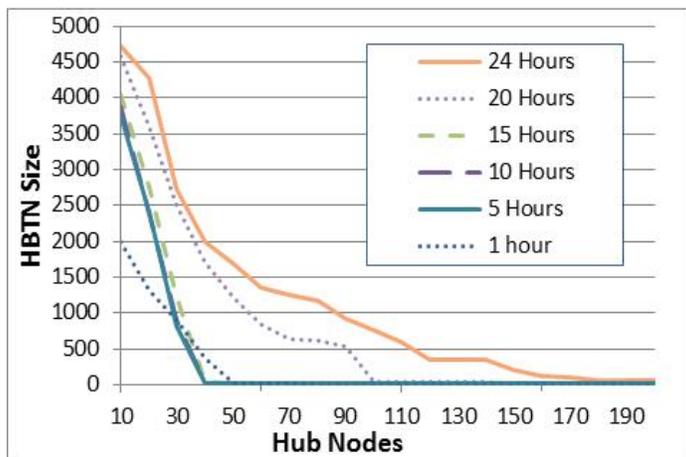
- Use graph-based methods to rapidly triage network nodes following an intrusion, minimize number of nodes to inspect to bound the attacker's influence using established communication pathways



Rapidly identify critical vertices to disconnect a 'tainted' portion of a graph, starting from an arbitrary node, with a minimal number of cuts, under time-varying adjacencies.

### Challenges

- Temporal ordering of communication between nodes does not permit use of standard breadth-first searches
- Existence of high-degree hub nodes collapses network diameter



Even 24-hours post-intrusion, securing 190 nodes (from a total of 7335) is sufficient to limit the mean taint set to a single node, regardless of initial entry point to the network.

### ARL Facilities and Capabilities Available to Support Collaborative Research

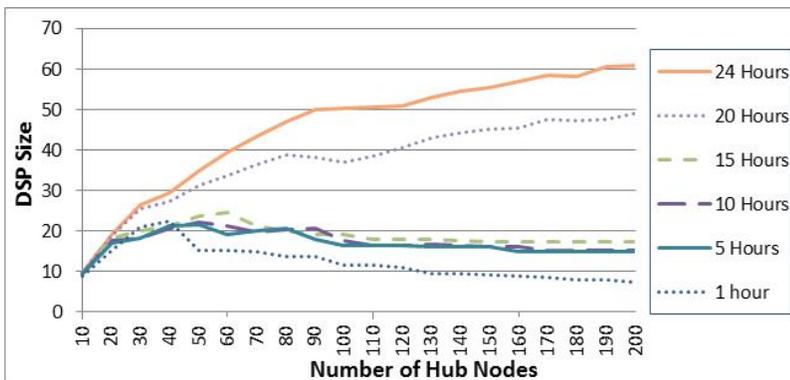
- ARL Cyber Lab
- Network Science Research Lab (Q3 FY15)
- DOD HPC supercomputing resource center
- ARL's real world network data and operational experience gives insight to operationally relevant and available data
- Operational data allows for empirical validation of theoretical results

### Results

- Empirical results show theoretical results are an upper bound (assortativity; approximation imposed by asymptotics)
  - Securing 190 hub nodes creates tainted node set of average size 1, for any point of intrusion
- Greedy method for node deletion performs well; order of magnitude improvement over theoretical upper bound based on node degree
- Mell; Harang; "Using network tainting to bound the scope of network ingress attacks" Best paper; SERE 2014

### Complimentary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Exploration of probabilistic flow models that can account for varying size/duration of flows
- Imputation methods for missing flow observations
- Additional data sets



At 24 hours post-infection, of 190 hub nodes, on average only 61 will actually require examination (remaining hubs vertex-separated from taint by those 61).