Cyber Defense Technology Networking & Evaluation

Esha Desai
USC ID: 6993245898

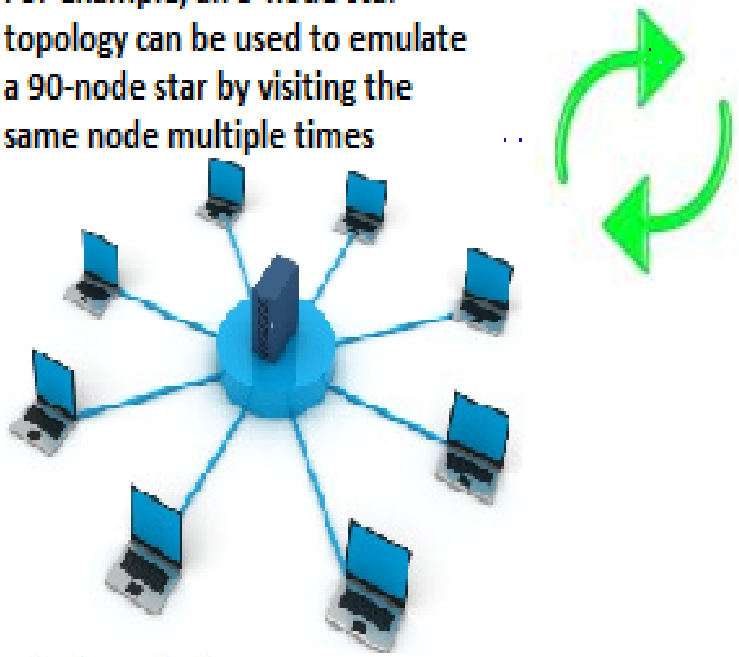
Objective

- Cyber Defense Technology Experimental Research (DETER):Experimental infrastructure for developing security technologies
- Evaluation Methods for Internet Security Technology (EMIST): Develop classes which represent network attacks & defense mechanisms
- Focus on 3 classes of attacks : Worms, DoS & attacks on Internet's routing infrastructure
- Evaluate particular attack/defense using testing scenarios and unify the results
- Monitor new Internet security breaches
- Adapt to different testbeds including simulation(NS), emulation(Emulab) & hardware testbeds
- Include attack simulators, generators for topology, background traffic, live traffic
- Effectively combine emulation, simulation and real hardware to develop defense mechanisms
- Allow researchers to test their own defense mechanism designs

Testbed Architecture & Requirements

- Exists as three permanent network clusters at ISI(LA), ISI(Virginia) and UC-Berkeley.
- Testbed to be fully isolated from Internet
- Would generate destructive traffic to cause temporary network damage
- Would host around 1000 PCs each with multiple NICs.
- Would have routers, switches and a complex topology which can correlate with the Internet and it's benefit & attack traffic
- Software for Traffic generation, network monitoring, analysis, registration, archiving etc.
- X-Bone for node revisiting

For example, an 9-node star topology can be used to emulate a 90-node star by visiting the same node multiple times



PC with experimentation facility

Mapping desired Virtual Topology onto the Physical Topology

Network provides sufficient topological complexity to emulate a scaled down but functionally accurate representation of the hierarchical structure of the real Internet

Question

What problems were faced in developing Cyber Defense mechanisms? How did DETER bring a solution to it?

- The real Internet and the sort of attacks that happen were not really reflected by the Existing research facilities and mechanisms
- These facilities were too small scaled to mirror the complex Internet and the attacks
- DETER converged emulation, simulation and real hardware to achieve this. It merged an experimental infrastructure with testing methodologies that reflected real attack sets. It serves as a platform for researchers to evaluate their defense mechanisms against realistic attack traffic.