Understanding Worms' Impact on the Internet Infrastructure through Realistic Simulation

Bob Bradley and Lan Wang
Computer Science Department
The University of Memphis
(bbradley@utm.edu,lanwang@memphis.edu)

Internet worms pose a significant threat to the stability of the Internet infrastructure. First, the huge amount of traffic generated by infected hosts causes Internet links to become congested. Second, the random scanning used by most worms may cause routers to become unstable. For example, since a large number of the random probes go to unused IP addresses, edge routers in some networks could quickly fill up their ARP tables (and could crash in extreme cases) as they try in vain to find the MAC addresses associated with the unused addresses. Furthermore, the increased traffic load and router crashes could cause the routing sessions between the routers to reset, leading to more routing instabilities [1].

Determining the exact effect that the worms had on the Internet infrastructure is difficult, due to the difficulty of obtaining concrete data from a large number of ISPs. On the other hand, BGP routing updates collected by public monitoring points during the worm attacks can be hard to interpret and such indirect inferences usually do not give us precise answers [1]. However, as worms become faster and more vicious, it is important for us to fully understand the potential impact of the worms.

Previous studies on Internet worms have used mathematical models to predict the worms' propagation rate (e.g. the AAWP model in [2]). However, a pure mathematical model does not allow us to observe the detailed protocol interactions that lead to the instability during a worm attack. In particular, we could not use this model to generate realistic packet data for use in real world experiments, nor could we use this model to directly determine the effects that the random scanning has on routers. Because of this limitation, we are designing a new "full-scale packet-level" worm simulator. We use a combination of detailed and abstract models to simulate individual vulnerable hosts, routers, subnets, and Autonomous Systems. While [3] suggests that similar results can be obtained by "scaling down" the IP address range and the number of machines simulated, we have chosen to use the full 32-bit address range, because we believe that studying some of the protocol interactions will require a full-scale model.

Using the same parameters as the AAWP model, our new model can generate similar population growth data for a variety of different worms. Furthermore, with this new model we can measure the amount of traffic that would be created between any two Autonomous Systems, given a BGP routing table. We can keep track of not just the amount of packets passing trough a router, but the number of unique flows and the number of to/from addresses at any given time. This new data is crucial if we hope to be able to estimate an upper bound on the overhead imposed on routers by worms including traffic load, memory load, ARP table load, ICMP, etc. Using this new model we also plan to study other worm related issues such as:

- The effects that different router ARP cache replacement schemes would have during a worm attack;
- The effect that the worm attacks have on BGP routing protocol and sessions;
- The effect that NAT addresses have on the spread of the worm.

We also plan to perform experiments on real routers using the packet data generated by the simulator, and hope to develop new enhancements and security measures that will help prevent Internet worms from adversely affecting routing in the future.

REFERENCES

[1] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, L. Zhang, Observation and Analysis of BGP Behavior under Stress**,** in *Proceedings of the Second ACM SIGCOMM Internet Measurement*, Nov. 2002

[2] Z.Chen, L. Gao, and K. Kwiat, Modeling the Spread of Active Worms, in *Proceedings of IEEE INFOCOM 2003*, Mar. 2003

[3] N. Weaver, I. Hamadeh, G. Kesidis and V. Paxson, Preliminary Results Using ScaleDown to Explore Worm Dynamics, in Proceedings of *ACM CCS WORM*, Oct. 2004.