[1] M. Abdelhafez and G. Riley. Evaluation of worm containment algorithms and their effect on legitimate traffic. In *Third IEEE International Workshop on Information Assurance (IWIA)*, March 2005. [bib]

[2] P. Ammann, D. Wijesekera, and S. Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM conference on Computer and communications security (CCS)*, pages 217-224, New York, NY, USA, 2002. ACM Press. [bib | DOI]

[3] K. Anagnostakis, M. Greenwald, S. Ioannidis, A. Keromytis, and D. Li. A cooperative immunization system for an untrusting Internet. In *Proceedings of the 11th IEEE International Conference on Networks (ICON)*, September 2003. [bib]

[4] R. Bajcsy, T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, S. Floyd, W. Hardaker, A. Joseph, G. Kesidis, K. Levitt, B. Lindell, P. Liu, D. Miller, R. Mundy, C. Neuman, R. Ostrenga, V. Paxson, P. Porras, C. Rosenberg, J. D. Tygar, S. Sastry, D. Sterne, and S. F. Wu. Cyber defense technology networking and evaluation. *Commun. ACM*, 47(3), 2004. [bib]

[5] S. Braynov and M. Jadiwala. Representation and analysis of coordinated attacks. In *Proceedings of the 2003 ACM workshop on Formal methods in security engineering (FMSE)*, pages 43-51, New York, NY, USA, 2003. ACM Press. [bib | DOI]

> In this paper, we propose a formal model of coordinated attacks in which several attackers cooperate towards a common malicious goal. The model investigates both attack planning and vulnerability analysis, thereby providing a uniform approach to system and adversary modelling. In addition, the model is general enough to explain both coordinated and single attacks.
>
> In the paper, we define the notion of coordinated-attack graph, propose an algorithm for efficient generation of coordinated-attack graphs, demonstrate how coordinated-attack can be used for vulnerability analysis, and discuss an implementation of a coordinated-attack graph.
>
> Coordinated-attack graphs can facilitate a wide range of tasks, such as model checking, opponent modelling, intrusion response, sensor configuration, and so forth. In addition, they can be used in robotic warfare, where several intelligent software agents automatically produce and launch coordinated attacks.

[6] L. Briesemeister and P. Porras. Microscopic simulation of a group defense strategy. In *Proceedings of Principles of Advanced and Distributed Simulation (PADS)*, June 2005. [bib]

> We introduce a novel worm containment strategy that integrates two complementary worm quarantine techniques. The two techniques are linked, with one strategy employing the other as an indicator of worm infection. A group defense mechanism shares such indicators among neighboring networks, and when enough corroboration occurs, the network engages in traffic filtering to halt infection attempts.
>
> We present an SSFnet-based microscopic simulation of the containment strategy against random scan worms, and explore various performance characteristics of the group defense mechanism. The simulation results help to characterize the conditions and degree to which the integrated quarantine strategy can both slow worm propagation and prevent the worm from reaching its full saturation potential.

[7] S. Chen and Y. Tang. Slowing down internet worms. In *Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS)*, pages 312-319. IEEE Computer Society, March 2004. [bib | .html]

> An Internet worm automatically replicates itself to vulnerable systems and may infect hundreds of thousands of servers across the Internet. It is conceivable that the cyber-terrorists may use a wide-spread worm to cause major disruption to our Internet economy. While much recent research concentrates on propagation models, the defense against worms is largely an open problem. We propose a distributed anti-worm architecture (DAW) that automatically slows down or even halts the worm propagation. New defense techniques are developed based on behavioral difference between normal hosts and worm-infected hosts. Particulary, a worm-infected host has a much higher connection-failure rate when it scans the Internet with randomly selected addresses. This property

allows DAW to set the worms apart from the normal hosts. We propose a temporal rate-limit algorithm and a spatial rate-limit algorithm, which makes the speed of worm propagation configurable by the parameters of the defense system. DAW is designed for an Internet service provider to provide the anti-worm service to its customers. The effectiveness of the new techniques is evaluated analytically and by simulations.

[8] L. de Moura, S. Owre, H. Rueß, J. Rushby, N. Shankar, M. Sorea, and A. Tiwari. SAL 2. In R. Alur and D. Peled, editors, *Computer-Aided Verification, CAV*, volume 3114 of *LNCS*, pages 496-500. Springer, July 2004. [bib]

[9] S. Jha and J. M. Wing. Survivability analysis of networked systems. In *Proceedings of the 23rd International Conference on Software Engineering (ICSE)*, pages 307-317, Washington, DC, USA, 2001. IEEE Computer Society. [bib]

Survivability is the ability of a system to continue operating despite the presence of abnormal events such as failures and intrusions. Ensuring system survivability has increased in importance as critical infrastructures have become heavily dependent on computers. In this paper we present a systematic method for performing survivability analysis of networked systems. An architect injects failure and intrusion events into a system model and then visualizes the effects of the injected events in the form of scenario graphs. Our method enables further global analyses, such as reliability, latency, and cost-benefit analyses, where mathematical techniques used in different domains are combined in a systematic manner. We illustrate our ideas on an abstract model of the United States Payment System.

[10] X. Jiang, D. Xu, S. Lei, P. Ruth, and J. Sun. Worm meets beehive. Technical Report CSD TR 04-027, Purdue University, Department of Computer Sciences, May 2004. [bib | .html | .pdf]

[11] H. K. I. Kang. On the functional validity of the worm-killing worm. In *Proceedings of the IEEE International Conference on Communications*, volume 4, pages 1902-1906, Jun 2004. [bib | DOI | http]

The notion of worm-killing worm has been in the folklore for some time. However the obvious fear of the killer worm itself being compromised, or of any self-propagating code set loose (possibly over administrative boundaries), has barred serious exploration on the practical aspects of the idea. In this paper, we suspend such concerns momentarily, and investigate its functional validity. This effort is motivated by recent fast worm epidemics exemplified by that of SQL slammer, which was overwhelmingly faster than traditional human-intervened response. Specifically, this paper evaluates the killer worm in terms of the prevention effect and the incurred traffic cost. Above and beyond, we consider supplementary techniques that could boost the performance and mitigate the harmful side-effects of the worm-killing worm.

[12] J. O. Kephart and S. R. White. Directed-graph epidemiological models of computer viruses. In *IEEE Symposium on Security and Privacy*, 1991. [bib]

[13] C. E. Landwehr. Formal models for computer security. *ACM Comput. Surv.*, 13(3):247-278, 1981. [bib | DOI]

[14] M. Liljenstam and D. M. Nicol. Comparing passive and active worm defenses. In *Proceedings of the First International Conference on the Quantitative Evaluation of Systems (QEST)*, pages 18-27, September 2004. [bib | .pdf]

[15] M. Liljenstam, D. M. Nicol, V. H. Berk, and R. S. Gray. Simulating realistic network worm traffic for worm warning system design and testing. In *Proceedings of the 2003 ACM workshop on Rapid Malcode (WORM)*, pages 24-33. ACM Press, 2003. [bib | DOI]

Reproducing the effects of large-scale worm attacks in a laboratory setup in a realistic and reproducible manner is an important issue for the development of worm detection and defense systems. In this paper, we describe a worm simulation model we are developing to accurately model the large-scale spread dynamics of a worm and many aspects of its detailed effects on the network. We can model slow or fast worms with realistic scan rates on realistic IP address spaces and selectively model local detailed network behavior. We show how it can be used to generate realistic input traffic for a working prototype worm detection and tracking system, the Dartmouth ICMP BCC:

System/Tracking and Fusion Engine (DIB:S/TRAFEN), allowing performance evaluation of the system under realistic conditions. Thus, we can answer important design questions relating to necessary detector coverage and noise filtering without deploying and operating a full system. Our experiments indicate that the tracking algorithms currently implemented in the DIB:S/TRAFEN system could detect attacks such as Code Red v2 and Sapphire/Slammer very early, even when monitoring a quite limited portion of the address space, but more sophisticated algorithms are being constructed to reduce the risk of false positives in the presence of significant “background noise” scanning.

[16] D. Nojiri, J. Rowe, and K. Levitt. Cooperative response strategies for large scale attack mitigation. In *Proceedings of the 3rd DARPA Information Survivability Conference and Exposition*, April 2003. [bib]

[17] A. Pnueli. The temporal logic of programs. In *Proceedings of the 18th IEEE Symposium on Foundations of Computer Science*, pages 46-67, 1977. [bib]

[18] The SAL intermediate language, 2003. Computer Science Laboratory, SRI International, Menlo Park, CA. http://sal.csl.sri.com/. [bib]

[19] P. K. Singh and A. Lakhotia. Analysis and detection of computer viruses and worms: an annotated bibliography. *ACM SIGPLAN Notices*, 37(2):29-35, 2002. [bib | DOI]

This annotated bibliography reviews research in analyzing and detecting computer viruses and worms. This document focuses on papers that give information about techniques and systems detecting malicious code.

[20] Y.-K. Zhang, F.-W. Wang, Y.-Q. Zhang, and J.-F. Ma. Worm propagation modeling and analysis based on quarantine. In *Proceedings of the 3rd International Conference on Information Security (InfoSecu)*, pages 69-75, 2004. [bib | DOI]

In recent years, the worms that had a dramatic increase in the frequency and virulence of such outbreaks have become one of the major threats to the security of the Internet. In this paper, we provide a worm propagating model. It bases on the classical epidemic Kermack-Kermack model, adopts dynamic quarantine strategy, dynamic infecting rate and removing rate. The analysis shows that model can efficiently reduce a worm's propagation speed, which can give us more precious time to defend it, and reduce the negative influence of worms. The simulation results verify the effectiveness of the model.

This file was generated by bibtex2html 1.96.