

# Research Statement

Cliff C. Zou

czou@ecs.umass.edu

My research interest is computer and network security. In recent years, scan-based worms (such as Code Red, Slammer, Blaster, Sasser, etc.) and mass-mailing email worms (such as SirCam, MyDoom, etc.) have posed tremendous threats to computer networks. My Ph.D. research focuses on modeling of and defense against these malicious worms.

Under excellent guidance from Prof. Weibo Gong and Prof. Don Towsley, I have learned how to identify important research problems and how to approach research topics systematically. Because of my control system and engineering background, my research methodology is to approach a research problem from a system and analytical point of view, using various mathematical methods to model and analyze the problem, and then to examine the results through simulations and real experiments. Through mathematical analysis of abstract models I achieve a fundamental understanding of research problems, often leading to effective solutions. In addition, my approach makes manifest the underlying principles of a research problem, which often enlightens my understanding and stimulates me to find further research problems.

## Dissertation Research

My Ph.D. dissertation concentrates on modeling, analysis, and mitigation of Internet worm attacks. I also study defense against various Distributed Denial-of-Service (DDoS) attacks. I try to answer the following questions to understand defense of worm and DDoS attacks: How can I model a worm's propagation? How is a worm's propagation affected by attackers changing the worm's infection strategy? How can we detect the presence of a worm at its early stage? How can we protect an enterprise network from worm attack? How can we implement automatic defense in a cost-effective way?

### *Modeling and Analysis of Internet Worms*

Scan-based worms, such as Code Red, Slammer, Blaster, Sasser, etc., find and infect vulnerable hosts through randomly scanning IP addresses. After the Code Red incident in 2001, I extended the epidemic model to present a two-factor worm model, described by differential equations, that considered the impacts of human countermeasures and network congestions on a worm's propagation behavior [1]. It was the first worm model presented in security research to consider the impact of network congestions, an impact clearly exhibited a half-year later by the bandwidth-limited worm Slammer.

Through infinitesimal analysis, I derived a uniform-scan worm propagation model that was described by concrete parameters of worms instead of by the abstract parameter in the traditional epidemic model. Based on this worm model, I derived and analyzed how a worm propagates under various scanning strategies, such as local preference scan, sequential scan, routable scan [9], hit list scan. Based on the unique destructive behavior of Witty worm, I modeled the crashing time of a Witty-infected host as an exponentially distributed random variable [11]. This model matched and explained well the worm's dynamic behavior exhibited in a real worm trace (collected by Univ. Michigan "Internet Motion Sensor"). In addition, I proposed a general matrix-format model to model a worm's propagation considering Internet topology, network bandwidth, and quarantine defense. I summarized the above modeling in a paper [7] and submitted it to the Journal of Performance Evaluation.

Email worms propagate via email communication. Their propagation behavior is affected by the email-address topology and email users' interactions. Through studying the topology of Yahoo email groups, I believe that Internet email topology is heavy-tailed distributed. Compared with small-world topology and random-graph topology, I found that email worms propagate faster on a heavy-tailed email topology, but that immunization defense is more effective on such a topology [5].

# Research Statement

## ***Early Detection of Internet Worms***

To defend against worm attacks, we first need to detect the presence of a worm as early as possible to ensure having time for defense. I found that Internet worms propagate exponentially at their early stage. Based on this phenomenon, I presented a novel detection methodology, trend detection, by deploying a Kalman filter to detect the exponential growth trend, not the traffic burst, in monitored data. This detection method was robust to monitored background noise. In addition, I provided formulas to predict the vulnerable population size and correct the bias in the observed number of infected hosts [2]. I conducted further research based on the conference paper [2], and the extended paper was accepted recently by *IEEE/ACM Transactions on Networking* [3].

## ***Defense against Worm Infection and Distributed Denial-of-Service (DDoS) Attacks***

Learning from the experiences of real-world epidemic disease control, I derived two defense principles: preemptive quarantine and feedback adjustment. Based on these two principles, I developed a feedback dynamic quarantine defense system for Internet-scale worm defense [4]. Since enterprise networks have more incentive and control to deploy automatic mitigation than the global Internet, I designed two worm defense systems for enterprise networks: one was Firewall Network System, which protected an enterprise network from scan-based worms [8]; another was feedback email worm defense system, which protected an enterprise network from email worms [6].

In the summer of 2004 I was a graduate intern in AT&T Labs Research, under the supervision of Nick Duffield. I studied how to design a self-tuning defense system, because such a defense system was needed to deal with various network conditions and dynamically changing attacks. I presented an adaptive defense principle based on cost minimization—a defense system adaptively adjusts its configurations according to the network condition and attack severity in order to minimize the combined cost introduced by false positives (misidentified normal traffic as attack) and false negatives (misidentified attack traffic as normal) at any time. I presented detailed adaptive defense systems for defending against worm infections and various DDoS attacks [10].

## **Future Research**

In the short term, I am continuing on several promising research problems that follow directly from my current Ph.D. research:

**Analysis of real worm propagation data.** In my Ph.D. thesis, I present modeling, analysis, early detection, and dynamic quarantine for Internet worms. What I lack in my research is verification of my studies on more worm propagation traces, which will reveal what other issues I should consider in my models and analyses; in addition, I can find new research problems through this approach. I plan to pursue active collaborations with other researchers to set up monitoring systems and collect real worm propagation data.

**Feedback dynamic defense system.** For worm quarantine defense, I have only modeled and analyzed the open-loop dynamic quarantine system. The adaptive defense systems I present in our recent submission are the first step in deriving a feedback dynamic defense system. Future work includes defining more accurate cost functions for the defense system, modeling the dynamics of the network under changing defense actions, and deriving the optimal control for the whole system.

**Large-scale worm propagation simulation.** I have derived many worm propagation models and am strong in modeling and analysis. Other researchers have designed or set up large-scale simulation networks, and I plan to pursue active professional collaborations to realistically simulate Internet-scale worm propagation.

# Research Statement

In the long term, I intend to extend my work into other security research areas. I will continue to study statistical-based anomaly intrusion detection, the basis for various security defenses in my current research. In addition, I am interested in studying the fundamental principles of Internet security, e.g., the relationship between accountability, understandability, and security. For example, current Internet routing topology is complex and messy, and we don't know with any certainty where to enforce security and who is responsible; an anonymity network can provide privacy for users but it obscures accountability, thus it has potential problems when facing Denial-of-Service attacks; and, in the near future, radio frequency identification (RFID) will be deployed almost everywhere, but it will raise many security and privacy issues in our everyday life. All these security-related topics have many open but related research problems that interest me.

## Summary

I am enthusiastic to pursue research that is motivated by real world problems. I seek to better understand the underlying principles of these problems, and then provide solutions that either enlighten further research or that are practical. From my graduate research training, I have acquired the ability to discover potential research topics, to formulate valid research problems, and then to solve them step-by-step through the combination of mathematical analyses, simulations, and real experiments. I look forward to continuing this style of research in an academic department that encourages discussion and collaboration.

## References

- [1] C. C. Zou, W. Gong, and D. Towsley. "Code Red Worm Propagation Modeling and Analysis," In *Proc. 9th ACM Conference on Computer and Communications Security (CCS'02)*, October 2002.
- [2] C. C. Zou, L. Gao, W. Gong, and D. Towsley. "The Monitoring and Early Warning of Internet Worms," In *Proc. 10th ACM Conference on Computer and Communications Security (CCS'03)*, October 2003.
- [3] C. C. Zou, W. Gong, D. Towsley, and L. Gao. "The Monitoring and Early Detection of Internet Worms," *IEEE/ACM Transactions on Networking* (to appear).
- [4] C. C. Zou, W. Gong, and D. Towsley. "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," In *Proc. ACM Workshop on Rapid Malcode (WORM'03)*, October 2003.
- [5] C. C. Zou, D. Towsley, and W. Gong. "Email Worm Modeling and Defense," In *Proceedings of 13th International Conference on Computer Communications and Networks (ICCCN'04)*, October 2004.
- [6] C. C. Zou, W. Gong, and D. Towsley. "Feedback Email Worm Defense System for Enterprise Networks," *Technical Report TR-04-CSE-05, UMass ECE Dept.*, April 2004.
- [7] C. C. Zou, D. Towsley, and W. Gong. "On the Performance of Internet Worm Scanning Strategies," *Technical Report TR-03-CSE-07, UMass ECE Dept.*, November 2003.
- [8] C. C. Zou, D. Towsley, and W. Gong. "A Firewall Network System for Worm Defense in Enterprise Networks," *Technical Report TR-04-CSE-01, UMass ECE Dept.*, February 2004.
- [9] C. C. Zou, D. Towsley, W. Gong, and S. Cai. "Routing Worm: A Fast, Selective Attack Worm Based on IP Address Information," *Technical Report TR-03-CSE-06, UMass ECE Dept.*, November 2003.
- [10] C. C. Zou, N. Duffield, D. Towsley, and W. Gong. "Adaptive Defense Against Various Network Attacks," *Submitted for publication*, October 2004.
- [11] C. C. Zou. Witty Worm Propagation Modeling. <http://tennis.ecs.umass.edu/~czou/research/wittyModel.html>