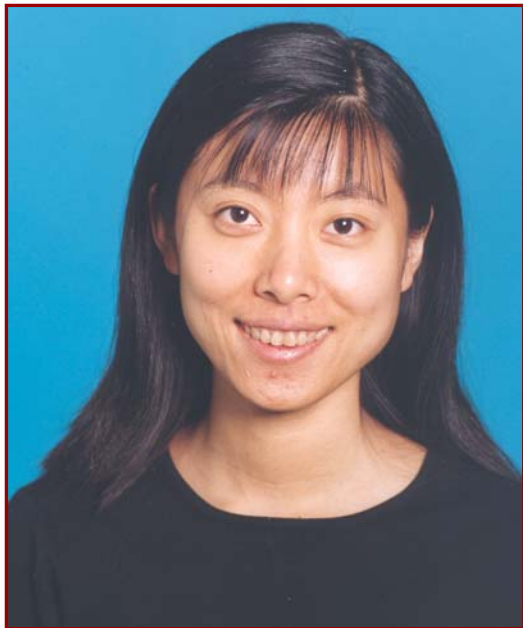


THURSDAY  
FEBRUARY 16, 2006

Scaife Hall Auditorium  
Room 125

4:00 PM  
Refreshments—3:30 PM



**DAWN SONG**

**CARNEGIE MELLON UNIVERSITY**

Dawn Song is an Assistant Professor at Carnegie Mellon University. She obtained her PhD in Computer Science from UC Berkeley. Her research interest lies in security and privacy issues in computer systems and networks. She is the author of more than 35 research papers in areas ranging from software security, networking security, database security, distributed systems security, to applied cryptography. She is the recipient of various awards and grants including the NSF CAREER Award and the IBM Faculty Award. She has served on numerous program committees of prestigious conferences including Symposium on Operating Systems Design and Implementation (OSDI), ACM Computer and Communication Security (CCS), USENIX Security Symposium, Network and Distributed Systems Security Symposium (NDSS), USENIX Annual Technical Conference, Symposium on Recent Advance in Intrusion Detection (RAID), IEEE Infocom, ACM Sensor Networks and Systems Conference (SenSys).

James C. Hoe, ECE Seminar Host  
[jhoe@ece.cmu.edu](mailto:jhoe@ece.cmu.edu)

For more information:  
<http://www.ece.cmu.edu/seminar>

## STING:

### *AN AUTOMATIC DEFENSE SYSTEM AGAINST ZERO- DAY WORM ATTACKS*

Software vulnerabilities have had a devastating effect on the Internet. Worms such as CodeRed and SQL Slammer can compromise millions of hosts within hours or even minutes. To successfully combat such fast automatic Internet attacks, we need fast automatic attack detection and defense mechanisms.

In this talk, I will present Sting, a new automatic defense system that aims to be effective even against zero-day exploit attacks. Sting is a distributed system that automatically defends against new exploit attacks in three steps: (1) automatically detect new exploit attacks quickly and accurately, (2) automatically generate filters/signatures that can be used to filter out attack packets efficiently, (3) automatically disseminate the filters/signatures to vulnerable hosts and network-based intrusion detection systems to filter out attacks.

Sting employs a novel method, dynamic taint analysis on binaries, for automatic detection and analysis of software exploit attacks. This method allows us to pinpoint the vulnerability and how the vulnerability is exploited, as well as automatically generate anti-bodies (e.g., signatures/filters and hardened binaries) to filter out attack packets. Compared to previous defense mechanisms, Sting utilizes semantic information about the exploit attacks, and thus has a much lower false positive and false negative rate for detection with a much faster detection and reaction time. Since the attack detection and signature generation methods used in Sting do not require source code, Sting is easier to deploy and works on commodity software.

Moreover, Sting's signature generation aims to be effective even for polymorphic worms. By using both new semantic-based analysis (i.e., analysis based on the precise information about the vulnerability and exploit) and machine learning methods, Sting identifies parts in packets that need to stay invariant for an exploit to be successful (even in case of polymorphic worms). These invariants can then serve as signatures to filter out attack packets.

Thus, the signatures generated by Sting are more accurate than previous approaches and can be effective even against polymorphic worms.

In addition, I will also briefly describe another project of interest, TrafficComber, an automatic traffic analysis system that detects anomalies and correlations in network traffic and identifies misbehaving or malicious hosts using novel streaming algorithms and machine learning methods.