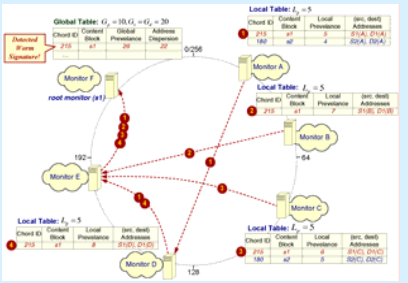
Worm Containment and DDoS Attack Defense

Min Cai and Yu Chen, {mincai, cheny}@usc.edu

WormShield: Collaborative Internet Worm Containment

- A distributed worm *signature detection* and *dissemination* system deployed at multiple edge networks
- *Distributed aggregation trees* (DATs) are constructed to aggregate global information
- A signature is identified if both the *global prevalence* and *address dispersion* are greater than thresholds
- Signatures are disseminated to other monitors using *efficient broadcasting* on Chord overlay



Related Publications:

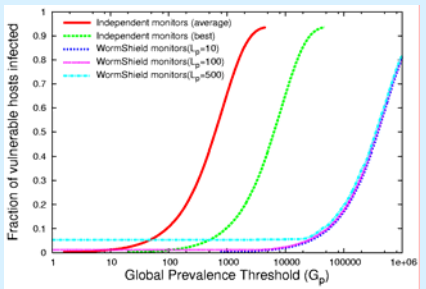
[1] M. Cai, J. Pan, Y.-K. Kwok, K. Hwang, "Fast and Accurate Traffic Matrix Measurement Using Adaptive Cardinality Counting," in *ACM SIGCOMM Workshop Mine-Net'05*, 2005.

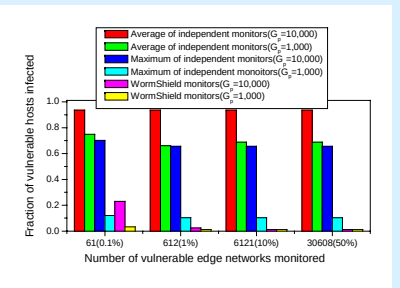
[2] M. Cai, R. Zhou, K. Hwang, C. Papadopoulos, and S. Song, "WormShield: Collaborative Worm Signature Detection Using Distributed Aggregation Trees," *NSDI'05 Poster*, Boston, 2005.

[3] M. Cai, K. Hwang, Y.-K. Kwok, S. Song, Y. Chen, "Collaborative Internet Worm Containment," in *IEEE Security and Privacy* Magazine, June 2005.

Large-scale Worm Simulation Results

- Simulated CodeRed-like worms on an Internet configuration of 105,246 edge networks and 338,562 vulnerable hosts
- Use BGP table snapshot on July 19th, 2001 from RouteViews
- Collaborative monitors detect signatures about 10 times faster than using independent monitors when G_p=10,000
- About 27 times reduction of infected hosts as 1% of vulnerable edge networks being monitored





Defense against Shrew DDoS or Reduction-of-Quality (RoQ) Attacks

- Periodic shrew DDoS attacks throttle legitimate TCP flows by creating low-rate pulsing type of congestions
- Characterized as stealthy and harder-to-detect attacks beyond the capability of ordinary traffic volume analysis tools
- Cause more damages as the victims may not be aware of the shrew attacks for a long time

Related Publications:

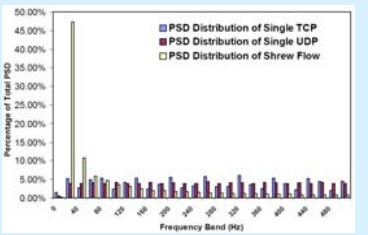
[1] Y. Chen, K. Hwang, and Y.-K. Kwok, "Collaborative Defense against Periodic Shrew DDoS Attacks in Frequency Domain," *ACM Transactions on Information and System Security (TISSEC),* submitted May, 2005

[2] Y. Chen, K. Hwang, and Y. K. Kwok, "Filtering of Shrew DDoS Attacks in Frequency Domain," *the First IEEE LCN Workshop on Network Security* (WoNS-2005), Sydney, Australia, November 15-17, 2005

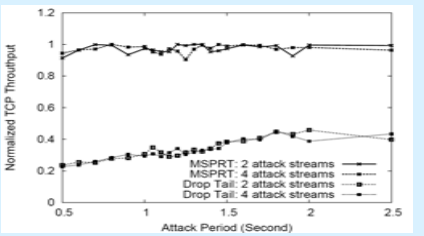
[3] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: Halting Anomalies with weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks," *IEEE ICCNMC 2005,* China, August 2-4, 2005.

NS2 Simulation Experiments and Research Findings

- The defense solution is based on the recognition of very low power spectral distribution in shrew DDoS flows
- Through NS2 simulation experiments, we proved that the defense scheme can effectively segregate malicious shrew DDoS flows from the legitimate TCP flows
- The legitimate TCP flows are thus rescued under shrew attacks



Shrew DDoS attack flows present low frequency energy distribution compared with other Internet flows



Compared with *Drop Tail* algorithm, our scheme effectively saves TCP flows by filtering out the malicious flows