Adaptation = Vulnerability
Under RoQ Attacks

Mina Guirguis, Azer Bestavros and Ibrahim Matta

Denial of Service (DoS)

How: Subject a service to a load that exceeds its capacity!

Bad News:
- MyDoom $26B of lost productivity!!!

Good News:
- Takes a lot of resources to mount
- Easy to tell if a resource is under attack

RoQ Attacks on AQM

Adaptation is an Optimization Process

Adapation Versus RoQ

Drives the system to a quiescent, stable, efficient operating point

\[ \frac{d}{dt} x_r(t) = I(x(t), p_e(x(t))) - D(x(t), p_e(x(t))) \]

RoQ exploits STEADY-STATE behavior

Can Really Happen!

- Can’t trace-back
- Spoof source
- Destination may not exist
- Use zombies in round-robin fashion

Attack Shape: Square wave

TCP/AQM

Adaptation Goal: Match the sending rate to the connection’s fair share + stabilize the queue at a target level (AQM)

How: Connections observe packet losses and react to them through AIMD

RoQ Goal: sends packets at high rate—enough to cause lots of flows to slow down exponentially fast causing underutilization + queue oscillations and then shuts off. This process repeats, possibly through an online controller

Shrew attack

Attacker Maximizes Potency

- Marginal utility of attack traffic
- Various instantiations for damage and cost: Bandwidth, Delay Jitter
- Takes aggressiveness of attacker into account: Families of DoS attacks

Conclusions

1. Examining system dynamics is crucial
2. Introduced “Potency”, marginal utility of attack traffic
3. Need to develop more resilient adaptation mechanisms, for detection and taking counter-measures


This work was supported in part by NSF grants ANI-0095988, ANI-9986397, EIA-0202067 and ITR ANI-0205294. A paper partly based on this work has been submitted to IEEE ICNP 2004.