Adaptation = Vulnerability Under RoQ Attacks

Mina Guirguis, Azer Bestavros and Ibrahim Matta

BOSTON UNIVERSITY

Denial of Service (DoS)

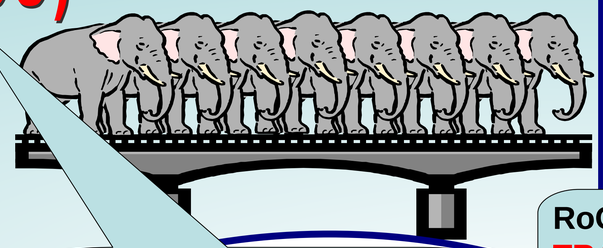
How: Subject a service to a load that exceeds its capacity!

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



DoS exploits STEADY-STATE behavior

RoQ exploits TRANSIENT behavior

Reduction of Quality (RoQ)

How: Subject a service to the minimum load that would produce the maximum damage

Bad News:

- Doesn't take a lot of resources
- Couldn't tell if under attack
- Higher potency than DoS and Shrew Attacks

Good News: None So Far

Attack Shape: Square wave

$$y(t) = \begin{cases} \delta & t \bmod T \leq \tau \\ 0 & \text{otherwise} \end{cases}$$

Adaptation Versus RoQ

Adaptation is an Optimization Process

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

Knocks the system off whenever it is about to stabilize

RoQ hinders convergence by disturbing prices fed-back to adaptation mechanisms

$$\frac{d}{dt}x_r(t) = \mathcal{I}(x(t), p_l(x(t))) - \mathcal{D}(x(t), p_l(x(t)))$$

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

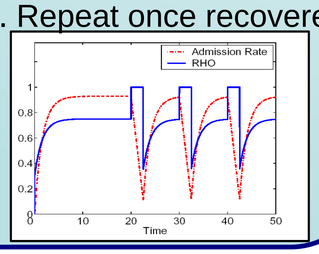
RoQ Goal: sends packets at high rate—enough to cause lots of flows to slow down exponentially fast causing underutilization + queue oscillations and then shuts off. This process repeats, possibly through an online controller

End-Systems

Adaptation Goal: Operation at a target utilization

How: Use PI controller to adjust the admission ratio

RoQ Goal: Drive the system to thrash, through injecting a lot of requests in a very short time. Repeat once recovered

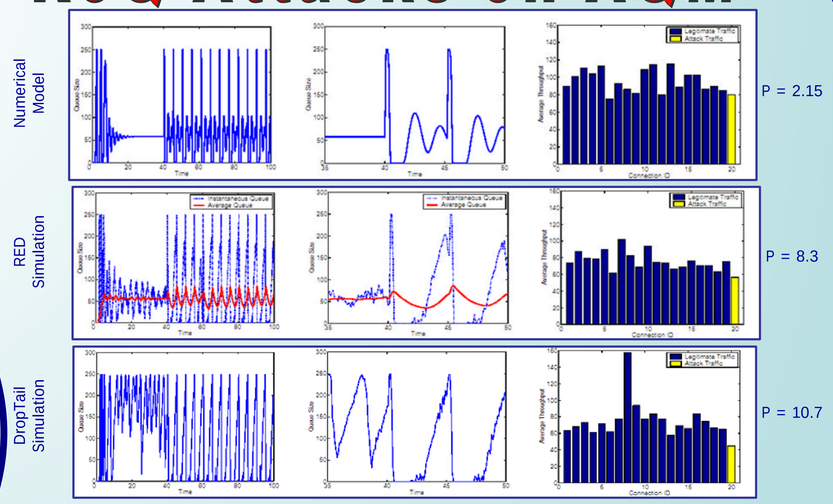


$$\text{Potency} = \Pi = \frac{\text{Damage}}{\text{Cost}^{\frac{1}{\Omega}}}$$

Attacker Maximizes Potency

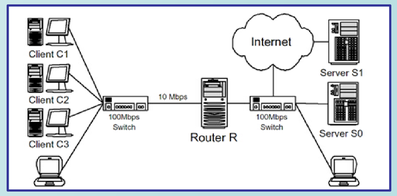
- **Marginal utility of attack traffic**
- **Various instantiations for damage and cost: *Bandwidth, Delay Jitter***
- **Takes aggressiveness of attacker into account: Families of DoS attacks**

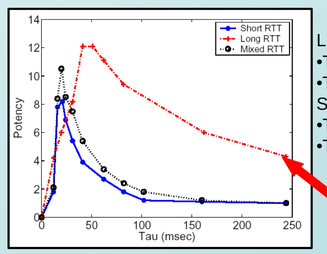
RoQ Attacks on AQM



Can Really Happen!

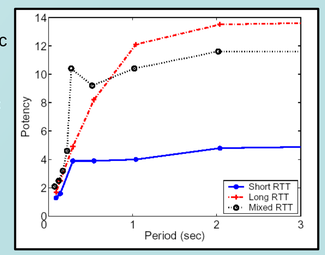
- Can't trace-back
- Spoof source
- Destination may not exist
- Use zombies in round-robin fashion





Long RTT : 120 msec
•T = 1040 msec
•Tau = 40 msec
Short RTT : 15 msec
•T = 270 msec
•Tau = 20 msec

Shrew attack



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

Reference : Guirguis, Mina; Bestavros, Azer; Matta, Ibrahim. Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources, Jan 30, 2004. BUCS Technical Report

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.