Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources*

Mina Guirguis
Dept. of Computer Science
Boston University
Boston, Massachusetts
msg@cs.bu.edu

Azer Bestavros
Dept. of Computer Science
Boston University
Boston, Massachusetts
best@cs.bu.edu

Ibrahim Matta
Dept. of Computer Science
Boston University
Boston, Massachusetts
matta@cs.bu.edu

Motivation and Overview of Work: Over the past few years, Denial of Service (DoS) attacks have emerged as a serious vulnerability for almost every Internet service. An adversary bent on limiting access to a network resource could simply marshal enough client machines to bring down an Internet service by subjecting it to sustained levels of demand that far exceed its capacity, making that service incapable of adequately responding to legitimate requests. In that sense, DoS attacks can be regarded as exploiting the system's steady-state capacity. In this work, we turn our attention to unorthodox adversarial attacks, which we term Reduction of Quality (RoQ) attacks, that exploit the transients of a system's adaptive behavior, as opposed to its limited steady-state capacity. Modern computing and networking systems rely on adaptation to drive the system into quiescent regions of operation that would maximize the overall system's gain, in addition to being stable, fair and efficient. In this work, we analytically capture the effect of RoQ attacks that would deprive an Internet element from reaching steady state by knocking it off whenever it is about to stabilize. For instance, an attacker can continually disturb the stability of a router by affecting the congestion signals (prices) fed back to the rate-adaptive sources. We formalize the notion of attack "potency", which exposes the tradeoff between the "damage" inflicted by an attacker (*e.g.*, waste in bandwidth) and the "cost" of the attack (*e.g.*, average attack rate). Moreover, our notion takes aggressiveness into account(*i.e.*, the level of exposure risk that the attacker is willing to take), enabling us to identify different families of DoS attacks based on their aggressiveness. We give examples of RoQ attacks on a number of common adaptive components currently incorporated in computing and networking systems. But below, we only focus on network adaptation, keeping in mind the bigger range of applicability of RoQ attacks on other systems.

Network Adaptation Mechanisms and Vulnerabilities: End system protocols (*e.g.,* TCP) rely on feedback mechanisms to adapt their sending rates to match their "fair share" of network resources. Buffer management schemes play an important role in the effectiveness of transmission control mechanisms as they constitute the feedback signal (by marking or dropping packets) to which such mechanisms adapt. Active Queue Management (AQM) techniques have been developed that try to maintain the queue size at a target level and employ probabilistic dropping. Stabilizing the queue at a low target guarantees efficiency while minimizing jitter and round trip time in general.

Attack Definition: We focus on attack techniques that would hinder an AQM from stabilizing its queue, and hence resulting in a noisy feedback signal to the end-system transmission controllers, which in turn would lead to high jitters due to oscillations, unfairness as well as inefficiencies due to queue drainage, *i.e,* the input rate can't saturate the link capacity. For simplicity, we consider an attack comprising a burst of M packets transmitted at the rate of δ packets per second over a short period of time τ. This process is repeated every T units of time.

Attack Goal: We define Π, the *attack potency*, to be the ratio between the *damage* caused by that attack and the *cost* of mounting such an attack. Clearly, an attacker would be interested in maximizing the damage per unit cost—i.e., maximizing the attack potency.

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

The above definition does not specify what constitutes "damage" and "cost". In this work , we consider various instantiations of these metrics(e.g., bandwidth, delay jitter, etc..). Ω is introduced to model the aggressiveness of the attacker. Our results confirm that RoQ attacks can degrade the performance of any AQM scheme, degenerating them to Drop-Tail, while injecting the minimum attack traffic. Moreover, RoQ attacks can achieve higher potency than "shrew" (targeting timeouts in TCP) and DoS attacks (brute-force).

Vulnerability Assessment: We used a control-theoretic model to underline the complex interplay between the efficiency-load behavior of a resource and the adaptation mechanisms of both the resource and its consumers. The adaptation is modeled as an optimization process driving the system to a quiescent stable operating point. An optimized RoQ exploit would then keep the system oscillating between different states, in presence and absence of the attack traffic. We developed associated metrics to quantify the system's vulnerabilities. We present numerical and simulation results, which we validate with observations from real Internet experiments. We are currently investigating adaptation mechanisms that are more resilient to these new forms of attacks by exploiting tradeoffs between performance and vulnerability. Our plan is to develop efficient techniques for the detection of RoQ exploits when they do occur as well as invoking proper counter-measures.

URL: `http://cs-people.bu.edu/msg/research/roq`

Reference: M. Guirguis, A. Bestavros and I. Matta. *Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources*, To appear in ICNP 2004, Berlin, Germany.

*This work was supported in part by NSF grants ANI-0095988, ANI-9986397, EIA-0202067 and ITR ANI-0205294.