# Reduction of Quality Attacks on Content Adaptation Mechanisms

Joshua Tharp, Mina Guirguis

*Department of Computer Science*
*Texas State University*
*601 University Drive, San Marcos, Texas, USA*
{jt1238,msg}@txstate.edu

**Motivation and Overview of Work:** Internet server farms and grid computing architectures employ sophisticated adaptation mechanisms to mitigate overload conditions. Of those widely used are: admission controllers, load balancers and content adaptation controllers. For example, server farms experience performance degradation as more clients connect and submit requests to the servers and as the number of requests increase, the servers will experience an increased strain on their resources eventually reaching the point of overload. To prevent and mitigate such overload conditions, one (or more) of the above mechanisms is typically present. This work focuses primarily on content adaptation controllers and their security implications.

In a content adaptation setting, the content adaptation controller decides the quality of the content being served, based on the measured load from the servers [1]. Serving degraded content requires fewer resources to deliver, whether it is a smaller web-page, smaller or less embedded objects, or less intensive database calls. As long as serving degraded content relieves stress on the servers, the servers can keep serving clients without reaching a point of overload, where they have to drop or refuse the admission of new clients.

The presence of content adaptation controllers while ensures optimized performance during overload conditions, it opens a door for a new instantiation of Reduction of Quality (RoQ) attacks to be mounted [2]. Unlike traditional Denial of Service (DoS) attacks, where an attacker saturates a given system with a sustained load so that it becomes unresponsive over the period of attack, RoQ attacks induce constant oscillations between overload and underload states, without sustaining the attack traffic. This is achieved by timing the attack traffic and its magnitude to exploit the dynamics of the system. The example below illustrates this point.

**An illustrative Example:** Consider a content adaptation controller that sets the quality level of the content served based on the measured load from the server(s). Now, consider a point in time when the offered load is low enough for the server to serve full content to all requests. At this point, an adversarial burst in demand arriving in a very short time would push the server into overload. This, in turn, would trigger the content adaptation controller to reduce the quality of the served content in order to bring the server out of this overloaded state. Due to the server thrashing, recovering from such conditions takes a long period of time. But once the servers recovers from the effect of this burst and stabilizes, the attacker would repeat this process.

**Methodology and Vulnerability Assessment:** We used a discrete-time model to capture the impact of RoQ attacks on a content adaptation controller. An optimized RoQ attack keeps the system oscillating between different states, in the presence and absence of the attack traffic. We present numerical results, which we validate with observations from real Internet experiments performed in our lab.

We assess the impact of RoQ attacks through the potency metric, where an attacker is interested in maximizing the damage per unit cost—i.e., maximizing the attack potency [2]:

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

where $\Omega$ is introduced to model the aggressiveness of the attacker. This project investigates different instantiations for "damage" and "cost". For example, The "cost" of an attack can be instantiated as the magnitude of the attacking burst. The "damage" can be instantiated as the number of legitimate requests receiving degraded content, the increase in their response time, and the number of timeouts occurring, among others metrics.

Through the potency metric, this project explores: (1) the most effective attack orchestration that causes the maximum damage or the maximum damage per unit cost, (2) the extent to which defense mechanisms can detect and defend against RoQ attacks, and (3) the impact of different parameters in exposing the trade-offs between vulnerability and resilience against RoQ attacks.

**RoQ Attacks Web-site:** http://csr.bu.edu/roq

## References

[1] T. Abdelzaher and N. Bhatti,"Web content adaptation to improve server overload behavior," in Eigth International World Wide Web Conference, Toronto, Canada, May 1999.

[2] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang. "Reduction of Quality (RoQ) Attacks on Internet End Systems". In Proceedings of INFOCOM, Miami, Florida, March 2005.