Denial of Service Attacks and Defenses

The purpose of Information Technology is to enhance and streamline the core competencies of your business. However, when IT security is compromised, it quickly becomes priority one. Through flexible, full-service **Managed Services** or **Project Consulting** engagements, Casaba helps companies of all kinds identify and correct vulnerabilities so they can focus on their core business.

Denial of Service (DoS) Testing

Overwhelming a system's processing resources in an attempt to deny service to legitimate users is a tactic often used to distract attention from more harmful attacks, or simply to cause chaos for its own sake. Classic Denial of Service (DoS) attacks typically assault an organization's network with a high volume of traffic. There are well-established procedures in place to stress test networks and measure and manage their tolerance for load-based DoS attacks.

Casaba's expertise, however, is concentrated on the far more challenging realm of application-layer Denial of Service, which requires a highly specialized set of skills and knowledge. Rather than merely pile load on a system, those who target the application typically employ a more tactical, "asymmetrical" approach that confuses the application's logic with minimal input that eats up far more processing power than it should.

For example, asking an application to decrypt a password of extraordinary length takes little effort on the side of the perpetrator, yet can tie up the application and underlying server for an indefinite amount of time. The same goes for deadlocks, spins and other asymmetrical attacks.

There is an art to anticipating and countering these types of DoS attacks. It requires a deep knowledge of an application's architecture and functionality, as well as a thorough understanding of the way a hacker thinks. As with most aspects of IT security, there is no such thing as 100% protection from DoS attacks. Resistance is the name of the game.

Casaba has extensive experience implementing strategies that can be very effective when executed with skill and creativity, particularly those commonly known as throttling and traffic shaping. Simply put, throttling controls the amount of processing committed to specific requests by quickly identifying and rejecting potential malicious activities. Traffic shaping employs rules and requirements designed to reset the symmetry between the system and the user.

The Casaba Approach and Process

Our team's rich competencies in code review, fuzz testing and security planning can all come into play when helping our clients make key decisions regarding the flow and configuration of authentication, input validation, parsing, encryption and other application security processes that can be tricked into initiating a debilitating drain on resources.

Casaba can work with you to apply these and other strategies to mitigate risk in the context of your operational goals and overall security framework.

About Casaba

Casaba is a strongly integrated team of security pioneers with a reputation for relentlessly researching, developing, and implementing innovative solutions to the most difficult security problems. We are prepared to assist in every phase of security consulting and auditing, and we are fully bonded and insured by Lloyds of London.

Get Started

Contact us today for a free consultation and security review:

- Phone: 1-888-869-6708
- Email: info@casaba.com
- Web: www.casaba.com