Chapter 1.1 E-Government and Denial of Service Attacks

Aikaterini Mitrokotsa
University of Piraeus, Greece

Christos Douligeris
University of Piraeus, Greece

ABSTRACT

The use of electronic technologies in government services has played a significant role in making citizens' lives more convenient. Even though the transition to digital governance has great advantages for the quality of government services it may be accompanied with many security threats. One of the major threats and hardest security problems e-government faces are the denial of service (DoS) attacks. DoS attacks have already taken some of the most popular e-government sites off-line for several hours causing enormous losses and repair costs. In this chapter, important incidents of DoS attacks and results from surveys that indicate the seriousness of the problem are presented. In order to limit the problem of DoS attacks in government organizations, we also present a list of best practices that can be used to combat the problem together with a classification of attacks and defense mechanisms.

INTRODUCTION

Since we live in a world where electronic and Internet technologies are playing an important role in helping us lead easier lives, local and state governments are required to adopt and participate in this technology revolution. Digital government or e-government technologies and procedures allow local and national governments to disseminate information and provide services to their citizens and organisations in an efficient and convenient way resulting in reducing waiting lines in offices and in minimizing the time to pick up and return forms and process and acquire information. This modernization of government facilitates the connection and cross cooperation of authorities in several levels of government—central, regional, and local—allowing an easy interchange of data and access to databases and resources that would be impossible otherwise.

E-government undoubtedly makes citizens' lives and communication easier by saving time, by avoiding and bypassing the bureaucracy, and by cutting down paper work. It also provides the same opportunities for communication with government not only to people in cities but also to people in rural areas. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes.

This shift to technology use and the transition to a "paperless government" is constantly increasing. According to Holden, Norris, and Fletcher (2003), in 1995 8.7% of local governments had Web sites, while in 2003 this number showed an increase that reached 83%. Despite these encouraging statistics, the adoption of digital government proceeds with a slow pace as security issues, like confidentiality and reliability, affect the fast progress of e-government. Since e-government is mainly based on Internet technologies, it faces the danger of interconnectivity and the well-documented vulnerabilities of the Internet infrastructure. The Institute for E-Government Competence Center (IFG.CC, 2002) states that in 2002, 36 government Web sites were victims of intrusions. Most of the e-government attacks have taken place in Asia (25%) and more precisely in China and Singapore (19%), as well as in the USA (19%).

According to the U.S. Subcommittee on Oversight and Investigations (2001), the FedCIRC incident records indicate that in 1998 the number of incidents that were reported was 376, affecting 2,732 U.S. Government systems. In 1999, there were 580 incidents causing damage on 1,306,271 U.S. Government systems and in 2000 there were 586 incidents having impact on 575,568 U.S. government systems. Symantec (2004) (Volume VI, released September 2004, activity between January 2004 and June 2004) gives information about Government specific attack data. In this report, one can see that the third most common attack e-government has faced, besides worm-related attacks and the Slammer worm, is the TCP SYN Flood denial of service attack.

So in order to have effective e-government services without interruptions in Web access as well as e-mail and database services, there is a need for protection against DoS attacks. Only with reliable e-government services not threatened by DoS attacks governments may gain the trust and confidence of citizens.

Moore, Voelker, and Savage (2001) state that the denial of service (DoS) attacks constitute one of the greatest threats in globally connected networks, whose impact has been well demonstrated in the computer network literature and have recently plagued not only government agencies but also well known online companies. The main aim of DoS is the disruption of services by attempting to limit access to a machine or service. This results in a network incapable of providing normal service either because its bandwidth or its connectivity has been compromised. These attacks achieve their goal by sending at a victim a stream of packets in such a high rate so that the network is rendered unable to provide services to its regular clients.

Distributed denial of service (DDoS) is a relatively simple, yet very powerful, technique to attack Internet resources. DDoS attacks add the many-to-one dimension to the DoS problem making the prevention and mitigation of such attacks more difficult and their impact proportionally severe.

DDoS attacks are comprised of packet streams from disparate sources. These attacks use many Internet hosts in order to exhaust the resources of the target and cause denial of service to legitimate clients. DoS or DDoS attacks exploit the advantage of varying packet fields in order to avoid being traced back and characterized. The traffic is usually so aggregated that it is difficult to distinguish between legitimate packets and attack packets. More importantly, the attack volume is often larger than the system can handle. Unless special care is taken, a DDoS victim can suffer