King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

COE 540 – Computer Networks (T082)

Project Description – (Modified: Sunday 22/03/2009)

Introduction:

The Internet has become an essential means for reachability and communication in the new information age. From a strategic point of view for the Kingdom of Saudi Arabia (KSA), it is very critical to improve the Internet resilience including not having to rely on a single international Internet Service Provider (ISP) for providing Internet connectivity to the country.

Causes for the Internet unavailability or outage can be categorized into either non-malicious or malicious including hardware and/or software failures, denial of service attacks, terrorists' attacks, and deliberate denial of Internet access by ISPs. The initial literature review in the area of Internet availability and resilience classified the Internet unavailability causes and found that they occur at three levels: application, routing, and physical. The current status of the literature indicates that the subject of deliberate denial of Internet access by the ISPs has not been researched, and no known commercial solutions are available to address the issue. Thus, the main objective of this project involves investigating the Internet unavailability due to the malicious act of denial of Internet access by international ISPs, and proposing effective counter measures to increase the resilience of Internet services. Furthermore, the project is to address this specific cause at the application level (at the root DNS level to be more specific). The developed solution should follow the standards as closely as possible, be suitable for deployment for typical local and global needs, and require a minimal additional cost. Finally, the recommended solution will be further tested and evaluated through simulations.

Project Requirements:

Devise a peer-to-peer solution to address the Internet unavailability due to the malicious act of denial of Internet access by international ISPs at the root DNS level. To achieve that requirement the following steps are needed:

1. Perform an extensive literature review of peer-to-peer solutions that have been proposed to address the Distributed Denial of Service (DDoS) attacks on the root DNS servers.
2. Identify a peer-to-peer solution from step (1) that can be possibly used to address the Internet unavailability due to the malicious act of denial of Internet access by international ISPs at the root DNS level.
3. Based on step (2), outline your proposed peer-to-peer solution. The devised peer-to-peer solution should follow the standards as closely as possible, be suitable for deployment for typical local and global needs, and require a minimal additional cost.
4. Test and evaluate the proposed peer-to-peer solution through simulations.

Deliverables:

	Deliverable	***Deadline***	***Weight***
1.	• Progress report (1): Literature review.	***04/14/09***	**04%**
2.	• Progress report (2): Identify the selected DDoS peer-to-peer solution, and your proposed peer-to-peer solution for the malicious act of denial of Internet access by international ISPs at the root DNS level.	***05/05/09***	**04%**
3.	• Progress report (3): Preliminary simulation results.	***26/05/09***	**05%**
4.	• Publication-quality term paper. • Presentation slides. • Final report.	***16/06/09***	**12%**

Notes:

1. You can work in teams of at most 2 students.
2. You can consult Dr. Farag Azzedin (ICS) on peer-to-peer issues.