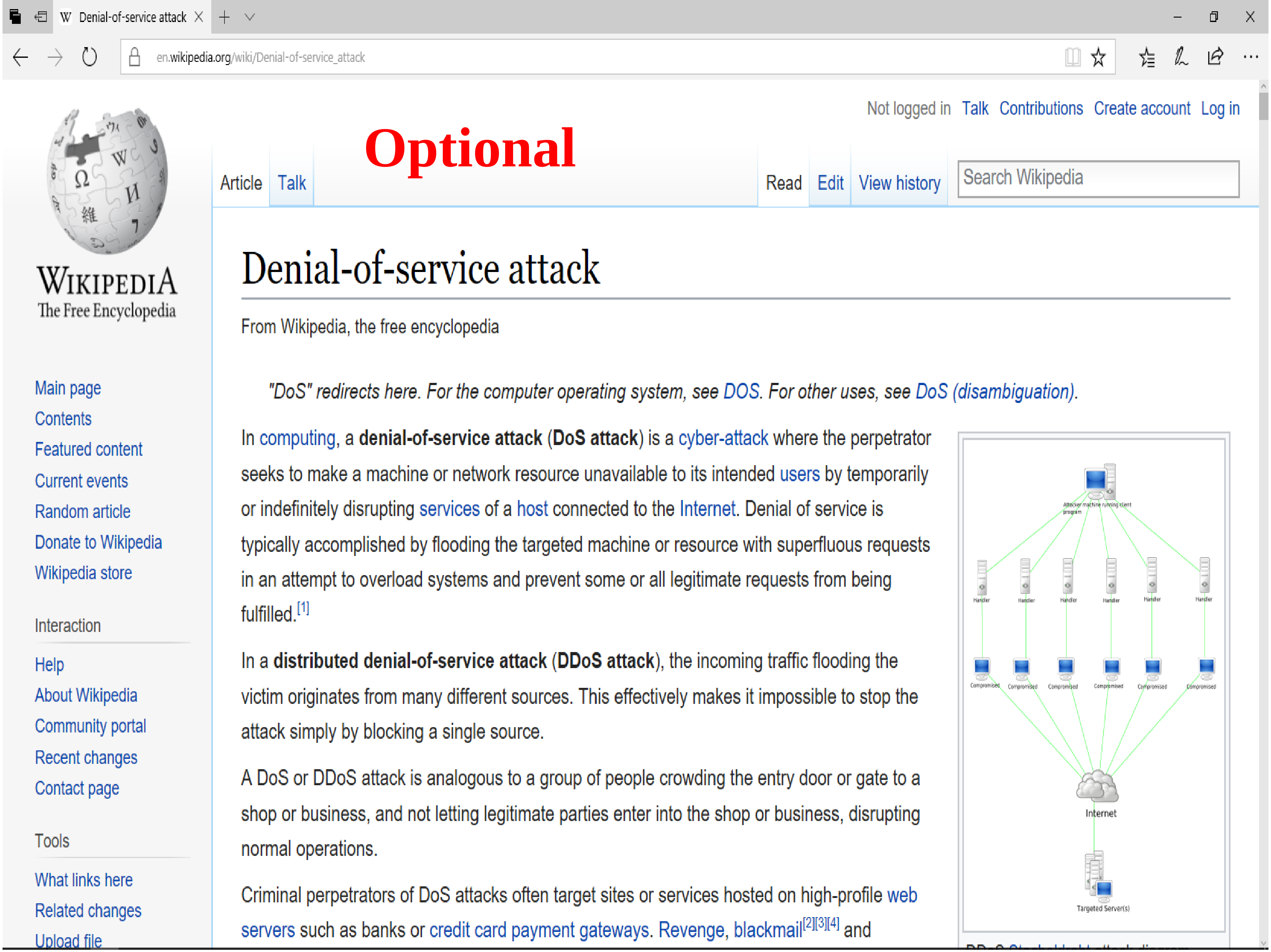
Assignment #3: Due October 27

1. Read Chapter 2 of Textbook #1: TCP/IP Sockets in Java, but you may skip Section 2.3 UDP Sockets.
2. Fully understand how TCPEchoClient.java & TCPEchoServer.java work, which I explained in class in great detail.
3. Answer Question #4 of Section 2.4 Exercises (on page 38), but ignore the part that involves UDPEchoServer.java.
4. Based on your answers to Step 3, or more specifically, your answers to "Examine the server examples (TCPEchoServer.java in our case) and list anything you can think of that a client might do to cause it to give poor service to other clients," revise TCPEchoClient.java to implement such a client, which I call a **bad client**. Your **bad client** should attempt to cause the server to provide poor services, in at least 2 different ways. ***(5 points, 2.5 for each bad behavior)***

Assignment #3: Due October 27

5. Based on your answers to Step 3, or more specifically, your answers to "Suggest improvements to fix the problems that you find," revise TCPEchoServer.java to incorporate those improvements. You can call this improved server a **bullet-proof** server. ***(5 points, 2.5 for each improvement)***
6. Submit i) your answers to Step 3, ii) the revised client program (the bad client) resulting from Step 4, and iii) the improved server programs (the bullet-proof server) resulting from Step 5, via Blackboard.
7. Please compile and test your Java programs before submitting them to Blackboard.
8. Please bring your questions about any aspect of this assignment to the class, if possible, so that I don't have to repeat myself many times during my office hours. Thank you very much.



Optional

Denial-of-service attack

From Wikipedia, the free encyclopedia

"DoS" redirects here. For the computer operating system, see DOS. For other uses, see DoS (disambiguation).

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]

In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail[2][3][4] and