Tasks to be accomplished in Weeks 12 through 14 (11/20 - 12/10):

1. Read textbook Chapter 7 (skip math/hash/encode/decode formula).
2. In Discussion Board forum for this time period, answer the following question by clicking on the reply link for the question (you can incrementally post your answer by modifying your already posted answer; please don’t spread your answer into multiple postings):
   a. Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.
      i. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm
      ii. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).
      iii. Replay Attack: Earlier SSL handshake messages are replayed.
      iv. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
      v. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.
      vi. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.
      vii. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.
      viii. SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the “half-open connection” around for a few minutes. Repeated SYN messages can clog the TCP module.
3. In Discussion Board forum for this time period, provide your concise answer to the following Course Research Project:
   Within five years the Internet will be replaced by Internet 2 (http://www.internet2.edu/) as the commercial network platform. Internet 2 is supposed to be hundreds-time faster than the Internet and will greatly improve real-time multi-media services. In 2001 I participated in an NSF grant application for providing Internet 2 connectivity to Pace University. But so far our staff still hesitates to connect Internet 2 to our School servers due to security concerns. Please list the major new security issues in the Internet 2 environment. Please use your own language to summarize concisely what you learn on the Web and make sure your fellow students can understand your logics.
4. Take an open-book quiz 6 in Blackboard Course Documents from 9am of December 8 to 10pm of December 10. You must complete your quiz within one hour in a single session. Make sure
you don’t leave the quiz Web page during your quiz session, and you click on the Submit button at the end of your session. If accidents happen and you cannot access your quiz again, send me an email and I will reset the quiz for you. All the quiz questions are conceptual, and they check your understanding of the topics covered in the recent five weeks and whether you have completed the assigned tasks for the time period.

**Important concepts/terms worth attention:**

IPSec, Secure Socket Layer (SSL), TCL, SSL architecture, SSL session, SSL connection, SSL handshake protocol, Secure Electronic Transaction (SET), SET architecture, SET process for e-commerce transactions.