1.264 FINAL EXAM
FALL 2012

NAME _____

Exam guidelines:

1) 80 minutes are allowed to complete the exam.
2) Open notes; open book.
    a. You may use a web browser on a laptop computer to access the online course texts. No other web pages may be accessed and no other applications may be open at any point during the exam.
3) There are 4 questions (100 points) and 8 pages (including this one) in the exam booklet.
4) Laptops are allowed to access online course books. No cell phones or messaging devices are allowed. Please turn off any that you have brought.
5) Calculators are allowed.
6) Please write legibly – you are welcome to use both sides of the paper; we can provide additional paper if necessary.

PART I: WEB SERVICES AND TELECOM
(60 POINTS; SUGGESTED TIME: 50 MINUTES)

An airline operates a set of flights. A flight has a flight number, an origin airport and a destination airport. All flights operate daily. When a passenger books a ticket, the airline registers their name, and assigns them a specific seat on a flight on a departure date. Assume all simple types are #PCDATA, except airports, which are either "BOS", "SJU", "SFO", "JFK", "DCA" or "MAD".

1. Write a DTD file for the airline's set of flights and passenger info. The first line is provided. You may wish to draw a data model and write the XML file (part 2) first. (15 points)

<?xml version "1.0" encoding "iso-8859-1"?> (PROVIDED)

2. Write an XML file that conforms to the DTD that you created in the previous step. Create 2 flights on 2 dates with 2 passengers per flight. (15 points)

a. XML File

b. How will the airline alter the tag names when sending XML to a partner airline, if a partner's XSD or DTD is slightly different for a request or response? (2 points)

c. Can the XML file be sent as a Web service response to a request? What are the parameters in the request? (2 points)

d. Your airline sends just XML documents to each gate at each airport. What XML standard must a manager at an airport use to display the XML that is sent, so he or she can read it formatted well in a browser? (3 points)

e. Your airline is expanding to several airports in Africa, each served by a VSAT terminal with a bandwidth of 9.6 kbps. You send 500 XML messages per hour to each airport; there are many changes in reservations and connections. The XML messages use the format you defined in part (2a) above, and contain 1200 characters (bytes) on average. This XML message traffic is 90% of the traffic on these VSAT links. Will a VSAT link provide sufficient bandwidth to an airport? If not, suggest changes that would make this workable. (4 points)

f. Should your African airports validate each XML message against the DTD published on your Web site, by getting the DTD from the Web site for each message received, or is there a simpler procedure that is acceptable? (3 points)

g. What technology would you use if you were in the same city as the VSAT carrier and you wanted to do this at lowest cost? The VSAT carrier has access to the open Internet and also subscribes to a carrier's Metro Ethernet service, which would cost you $3,000 per month to use and provides 1 Gbps. You are two miles from a central office that offers a wide range of data services, and you are served by a CATV company that offers data services at your location. The telco (central office), CATV and open Internet services cost about $300 per month for 1.5 Mbps (3 points).

h. In question (g), what security measures would you use? Briefly justify. (3 points)

i. Does each African airport need a Web server for its end of these transactions? An app server? A database server? Explain why or why not. All applications used by any airport are provided from the airline's main data center and are accessed via Web browsers. (3 points)

j. Does each African airport need a load balancer? A firewall? A router? Explain why or why not. (3 points)

k. The CATV carrier serving one of the African airports offers you dedicated use of one 6 MHz CATV channel over which you can run Ethernet between the airport terminal and your maintenance facility on the other side of the airport. The signal-to-noise ratio of this channel is 27; the maximum utilization for Ethernet is 50%. What is the bandwidth, in megabits per second (Mbps), of this channel? Would this be sufficient to stream 4 MPEG-2 (6 Mbps) high-quality security video feeds between the terminal and the maintenance facility? (4 points)

PART II: SECURITY (40 POINTS; SUGGESTED TIME: 30 MINUTES)

3. Medical Supply Chain Security (20 points)

a. Outline how an attack can be launched against a user with a laptop at an Internet café who logs into a medical supply chain Web site from an http (not https) home page, even if all subsequent pages are https (SSL) pages. (7 points)

b. Suppose the supply chain companies form a consortium to issue password generator cards that create a new 8 digit passcode every 30 seconds (e.g., Secure-ID) to all their employees. The employee must enter this 8 digit code as part of their password. (There is also a fixed password that the employee chooses and enters, as usual.) They leave their home pages as before (http, but with all pages after login as https). Does this combat the attack in part a above? (7 points)

c. What new vulnerability, if any, has the consortium introduced in part b above? (3 points)

d. Some of the password generator cards are stolen, or not returned by employees who leave their companies. Is this a security risk? Briefly give your reasons pro or con. If it is a risk, describe at least one attack that can be executed with a stolen password generator card. (3 points)

4. Truck at a Security Gate (20 points)

a. Write the protocol notation for the following security system: (5 points)

- Truck pulls up to gate at terminal
- Truck electronic card sends its id and a nonce (sequential number) to gate, encrypted with gate public key
- Gate checks its database, opens if ID is valid and nonce is greater than the last nonce sent, unless last nonce sent and stored in database was largest number possible. In that case, any nonce is accepted

b. List at least two possible attacks against this protocol that may succeed. (10 points)

c. List one possible attack against security protocols that this protocol can usually withstand. (5 points)

1.264J / ESD.264J Database, Internet, and Systems Integration Technologies
Fall 2013