**TAKE HOME EXAM – CSCE 813**
**TEST 3**
**Fall 2006**

**RETURN (hard copy) BY December 11, 2:00 pm**

**Name:**
**e-mail:**

You may use any materials to answer the questions, however, you need to present YOUR solution and not the copy of a reference material. Include all URLs, references you used (was inspired by) for each answer. Staple all papers before submitting.

**This must be individual work!**

**Warm Up**

**1. (*10 points*) – Internet Security**

In discussing AH processing, it was mentioned that not all of the fields in an IP header are included in MAC calculation.

- (*5 points*) For each fields in the IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable. Justify your decision for each field.
- (*5 points*) Do the same for the IPv6 header and IPv6 extension headers. Justify your decision for each field.

**2. (*15 points*) -- CSP**

Suppose that someone suggests the following way to confirm that the two of you have the same secret key: you create a random bit string the length of the key, XOR it with the key and send the result to the other party. Your partner XORs the received message using the secret key and sends the result to you. If the result is the original random string, then you know that both of you have the same secret key, yet neither of you ever transmitted the secret key.

- (*5 points*) Model the protocol using CSP, including the security requirement of key secrecy.
- (*5 points*) Is this protocol secure? Justify your answer.
- (*5 points*) Show the attacker model of your justification and all the information the attacker can infer.

**Let's get serious**

## 3. (*25 points*) – WS Federation

Distributed authentication over different web services (WS) is a serious problem. If a user U wants to use services of WSs A, B, C, and D, each time U requests a new service he has to be authenticated by A, B, C, and D. This is very inconvenient for U as well as extra work for A, B, C, and D. A potential solution is to form a federation of A, B, C, and D; and support authentication of users via the federation.

- (5 points) Describe the problem of identity management for WS federation.
- (10 points) Propose an architecture for WS federation to
    - simplify user authentication and
    - support the enforcement of the access control requirements over the components and the federation
    - briefly describe your architecture
- (5 points) How identity management and federated access control are supported by the relevant WS standards? -- be brief (max. ½ page)
- (5 points) Extend your model such that U's identity is not revealed to A, B, C, and D, however there is a way that U can be billed for the requested services, i.e., provide accountable anonymity for the user.

## 4. (20 *points*) – AVISPA

In this exercise you practice with the AVISPA tool for protocol analysis. For this, you can use the web interface without downloading the tool. The web interface is at http://www.avispa-project.org/web-interface/

First, look at the Needham-Schroeder Public-Key Protocol that supports mutual authentication of the two communicating parties. The demo representation of this protocol is the test file: NSPK-KS-fix.

- (5 points) Run the test NSPK-KS-fix test file and interpret the results and include the result files.
- (10 points) Modify the model such that only Bob is authenticated to Alice but Alice is not authenticated to Bob. Show the modifications of the original model (e.g., underline the changes).
- (5 points) Interpret you results and include the result files.

## 5. (*15 points*) – WS Security and Process Choreography

Read the article "Adding BPEL to the Enterprise Integration Mix"
by Praveen Chandran and Arun Poduval, available at
http://www.oracle.com/technology/pub/articles/bpel_cookbook/chandran.html Based on this article (*5 points*), other articles of your finding (*5 points*), and you own expert knowledge (5 *points*), evaluate the impact of BPEL on Web Services security.

**Cool Down**

**6. (*15 points*) – Internet Security**

Briefly describe 3 different approaches (max. ½ page each) to support secure remote login to an intranet. List the advantages and disadvantages of each approach.

---

BONUS

*(5 points)*

In electronic commerce, one might want to make a purchase anonymously. One may also want to complain if one receives poor service (or the wrong goods). Can you think of some ways to reconcile these properties? What additional information is needed from the purchase protocol to accomplish this?