Examination 3
CEN 5540 Computer and Network Security
23 June 2000

Instructions:

• Failure to follow instructions may result in loss of points.
• Do not start the examination until instructed to do so.
• This test is closed book, but you may use one 8.5” by 11” sheet of notes you have prepared.
• Answer two (2) questions below.
  • Start the answer to each question on a new page (i.e., do not put the answer to more than one question on the same page).
  • Show your work.
  • Clearly label your answers with the numbers as given in the exam below.
  • Assemble your answers in numerical order of the questions when you submit them.
• Leave a 1” square in the upper left corner for a staple.
• Be sure to include your name on your answer sheets.
• You have 60 minutes to complete this examination.

• Read and sign the following statement. You may write this on your exam and sign it there if you wish to take the exam questions home with you today. Do not discuss this exam with anyone in this course who has not yet taken this exam.

On my honor, I have neither given nor received unauthorized aid on this examination, and I will not discuss the contents of this examination with any student who has not yet taken this examination.

Signed:
1. (a) (5) Explain how both Nancy and Pete can verify that the other has not cheated in the Oblivious Transfer protocol. Exactly how do they know the other has not cheated, and what information is necessary for them to do this?

(b) (4) Show how the Mental Poker protocol can be adapted to perform the same function as Oblivious Transfer. Prove informally that it performs the job correctly.

(c) (6) Oblivious Transfer allows for “flipping a fair coin” in a distributed manner. Can the protocol be altered to “rolling a fair die” (i.e., picking one out of six possible choices) in a distributed manner? Provide such a protocol based on Oblivious Transfer and argue its correctness, or argue that it is not possible.

2. (a) (5) What are the most obvious shortcomings in BAN logic? Explain.

(b) (10) Use BAN logic to analyze the following protocol. \(N_x\) is a nonce generated by \(X\), \(K_{x,y}\) is a symmetric key used by \(X\) and \(Y\). Be sure to include needed assumptions and indicate any of the usual goals that are not achieved by the protocol. If there is a goal not achieved by this protocol, how may it be achieved?

\[
\begin{align*}
M_1: & \quad A \rightarrow B: \quad A, B, N_a \\
M_2: & \quad B \rightarrow S: \quad \{A, B, N_a, N_b\}_{K_{b,s}} \\
M_3: & \quad S \rightarrow A: \quad \{A, B, N_a, N_b, K_{a,b}\}_{K_{a,s}}, \{B, A, N_b, N_a, K_{a,b}\}_{K_{b,s}} \\
M_4: & \quad A \rightarrow B: \quad \{B, A, N_b, N_a, K_{a,b}\}_{K_{b,s}}
\end{align*}
\]

3. (a) (4) Describe two distinct ways in which ICMP may be used in network attacks.

(b) (3) Why is TCP harder to spoof than UDP?

(c) (4) What are two vulnerabilities presented by portmapper? Evaluate their possible consequences.

(d) (4) Why is RIP in some ways less secure than OSPF?

4. (a) (4) Why should a firewall filter both incoming and outgoing packets? Give examples including possible consequences of failure to do either.

(b) (5) What are the advantages and disadvantages of application proxies versus packet filtering firewalls?

(c) (6) Name three ways in which the Gemini Trusted Guard Base (GTGB) offers higher assurance than a standard packet filtering firewall. Explain how these characteristics provide a greater level of security.