Final Exam  
ECT 582, Prof. Robin Burke  
Winter 2004  
Take home: due 3/17/2004 9:00 pm  
NO LATE EXAMS ACCEPTED  

Name:  

1) (20 points) Alice has a digital certificate from Bob. She wants to verify it. Given the set of trust relationships described below, answer questions i-iv.

- Alice uses certification authority $Y$ and has a public key certificate issued by $Y$.
- Bob has multiple trust points. He uses certification authority $W$ and has a public key certificate issued by $W$, and he also uses $X$ as a secondary trust anchor, and has a copy of its public key certificate.
- $X$ is the root of a local CA hierarchy.
- $W$ is the root of a different CA hierarchy.
- $V$ is a CA certified by $W$.
- $Y$ has a CA certificate signed by $X$.
- Both $X$ and $W$ participate in a bridge certification arrangement with bridge CA $Z$.
- All of the CAs have directory services in which certificates signed by those authorities can be retrieved as well as the CA's own certificate(s).
- Both Alice and Bob use the same public key software, which searches for the shortest certification path.

i. What would the certification path be for Alice to certify Bob's certificate?

ii. List the steps by which that path would be built.

iii. Suppose the situation were reversed and Bob were seeking to certify Alice's certificate. What would Bob's certification path be for Alice? Is it the same as in step (i)?

iv. List the steps by which Bob's path would be built.
2) (20 points) You have passed ECT 582 with flying colors and are now in great demand as an e-commerce security consultant. Your client is the Aliceville Public Library. Out of concern for the privacy of its patrons, the library has instituted a new policy of anonymous book lending and is beginning a project to implement a new system, which must have the following properties:

a) The main library system, M, will maintain patron accounts and IDs, and must respond to requests of the following form: for a given patron ID, is there a corresponding valid account?

b) M does not keep track of which books a patron has checked out. No information about books should be sent to M, except as provided in (d).

c) Each branch library system, B, must keep track of which books are lent, but should not track the identity of the patron. No information about patrons, including patron ID, should be available to B.

d) The only exception to the anonymity protection occurs if a book is overdue. Then M will need to send a reminder to the patron to return the missing book(s).

e) You may assume that each patron will have a smart card as his/her library card that can store the patron ID and other data, and perform cryptographic operations.

f) You may also assume that M and each B have certificates and participate in an internal PKI system, in which M has the role of CA. It is not necessary for each patron to have his/her own certificate.

Design a lending protocol that will have the desired properties, namely that B’s patrons are anonymous to B and that the books borrowed by patrons are unknown to M. (Hint: compare this situation with the SET protocol.) Your protocol should also have the provision for disclosing identity when books are overdue. Your protocol should describe what messages are exchanged at each step for book check-out, book check-in and detection of overdue books. Your answer should also indicate what information is stored by M, by B and by the patron's smart card.
3) (20 points) You have passed ECT 582 with flying colors and are now in great demand as an e-commerce security consultant. Your client Alice is the CIO of a company with the network configuration shown in Diagram I. The company's firewall consists of a multi-homed bastion host B that also serves as the web server, and a packet-filtering router R on the Internet side. B is configured to allow no in-bound connections from the Internet to the internal network, although outbound connections from internal users to the Internet are permitted. The web server contacts some internal databases and ERP applications.

Alice has recently rolled out a number of new e-commerce applications that are popular with her customers and with the added load, her engineers have detected performance problems on B. Alice has decided to add a separate web server to her configuration to relieve B of this load. Her engineers disagree about where the new server should be placed. Four possibilities are shown in Diagram II. The web server could go (1) outside of the area controlled by R, (2) between R and B, (3) parallel to B with a connection to both networks, or (4) between B and the internal network.

a) (10 points) Describe what the impact would be of each of the four options on the security of the web server and of Alice's internal network as a whole.
b) (5 points) What changes, if any, to the configuration of B's firewall would be required for each option to be successful?
c) (5 points) Which option do you recommend? Are there other options Alice should consider?