CS4410 Spring 2009 Homework 7

Self-test questions about the Internet, web, security.

Ungraded. Solution set to be posted in a week.

1. Consider the following ways of sending your credit card information to a vendor:
    a. A browser window with an https URL and only "secure content" on the page. You fill in the boxes and click "Confirm my purchase"
    b. Same browser window, but you saw a warning "This page mixes secure and insecure content. Display the insecure content too?". You clicked "OK" (e.g., "yes")
    c. You sent email to the vendor
    d. The vendor provided a phone number. You call and give the vendor the credit card information by phone.
    e. You made the purchase in a store and swiped your credit card.

    Could an attacker who doesn't actually work at the vendor's store steal your credit card data? If so, how would he do it? If not, why?

2. A brilliant PhD student from Mathematics takes cs4410. The class is discussing the RSA algorithm, in which the public key is a pair *(e,n),* where *n* is a product of two large, randomly selected prime numbers. Being bored, he starts thinking about factoring and invents a brilliant new algorithm for factoring large numbers that are a product of exactly two prime numbers. The algorithm runs in time polynomial in the number of digits in *n.*
    a. True or False (why?): This algorithm has the potential to defeat the security of the RSA scheme and eliminate security for much of the modern Internet.
    b. True or False (why?): The answer to (a) depends on the polynomial.

3. The Cornell chapter of the Skull and Bones society is developing a new security architecture for calling top-secret meetings, sending each other recipes and announcing the birth of children, weddings, and other life-and-death purposes. They've decided to send cryptographically encoded messages using email.
    a. Invent a reasonably simple scheme that ensures that (i) a message can be sent as a single email with a list of destinations, (ii) any legitimate Skull and Bones member can decode these messages, but (iii) no intruder who intercepts such a message can read it. Keep in mind that new members are added every year (once a member, though, a member for life).
    b. Over time, some Skull and Bones members die, and when this happens, you must assume that outsiders might gain possession of their laptops, passwords, USB keys, and so forth. Can your proposal from part (a) protect against such problems?
        i. First, assume that the last act of a Skull and Bones member, about to pass away, is to send out a message "Goodbye, cruel world". How would you solve the problem of "cutting off access" to future emails?
        ii. Next, assume that some members die without sending a final goodbye. Eventually, some living Skull and Bones member finds out, but it may take a while, at which point a "Poor John is gone" message would be sent by the member. How does this change the situation?

c. A new society, Blood and Gore, is competing with Skull and Bones. Sometimes they try and infiltrate their members into the Skull and Bones community. To reduce this risk, Skull and Bones starts to require signed "vouchers" from a minimum of five current members before a new member can be trusted. How would you implement these vouchers? What issues are introduced by the scenario of part b/ii?

4. You are developing a honeyfarm that Citigroup will employ to detect virus attacks on its computer. Your boss, however, is balking at the expense of purchasing 5000 Xen VMM licenses for a each honey server: she thinks that 1 O/S should be just fine for 1 machine. How would you explain to her the benefits of using virtualization in a honeyfarm?