

Homework 5

Due: April 24, 2009, 10:00 PM EST

Please hand in your solutions as a pdf document

Problem 1 In class you were introduced to two electronic voting systems, namely *Punchscan* and *Threeballot*. This homework problem will test your understanding of the systems:

1. Name three important security properties offered by Punchscan.
2. What is the purpose of binary vectors F_1 and F_2 in Punchscan?
3. When using Punchscan, can the election authority (EA) associate the ballot votes to the IDs of the ballots? Suppose ballot i is marked 0, i.e., $M[i] = 0$. If $F_1[i] = 1$ and $F_2[i] = 0$, what is the actual vote $V[i]$ for ballot i ?
4. How does the audit process for ballot i work in Punchscan? Why does the EA reveal either $P_1^{-1}[i], S_1[i]$ or $P_2[i], S_2[i]$ but not both? What could happen if the EA reveals both pieces of information?
5. Name three important security properties offered by Threeballot.
6. What is the purpose of the checker machine in Threeballot? How can we ensure (and why this is important) that the voter does not keep copy of the serial numbers of the ballots he used?
7. Explain why one can allow also traditional single ballots in Threeballot without affecting the vote tally.
8. Compare the two voting systems in terms of secrecy, accountability and usability.

Problem 2 You want to plant a bug in Company X's office to acquire business intelligence because they are a competitor. The package needs to get into their server room and get hooked up to sensitive hardware. You know the complex hires several guards from a private security company that regularly patrol and check for authentication by using well-known badges. You know that they regularly outsource several functions including janitorial staff, pest control and purchasing IT equipment (think Staples delivery trucks). These jobs have a high turnover rate, but require authentication in order to get access to the premises in the form of a work order for IT supplies and pest control. The janitorial staff is a recurring service, but with a lower turnover rate. They are also periodically inspected by officials like the city or OSHA, but are usually provided with advanced notice of their arrival.

1. What is your high level plan of action?
2. A guard challenges you when you enter, how do you continue your mission? What is your legend? What is your story? Why is this a good plan?
3. What are your options for acquiring access to sensitive areas?
4. You realize you are a target to this attack. How will you defend against it?

Problem 3 A variation of the following biometric authentication protocol was experimentally tested several years ago at immigration checkpoints in major U.S. airports.

A user registers in person by showing her credentials (e.g., passport and visa) to the *registration authority* and giving her fingerprint (a “palmprint” was actually used). The registration authority then issues to the user a tamper-resistant *smartcard* that stores the reference fingerprint vector and can execute the matching algorithm.

The checkpoint is equipped with a tamper resistant *admission device* that contains a fingerprint reader and a smartcard reader. The user inserts her smartcard and provides her fingerprint to the admission device, which forwards it to the smartcard. The smartcard executes the matching algorithm and outputs the result (“yes” or “no”) to the admission device, which admits or rejects the user accordingly.

1. How can a smartcard holder defeat this type of authentication? The attacker can program new smartcards and is allowed to have an input-output interaction with a valid smartcard but cannot obtain the data stored inside it.
2. Show how to modify the scheme to defeat this attack with high probability. Namely, the admission device needs to make sure that it is interacting with a valid smartcard issued by the registration authority. You can assume that the smartcard and the admission device can share a secret value, generate random values and perform cryptographic hashing, but no other cryptographic operation.

Problem 4 This problem refers to the digital cash scheme described in class.

1. Consider the basic scheme based on RSA blind signatures. In this scheme, a coin is a random identifier that is signed by the bank using a blind RSA signature. Show why the blinding value r picked by the customer must be relatively prime to the RSA modulus N .
2. During the withdrawal protocol why is the coin valid with a probability of $1 - 1/k$ upon withdrawal?
3. Show how to modify the above basic scheme to allow coins to have different values (for example \$1, \$5, \$10, or \$20). A coin is now a pair (x, v) , where x is the identifier and v is the value. The bank cannot blindly sign the coin in the withdrawal transaction since it does not know the value of the coin and may let the customer withdraw a coin of value larger than what the customer paid for it. You should modify the scheme in a way that allows the bank to learn the value of the signed coin with high probability but keeps the identifier of the coin secret. Note that you do not have to deal with the double spending issue.
4. Consider now the method for discouraging double spending based on storing in each coin n commitment pairs for the identity of the customer. Provide a detailed justification of the fact that if a customer double spends a coin, then the bank finds out the identity of the customer with probability $1 - 1/2^n$.

Problem 5 Based on commitment protocols, derive a way for n parties to throw a k -sided dice together. Namely, the parties all want to bet on the outcome and no one can agree to trust a single party to be in charge of the throw. For simplicity, assume that k is a power of two.