

Problem 1. [Auctions] (20 points)

This question will consider different types of auctions. For each auction type, we will ask you to describe how it works, and then to describe whether it ever makes sense for a bidder to bid less than his or her actual valuation (that is, the amount he or she considers to be a fair price for the item being sold.) Of course, the bidder wants to achieve the lowest price possible. Here is an example:

- (x) How does a sealed bid auction work? Does it ever make sense for a bidder to bid less than the actual valuation?

A: In a sealed bid auction, each of the bidders sends a sealed, secret bid to the auctioneer, that only the auctioneer can read. The auctioneer sells the item to the highest bidder at the price bid. In some cases, it makes sense to bid less than the actual valuation; if a bidder suspects she will be the highest bidder, then she should only bid slightly more than what she expects the second highest-bid to be: in that way, she can save substantial money.

Answer the following (maximum 4 sentences each):

- (a) (10 points) How does a Dutch auction work? Does it ever make sense for a bidder to bid less than his or her actual valuation?

*The price starts high and goes down.
The first person to bid wins, and pays whatever price the bid was at.
If you know that everybody else is going to wait until a low price to bid, it makes sense to bid below your actual valuation.*

- (b) (10 points) How does a second price "Vickrey" auction work? Does it ever make sense for a bidder to bid less than his or her actual valuation?

*Bids are submitted secretly.
The high bid wins, but the winner pays the second to highest bid. It never makes sense to bid below your actual valuation; you can't save money by underbidding because the second place bid sets the cost.*

Problem 2. [Attacks] (24 points)

Consider the Berkeley CalNet Authentication Web Server, which uses a web page with a user name and user password (the password must be between 9 and 255 characters, and must contain at least three of the following: uppercase letters, lowercase letters, numbers, punctuation, and all other characters), connected via SSL to net-auth.berkeley.edu.

Give at least 3 different plausible ways to attack such a system and gain unauthorized access (1-3 sentences each). (8 points each)

*Possible methods include key logger on client, observation, phishing, intelligent guessing, etc.
Answers that might work with other web sites but not this one, such as SQL injection, breaking encryption, etc. generally received half credit.
Exhaustive search of keys is not feasible in this case.
Vague answers (e.g., find a vulnerability in the server and exploit it) received no credit.*

Problem 3. [Short answer] (30 points)

Give a 1-2 sentence answer for each question. (6 points each)

1. Why is having a non-executable stack and heap insufficient to protect against buffer overflow code execution attacks?

The return address can be overwritten to return to any code already loaded. In particular, the attacker may be able to cause a return into the libc `execve()` function with `"/bin/sh"` as an argument.

2. Firewalls can be used to block all distributed denial of service attacks while allowing all authorized communications. True or false, and why?

False. It is easy to make malicious traffic blend in with authorized traffic, and the distributed nature of the attack prevents any useful filtering on source IP at any point.

3. How can a targeted worm or virus avoid detection by a virus scanner? Give the most relevant answer.

A targeted worm or virus will be new so virus scanners (which are based on signatures) will not detect it.

4. Joe wants to protect himself against rootkits, so he runs a virtual Windows XP system on top of Mac OS X. Is Joe vulnerable to Windows XP rootkits? Why or why not?

Yes, the guest OS can be infected with a rootkit just like a native system can, since the virtual machine simulates the full (or nearly full) hardware interface.

5. In a Mandatory Access Control system, how can an insider with access to a high-security file leak information to a low-security process using the virtual memory system? What is this type of attack called?

*One could leak information through the use of a shared resource.
(Note this does not include shared virtual memory, since that is not allowed in mandatory access control systems.)
The name for the attack is a "covert channel" attack.*

Problem 4. [E-Voting] (26 points)

Your task is to help the State of California develop certification standards for electronic voting machines (DREs).

For each of the three phases of electronic voting at a polling place, give the necessary preconditions and postconditions for a DRE to preserve the *integrity* of the vote. Assume that there are several multiple candidate races, each race has only one winner, and voters may vote for at most one candidate per race (voters may chose to leave any race blank).

Here are the three phases you will consider:

1. Machine preparation on Election day (before polling starts)
2. Accepting a cast vote (repeated throughout election day)
3. Finalization after the polls close

You do not need to consider transparency, privacy, or secrecy for this problem. Please limit yourself to conditions necessary for integrity. State your conditions clearly and precisely, and you shouldn't need additional explanation.

(a) (8 points) The first phase is preparation of the machine on election day before polling begins.

Preconditions:

Valid machine: maches spec, correct make, model, sw version.

No visible tampering.

Machine in working order - power, etc.

All cards/votes/ballotes cleared. Only authenticated users may operate machine.

Postconditions:

No cast votes (counter is 0). All votes/ballots cleared: all vote totals are zero, no candidate has a vote.

Machine in working order.

Cards/ballots are cleared and in working order.

Machines will only accept valid cards/ballots. Machines display correct races and candidates.

All preconditions hold.

All poll workers agree machines are zero.

- (b) (10 points) The second phase is casting of each vote. Specify the preconditions before a vote is cast and the postconditions after a vote is cast.

Preconditions:

*Number of cast votes equals the number of previous voters.
Current user has not already voted.*

Postconditions:

*Number of cast votes equals previous value plus 1.
For each race, the difference between previous and current candidate values has changed by at most one for each candidate.*

- (c) (8 points) The final phase is finalization of vote totals at the end of election day after the polls close.

Preconditions:

*No additional voting allowed.
Number of cast votes is greater than or equal to zero.
Number of votes cast for each candidate is greater than or equal to zero.
Total number of votes cast is the sum of votes cast for each candidate + blank votes.*

Postconditions:

Same as preconditions.