

Spring 2009 – 22c:086 Networking & Security for Informatics
Assignment #2 Due by 11:59pm on March 7th.

Problem 1: Spam filtering Read the instructions at <http://cs.its.uiowa.edu/email/nospamtoolhelp.shtml>. These instructions describe actions you can take based on the probability of each email being spam.

Problem 1a If we use regular expression rules to compute these probabilities, what are the pros and cons?

Problem 1b Instead of using thresholds on these probabilities, we can use a ranking system. We can sort emails in your inbox using these probabilities in the descending order, and reject the top 10% (or any percentage of your choice) from your inbox. What are the pros and cons of this method?

Problem 2: Online game website with PKI When a user sets up an account, ZBoxlive.com provides a unique public and private key pair. When the user comes back to ZBoxlive.com, he sends (username, password encrypted with his private key) to the server. The website pulls the password and the public key for that user from its database and compares the decrypted password with the password stored in the database. If the two passwords match, access is granted.

Problem 2a Describe how you can log into another user's account on ZBoxlive.com.

Problem 2b Design an authentication scheme in which passwords are encrypted with private keys, but the attack you discovered in Problem 2a is no longer feasible.

Problem 3: Insecure Hash Function, Insecure cookies Secure hash functions must have two properties, one-wayness and collision resistance. Let's say a website 22c086.com uses a hash function H to construct cookies for clients. For each client c , if c passes the authentication, then 22c086.com gives $H(c's\ id\ | \ 22c086.com's\ secret\ | \ IP\ address\ | \ timestamp)$ so that the client can provide this cookie as proof of authentication during the session.

Problem 3a Imagine H does NOT provide one-wayness, but collision resistance. What's the problem with this cookie?

Problem 3b Imagine H does NOT provide collision resistance but one-wayness. What's the problem with this cookie?

Problem 4: SMTP relay SMTP servers only send emails composed by known users. For example, any webmail requires you to login before you compose and send a mail. Also, SMTP servers only receive emails that are addressed to known users. For example, if you send an email to a non-existing user name at cs.uiowa.edu from your cs.uiowa.edu email address, it is not accepted by the SMTP server citing non-existing user. In other words, the first SMTP server checks the sender and the last SMTP server checks the receiver of each email. Somehow we still have spam, thanks to rogue relay servers. Explain how these relay servers can send spam.