1. **Protocol Droid.** Artoo and C3P0 often fly on different starships and need to alert each other to their presence when their ships come in contact - otherwise they might accidentally blow each other up! They agree on a shared key $K$ and a MAC algorithm that outputs $t$ bit tags to use in the following protocol.

1. $A \rightarrow C$: a random $t$-bit string $N_A$ and $MAC_K(N_A)$.

2. $C$: on message $n, t$ checks that $MAC_K(n) = t$, and if so, he accepts $A$, otherwise he blows up the other party.

3. $C \rightarrow A$: $MAC_K(t)$.

4. $A$: on message $t'$ checks that $t' = MAC_K(MAC_K(N_A))$. If so, he accepts $C$, otherwise he blows him up.

The idea being that $A$ proves he is $A$ by correctly MACing $N_A$ (which, if the key is secret, only $A$ or $C$ could do) and $C$ proves he is $C$ by MACing the MAC. But...

(a - 5 points) $A$ and $C$ use this protocol for a while and then discover, to their dismay, that sometimes the Emperor, $E$, has been successfully fooling $C$ into believing he is $A$. Supposing that middleperson attacks (and “using the force”) are prevented by speed-of-light limitations, what is a simple way for him to do this?

(b - 5 points) $A$ and $C$ decide that one way to prevent the attack is for $C$ to remember every value of $N_A$ used in a previous challenge and reject if one is ever reused. Suppose $E$ sees one authentication between $A$ and $C$. How can he fool $C$ into believing he is $A$ as many times afterwards as he wants?

2. **Denial of Service Denial.** Sly and Carl are really concerned about the possibility of DoS attacks against their web server program. Since one way to defend against DoS attacks is to make the attacker do more work, Sly has developed a new module for his web server that he claims will prevent DoS attacks by slowing them down. In Sly’s module, every incoming HTTP request is put into a queue, with a timestamp and a “delayed” bit marked as false. When it is ready to serve a request, the web server takes the first request in the queue. If the “delayed” bit is false and there are no other requests from the same IP address in the queue, it serves the request immediately. If the “delayed” bit is false and there is at least one other request from the same IP address in the queue, the “delayed” bit is set to true and the request is re-inserted at the end of the queue. If the delayed bit is set to “true,” then the request is served if the current time is at least 1 second greater than the request timestamp, and otherwise the request is sent to the end of the queue again. This approach extends the time needed for an attacker to fill the web server’s request queue.
Inspired by BitTorrent, Carl has a different suggestion for preventing DoS. In Carl’s solution, whenever client C downloads a page, he also downloads an ActiveX control that acts as a mini web server for that page and its contents only. Then when the main server starts to be overloaded, it uses HTTP redirects to point new clients to servers running on old clients. The new clients can then download the pages from old clients directly, without using any more of the main server’s bandwidth.

(a - 10 pts) Will Sly’s scheme work, or not, and why? Give a detailed explanation.

(b - 10 pts) Will Carl’s scheme work? Why or why not? (Note that there are clearly some implementation issues to address, such as avoiding the use of clients that are unreachable due to firewalls or closed browsers, but let’s assume these are adequately solved)

Paper Review If you are a graduate student, you are expected to also include with this exercise set a paper review of one of the papers posted as graduate reading over these two weeks. Your paper review is not supposed to be a full paper in and of itself, but rather a summary in your own words and some evidence that you’ve thought about what the paper is trying to do, if they achieve their goals, how useful their goals are, and how it could be improved. Your paper review should have the following components.

- A brief summary in your own words about what the paper was about. You should cover what problem the paper was trying to solve or highlight, how the authors proposed achieving their goals, and how the authors evaluated their success. This should NOT simply be a re-statement of the abstract hit with a thesaurus until un-recognizable, I do not mind if you did not fully understand the paper, if something was confusing, or you did not understand a concept, feel free to state that. (1-2 paragraphs)

- State one problem with the paper. Every paper has a problem, be it an evaluation that does not actually measure what it should, a poor assumption, an incorrect threat model, an obvious attack/defense, etc. Find one thing that you think is a flaw in the paper, and briefly explain why you think it is a flaw. (2-3 sentences)

- State two possible things that could be done for future work. This could be expanding the attack/defense to work under different assumptions or in different deployments. It could be a different set of evaluations. It could be an improvement to how the system is constructed. Try to be specific. (1-2 sentences each)

Choose a paper from the weeks listed as “2 Factor Authentication and Biometrics” or “DDoS”.

2