1. Consider the Intrusion Detection System (IDS) described in class (see slide, page 28). Let \( M \) indicate the presence of malicious activity in an audit log. Let \( A \) indicate when the IDS sounds an alarm. The IDS has the property that \( \text{Prob}(A|M) = 99\% \) and \( \text{Prob}(A|\bar{M}) = 2\% \).
   
   a. Suppose the IDS is examining 1,000,000 audit logs. What should \( \text{Prob}(M) \) be so that among the audit logs that it identifies as malicious at least half are truly malicious.
   
   b. Suppose this time we know that \( \text{Prob}(M) = 1/5 \). We now want an IDS whose false-positive rate (i.e., \( \text{Prob}(A|\bar{M}) \)) is small enough so that the systems administrators will not be bogged down investigating audit logs that turn out not to be malicious. What should \( \text{Prob}(A|\bar{M}) \) be so that if this IDS examines 1,000,000 audit logs, at least 3/4 of the audit logs that it identifies as malicious are truly malicious?

2. Read about HTTPS Everywhere. First, describe how it works. Next, describe what security measures it provides. Finally, does it mean that if a person uses HTTPS Everywhere, he or she will be safe on the web (i.e., they’re protected from the attacks we’ve described in class)? Why or why not?

3. What is a third-party cookie? What are some good reasons for disabling such cookies? Is there ever a good reason for letting your browser keep such cookies? Please explain.

4. C-7.9, C-10.3.

---

\(^1\)Better yet, download it and see how it works!