Communication Protocols and Internet Architectures
Harvard University, CSCI S-40, Summer 2018
Homework Assignment #4 due by 1 PM on Friday, July 27, 2018

Please submit your homework on the day it is due using the homework submission tool on the course website. You will need your HarvardKey to use this feature. Please do not email your homework to a TA or the instructor.

Your homework must use text format, PDF or MS Word. Do not use any fancy layout and do not use macros of any type. In other words, the simpler the format the better.

The file name for your homework must include your name and the specific hw# and the file name must not contain any spaces. In addition, you must always include your name and your email address as part of the document. We will not grade homework that does not follow these naming conventions.

There is a penalty for late homework and homework will not be accepted once the solutions are available. Graded homework will be posted on the course website or emailed back to you. Please note that the point assignment included next to each question might change as we refine the answer key for the assignment.

Your homework must be your own work, in your own words. The use of material from other sources, even when it is properly quoted and cited, should be limited. Please see, *Writing with Sources: A Guide for Harvard Students* if you have questions. We realize that some of the homework questions (or comparable questions) have been asked in previous terms but it is important that you learn the material covered by the question; it is never acceptable to copy an answer directly from another source. The teaching staff and the University take the issue of Academic Honestly very seriously.

Please note that the answer to a homework question is rarely longer than three or four paragraphs in length (plus any diagrams.) **If your answer is more than a page long, it means that you are probably not answering the question we asked, or your answer is not as concise as it should be. In either case, you will not receive full credit for your answer.** Finally, note that some of this homework requires that you do additional background reading and research.

HOMEWORK #4 QUESTIONS

Assume for the following questions that we are referring only to IPv4.

1.) (3 points) The US Computer Emergency Readiness Team (US-CERT) publishes what are called Technical Cyber Security Alerts and Vulnerability Notes and these documents alert users to potential threats to the security of their systems. Select a Technical Security Alert or Vulnerability Note published in the last twelve months that has a network related component to it and research the reported problem and the suggested solution (if one is available.) Analyze and describe the problem, and the solution paying close attention to the network related issues that it raises. We are interested in reading your analysis, and not a cut-and-paste of what is on the website. The listing of recent Technical Security Alerts can be found at: https://www.us-cert.gov/ncas/alerts and the listing of Vulnerability Notes is at https://www.kb.cert.org/vuls

IMPORTANT NOTE: You should not select the Security Alerts related to the various DDOS attacks for analysis since they have been covered to such a large extent in the technical press.

2.) (4 points total) The following questions all relate to email. Answer each question in detail.
a). Explain the structure of the envelope, the header and the body of an SMTP message.
b). Explain how MIME is used to send non-ASCII, binary data (such as images) as an attachment.
c). Give 2 examples of the differences between POP and IMAP.
d). What is SMTP relaying and why is it not a good idea? How can it be used maliciously?

3.) (2 points) Web browsers have a configuration field for a Proxy Server. Describe the technical operation of a proxy server and give at least two technical reasons why a company would implement a proxy server on their network.

4a) (4 points total) Assume that you are using a PC at Harvard and that no machine or DNS at Harvard has ever communicated with a machine at Yale. Now, assume that your machine is trying to reach www.yale.edu. Describe the process used by your web browser, the computer it is running on, the local DNS server it is configured to use, and the multiple intervening DNS servers, in order to resolve the IP address for the machine at Yale.
4b.) What is DNS caching? How and why is it used?

5) (3 points total) Determine the public IP address of your Internet connection at your home, school, or office, and then identify the Autonomous System Number (ASN) that corresponds to your public network address. You can use the various tools we have demonstrated in lecture to learn your public IP address and the corresponding ASN.
5a.) What is your public IP address and what is the AS number for this network?
5b.) In order to communicate with the rest of the Internet, the autonomous system of which you are a part, connects to other autonomous systems. For example, Harvard's AS number is AS1742 and two of its upstream connections are to AS numbers ASN174 (Cogent Communications) and AS3356 (Level-3 Communications.)

Identify two upstream autonomous systems that are connected to the autonomous system you are part of (as identified in part a.) What are the names and ASN of these two upstream autonomous systems?

6.) (4 points) In February 2015 security researchers discovered that Lenovo had pre-installed adware software on some specific models of their computers that made the machines very vulnerable to TLS/SSL spoofing attacks without a warning to the user. (As you know TLS/SSL is used to encrypt traffic in HTTPS.) This meant that these systems were vulnerable to a man-in-the-middle (MITM) attack which would allow an attacker to redirect a web request without warning, and to intercept and read supposedly secure HTTPS traffic between the browser (such as Chrome or IE) and a server.

The US-CERT security alert about this is at:
https://www.us-cert.gov/ncas/alerts/TA15-051A

Given the large amount of press coverage about the problem at the time, it is not a surprise that some of the details and information that was published was confusing and contradictory. Review the literature and technical reports on the problem and write up a succinct description of the problem including a technical explanation of how an attacker would take advantage of the adware software that had been installed. Your description should be in your own words (i.e., not a cut-and-paste of other material) and should be one page or less (exclusive of any diagrams.)

As a starting point you might want to review the following articles:

http://tinyurl.com/cscie40b
points to https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops

http://tinyurl.com/cscie40c
points to https://blog.mozilla.org/security/2015/02/27/getting-superfish-out-of-firefox/

http://tinyurl.com/cscie40d
points to http://www.networkworld.com/article/2887293/superfish-security-flaw-also-exists-in-other-apps-nonlenovo-systems.html

http://tinyurl.com/cscie40e
points to https://www.facebook.com/notes/protect-the-graph/windows-ssl-interception-gone-wild/1570074729899339

6.) Submit your homework via the course website. Please make sure that your name is on your homework assignment, and also confirm that your last name and the hw# are a part of the file name.

