Harvard University
CSCI S-40, Communication Protocols and Internet Architectures
Reading Assignment for Lecture 10

**** IMPORTANT NOTE - - This material is not covered on the midterm.***

Email and SMTP: The first part of Lecture 10 discusses email and SMTP.

- In the course textbook Internetworking with TCP/IP Volume One - 6th Edition
  * Read Chapter 24 (SMTP)

- Read RFC 5321, pages 1 – 22
- Read RFC 5322, pages 1 – 9 and 42 – 49

Network Security: Learning about network security is an important part of the course and we discuss it in Lecture 10, Lecture 11, and the first part of Lecture 12. The reading assignment below applies to this portion of the course. We suggest that you start by reading the material in the textbooks, and then continue with the RFCs and the material on the various websites. We expect that it will take more than a week to complete this reading assignment.

- The textbook Computer Networks: a Systems Approach, 5th edition by Peterson and Davie is available online via the Harvard library system (called HOLLIS.) The book is published by Safari Books Online and although we have not run into a problem in the past, the license arrangement with Safari means that only a limited number of users can simultaneously access a specific book. Therefore, if the book is not available online when you first try to access it, check again at a later time. Note that this was the course textbook last year and so it might be available at the Coop or from other students. It is an excellent reference book on networking and we plan to have a number of reading assignments from it this semester.
  * Read chapter 8 on security. **(Required Reading)**

- In the course textbook Internetworking with TCP/IP Volume One - 6th Edition
  * Read Chapter 29 on security. **(Required Reading)**

- Read RFC 4301, "Security Architecture for the Internet Protocol" (Required Reading)
  Read up through and including section 4.2.
- Read RFC 6071, "IPsec and IKE Document Roadmap" (Required Reading)
  Read pages 1 – 12.

- Read RFC 6194, "Security Considerations for SHA-0 and SHA-1" This RFC explains why these hash algorithms are no longer secure. (Required Reading)

- Read these articles regarding security bugs in SSL. ciphers, hashes and browser certificates.
  https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/
  https://blog.mozilla.org/security/2015/09/11/deprecating-the-rc4-cipher/
  https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
  https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

- Read https://www.cert.org/contact/sensitive-information.cfm and locate their public key

- US-CERT publishes weekly bulletins of system and software vulnerabilities. Review two recent weekly bulletins to understand the scope and extent of these security issues. The weekly listing is at:
  https://www.us-cert.gov/ncas/bulletins

- The GNU Privacy Guard (GnuPG) and OpenPGP are based on the original version of PGP. Familiarize yourself with this area of work by reading the following:
  Read RFC 4880, sections 1 and 2
  http://en.wikipedia.org/wiki/Pretty_Good_Privacy
  http://en.wikipedia.org/wiki/GNU_Privacy_Guard

OPTIONAL Material: Relevant Websites and information on vulnerabilities

- As you would expect, we can only cover selected topics in this area of work. The following sites and readings are optional, but they are all good sources of information.
  http://cve.mitre.org/ (Source of information on CVE.)
  http://www.us-cert.gov/alerts-and-tips/
  http://csrc.nist.gov/
  http://www.gnupg.org/
  http://www.gpg4win.org/index.html
  http://www.cert.org/
  http://www.sans.org/
  https://datatracker.ietf.org/wg/#sec
  http://trac.tools.ietf.org/area/sec/trac/wiki
  http://www.us-cert.gov
  https://googleonlinesecurity.blogspot.com/
  https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final
  http://openpgp.org

The following discusses the recent problems with Wi-Fi security (WPA)
http://www.kb.cert.org/vuls/id/228519

The following discuss the problem when root CA certs are improperly installed
http://www.kb.cert.org/vuls/id/446847
https://community.rsa.com/community/products/netwitness/blog/2017/11/03/inaudible-subversion-did-your-hi-fi-just-subvert-your-pc

Background Reference:

A glossary and reference document is RFC 4949 (FYI: 36.) The title of the document is Internet Security Glossary (version 2) and it is about 360 pages long. Of course this is not required reading.

(doc id 201709axx34eefs456788LNE