University of St Andrews School of Computer Science

CS2003 — Internet and the Web — 2020/21

Tutorial 9: Security
Date: Week 11: 26-27 Nov 2020

This week's tutorial questions cover this final week's material on security.

1. Security (?)

   Your PHB (Pointy-Haired Boss) is concerned about securing the sensitive data held by your company. Rather than store data in plaintext, the PHB has created the program `Encrypt.java` to obfuscate the data. You can compile and run this program as follows:

   ```
   javac -cp commons-lang3-3.11.jar Encrypt.java
   java -cp commons-lang3-3.11.jar:. Encrypt super-sensitive-data
   ```

   a) How does this program work?

   b) How does it address the three aims of security?

2. Certificates

   Let's Encrypt was mentioned in lectures as a source of free TLS certificates. Please read this recent blog entry from the Let's Encrypt website: https://letsencrypt.org/2020/11/06/own-two-feet.html

   a) Operating systems and web browsers have a set of trusted root certificates. Why do you think this is? Would it be better if this set of certificates was chosen by the owner of a device?

   b) What is the problem with Android highlighted by that blog entry? Can you think of some solutions?

   c) In 2011 the Diginotar Certificate Authority was attacked, which resulted in it issuing fraudulent certificates for a variety of sites including google.com. See https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html for a good article on this incident. One outcome of this is that *certificate pinning* is now much more common, where clients are statically configured to only accept particular certificates. What might this mean for system upgrades or any changes to code?

d) Free certificates are often used for attacks (e.g., a *phishing* attack might involve registering the domain name www.st-andrew.ac.uk and using a Let’s Encrypt certificate to make it look as if everything was secure). Read this article:
https://news.netcraft.com/archives/2015/10/12/certificate-authorities-issue-hundreds-of-deceptive-ssl-certificates-to-fraudsters.html

   How does an *Extended Validation* certificate make it harder to perform a phishing attack?

3. Contact Tracing

   A large technology story this year (in England and Wales at least) has been the development of the NHS Covid contact-tracing app. You can read more about the history of this app here:
   https://www.digitalhealth.net/2020/09/timeline-what-happened-to-the-nhs-contact-tracing-app/

   You should also read this article and (optionally) this open letter from academics:

   - https://news.sky.com/story/coronavirus-nhs-contact-tracing-app-could-be-abused-by-spies-security-experts-warn-11980596
   - https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view

   The original version of the app used TLS to send contact-tracing data from phones to the NHS. As such it provided security on the wire. Why then were some experts worried about the app? Do you think that they were right to be worried?

4. Create one question on PeerWise covering the topics from week 11, and tag this question with the tag “week-11”. You should also try to answer at least one question with the same tag. Your tutor will pick a question at random during the tutorial and you can go through it together as a tutorial group.