Session 3 Reading List

This is a list of useful documents that will enhance your understanding of the course material. The reading list is session-by-session. “Primary” material means something you would be expected to read if you are serious about the course, and may help you to do the weekly exercise; “Additional” material you may want to read if you would like to deepen your understanding on a specific area.

Primary material

- Have a look at the BSIMM software security activity list at http://bsimm.com/online/. This is a list of software security activities that many companies have been observed as performing. Under each activity, there are a number of examples of how companies have actually done this.
- Have a look at Microsoft’s SDL process guidance at https://www.microsoft.com/security/sdl/default.aspx. You can click on the various phases of the SDL to see what sort of activities Microsoft would mandate in their development.

Additional material

- Ross Anderson: Security Engineering, 2nd Edition, 2008. This is a great book, and fun to read, although you could probably build a house using them as bricks. If you want to get serious about security engineering - especially systems which have unique properties, and not just run-of-the-mill web apps - then I would really recommend reading this book in its entirety at some convenient time. For the purposes of this session, the Chapter 25, Managing the Development of Secure Systems, is interesting.
- From Gary McGraw: Software Security: Building Security In, “Application Security Testing Tools: Good or Bad?” from Chapter 1; Chapter 3, “Introduction to Software Security Touchpoints”; and before the weekly exercise, the sections “Tools from Researchland” and “Commercial Tool Vendors” from Chapter 4 could be interesting.
- Gary McGraw: Software Security: Building Security In, Chapter 10: An Enterprise Software Security Program. This is something you may want to think when reviewing where the tools fit in in a larger organisation.