Session 4 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

- Adam Shostack: Threat Modeling: Designing for Security. (This book was just published when the course started, but we list this here for posterity. This probably should be the primary book of these if you’d want to learn practical threat modeling from a book.)
- Have a look at the playing cards of Microsoft’s Elevation of Privilege card game, http://www.microsoft.com/security/sdl/adopt/eop.aspx, or the physical cards, if you magically have obtained those… (Thanks, Steve Lipner at Microsoft!)

Additional material

- The rest of McGraw’s Chapter 5, above.
- Danny Dhillon: Developer-Driven Threat Modeling. IEEE Security & Privacy, Jul-Aug 2011. Available also at http://www.infoq.com/articles/developer-driven-threat-modeling. This article tells the story of how EMC started to do security risk analysis, use data flow diagrams, and how they ended up scaling it. You can feel the challenge of not having security folks in every team; EMC describes using a “threat library”, which approaches a checklist.