Session 5 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

- The “OECD Guidelines”, a well-known information privacy guideline from 1980, was updated in 2013. The part to read is the “Annex” Part 1 and Part 2. The guidelines list a number of principles that are usually understood as defining information privacy in the context of data flows (so it fits our threat modelling technique well). The current EU directive, and as a result, the national legislation, also echo the same OECD guideline principles. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatal.htm
- For another discussion on integrating the technical parts of privacy impact assessment into technical threat modeling, see Adam Shostack: Threat Modeling: Designing for Security, chapter 6: Privacy Tools.

Additional material

- For a discussion on data flows in cloud services and their legal basis, see Christopher Millard (ed): Cloud Computing Law. Chapter 10, How Do Restrictions on International Data Transfer Work in Clouds?
- 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 following chapters have interesting background:
  - For the design patterns: Chapter 8, Multilevel Security, and Chapter 9, Multilateral Security.
  - For the security-through-obscurity designs: Chapter 22, Copyright and DRM.
- On the subject of using crypto properly, I can recommend Ferguson et al.: Cryptography Engineering. Part I, Chapter 1: Introduction and Chapter 2: Introduction to Cryptography discuss using cryptography in the context of the system’s architectural risk model. The book is very good otherwise as well; if you are planning a career in this field, I recommend you get your hands on it (as well as Anderson’s Security Engineering).
A recent paper that looks at design principles behind engineering systems that need to provide evidence about how the systems were used or how they behaved. This has a lot to do with openness and a clear definition of a Trusted Computing Base. Steven J. Murdoch & Ross Anderson: Security Protocols and Evidence: Where Many Payment Systems Fail, 2014. http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf

If you implement any systems for the EU internal market that process private data, you will also have to look at your (and your customers’) national legislation. Currently the national laws are based on Directive 95/46/EC (often referred to as the Data Protection Directive) from 1995 with various national quirks. However, at the time of writing this in early 2014, the EU bodies are debating about replacing the directive with an EU Regulation that will be uniformly applied throughout the EU and may impose significant new business requirements. Having said that, mapping the privacy domains and discussing the TRIM aspects as explained earlier, as well as following the OECD guidelines, will all remain valid approaches.

Kerckhoffs enters the stage in David Kahn’s excellent history of symmetric cryptography, “Codebreakers”, chapter 8: “The Professor, The Soldier, And The Man On Devil’s Island”. Codebreakers is about a thousand pages, but a fun read. Unfortunately it stops short of making any serious attempt at any post-World War II crypto, including the public key algorithms.

Give a quick glimpse at Munawar Hafiz’s (Assistant Professor at Auburn University) Security Pattern Catalog at http://www.munawarhafiz.com/securypatterncatalog/index.php. He lists almost a hundred security patterns with explanations, some fairly technology specific and others high-level.