Ford Tang – 46564602

October 12, 2013

Informatics 43

Big Assignment 1

From Volume 27: Issue 49 of “The Risks Digest”, the article titled “NHS IT system one of ‘worst fiascos ever’, says MPs” discusses one of the largest failed software projects for the United Kingdom. Like many other projects centered on updating and improving existing systems, the project proved too large and too daunting, and was abandoned. This article caught my eye since the amount of time put into this project was astounding. The project was contracted in 2002, by 2008 they invested about $21 billion into it and in September of 2013, they abandoned the whole project. In a system this complicated, it is hard to say what exactly went wrong and where it could have been improved, mostly when I have relatively little experience in this area. From class, we discussed preplanning of a software system, and perhaps if they spent more time with preplanning they could have created a system that worked. From the article, it sounds like many of the systems were cobbled together from other software created for different implementations but they tried to get them to work together. The interactions between these different softwares probably increased the already difficult task by many magnitudes.

From Volume 27: Issue 45 of “The Risks Digest”, the article titled “Shutdown at Nasdaq is Traced to Software (Michael J. de la Merced)” recounts the events of the stock market on August 22nd, 2013 when a connection issue caused the Nasdaq servers to go offline, halting the stock market completely. This article was interesting to see that something as vast as the stock market could stop due to software issues. The dependency that we have on software is shocking. One of the major issue with this event was that the servers were not ready for this type of error. If test were performed regularly, they could have caught and prevented any mishaps like these.

Also from Volume 27: Issue 45 of “The Risks Digest”, the article titled “More Garbage from Facebook (Vindu Goel)” analyzes Facebook’s privacy policy that was implemented on September 5th of 2013. Facebook’s privacy controls are notoriously difficult and the new policy and statement aren’t any different or any easier. This is a rather disconcerting topic of online privacy. Facebook is in a position with absolute power when it comes to social information. I believe that their privacy policies are created to be intentionally difficult as to have use of any and all information provided to them from the users with little to no control from the user. Sadly, it is not like the user will up and leave Facebook, since everyone else is also so well connected to it, it becomes a necessity for socializing. From a software engineer perspective it would be relatively easy to allow end users to control what information can and will be access as long as they are well defined and easily controlled by the end user. Perhaps with better information and UI/control layout, but Facebook is made to prevent users from certain control so that their information can be exploited by advertisers and such. Facebook 1, users 0.

From Volume 27: Issue 42 of “The Risks Digest”, article “Lamp-post lamp-oon” describes a rather hilarious event of a New Zealand electric company sending a bill to a lamp post. The electric company uses an automated software that processes billing and for some reason the light pole was marked as a paying customer. It’s unclear on why this suddenly happened but it must have been inputted into the system incorrectly or a glitch caused the system to mark the light pole as a customer. From the software engineering side, a simple check case on the billing side could have caught this error, but at the same time, it’s hard to say since it could have been cause by simple human error.

From Volume 25: Issue 8 of “The Risks Digest”, article “Hacking a pacemaker” describes how a team of security researchers was able to gain wireless access to a pacemaker (in a laboratory) and were able to shut down the device, or make it deliver fatal jolts of electricity. This was briefly touched upon in class, and the possibility is really scary. From an engineering and safety viewpoint, I believe that making the device communicate only by physical contact or very near field communications could help protect a patient against that. Perhaps also to encode access with some security that is on file before any further communication will be possible with the device.