File 20110527.0830: Notes from meeting with Dr Martin this morning, 0745:

I told Dr Martin about the new paper from IEEE Security & Privacy in Oakland. It is an extension of the work done last year by another group on language identification in encrypted VoIP conversations; the Oakland authors found another exploitable side channel in Skype. Variable bit rate codecs leak information. The whole second half of the paper is statistics; what they did was to extract a high probability stream of phonemes from the encrypted VBR codec data, which is not English text, but pronounced, sounds like it to English speakers. It was suggested in a blog posting about the paper that the Google voice mail transcription service could make use of this advance. The paper is a little too close to the language identification paper that we did last term in Reading Group, but it might be of interest for the statistical methods.

Dr Martin described the results of the new lecturer interviews they did yesterday. He said they had six, followed by a long series of interviews in the afternoon, and it went well. They are going to extend an offer, and he is hopeful that the candidate will accept. It will be a good boost for the department, specially for Ivan. Dr Martin hinted at some important and pleasing announcement to be made soon, but would not say what it was.

I have been slapped down a few times for my writing style, so I am sensitive about the academic style of this chapter page I sent to Dr Martin. I asked for his feedback.

The style of this section violates some of the norms. It reads like a thriller, not an academic dissertation. On about page three it would be all right, perhaps set off with bars or indentation and then followed by commentary on the specialised vocabulary that CDS installers must deal with, embedded in war zones, shipboard, aircraft, and computer rooms. Don't overdo the commentary; make it concise, but explaining the unique problem that CDS installers have in getting into a new environment every time, needing to integrate into a specialised environment, often with specialised language and very often hostility amongst different data owners thrown together by a shared problem, with all the mutual distrust and the CDS installer at the centre of it. A warship is a three-dimensional maze and this kind of information is relevant to the cross domain system installer, who needs to know this sort of information, 'on the O3 deck to admidships, forward of the island, in the CDC'.

Overuse of acronyms and abbreviations. Need an appendix of terms at the very least. Instead of defining an acronym or abbreviation the first time it is used and then using only the abbreviation thereafter, consider—in the first chapter—spelling out the term 'cross domain systems' every time, and after the reader has seen it twenty or thirty times, then abbreviate it later. I have to teach the reader a specialised language in order to explain why this is not just a firewall, and to justify the interestingly different sort of environment that cross domain systems are installed in. The blizzard of acronyms are 'bamboozling to the reader'. It is easy to overdo abbreviations.

One that might work is to think about how people present maths. Definitions, followed by lemmas, followed by theorems and proofs. Consider putting your definitions up front, even formatted like dictionary definitions, even numbered definitions like in a maths article. Dr Martin advised to format it like an except from a glossary.

'Where does all the work come from?' We talked about what is going on in the department, and I related the story of Lockheed Martin sending out new RSA tokens by overnight express to everyone today. Shortly after the announcement of the RSA breach in mid March, RSA recommended to users that they change their login process to include a password, presumably because the two-factor authentication was no longer two-factor. Lockheed followed that guidance, but then about a week ago the entire VPN became unavailable, then it reverted to no longer requiring the extra password, and now they are shipping out new tokens to everyone, which has got to be expensive. I wonder if they will enforce PIN length, or even a passphrase. Dr Martin asked a good question, which was are they sending out RSA tokens, or some other vendor? I promised to let him know after the new token arrives, which is expected to be today.

I also told the story of police raids in North America on suspected marijuana growing operations, which turned out to be Bitcoin miners. He laughed at that.

Next meeting set up for Friday, 3rd June at 1445 BST. I am to bring a whole chapter, preferably two.

Call ended 0823.

# References