File 20111118.0013: Weekly activity report 0215:

weekly activity report 215 (loughry)
Joe Loughry
Sent: 18 November 2011 00:13
To: Joe Loughry

Weekly activity report no. 20111117.1628 (GMT-7) sequence no. 0215, week 6 MT

I reported a return to making progress Thursday this week in a meeting with Dr Martin. I have been re-reading to catch up, following the method of Charmaz to construct the grounded theory model that was missing in September. I intend to have the model in shape to show to Dr Flchais soon. I reported that I have funding until January, but my priority must be to finish in the shortest amount of time possible. Dr Martin asked about filing paperwork with the department; I replied that I have already talked to Julie Sheppard about it; she requested that I should wait until early December to do that; she is expecting the paperwork then and there will be no problems with it. We talked about GSS reports---due next week. I should schedule a meeting with Dr Flchais as soon as I have the model in hand. I suggested the Applidium report for reading group the week after next.

We talked about Applidium's attack on the Siri protocol, and what might happen to the F-35 (a flying cross domain system, and one on which I have friends working) in light of the announced sale of seventy-four UK AV-8B Harrier aircraft, engines, and spare parts to the U.S. I speculated that Congress would soon terminate the F-35 programme, counting on EMALS to make something other than the F-35B flyable off the Queen Elizabeth class, the F-35C to be abandoned in favour of new F-18s, and the F-35A to be replaced by re-starting production of the F-22. This solution neatly sidesteps the risk of handing the fifth generation over to China's J-20 and Russia's Su-50, follows historical precedent by apportioning work evenly to Boeing and Lockheed, and saves a trillion dollars. An export licence will be quietly issued for the F-22 to Japan. I predict this is what will happen 23rd Nov.

Security Reading Group discussed 'J-PAKE: Authenticated Key Exchange without PKI' by Hao and Ryan (Trans. Comp. Sci. XI, LNCS 6480, pp. 192--206, 2010). John Lyle suggested this paper because the protocol seems to be doing magic; with only rubbish passwords and no trusted third party, it provides both forward security and resistance to off-line attack. The magic, it seemed to me, reduces to a couple of places where the protocol depends on the vanishingly small probability that two randomly chosen values will ever coincide, or that neither of two other computed values will collapse to zero or one. The really interesting feature, as John pointed out, is the off-line attack resistance. The effective lifetime of the password is only two rounds of the protocol when the session key is being established. Even if the attacker later learns a password, it cannot be used by either a passive or an active attacker to compromise an existing session key. The only instance where this protocol fails is in the case where an attacker might repeatedly be able to try one good password against many usernames.

We argued over the two-round protocol. I think the first round provides a useful check on the bounds of two important values, protecting against a catastrophic failure of the second round. Justin maintained that the first round was simply a necessary exchange of values. The authors of the paper call it an implicit authentication. Everyone agreed this is a well-written paper; the details of the protocol are well worked out and sufficient background was provided for the reader to get the protocol without having to seek out all the references and read them first.

Joe Loughry
Doctoral Student in the Department of Computer Science
St Cross College, Oxford

End of WAR 0215.

References