COMP 5900H: Research summary, mesh network key exchange (due before 25 Sept 2020, 23:59hrs)

Weight: 15% Max length: 5 pages Format: PDF file

This assignment is about the "*Dragonfly*" key exchange protocol.

This is a cryptographic key establishment protocol used to derive Wi-Fi encryption keys. This assignment is about the details of the protocol. Wi-Fi encryption and wireless LANs are the subject of classes 2-4 of COMP 5900H (Sept. 2020).

More specifically, Dragonfly is the cryptographic protocol used in an authentication method called "SAE". This method appeared in the IEEE Standard 802.11-2012 (Table 13.3 [1]). The 2016 version of the standard, IEEE 802.11-2016, adopted this as the method to derive a "pairwise master key" (PMK), replacing the pre-existing "PSK" (pre-shared key) method. As noted [1], *Dragonfly* is mandatory in WPA3 (2018) "Personal mode" as the method to establish a master key based on a pre-shared key.

The objectives of this assignment are:

- to understand and explain the details of the *Dragonfly* key exchange protocol;
- to identify different versions of the protocol that exist; and
- to be aware of the general nature of the problems that motivated different versions.

Your task for this assignment is to write a short report addressing the above objectives.

You should define all mathematical notation used in your descriptions of the protocol.

You can choose to give either a "finite field cryptography" (arithmetic over the integers modulo p, where p is a prime), or an "elliptic curve" description of the protocol— choose whichever you are personally most familiar with. You do not need to do both.

Useful references on *Dragonfly* are given in notes from class (Section 13.8 "End notes" [1]), including these references from that chapter: [13], [14], [15], [16], plus [18] (which includes various versions of 802.11), and the "Dragonblood" paper [46] of M. Vanhoef and E. Ronen.

Grading scheme. 15 marks as follows:

- o 3: professional presentation including: formatting, grammar/spelling, attention to detail
- o 3: context and background, on how SAE/Dragonfly fits into 802.11 WLANs
- o 3: self-contained protocol descriptions, including notation and terminology
- o 3: technical clarity, details and accuracy
- o 1: proper citations (with a separate references section at the end of your report).
- o 2: insight and understanding of the protocol, as conveyed to the reader (Instructor)

Submission: must be a PDF file, uploaded to cuLearn.
Maximum length: 5 pages excluding cover page (if any) and references.

[1] P.C. van Oorschot. "Chapter 13: *Wireless LAN Security: 802.11 and Wi-Fi*". Version: 21 August 2020. Distributed to COMP 5900H students via cuLearn during week of Sept.7, 2020.