TTM4137 Exam Dec. 1, 2008
Solution Outline
Dec. 20, 2008

Part I. Wireless Networks Security Facts

1c, 2a, 3c, 4a, 5b, 6a, 7d, 8c, 9d, 10c, 11c, 12b, 13a, 14b, 15d, 16c, 17c, 18d, 19b, 20c, 21b, 22c, 23d, 24c, 25c.

Part II. Authentication Protocols

26. See Figure 2.1, 2.2, 2.3 and 2.4 in the UMTS book page 31-35.
27. A random generator $f0()$ assigning value to RAND1. $f0()$ can be a pseudo-random generator seeded by the key and a time value.
28. We assume all variables are 128 bits long, the lenght of IMSI cancels out in computing the difference. P's first message includes the RAND1 extra, so P communicates 128 bits more than U.
29. This and question 31 are the hard "A" questions of this exam.
1) Chosen plaintext attack by RAND1 on $f2_K()$ cannot be done in U.
2) There is no cryptographic binding between RES1 and RAND2, this makes it possible to use the first "half" transcript from one session and the other "half" of the exchange from another session.
3) Traceability of sessions to the same subscriber because no use of temporary identity (TMSI) is indicated.
4) The access network (TRAN) can control the values of CK and IK. For instance, selecting RAND2 = RAND1 result in $f_K(0)$. A better solution is some nonlinear combination of RAND1 and RAND2.
30. The session keys CK and IK are now generated with input from both parties. For instance, if RAND1 is kept constant, randomization of RAND2 will ensure proper randomization of the key generation.
31. This question depends on the answer to question 29 and is open to creative ingenuity. Of course, one method is the U protocol. Another method is along the ISO 9798-2 "three-liner" presented in the lecture Sep 5, but this requires decryption at UE, and verification at AuC.

UE $\rightarrow$ TRAN: IMSI, RAND1
UE $\leftarrow$ TRAN: E_K(RAND1,RAND2, "AuC")
UE $\rightarrow$ TRAN: E_K(RAND2, RAND1)

Part III. Analysis of IV implementation

32. The requirements are:
1) The main key is fixed and used directly in WEP.
2) MAC-frames should be cryptographically self-contained at the receiver side.
3) The RC4 key must vary with each frame because the keystream must never be used twice.
Solution: An IV variable generated for and carried by each frame.
33. Truly random, pseudorandom, counter, fixed, or a combination.
34. See Item 3 in 32. Fixed IV $\Rightarrow$ fixed cipherkey $\Rightarrow$ all frames will be encrypted with the same key stream. Known plaintext attack will reveal the key stream. If an attacker obtains this key stream, all traffic can be decrypted without knowing the key value.
35. $2^{24} = 16,777,216$ values.
36. Only 1 million out of 16 million values have been observed, still the remaining unobserved values are becoming scarce.
37. Hypothesis: There is $\log_2(1043822) = 19.99344428$ approximately 20 bits

of entropy in the IV.
38. See Table 1
39. See Figure 1
40. Yes, this information supports the hypothesis. Four of the bits (position 1, 3, 9 and 24 counting from the left) are constant, the remaining 20 are variable bits in the IV.

Elapsed Time (minutes)	# Data	$E(X)$ 2^{20} IVs	$E(X)$ 2^{24} IVs
2	76 874	78 728	81 641
23	629 428	621 216	915 248
30	727 198	723 371	1 183 763
40	824 629	828 447	1 559 491
50	896 612	899 573	1 926 165
60	945 423	947 717	2 284 003
80	1 001 550	1 002 364	2 974 022
100	1 026 429	1 027 403	3 631 189
120	1 038 326	1 038 875	4 257 069
140	1 043 822	1 044 131	4 853 150

Table 1: Observed number of unique IVs and expected number of unique IVs

Figure 1: The expected number of new IVs as a function of elapsed time in minutes.