TTM4137 Exam Dec. 3, 2010 Solution Outline

Stig F. Mjølsnes, Dec. 16, 2010

Part I. Wireless Networks Security Facts

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

Part II. Authentication Protocols

26. See Figure 2 and 3 in syllabus Ref. [3] and Figure 1.3 in the UTMS book.
27. The VLR authentication decision is (SRES $\overset{?}{=}$ XRES). The SIM receives a value SRAND and computes SRES $= A3(K_i, \text{SRAND})$. The AuC generates a random value RAND and computes the value XRES $= A3(K_i, \text{RAND})$. Assumptions:
1) Only the authorized AuC and the SIM of subscriber i can input K_i.
2) The $A3()$ is a oneway function.
3) The XRES is computed correctly by the AuC, and received correctly by the VLR.
4) The XRES is kept confidential.
5) The RAND value is not replayed by AuC or VLR.
28. The Malice BS will prompt the victim MS to send the IMSI by an *Identity Request* message, then send an arbitrary challenge value RAND, disregard the reply SRES, and then send the *Cipher mode off* command to the victim MS, enabling a non-encrypted voice stream call setup. The Malice MS can forward the victim MS call by normal network access.
29. Multiple solutions are possible and acceptable here, the students will have to engage their creativity in the synthesis. Let us use the notation introduced in the lectures where $[m]_K$ represents the cipher text of m encrypted under a key K. One solution would be to introduce a sequence counter SQN, similar to the implicit authentication mechanism of the UMTS access network, where AuC will provide an encrypted value $[\text{SQN}]_{K_i}$ to be verified by the MS. Subsequently, a two-way handshake interaction between the MS and the BS with respect to the session/call key K_c can be done by the MS sending $[\text{SRES}, \text{NONCE}]_{K_c}$ and the BS responding with $[\text{CellID}, \text{NONCE} + 1]_{K_c}$.
30 and 31. Answers depends on the solution in 29.

Part III. Analysis of IV implementation

32. Electrical noise signal, cryptographic pseudorandom generator, sequence counter register, realtime clock, or a combination
33. $2^{24} = 16777216$.
34. After 140 minutes only $\frac{1}{16}$ of the possible values have been observed, but the rate of unobserved values decreases notably. Since the rate is tapering off but does not suddenly end, it cannot be a sequence or clock time that "wrap around" early. It might be a skewed noise source or pseudorandom generator.
35. The length of the binary representation is $\log_2 1043822 = 19.99344428$. Alice was surprised because the IV domain is 2^{24} and the speed of collecting

new values should not decrease at that rate at around $\frac{1}{16}$ of the whole set.
Hypothesis: The entropy of the pseudorandom generator is 20 bits.

36. See answer to question 38, exam Dec 1, 2008.

37. See answer to question 39, exam Dec 1, 2008.

38. See answer to question 40, exam Dec 1, 2008.

—