Errata

Publication I

Here is the key agreement protocol in the right column, third page of the publication:

(1) $M_n \rightarrow \text{ALL} : M_n, P(E)$

(2) $M_i \rightarrow M_n$: $M_i, P(E(R_i, Si))$, $i = 1, \ldots n-1$

(3) $M_n \rightarrow M_i$: $R_i(\{Sj,\ j = 1, \ldots n\}); i = 1, \ldots n-1$

(4) $M_i \rightarrow M_n$: $M_i, K(S_i, H(S_1, S_2, \ldots S_n))$, for some i

Two modifications can be made to it based on the analysis in Steel, Bundy and Maidl [88]. The first is to include the sender's identifier in the encrypted part of steps (1) and (2):

(1) $M_n \rightarrow \text{ALL} : M_n, P(E, E(M_n))$

(2) $M_i \rightarrow M_n$: $M_i, P(E(M_i, R_i, Si))$, $i = 1, \ldots n-1$

Its goal is to detect attacker's switching the clear-text M_n, or M_i with another identifier.

The second is that step (4) should be addressed to all participants:

(4) $M_i \rightarrow \text{ALL}$: $M_i, K(S_i, H(S_1, S_2, \ldots S_n))$, for some i

The goal of this modification is to reduce somewhat the attacker's advantage when he is the leader M_n.

Publication II

Today I would have written "many", rather than "most" in the sentence "However, for most services cellular authentication would be good enough," in section 1, last paragraph.

Publication IV

1. Definition of SIZE(S) in Figure 5 on the fourth page of the publication as "fraction of buffer occupied by messages in S" implies that the messages in the set S are already in the node's buffer. This was not our intention. SIZE(S) is better defined as "the total size of the messages in the set S divided by the node's buffer size."

2. Third paragraph above the heading of section 5.2, on the fourth page of the publication: "Messages have a time-to-live (TTL) attribute set to 3 hours and their sizes are uniformly distributed between 100 and 2 MB." There should be "KB" after "100".

3. Fifth paragraph of section 6, on the fifth page of the publication: "We can estimate the time it takes to fill buffers by estimating the average buffer size and dividing by the average data generation rate. In our case: 20 MB/(10 messages/h × 1 MB/message), i. e., two hours."

The origin of the "10 messages/h" estimate in the data generation rate is not clear from the text; that value may have been obtained from simulations. Anyway, it seems too high by about 25%: Benign nodes, which constitute 90% of the population, generate one message per hour per node, while resource hogs, which constitute 10% of the population, generate 10 messages per hour per node. On the average, we have $0.9 \cdot 1 + 0.1 \cdot 10 = 1.9$ new messages/h per node. Message sizes were uniformly distributed between 0.2 and 2 MB. So the average message size was about 1 MB. The binary Spray and Wait routing protocol replicates these messages. With our setting of six initial "copies" the protocol replicates each message at most twice, so the total amount of copies of each message after the replications is (at most) four. Taking that as an estimate of the number of copies, we obtain that the data generation rate (including copies) is about $1.9 \times 4 \times 1$ MB = 7.6 MB per hour per node. The time it takes to fill the 20 MB buffer (and reach a steady state) at this rate can be estimated as 20 MB/7.6 MB, i. e., 2.6 hours. This estimate is still less than our three-hours TTL; and it is also more in line than two hours with what we see in Figures 6 and 8 of the publication.

4. The sentence above Figure 11: "At loads of 1000 and 2000 total messages the intermediary node buffers never become congested." should be "At offered loads of 1000 and 2000 total messages circulating in the network the intermediary node buffers never become congested." Similarly, the horizontal axis in Figure 12 should have the "Offered load" label.

Publication VII

The last sentence in the first paragraph on the right column of the Introduction section: “In both cases the fragmented data is re-assembled only at its destination,” is wrong: according to the RFC 5050 [24] also an intermediate node can re-assemble fragments into a new bundle.

Publication VIII

1. The last sentence in the third paragraph on the right column of the Introduction section: “In both cases the fragmented data is re-assembled only at its destination,” is wrong: according to the RFC 5050 [24] also an intermediate node can re-assemble fragments into a new bundle.

2. In the last sentence of the column below Figure 3, on the third page of the publication: “Please note that in reality the sender may also need to quantize a set of several messages; and we outline a way to do this for in-time delivery in the mean in B,” the words “in B” should be “in Appendix B”.

3. The description of the algorithm O2 on the fourth page, right column, continues until the bottom of the page. Hence the square sign “□” indicating the end of the algorithm’s description should be the last thing on the page, after Step 2.2.

Publication IX

In the caption of Figure 1, section II: “Schematic illustration of a chain of three disrupted links’ chain,” the words “of a chain” should be deleted.

In the last column of section III, first paragraph from the top, replace the second sentence with “For the limiting case where the fragmentation unit f is the smallest possible, we get a simple estimate by $T(x) = 2x$ because the link is in the ON state half of the time (in average) and it is possible to utilize the whole of each ON epoch for transmitting message fragments. This simple approximation ignores the well-known residual life paradox: when transmission starts during an OFF epoch, this first OFF epoch is expected to be longer than the average length of OFF epochs. But especially for longer messages, the effect of this error seems to be rather small.”

In section IV, fifth paragraph below Table I: the sentence “The relative errors were computed as the difference between the actual (simulated) value of $T_k(x)$ and our approximation to $T_k(x)$, divided by the actual value of $T_k(x)$.” should be

"The relative errors were computed as the difference between our approximation to $T_k(x)$ and the actual (simulated) value of $T_k(x)$, divided by the actual value of $T_k(x)$."