Weaknesses and fixes of pseudonym based approaches in solving identity privacy in 5G networks

Mohsin Khan, Kimmo Järvinen, Philip Ginzboorg, and Valtteri Niemi
mohsin.khan@helsinki.fi, valtteri.niemi@helsinki.fi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf Hällströmin katu 2b)
FI-00014 University of Helsinki
Finland
https://www.cs.helsinki.fi/en

Abstract.

1 Existing works:

The solutions proposed in [1, 2, 3, 4]. The below table summarizes some properties of these proposed solutions:

Solution	Shortname	ME or USIM	Back Compatible	PMSI sent or generated
1	MobiMedia16-HW-UH	ME	No	sent
2	MobiMedia16-eric	ME	No	gen
3	CCS15	USIM	yes	sent
4	SSR15	USIM	yes	sent

2 Weakness of Existing approaches

All the above proposed solutions are vulnerable to a DoS attack. In the context of CCS15 paper, the attack is as follows:

1. Both the UE and HN has two pseudonyms $P, P^{'}$
2. The attacker sends a pseudonym Q to a legitimate SN.
3. The legitimate SN sends the pseudonym Q to the respective HN
4. If the pseudonym $Q = P^{'}$ for a legitimate subscriber, then HN generates $P^{''}$. Now the HN has $P^{'}, P^{''}$
5. The attacker sends $P^{''}$ to HN via a legitimate SN, and the HN goes to the state $P^{''}, P^{'''}$. Which is completely different state than that of UE

Immediate question arises, how the attacker knows, $P^{'}, P^{''}$ at the first place. The answer is, the attacker does not know. But the attacker exhaustively tries

many pseudonyms. The attacker sends many pseudonyms to the HN via a legitimate SN in two rounds. In the first round the HN goes to $P^{'}, P^{''}$ state for many subscribers. In the second round the HN goes to $P^{''}, P^{'''}$ for many subscriber.

Let us assume an HN has x subscribers. Question arises: what is the probability that z many subscribers will lose synchronization if an attacker sends y pseudonyms in two rounds to the HN via a legitimate SN. It is a nice exercise to devise a probability mass function $t : \mathbb{Z}^3 \rightarrow R$ that takes x, y and z as input and outputs the probability that z many subscribers will lose synchronization. It is highly likely that almost all the subscribers of an HN will lose synchronization if $y = 10^{10}$.

2.1 Solution by using location update message:

The HN can wait for an acknowledgement from the SN that the AKA has been successfull before updating the pseudonym state. The location update message can act as such an acknowledgement. But that approach has another DoS attack:

1. A Fake SN can come in between a UE and a legitimate SN.
2. The fake SN collects a pseudonym $P^{'}$ from a legitimate UE.
3. Using the pseudonym $P^{'}$, the fake SN then impersonates the legitimate UE to the legitimate SN.
4. Consequently the fake SN receives RAND and AUTN from the legitimate SN.
5. The fake SN sends the RAND and AUTN to the legitimate UE.
6. Authentication becomes successful in between legitimate UE and the fake SN. Right? (The fake SN would not have the right keys and eventually the rest of the communication in between legitimate UE and fake SN will fail. But is there a concrete way for the legitimate UE to know that the authentication actually failed?) $\rightarrow$ the legitimate UE will get a new pseudonym and will go to state $P^{'}, P^{''}$
7. The fake SN would not participate in a authentication protocol with the legitimate SN $\rightarrow$ HN will never receive a location update $\rightarrow$ HN will not update to the new pseudonym and remain at the sate $P, P^{'}$ and $P^{''}$ reserved.
8. Now if the attacker again does the same attack as described in the above steps using $P^{''}$, the UE goes to state $P^{''}, P^{'''}$ whereas the HN remains at sate $P, P^{'}$ and reservers $P^{''}, P^{'''}$. In this way, the attacker can force the HN to exhaust its pseudonym space.

3 ME Based Backward Compatible Solution

The ericsson paper is an ME based solution.

1. Pseudonyms are not sent across the network but generated at ME and HN
2. It doesn't assign an initial pseudonym. Instead it uses public key cryptography in the first time.

3. When pseudonyms are lost, it uses public key cryptography to come back to syhncronized state
4. As it uses public key cryptography in lost pseudonym situation, the problem of moving SIM from one phone to another is also solved

But we want to solve the ME based solution solely based upon pseudonyms.

1. IMSI itself act as the first pseudonym. It also solves the problem of changin the SIM from one phone to another. It is such a rare event that the passive attackers can not really gain much from it. Possibly an active attacker can not trick an ME to a situation where the ME thinks it does not have a pseudonym
2. if pseudonym is lost (unsynchronized), the UE has to go to the shop in person or online to get synchronized. We try to make our solution so that it becomes an extremely rare event.

However, the pseudonyms can be obtained in two ways. One possiblity is that both ME and HN generates the pseudonyms at their respective ends. This approach has been used in MobiMedia16-eric paper. There is a problem:

It keeps track of last two pseudonyms P_i and P_{i+1} and generate a new pseudonym P^{i+2}only when the HN receives P_{i+1} from a legitimate SN. If the HN receives P_i then it responds with the same AV that was used while generating the pseudonym P_{i+1}. So, the HN can be forced to send the same AV in successively many failed AKAs. (We need to check closely if this is bad or not)

To mitigate the issue of reusing the same AV, another solution would be to use the approach of sending the new generated pseudonym by encrypting and embedding in the RAND. Such an approach will solve the issue of reusing the same AV but of course will introduce the chicken-egg problem for the key used for the encryption of the pseudonym. One solution of the chicken-egg problem is to run the AKA successively twice druing the first time the user connects to the network. During the first AKA, the user sends the IMSI, and after the AKA is completed, the HN and ME have CK,IK and the SN and ME have the TMSI. During the second AKA, the user sends the TMSI. During this AKA the HN generates a new pseudonym and a new pair of CK, IK. The HN encrypts the generated pseudonym with old CK,IK and embed it in the RAND. In this case also the HN maintains the history of last two generated pseudonyms P_i and P_{i+1}. The HN generates a new pseudonym only when it receives P_{i+1}.

However, this ME based solution suffers from the DoS attack that we have described in the previous section.

Bibliography

[1] Philip Ginzboorg, Valtteri Niemi: Privacy of the long-term identities in cellular networks. Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications Pages 167-175

[2] Karl Norrman, Mats Näslund, Elena Dubrova: Protecting IMSI and User Privacy in 5G Networks. Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications
Defeating IMSI Catchers

[3] Fabian van den Broek, Roel Verdult, Joeri de Ruiter : Defeating IMSI Catchers. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

[4] Khan M.S.A., Mitchell C.J. (2015) Improving Air Interface User Privacy in Mobile Telephony. In: Chen L., Matsuo S. (eds) Security Standardisation Research. Lecture Notes in Computer Science, vol 9497. Springer, Cham