# A DoS Attack by Exploiting a Weakness of Solutions to Defeat IMSI-Catchers

Mohsin Khan
University of Helsinki
mohsin.khan@helsinki.fi

Kimmo Järvinen
University of Helsinki
kimmo.u.jarvinen@helsinki.fi

Philip Ginzboorg
Huawei Technologies
philip.ginzboorg@huawei.com

Valtteri Niemi
University of Helsinki
valtteri.niemi@helsinki.fi

***Abstract*—Pseudonym based solutions to defeat IMSI-catchers have been published in the recent years. The idea of these solutions have been on the table of the 3GPP community for a couple of years. For some technical reasons, none of the pseudonym based solutions has yet been accepted as a 3GPP standard, even though there has not been any known fatal weaknesses in these solutions. However, we have found a vulnerability of the pseudonym based solutions. This vulnerability has also been reported in another publication (cite?) in the last month, July, 2017. Using this vulnerability, we show that a novel DDoS attack can be mounted against an entire mobile network. We analytically estimate the expected success rate of the DDoS attack. According to our analysis, we can send 50 percent of the subscribers of a mobile network out of service using a reasonably large (maybe mention the size?) botnet. We run a simulation of the attack and show that our analytical estimation is fairly accurate. We present a fix of the existing solution by using the location update message sent by the SN to the HN. By doing so, we obtain a modified AKA protocol as our solution. We present a detail analysis of our solution using a relevant state machine of the protocol. The state machine is constructed using the relevant variables involved in the protocol. We exhaustively look into all the possible states of the user equipment and home network, and show that, in our solution protocol, there does not remain any vulnerability that could lead to a DoS attack of the kind we have presented in this paper.**

## I. Introduction

Kimmo will write it

## II. Pseudonym Based Solutions

Mohsin will write the summary of all the proposed pseudonym based solutions

## III. Vulnerability/attack of the Solutions

All the solutions mentioned in the previous section have the same vulnerability

## IV. Simulation and analytical esimation of the succes rate of the attack

## V. Solution

### A. State Diagram at the UE side

- II = IMSI Inquiry
- IAV = Invalid Authentication Vector
- VAV_p = Valid Authentication Vector that has pseudonym $p$ embedded in it

### B. Post-war period

## VI. Conclusion

The conclusion goes here.

## Acknowledgment

The authors would like to thank...

## References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

Fig. 1. A Pseudonym Based Solution cite

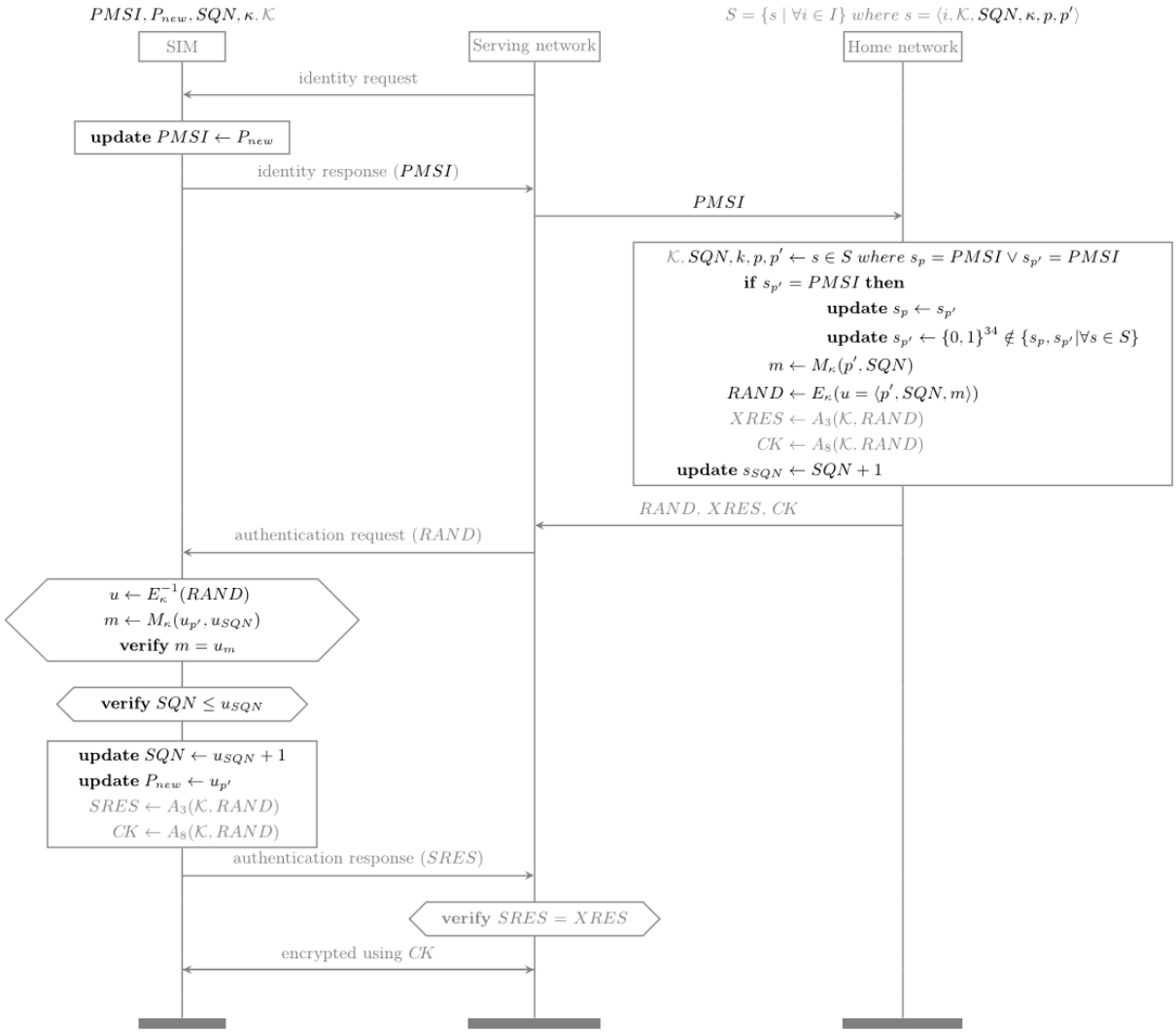


Fig. 2. A Pseudonym Based Solution cite

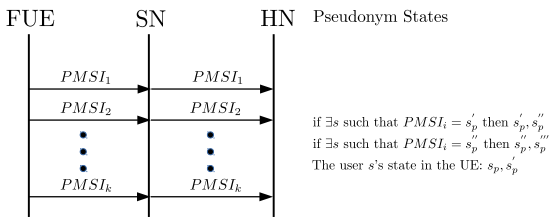


Fig. 3. State Diagram of UE

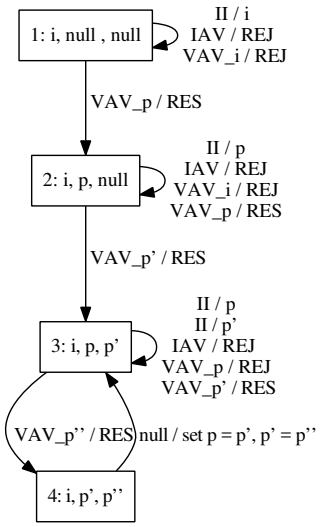

Fig. 4. State Diagram of HN