An Adaptive Three-Party Accounting Protocol

Gregory Detal, Damien Leroy, Olivier Bonaventure
Université catholique de Louvain (Belgium)

Context: Tunnel-based WiFi roaming

A mobile user, John Doe, is on a conference trip hosted by the Sapienza University and wants to connect to the Internet. The university does not want to be responsible for John's behavior. Therefore it leaves this responsibility to his home network.

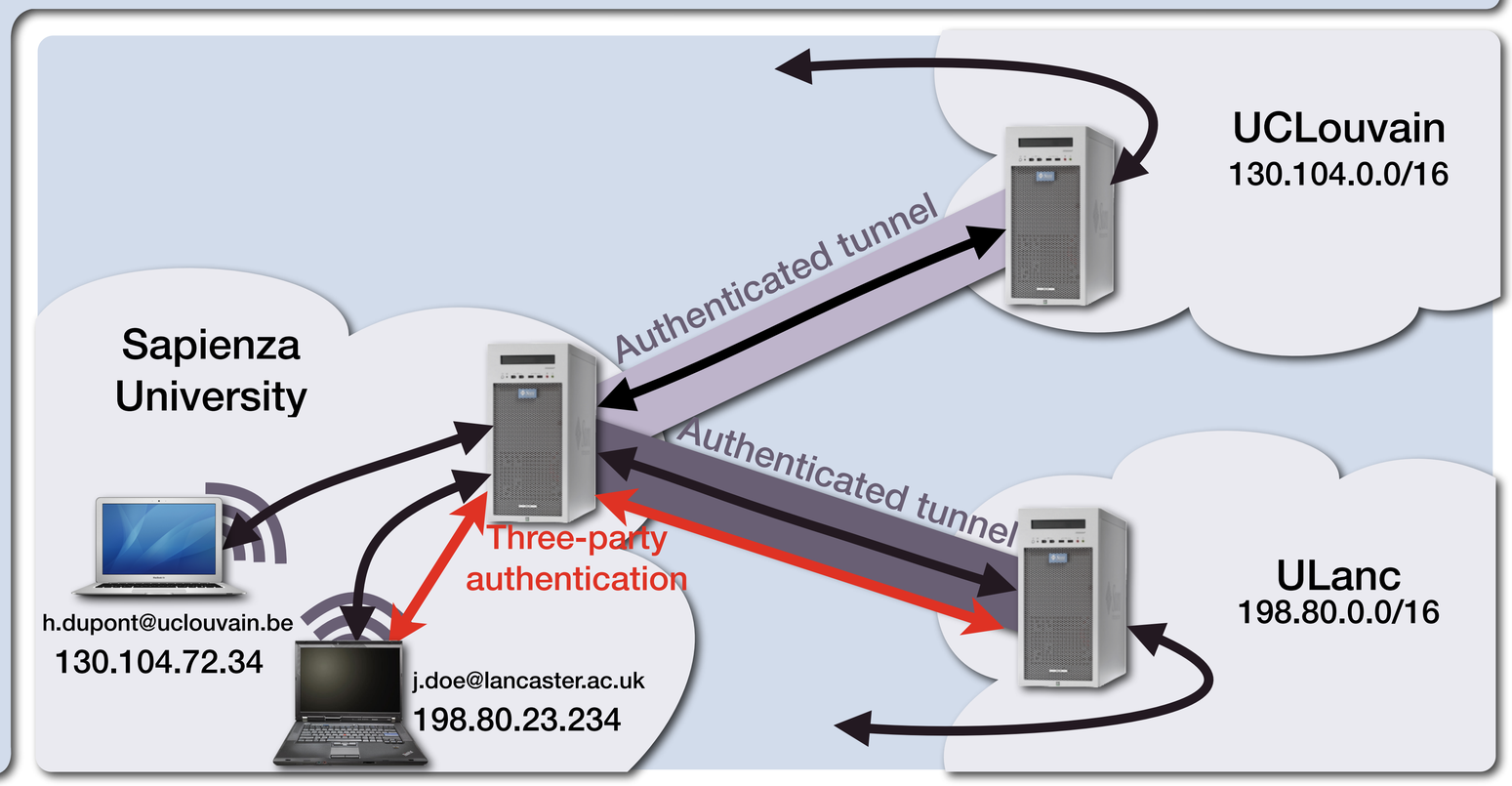
Three-party authentication

↓

Tunnel establishment between the home and visited networks

↓

Forwarding of all mobile's packets through the tunnel



Design of a non-repudiable accounting protocol

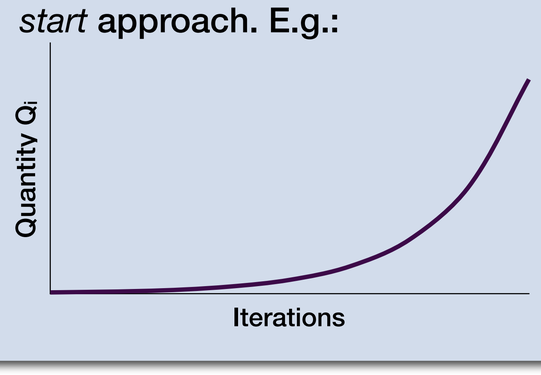
The protocol is defined so that if one party disconnects or claims that the other one has violated the agreement, the data volume not charged must remain below a certain threshold. In order to achieve this goal, the allocated bandwidth is iteratively increased according to the trust level between the entities.

1

★ Q_i is the accumulative quantity of byte exchanged on the whole session

★ Q_i is iteratively increased by the visited network in order to limit the quantity of data it can be scammed of

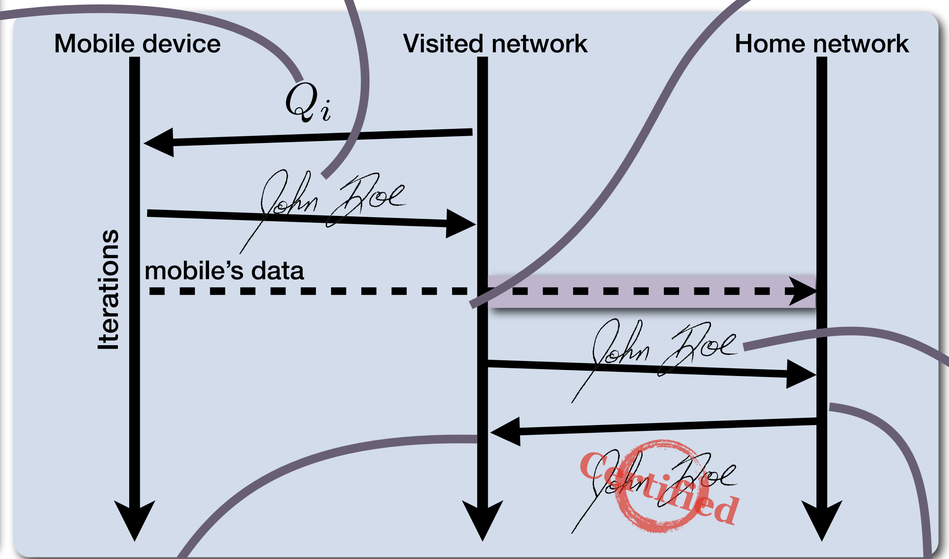
★ The values are chosen using a *slow-start* approach. E.g.:



2

★ If the mobile device agrees on the quantity, it sends a non-repudiable ticket proving its commitment

★ The ticket is a cryptographic signature based on a key shared with its home network



3

★ In parallel to the accounting protocol, data packets are continuously sent by the mobile device

★ At the same time each entities count the amount of data sent, transferred and received

★ A shaping policy must be performed at the edge of the visited network to avoid sending more than the established Q_i bytes of data

4

★ When Q_i bytes has been forwarded, the visited network sends a receipt request

★ The request contains the previous commitment signature of the mobile

5

★ Upon reception of the receipt request, the home network checks whether the signature corresponds to its mobile user

★ It verifies if the amount of data received corresponds to Q_i (considering a maximum loss threshold)

★ If so it sends the non-repudiable receipt, proving its engagement to pay for the consumption of its user

6

★ The non-repudiable receipt ensures the visited network that the home network agrees on the quantity exchanged and therefore sure to be paid

✦ *To avoid blocking the mobile device's traffic, the visited network can start, in advance, the next iteration before receiving the receipt*

http://inl.info.ucl.ac.be

The ACM CoNEXT Student-Workshop '09, 1st dec., ROME, Italy

This work is supported by the Belgian Walloon Region under its RW-WIST Program, ALAWN Project.