Homework lecture 9
Routing security

Harald Vranken
harald.vranken@ou.nl
May 20, 2019

Question 1
Why does routing security require both origin authentication and path authentication?

Answer
Origin authentication is required to provide that an AS can only announce prefixes that are actually assigned to it (hence, no fake prefix announcements).
Path authentication is required to provide that the complete path up to the origin can be verified (hence, attackers cannot announce incorrect paths for prefixes that still origin at the correct AS).

Question 2
How is origin authentication provided in RPKI?

Answer
When receiving a prefix announcement, the receiver of this announcement will look up the ROA (Route Origin Authorization) of this prefix in the RPKI repository. The ROA is a signed object by which the address space holder authorizes the AS to announce prefixes for (a set of) that address space. Hence, the prefix and AS in the announcement should match with the ROA. The signature of the ROA can be verified by the corresponding EE certificate (which attests the IP addresses that have been allocated to the address space holder). The signature of the EE certificate can be verified by the CA certificate, and the IP addresses in the EE certificate should be a subset of the IP addresses in the CA certificate. This is repeated for all CA certificates in the chain up to the root CA certificate (trust anchor).

Question 3
How is a SCION packet routed from source to destination address?

Answer
A SCION packet contains a path. SCION border routers forward packets to the next AS based on the AS-level path in the packet header (which is augmented with ingress and egress interface identifiers for each AS), without inspecting the destination address and also without consulting a routing table. Only the border router at the destination AS needs to inspect the destination address or packet purpose to forward it to the appropriate local host(s).