Security Threats and Security Requirements for the Access Node Control Protocol (ANCP)

IETF 70 - ANCP WG
December 02-09, 2007

draft-ietf-ancp-security-threats-03.txt

hassnaa.moustafa@orange-ftgroup.com
hannes.tschofenig@nsn.com
stefaan.de_cnodder@alcatel-lucent.be

Outline

- Draft status
- Objectives : reminder
- Changes since last version
  - Editorial changes
  - Enhancing some attacks definitions
  - Considering the attacks on the ANCP establishment phase
  - Multicast use case
  - Security requirements modification

Draft Status

- IETF 69th (Chicago)
  - Presenting version -02 of the draft
- WGLC (03-11 September 07)
- Draft update considering the WGLC
  - draft-ietf-ancp-security-threats-03

Objectives : reminder

- Investigating security threats that ANCP nodes could encounter and developing a threat model at the ANCP level.
- Deriving the security requirements for the ANCP.

Changes following the WGLC 1/4

- Editorial comments
  - re-wording and little modifications in the text following the WGLC recommendations.
- Adding an Acknowledgment Section (Section 11)
- Adding a statement in (Section 3.System Overview and Threat Model)
  - Confirming the fact that the threat model and security requirements in the draft (since its beginning) apply to the case where the NAS and the AN might belong to two different administrative realms.
- More clarification is given in Section 5. Potential Attacks (Section 5.4. Traffic Analysis)
  - Concerning messages' capture from the AN to the NAS containing clients-related information.

Changes following the WGLC 2/4

- In Section 7. Attacks against ANCP
  - In the introductory part (Communication between the NAS and the AN)
    "clarification is given showing that the threat model and security requirements take into consideration the data transfer between the NAS and the AAA server when this data is used within the ANCP protocol"
  - Adding a paragraph (before discussing the attacks against the 4 use cases) introducing the attacks that could take place during the ANCP establishment phase.
    "These attacks are mainly on-path attacks, taking the form of DoS or man-in-the middle attacks. No additional security requirement is added for this, as the existing requirements cover this case"

Changes following the WGLC 3/4

- Section 7.4. Multicast Use-case
  - Introductory paragraph: illustrating the role of ANCP in allowing the NAS to control the replication performed by the AN.
  - Addition of a point in the on-path active attacks of type DoS,
    - clarifying that DoS attacks can be done by tampering with the White/Black list configuration or by placing attacks to the bandwidth admission control mechanism.
  - Addition of a point in the on-path active attacks of type Man-in-the-Middle,
    - showing the existence of an additional risk concerning the tamper with accounting information. “Messages' modifications to tamper with accounting information, for example in order to avoid service charges or conversely in order to artificially increase service charges on other users”.
  - Addition of a point in the off-path active attacks concerning the DoS attacks that a user might create by sending many IGMP messages.
    - “DoS could also result from generating heaps of IGMP join/leaves by the HGW or CPE, leading to very high rate of ANCP query/response”.

Changes following the WGLC 4/4

- Section 8. Security Requirements
  - Removing the requirement “The protocol solution SHOULD distinguish the control messages from data”
  - Addition of a requirement “The protocol solution SHOULD ensure that operations in default configuration guarantees low level of AN/NAS protocol interactions"
  - Addition of some details in the requirement “The protocol solution MUST be robust against denial of service (DoS) attacks”
    - "In this context, the protocol solution MUST consider a specific mechansim for the DoS that the user might create by sending many IGMP messages"

Next Step

- Discussing the possibility of passing the draft to the IESG