Security Requirements of NVO3

draft-hartman-nvo3-security-requirements-00

Sam Hartman, Dacheng Zhang, Margaret Wasserman

IETF 86, March. 2013, Orlando, USA

Introduction

- **Propose a threat model in order to specify the attacks of concern**
- **Analyze the security requirements that the control plane and the data plane MUST or MAY fulfill in order to tolerate the attacks concerned**

Threat Model (1)

- **NOV3 should be secure even when an attacker has the capability of**
  - ➢Intercepting the packets transported through a virtual data center network
  - ➢Replaying the intercepted packets
  - ➢Generating fake packets and injecting them into the network
- **When using the above capability to perform a successful attack on a virtual data center network, an attacker may be able to**
  - ➢Obtain the data which it is un-authorized to access
  - ➢Analyze the traffic pattern of a tenant or a end device
  - ➢Disrupt the service quality of the network or the integrity of application running over the network

Threat Model (2)

- **Under the attacks performed by an attacker, a virtual data center network MUST guarantee the following security properties**

  ➢Isolation of virtual networks

  ✓ The traffic within a virtual network can only be transited into another one in a controlled fashion

  ✓ An entity cannot make use of its privilege obtained within a VN to manipulate the overlay control plane to affect on the operations of other VNs

  ➢Integrity and origin authentication of the control plane: All the control pane implementations of the overlay MUST support the integrity protection on the signaling packets.

  ➢Availability of the control plane: The design of the control plan must consider the DDOS or DOS attacks.

Threat Model (3)

- **The following properties SHOULD be optionally provided:**
  - ➢Confidentiality and integrity of the TES traffic
    - ✓If most of the TES data is headed towards the Internet and nothing is confidential, encryption is redundant
    - ✓in the cases where the underlay network is secure enough, no additional cryptographic protection needs to be provided
  - ➢Confidentiality of the control plane.
    - ✓On many occasions, the signaling messages can be transported in plaintext
    - ✓When some information contained within the signaling messages are sensitive to a tenant (e.g., the location of a TES, when a TES migration happens), the signaling messages related with that tenant should be encrypted.

Security Requirements Between NVEs and TESes

- **When a NVE and the TESes it supports can be deployed in a distributed way:**
  - ➢Optional security protection on the data traffic
  - ➢Integrity of signaling messages: Mutual Authentication needs to be provided
  - ➢Isolation between different VNs: data traffic and signaling messages (Authorization is required)
- **When a NVE and the TESes it supports can be deployed in a co-located way:**
  - ➢Isolation between different VNs
  - ➢Isolation of Memory and Computing Resources

Security Requirements within Overlays -Control Plane

- **The integrity and origin authentication of the signaling messages must be guaranteed**
- **DOS attacks**
  - The NVEs SHOULD be only allowed to send signaling message in the overlay with a limited frequency
  - Protection on the centralized servers
- **Inside attacks where one or more NVEs are compromised**
  - Authentication and authorization
  - Isolation enforced with cryptographic keys

Security Issues Imposed by the New Overlay Design Characteristics

- **Scalability**
  - If a NVE needs to securely communicate with a large number of peers, the scalability issue could be serious.
  - In[I-D.ietf-ipsecme-ad-vpn-problem], it has been demonstrated it is not trivial to enabling a large number of systems to communicate directly using IPsec to protect the traffic between them.
- **Influence introduced by data encryption on Security Devices**
- **Security Issues with VM Migration**
  - State Migration
  - Redirection

Questions?