Security Requirements of NVO3

draft-hartman-nvo3-security-requirements-01

S. Hartman

M. Wasserman

D. Zhang

Updates since -00

- Add the introduction of NVO3 Overlay Architecture
- Fill the Terminology Section
- Provide a new attacker category
- Add the discussion about the necessary of introducing automatic key management mechanisms
- Add an attacking analysis on the data plan of NVO3 overlay

Threat Model

- in this analysis work, attacks are classified into two categories:
  - inside attacks
    - An attack is considered as an inside attack if the adversary performing the attack (inside attacker or insider) has got certain privileges in changing the configuration or software of a NVO3 device (or a network devices of the underlying network where the overlay is located upon) and initiates the attack within the overlay security perimeter.
  - Outside attacks.
    - In contrast, an attack is referred to as an outside attack if the adversary performing the attack (outside attacker or outsider) has no such privilege and can only initiate the attacks from compromised TSes.

Outsider Capabilities

- The following capabilities of outside attackers MUST be considered in the design of a NOV3 security mechanism:
  - Eavesdropping on the packets,
  - Replaying the intercepted packets, and
  - Generating illegal packets and injecting them into the network.
- With a successful outside attack, an attacker may be able to:
  - Analyze the traffic pattern of a tenant or an end device,
  - Disrupt the network connectivity or degrade the network service quality, or
  - Access the contents of the data/control packets if they are not encrypted.

Insider Capabilities

- It is assumed that an inside attacker can perform any types of outside attacks from the inside or outside of the overlay perimeter.
- In addition, in an inside attack, an attacker may use already obtained privilege to, for instance,
  - Interfere with the normal operations of the overlay as a legal entity, by sending packets containing invalid information or with improper frequencies,
  - Perform spoofing attacks and impersonate another legal device to communicate with victims using the cryptographic information it obtained, and
  - Access the contents of the data/control packets if they are encrypted with the keys held by the attacker.

Security Properties (1)

- When encountering an attack, a virtual data center network MUST guarantee the following security properties:
  - Isolation of the VNs
  - Spoofing detection
  - Integrity protection and message origin authentication for the control plane
  - Availability of the control plane

Security Properties (2)

- When encountering an attack, The following properties SHOULD be optionally provided:
  - Confidentiality and integrity of the data traffic of TSes.
  - Confidentiality of the control plane

Basic Security Approach to Securing the Communications between NVEs and TSes

- If the NVE supports multiple VNs concurrently, the data/control traffics in different VNs MUST be isolated physically or by using VPN technologies.
- If the network connecting the NVE and the TSes is potentially accessible to attackers, the security properties of data traffic (e.g., integrity, confidentiality, and message origin authenticity) SHOULD be provided.
- Cryptographic keys need to be distributed to generate digests or signatures for the control packets (cryptographic keys need to be distributed to generate digests or signatures for the control packets.
  - The TSes belonging to different VNs MUST use different keys to secure the control packets exchanges with their NVE.
  - For a better damage confinement capability, different TSes SHOULD use different keys to secure their control packet exchanges with NVEs, even if they belong to the same VN.

Basic Security Approach to Securing Control Plane of NVO3 Overlay

- It is the responsibility of the NVO3 network to protect the control plane packets transported over the underlay network against the attacks from the underlying network.
  - The integrity and origin authentication of the messages MUST be guaranteed. The signaling packets SHOULD be encrypted when the signaling messages are confidential.
  - When the network devices exchange control plane packets, integrated security mechanisms or security protocols need to provided.
  - Keys need to be deployed manually in advance or dynamically generated by using certain automatic key management protocols
  - In order to enforce the security boundary of different VNs in the existence of inside adversaries, the signaling messages belonging to different VNs need to be secured by different keys.
  - It will be important to prevent a compromised NVE from impersonating the centralized servers to communicate with other NVEs.

Basic Security Approach to Securing Control Plane of NVO3 Overlay

- It is normally assume that the underlying network connecting NVEs are secure to outside attacks
- An inside attacker compromising a underlying network device may intercept an encapsulated data packet transported a tunnel, modify the contents in the encapsulating tunnel packet and, transfer it into another tunnel without being detected.
  - Signatures or digests need to be generated for both data packets and the encapsulating tunnel headers
  - NVEs SHOULD use different keys to secure the packets transported in different tunnels.

- Questions?