Quarantine Model Overview

“Quarantine model overview for ipv6 network security”
draft-kondo-quarantine-overview-00.txt

Satoshi kondo
satoshi_kondo@trendmicro.co.jp

59th IETF Seoul, Korea

IPv6 v.s. Firewall

- The benefits of IPv6 don't coexist with legacy firewalls
  - End-to-end communication
    - no-more NAT, IPsec, multicast, QoS, ...
  - Plug & Play
    - Non-PC Devices
  - Mobility
    - Mobile IPv6
- What should we do to provide security in IPv6 network?
  - Should we upgrade firewalls?
  - Should we design alternative way?

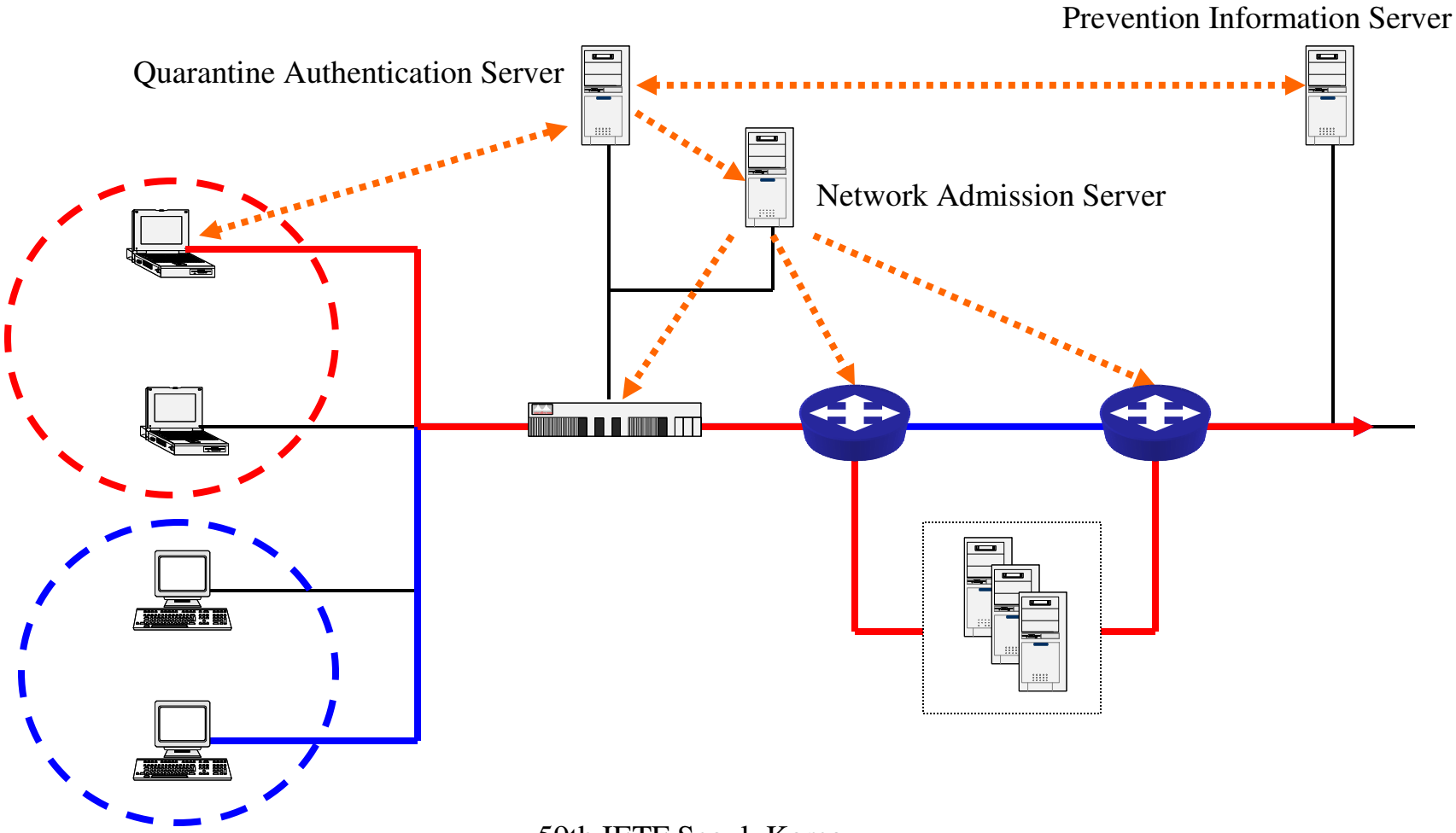
Limitation of Firewall

- It is difficult for firewalls to
  - block every network worms
    - via SMTP, HTTP
  - filter encrypted/tunneled packets
    - SSL, IPsec
  - control/manage nomadic nodes
  - pass through high-speed traffics
- These limitations stem from the basic firewall design (“Border Defense Model”)
  - we have to abandon firewall to create a new security framework for IPv6 (and IPv4)!

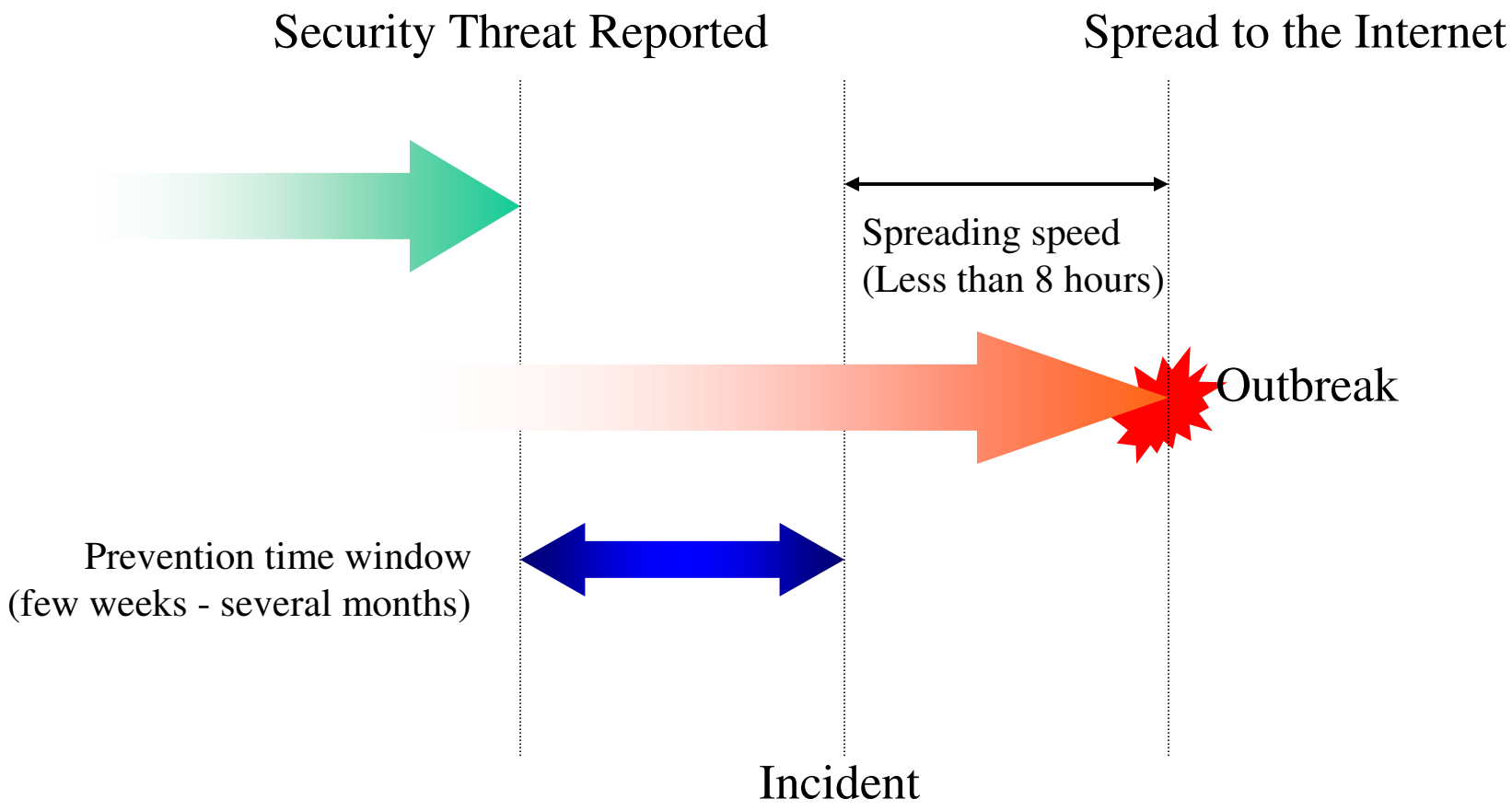
What Is “Quarantine Model” ?

- Combination of host-based security model and network-based security model to provide flexible and robust security management
- Consists of three steps:
  - 1. Quarantine the security credential of a node
    - when it is connected to the network
  - 2. Connect the node to a different network based on that result
    - a node is grouped by its security-level
  - 3. Apply different security policy for each networks to enforce site security policy
    - Enforce to apply security patches
    - Access control
    - Filtering rules
    - Packet inspection

Quarantine Model Diagram



Security Threat Window



Limitation of Firewall is solved

- Quarantine the security credential of a node when it's connected to the network
  - block network worms
  - control/manage nomadic node
- Separates nodes according to their security level, and allowing special communications only to high security-level nodes.
  - encrypted/tunneled packets
  - pass through high-speed traffic

Next Actions and Issues

- Experimental implementation
  - How to describe a site security policy?
  - How to make a network separation?
  - How to control network equipment (router/switch/firewall)?
- Standardization to provide interoperability
  - to avoid vendor-proprietary IPv6 network security model!
  - and vendors can implement vendor-specific solutions based on these interoperability.
    - Security prevention information
      - Data format, Delivering protocol
    - Credential information of network node
      - Data format, exchange protocol, security-level deprecation

Q&A

- Is this work necessary for IPv6 network security?
- If so, should it be an v6ops WG item?
  - if not, where is the right WG?
- Other comments are welcome!