Security Framework for the IPv6 Era

SUZUKI, Shinsuke (Hitachi, Ltd. / KAME Project / WIDE Project Secure-6 WG)
suz@crl.hitachi.co.jp / suz@kame.net
HIROMI, Ruri (Intec NetCore, Inc. / WIDE Project Secure-6 WG)
hiromi@inetcore.com

Outline

1. Legacy security framework
2. What is necessary in IPv6 network?
3. Quarantine Network

* Backbone-network issue is out of scope in this presentation (e.g. DoS, source-spoofing, Phishing)

1.1. Various kinds of Security Frameworks

- Perimeter Defense
  - e.g. Firewall, VPN
    - Legacy IPv4 operational security
    - to drop unnecessary traffic from inside / outside
- Edge Defense
  - e.g. IPsec (Transparent-mode), Personal Firewall
    - Current IPv6 protocol-level security
    - to keep Confidentiality/Integrity/Authentication of communication
- Object Defense
  - e.g. Data encryption, Access authentication, Mandatory Access Control, Anti-virus software
    - Recent IPv4 operational security
    - to drop application-level attack (e.g. spam, virus, worm, spy-ware, theft) on a PC

1.2. Assumptions in Each Framework

- Each framework has some assumptions
  - Perimeter Defense
    - "all the communication MUST goes through a firewall"
      - "communication" = Web/Mail/FTP
      - A host does not physically move so frequently
      - A host cannot have an external connectivity by itself
  - Edge Defense
    - "A user may make any communication as he/she wants"
  - Object Defense
    - "A user must/can defend oneself by him/herself"

1.3. Advantages/Disadvantages in Each Framework

- Perimeter Defense
  - Advantages
    - concentrated management
  - Disadvantages
    - uncovered security threats (e.g. insider attack)
    - difficulty in user-specific customization (e.g. “it’s secure, but I cannot work!”)
    - singular point of failure (e.g. network performance)
- Edge Defense
  - Advantages
    - user-specific customization (e.g. end-to-end encrypted session)
  - Disadvantages
    - difficulty in consistent management (e.g. security policy, traffic inspection)
- Object Defense
  - Advantages
    - detailed inspection
    - user-specific customization
  - Disadvantages
    - difficulty in consistent management (e.g. operational mistake, zero-day attack)

1.4. Current Deployment Status

- Perimeter Defense is still preferred by administrators, because it fully satisfies the administrators' requirement:
  - Administrators' requirement
    - manageable security
      - Enforce a security policy to all the nodes in a centrally consistent manner
  - Users' requirement
    - customizable and easy security
      - Obtain a user-specific security policy automatically

2.1. What Does Perimeter Defense Matter with IPv6?

- Perimeter Defense often unnecessarily restricts communication
  - Non-problematic user operation is denied, because of the management difficulty...
- Essentially not an IPv6-specific issue
  - but getting much more serious in IPv6, since it completely denies the benefit of IPv6 by nature
    - Plug & Play
    - non-PC equipment
    - end-to-end (encrypted) communication
    - new applications

2.2. What Is Necessary?

- Integration of “Manageable Security” and “Customizable and Easy Security”
  - automatic integration is desirable
  - should work in IPv4 as well as in IPv6

- Integration way is different, depending on
  - the definition of a “security policy”
  - network environment
- This makes the things complex...

e.g.) Security Policy Examples

- ISP network
  - Customers may make any communication, if it does not interfere with other customer's communication severely

    → Traffic management is important
- Enterprise network
  - Customers may make any communication, if it contributes to the profit of the enterprise

    → Detailed contents management is important
- SOHO network
  - Provide every service to the very limited number of customers

    → Customer authentication is important

2.3. How To Proceed?

- There are two ways
  - Newly create a protocol to synchronize between a host and a network manager
  - Just make use of such existing mechanism
- Each way has its own pros and cons
  - New protocol
    - vendor-neutral
    - general-purpose protocol is quite difficult
  - Existing Mechanism
    - Can be vendor-specific
    - easier because it is often dedicated for a single purpose solution
- The latter one seems practical

3.1. Quarantine Network

- Quarantine Network
  - Framework to provide a precise and refined network management
  - dynamic network separation based on the security level of a node
- Equivalent to a quarantine procedure in the immigration at an international-airport

3.2 Components of the Quarantine Network

- Security Level Management
  - by Quarantine Server
    - monitors the security level of a node
    - accomplished by a legacy auditing tool
- Dynamic Network Separation
  - by Policy Enforcer
    - accommodate the node to a network segment according to the security level of the node
    - accomplished by several methods (Layer2, Layer3, Layer4, Layer7)

e.g.) How to Integrate Security Framework in Quarantine Network?

- ISP
  - Security Level Measurement
    - Amount of traffic from a PC
  - Dynamic Separation
    - heavy-user, ordinary-user, malicious-user
- Enterprise
  - Security Level Measurement
    - Installed software on a PC (e.g. Anti-virus software)
  - Dynamic Separation
    - staff, staff not installing the required software, guest
- SOHO
  - Security Level Management
    - User authentication
  - Dynamic Separation
    - staff, guest

3.3. Implementation Status

- Security Level Management
  - Legacy auditing tools seems satisfactory
- Dynamic Network Separation
  - Layer2: IEEE802.1x (not specific to IPv6)
    - several vendors
  - Layer3: PANA/DHCPv6
    - WIDE Project Secure6 WG
  - Layer4: Tunnel-Broker
  - Layer7: Distributed Firewall
    - Euro6IX

3.4. Issues in Dynamic Network Separation

- Yet Another Management
  - Layer2
    - Layer3 address need be managed, together with Layer2 management
  - Layer7
    - How to describe/distribute/confirm a policy for every node?
- Encrypted Communication
  - Layer2, Layer3, Layer4
    - cannot manage encrypted communication in the middle
- Protocol Independence
  - Layer3, Layer4, Layer7
    - Need to do the same thing for IPv4, too.
- Access Concentration
  - Layer4
    - a bottle neck in performance, or a single point of failure

3.4 Remaining Issues

- Analysis of a Possible Vulnerability in Quarantine Network itself
- Evaluation in the Actual Operation
  - really IP-version independent?
  - tolerable delay /performance?
  - Comparison between installation/running-cost and the hedged risk

4. Conclusion

- (Automatic) Integration of Perimeter Defense, Edge Defense, and Object Defense is necessary in the IPv6 era
- Introduced Quarantine Network as an integration example

c.f.) What's going on in standardization?

- IETF v6ops WG
  - Trying to summarize IPv6 security overview
  - Based on that overview, ask Security Area people to work on specific items
  - slow and steady progress ….
- IETF netconf WG
  - XML-based network configuration protocol
  - Originally aiming at a router/switch configuration
  - protocol is almost done, and working on data-model