v6ops and security

IPv6 Transition/Co-existence Security Considerations

draft-savola-v6ops-security-overview-00.txt

Pekka Savola, CSC/FUNET

Overview

Overview

- □ Look at different kinds of issues
  - ○ IPv6 protocol
  - ○ Transition mechanisms in general
  - ○ Deployment
  - ○ + general observations
- □ What should we do about it?
  - ○ Very prominent in the charter, something needs to be done
  - ○ An abstract approach
  - ○ Which drafts would be applicable/which work should be initiated
  - ○ Adopt some drafts / initiate some new work?

Different kinds of issues

Different kinds of issues (the IPv6 protocol suite)

- □ Protocol itself (some generic, some more specific)
  - ○ Some people afraid of increased end-to-end transparency
    - ▹ people used to the NAT "security model"
    - ▹ education required; need a mechanism to control access
  - ○ Some people afraid of increased end-to-end encryption
    - ▹ people used to the perimeter firewall "security model"
    - ▹ due to key mgmt difficulties, may not be a huge problem
    - ▹ highlights the need for end-host, distributed, managed firewalling
  - ○ Issues in specifications
    - ▹ how hosts should parse Routing Headers
    - ▹ how privacy addresses’ applicability is not clear
    - ▹ how ICMPv6 messages may be generated in response to multicast packets
    - ▹ how neighbor discovery "on-link" sending model causes complications
    - ▹ etc.

Different kinds of issues

Different kinds of issues (transition)

- □ Transition/Co-existence tools
  - ○ Tunneling in general
    - ▹ UDP tunneling typically punches through NATs *AND* firewalls; breaking assumptions
    - ▹ configured IPv6-in-IPv4 tunneling slightly better (typically explicit allow/disallow)
  - ○ Automatic tunneling mechanisms
    - ▹ the risks of packet forgery and DoS attacks increase
    - ▹ the virtual topologies, especially ad-hoc ones, make the network architecture more complex
  - ○ Relay issues
    - ▹ communication with third parties in automatic tunneling
    - ▹ unless carefully done, increases the risk of DoS etc.

Different kinds of issues

Different kinds of issues (deployment)

- Issues in deployment
  - Problems with IPv4/6 dual stack use
    - certain cases of deployment may incur large timeouts (as presented)
    - quality of IPv6 routing globally is inferior to IPv4: worse quality
    - some applications don’t handle all the fallbacks properly
    - some DNS servers/load-balancers abuse AAAA-querying resolvers
  - Insecure service piloting
    - testing services/applications without proper access controls
  - Operational factors in network infrastructure
    - unstable(r) router software, causing virtual topologies or breaks for "production" v4
    - slower processing (non-line-speed), causing hacks like MPLS
    - missing features (e.g. no ability to turn off IPv6 telnet access)
    - insecure default configuration/assumptions (if IPv4 access is restricted, IPv6 may be allowed by default unless explicitly disallowed)
    - costs of running one protocol (multiple topologies) vs two protocols (double the processing)

Different kinds of issues

Different kinds of issues

- Things to note in general
  - Prefer native IPv4/IPv6
    - security issues greatly simplified
  - Accept configured tunneling
    - plain and simple
    - where necessary, try to avoid if possible
    - explicit knowledge of the end-points: a lot fewer risks
  - Avoid automatic tunneling
    - security properties typically difficult to handle
    - usually bring on a lot of complexity
    - may be difficult to retire ("sunset strategy")

What should we do?

What should we do about security?

- Charter lists a lot of items of IPv4/IPv6 operations
  - 1. solicit input on sec issues from operators/community
  - 2. provide feedback to IPv6 WG on specs which are likely to cause sec issues
  - 4. publish docs on security risks of the operations (w/ sec area)
  - 5. identify sec issues in deployment scenarios/solutions
- So..
  - We had better DO something!
  - Security is about the most important item on our charter
- But what to do?
  - Good question!
  - Feedback sought..

What should we do?

What should we do about security (generic)?

- □ We need more security expertise
  - ○ To evaluate security aspects of the proposals from the first
  - ○ And to help in figuring out an answer to the all of below
- □ We need better idea how to evaluate security
  - ○ How to deal with issues transparency etc. imply?
    - ▹ specify local access control mechanisms?
    - ▹ try to see if there's work on end-host firewalling?
  - ○ How to deal with issues NAT/firewall traversal imply?
    - ▹ do we need to do more than what other NAT traversal mechanisms have done (=nothing)?
    - ▹ probably yes, but what?
  - ○ How to deal with the evaluation of transition mechanisms?
    - ▹ how much complexity is "too much"?
    - ▹ how much security is "enough"?

What should we do?

What should we do about security (concrete)?

- Current drafts which could be applicable to this WG
  - draft-dupont-ipv6-rfc3041harmful-02.txt
  - draft-savola-ipv6-rh-ha-security-03.txt
  - draft-savola-ipv6-rh-hosts-00.txt
  - draft-cmetz-v6ops-v4mapped-api-harmful-00.txt + draft-itojun-v6ops-v4mapped-harmful-01.txt
  - draft-bellovin-ipv6-accessprefix-01.txt + draft-zill-ipv6wg-zone-prefixlen-00.txt
    - something like this is very much in scope
  - draft-savola-v6ops-6to4-security-02.txt
  - draft-savola-v6ops-firewalling-01.txt
  - draft-savola-v6ops-security-overview-00.txt
  - draft-okazaki-v6ops-natpt-security-00.txt

What should we do?

What should we do about security (concrete)?

- Adopt some of the previous drafts?
  - Good candidates
    - draft-savola-v6ops-6to4-security-02.txt
    - draft-savola-v6ops-firewalling-01.txt
  - If not adapt, push for being worked on (security area? IPv6 wg?)
    - draft-bellovin-ipv6-accessprefix-01.txt or draft-zill-ipv6wg-zone-prefixlen-00.txt
- Should we start working on something new?
  - Bring in that security input from the ops/users community!
  - How to go about those issues in IPv6 specs?
  - Need to create two documents on security? *ARE* there issues to document?
    - (ch4): potential security risks in the operation of IPv4/IPv6?
    - (ch6): identify open sec issues with deployment scenarios?
  - If so, maybe need a small editorial team (or DT).