

6to4 Security

Security Considerations for 6to4

draft-savola-v6ops-6to4-security-00.txt

Pekka Savola, CSC/FUNET

6to4 Security

Issues

- 6to4 spec is very terse on security considerations
 - describes the operational modes better
 - analyses the threats and remainder threats
 - gives examples of rules which could be used when implementing
 - problem: security checks difficult to implement if multiple (automatic) tunneling mechanisms are used in the same box
 - attack scenarios

- "Anyone spoofing the relay router" problem
 - a few thoughts on ways to solve the problem
 - more detail in the next slide

For more details, see the draft.

6to4 security - relay spoofing

Relay spoofing

□ Issue

- Anyone can send packets to 6to4 routers, spoofed to come from e.g. 2001::/16 addresses, pretending they come from a relay
- Relays' source address can be anything at all

□ Tentative patches (1)

- Relays use RFC3068 192.88.99.0/24 as their source address
- Attack would depend on being able to spoof 192.88.99.0/24
 - ▷ - slightly more difficult?
- But causes "anycast as source address" problems..

□ Tentative patches (2)

- Limited distribution of more specific 6to4 routes
- E.g. multihop eBGP sessions between all relays
 - ▷ - no global routing table pollution, scalability through hierarchy
- (More) bidirectional traffic flow, multicast might also be easier
 - ▷ - a concept of "home relay"

6to4 security - ways forward?

What to do?

- Relay problem

- is this a can of worms we must open?
- should it be moved to a separate draft? (other parts of the draft are ready, this is a tougher problem)
- should the proposed solutions be developed a bit more?

- Other parts of the draft ("old draft")

- need to push it e.g. as an Informational RFC?
- w.g. document?