

PCP Security Considerations

Paul Selkirk

IETF 79, Beijing
November 11, 2010

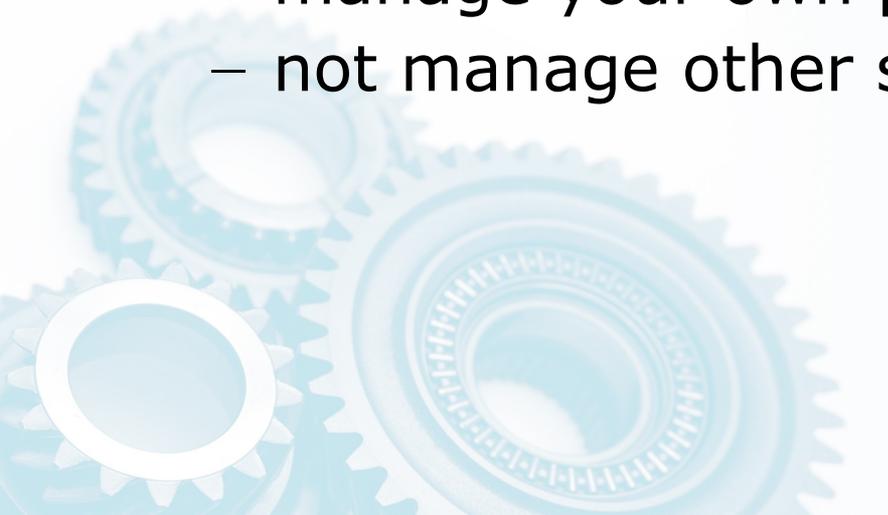


Threat Model

- Attacks against subscriber
 - delete mappings
 - steal mappings to steal traffic
 - create mappings to flood their site
 - create mappings to exhaust their quota
- Attacks against NAT/PCP server
 - create mappings to exhaust total mapping pool
 - create mappings with short lifetimes to thrash PCP server/NAT
 - reboot non-state-maintaining server to delete mappings

Basic Terminology

- Authentication - who are you?
 - subscriber identifier
 - currently subscriber address
- Authorization - what are you allowed to do?
 - manage your own port mappings
 - not manage other subscribers' port mappings



Local NAT scenario

- No security
 - because you can manage mappings on behalf of another local device



Non-local NAT scenario

- BCP 38 ingress filtering
 - needed for all traffic, should already be present
- ISP controls the path between the subscriber and the PCP server
- Renumbering breaks all mappings
 - don't reuse addresses before mappings expire
- see DS-Lite Security Considerations
 - PCP doesn't need stronger security

Questions?

