Balanced Security for IPv6 CPE

draft-v6ops-vyncke-balanced-ipv6-security

IETF86 Orlando

M. Gysi, G. Leclanche, E. Vyncke, R. Anfinsen

Status

- -00 posted on 25 January 2013
- Some comments on the list (see later)

Problem Statement /1

- The [famou] N[illegible] CPE [l]s provided for a [lt[illegible] [illegible]y wrt [illegible]
- For one S[illegible] [illegible]g [illegible]th[illegible] required to have a ‘f[illegible]rewal[illegible] place[illegible]
- And most network engineers, the end-to-end value of IPv6 is important

Beware!
This slide contains strong language and can lead to serious rat holes

Problem Statement /2
What do we do in IPv6?

- RFC 6092: Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
  - either blocking all inbound or allowing all inbound connections
  - Implementations exist in low-end CPE
- draft-vyncke-advanced-ipv6-security-03
  - Use more advanced filtering techniques such as IPS, reputation database, ...
  - More a Universal Threat Mitigation for large SMB/ organization
  - No implementation exists in low-end CPE

Balanced Security ?

Balanced Security?

- Based on Martin & Guillaume's idea for their Swisscom IPv6 CPE
  - Switzerland has 1.21% of IPv6-penetration dixit Google
  - Deployed for several months now in CH
  - Ragnar will do the same in NO
- Works like RFC 6092 in open mode
  - Allow all inbound traffic
  - **EXCEPT for well-known exceptions**

Exception?

- Some applications (identified by ports) are blocked:
  - Either inbound
  - or inbound_and_outbound
- Apps assumed to be too dangerous if exploited from outside
  - SSH, Telnet (!), HTTP (but not HTTPS), remote desktop
- Apps that should not cross the SP CPE ‘boundary’
  - RPC, NetBIOS, 445/TCP, AFP, ...

Meta-Exceptions?

- Users can override the default settings
- Exceptions are expected to evolved with time
- => suitable for SP-managed CPE

- I-D gives apps list for information only
  - Assumption is that the list will be selected by SP

Balanced Security: Summary

- Implemented
- Deployed
- Good balance between
  - Security even if not perfect
  - Global reachability for all hosts

Next Steps?

- Revise the document to handle some comments on the list
  - Refer to RFC 4890 for ICMP
  - Mobile networks?
  - Rules centrally enforced in the network?
  - Stateless or stateful filtering
- Not sure about becoming WG item but we feel that this was useful to document
  - Informational RFC?