Improving resilience of BGP system ./. implementation bugs

Rüdiger Volk, Deutsche Telekom

grow, IETF82, Taipei November 2011

observed bugs + problem pattern

- handling of certain attribute types/values will ***blow up*** on a router:
  - classified as malformed (old school: session reset)
  - crash routing process
  - generate malformed update on propagation
- trigger can be injected several eBGP or iBGP hops away

- several major vendors have contributed such bugs in recent years (often - but not limited to optional transitive attributes)
- handling of this error class is “security problem with DoS vulnerability” - usually implies that policies about restricted disclosure are applied
- usually emergency software upgrades required - often delay for development of patch

- DoS threat is largely due to old BGP error handling rule: only way to deal with bad update is session reset - IDR is working on improved error handling
- filtering tools to stop propagation of recognized triggers is desired
- when such tools are generally available and widely deployed reasoning about restricted disclosure can change

some simple filtering primitives could help

- strip attribute (by type number) on ingress BEFORE update processing
- classify updates to be treated as malformed (and handled as withdrawal under new error handling without session reset) if specified attributes (type number) occur
- add generic “attribute type number n present” as criterium in router policy language (so we can reject routes)

logging + monitoring

- for all filtering actions adequate logging is required
- also figure out ways to monitor and query the interesting attributes

smarter people might ...

- ... have ideas how to specify more general "signatures" for dangerous BGP updates
- "generic attribute type" helps with some of the observed bugs - clearly not with all we had
- operators will have to take the responsibility for not doing harm by the filtering
- guidance on using filters will be expected like support and guidance on selecting patches and upgrades