Security issues in the Internet

An Overview

Overview

- Who am I
- The three basic elements of the Internet
- Main issues

Who am I

- Internet user since 1982
- Current affiliation: NLnet Labs
- Member of SSAC (ICANN)
- Member expert group ENISA
- Active in other I* circles

Three basic Elements

- Routing
- Numbers
- Names

Routing Attack Methods

- Spoofing (of devices)
- Taking over of devices
- Replaying packages

- Falsification of information
  - Advertisement of invalid data

Threats to Routing

- Router resource exhausting
- Instability
  - No convergence
- Black holing or redirection of traffic
- Network congestion
- Partitioning

Instability to the Net

- Black holing or redirection of traffic
  - “Harmless” extra router could eave drop
- Network congestion
  - Raising costs
- Partitioning
  - DOS

Proposals for Improvement

- Standard bodies
  - IETF RPSEC-WG
- Vendors
  - Cisco
  - Juniper
    - PKI based solutions
- Government Agencies (DHS, ENISA)

Security of Addresses?

- Neutral but important resources
- Who “owns” them
- Coupling between entity and address resource
- Long history but badly documented
- Are they properly allocated
  - Allocated?

Trusted addresses

- Helps in- and egress filtering
- Fortifies the routing fabric

Secure addresses

- RIR’s and IANA
- Certificates
  - A role in the routing fabric?
- Behavior of users (trust)

Host/Domain Names

- Numbers are easy for machines, hard for people
- Host/Domain names are identifiers
- Just for *lookup*
  - If you the name, you get the mapping
- DNS: Domain name service
  - Not a directory service

DNS Security

- Doesn’t qualify anything about the answer
  - GIGO
- Adds authentication to answer
- Details: next presentation

DNSSEC Crowd

- IETF
- ICANN/IANA (Root zone)
- RIR for Reversed Lookup
- TLD’s
- ISP’s
- Vendors

?
?