Source Address Validation

Merike Kaeo, Double Shot Security

What Is Source Address Validation?

- Techniques to verify that source IP addresses of packets submitted to the Internet are valid:
  - Not assigned from private address space; and
  - Fall within a range of legitimately advertised prefixes for a given origin.
- Currently developed techniques:
  - bogon filtering; and
  - uRPF,unicast reverse path forwarding.

Why Is This Important?

Source address validation mitigates IP spoofing

- Internet Protocol (IP) spoofing is commonly used for:
  - Denial of service attacks;
  - Spam campaigns; and
  - Impersonation of originating host, where IP address is used as a form of authentication.

Prior Work

- IETF BCP 38
- SSAC SAC004
- NIST 800-82
- US-CERT Malware Threats and Mitigation Strategies
- NSA Router Security Configuration Guide
- SANS (numerous citations)
- ISSA

Current SSAC Activity

- Study existing prior work:
  - Eliminate confusion over egress/ ingress filtering confusion.
- Study filtering by ISPs or edge networks;
- Study new developments in source address validation techniques;
- Debunk myths:
  - Cost, overhead, complexity; and
- Study costs and benefits of a holistic approach.