



# Situation Awareness and Border Gateway Protocol

# Situation Awareness



- Baseline monitoring and norming
- Internal (vertical) and external (horizontal) information sharing
- Event identification
- Event management
  - Data correlation and management
  - Prioritization
  - Decision processes
- Forensics and Damage assessment

# Situation Awareness - BGP Vulnerabilities



- **Background**
  - BGP is a routing protocol to direct traffic efficiently through internal and external networks
  - BGP routers send updates to each other to advertise the best routes; peers are trusted
  - BGP routers then choose the best route for your network traffic
- **Problem**
  - The way the route is chosen is vulnerable to attacks like Man-in-the-Middle, Denial of Service, and Black hole attacks
  - If the route your traffic takes is hijacked, control and security of your data is lost
  - This is unacceptable for mission critical data – BGP routes must be protected
- **Solution**
  - Defend a network by validating BGP updates before the router applies the change
  - Use BGP monitoring and filtering to detect, and mitigate suspicious BGP update packets in a timely manner
  - Instill trust in the routes that are updated to protect your data

# Notable BGP Events

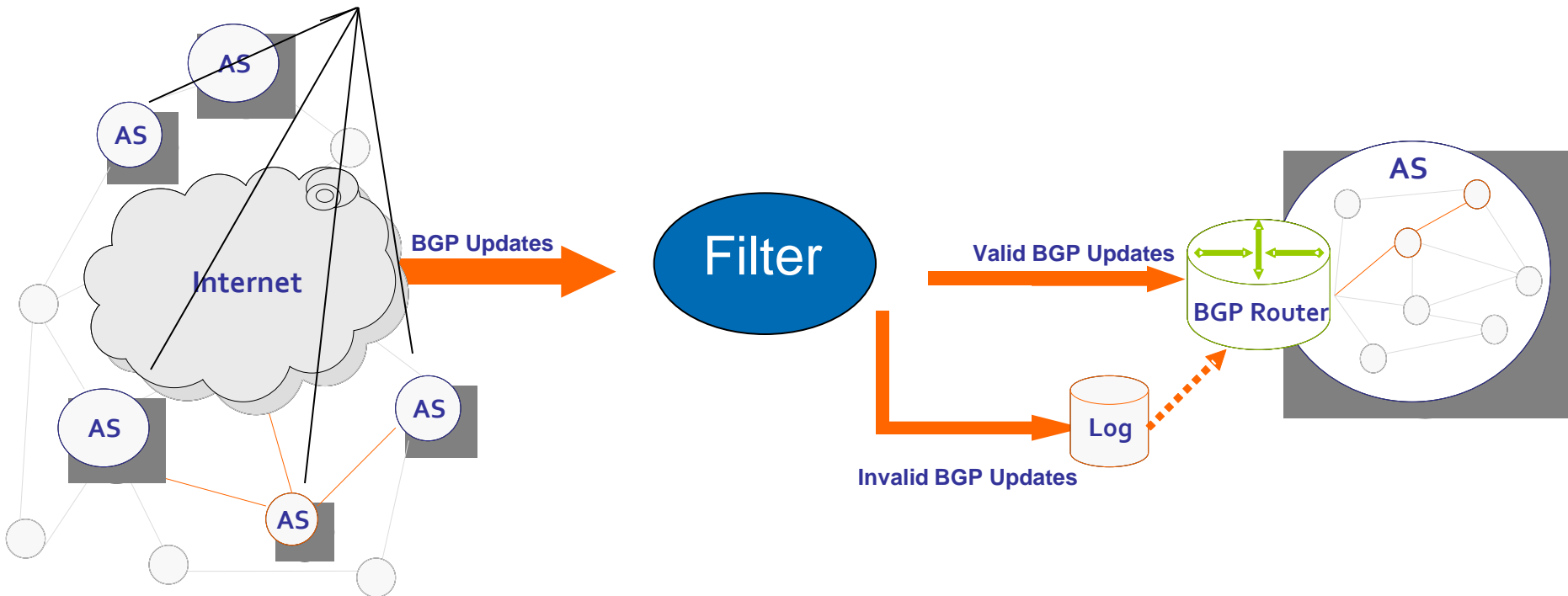


- 1997 MAI Network Services Blackhole (AS 7007)
- Man-in-the-Middle at DEFCON 2008
  - Kapela and Pilosov set up an autonomous system (AS) and demonstrated their BGP man-in-the-middle attack during their presentation
- Pakistan YouTube® Black hole
  - Misconfiguration of a BGP route update, which was meant to restrict YouTube access in Pakistan, caused all YouTube traffic to route to a Pakistan AS
- China Telecom misroute in Apr 10
  - 15% of world's internet routes misrouted via Beijing. Impacted .gov and .mil traffic for 18 minutes. Hijack, misconfig, or training?

# Potential Solutions



## Resource Public Key Infrastructure (RPKI)



# Implementation Strategies



- Topology
  - Closed or open networks
  - Peering
  - Internal vs. external BGP
  - Inline or passive filtering
- Policy
  - Trusted routes and AS e.g. RPKI
  - Untrusted autonomous systems
- Analysis and Visualization
  - Logging
  - Dashboard displays
  - Customized reporting features
  - External validation of routing

# Questions?



[robert.j.giesler@saic.com](mailto:robert.j.giesler@saic.com)