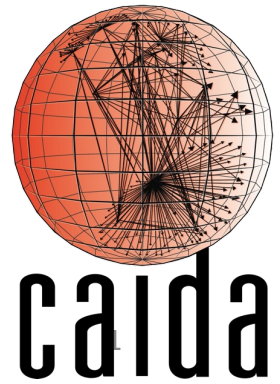
CSE291 Internet Data Science for Cybersecurity

MANRS

2/22/2023

Ben Du

UCSDCSE
Computer Science and Engineering



The MANRS Initiative

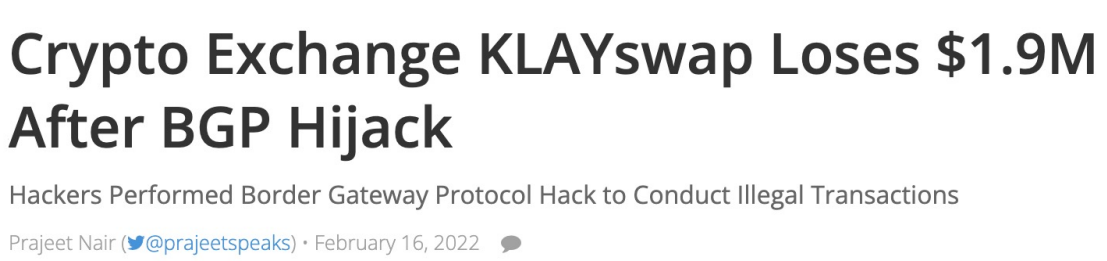
- The Mutually Agreed Norms on Routing Security initiative was launched by network operators in 2014.

- "MANRS provides crucial fixes to reduce the most common routing threats[1]". -- About MANRS

1. https://www.manrs.org/about/

Internet routing vulnerability

- The Border Gateway Protocol includes no mechanism to validate information exchanged between networks.
- Attackers can advertise IP address space without authorization. (BGP Hijacking)



Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack

Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

Prajeet Nair (@prajeetspeaks) • February 16, 2022

BORDER GATEWAY PROTOCOL INSECURITY —

How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

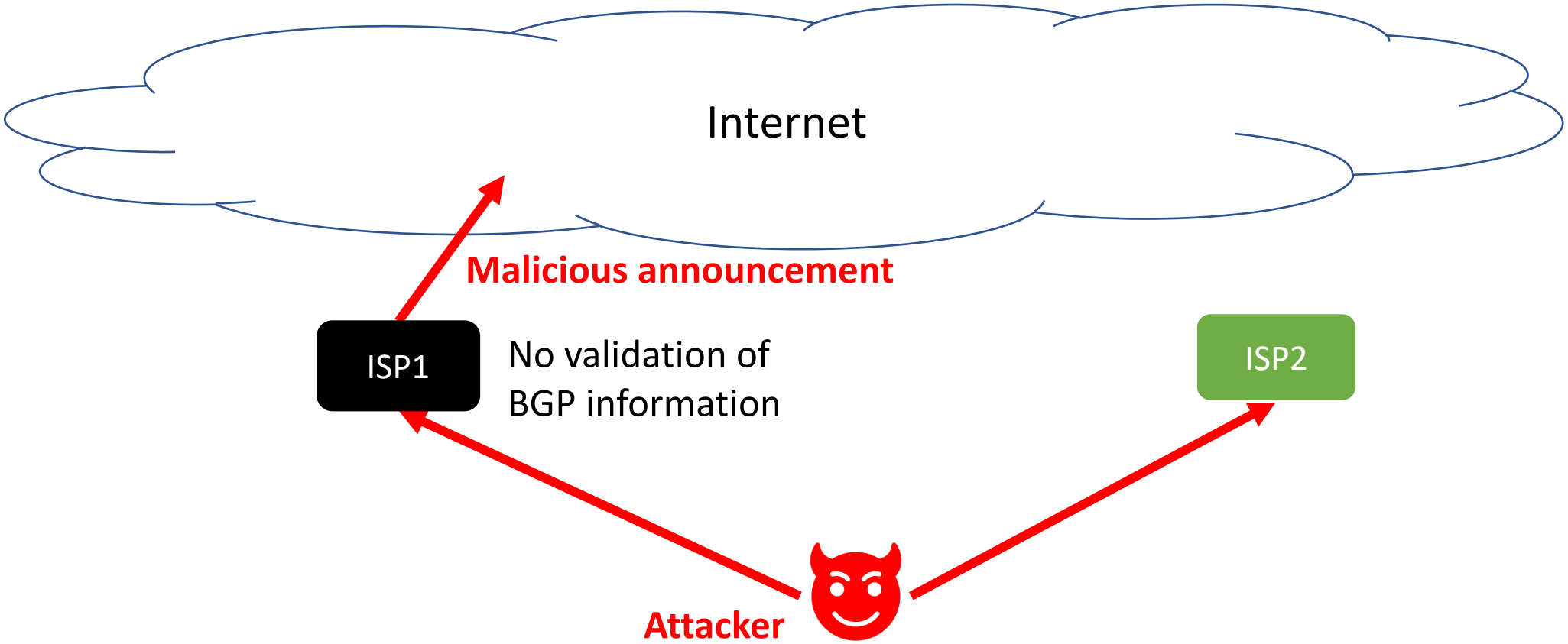
DAN GOODIN - 9/23/2022, 11:04 AM

Infrastructure to improve routing security

- One way to address routing threats is to validate received BGP information.
- **Routing databases** provide reference information.
- Internet Routing Registry (IRR)
- Resource Public Key Infrastructure (RPKI)
  - 5 RIRs as root of trust

Routing security is a collective action problem

- Networks need to collectively adopt routing security practices to improve overall routing security



MANRS security practices (actions)

- Networks have misaligned incentive to implement security practices.
- MANRS encourages networks to adopt routing security practices.

- Action 1: Use IRR/RPKI to check correctness of customers' BGP announcements.
- Action 2 (optional): Filter outbound traffic with spoofed source IP and run the CAIDA Spoofer software to prevent DDoS attack traffic from being originated from the participant's network.
- Action 3: Maintain up-to-date network contact information in IRR databases or PeeringDB.
- Action 4: Register intended BGP announcements in IRR or RPKI.