Aktiviteter för säkert trafikutbyte

Sårbarheter i Border Gateway Protocol

Björn Hesthamar
Avdelningen för säker kommunikation

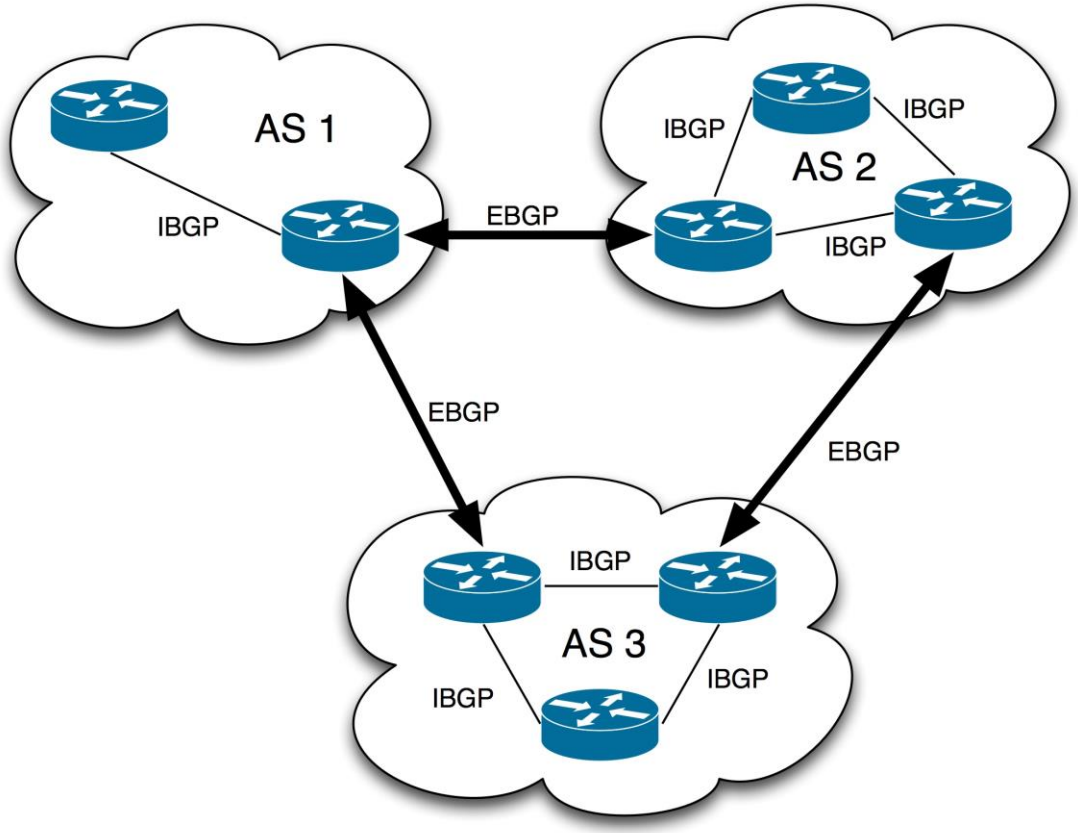
PTS

BGB 101 – BGP på 60 sekunder

- Protokollet för att ”hitta lämpligaste vägen på internet”.
- Bygger på centralt tilldelade **AS nummer** för att identifiera organisationers olika nätverk och **IP-adresser** för att identifiera enheter i olika nätverk
- AS-nummer tilldelas av ICANN (IANA) och de fem olika ”Regional Internet Registers” (RIPE i Europa)
- BGP möjliggör trafikutbyte (peering) mellan olika nät (AS).
- Kan ske direkt eller hos en 3:de part / knutpunkt (IXP)

BGB 101 – fortsättning

- Peering lönar sig oftast, en ISP får kortare väg till fler kunder genom att koppla om och skriva lite routingtabeller
- Peering ökar ofta komplexitet och risk
- När peering skapas så talar routrarna kontinuerligt med varandra över BGP och skapar en routingtabell för vilken trafik till olika AS-nummer som det är lämpligt att sända över de olika förbindelserna
- Ett AS-nummer är en förutsättning för att kunna hålla en helt redundant förbindelse
  (exempelvis därför har PTS ett AS-nummer)


AS 1
IBGP
EBGP
IBGP
IBGP
AS 2
IBGP
EBGP
EBGP
IBGP
AS 3
IBGP
IBGP

Syns du inte,
så finns du inte

Vad som saknas i BGP

- Stammar från en tid där alla aktörer litade lika mycket på varandra
- Verifierar inte rätten att annonsera en rutt
- Autentiserar inte avsändare och skyddar inte riktighet för den information som annonseras
- Detta möjliggör ett flertal sårbarheter

Kända sårbarheter

- Felaktiga annonseringar av autonoma system
- De-aggregation
  - En mer specifik rutt annonseras
- Path-attribute manipulation
  - Styr om trafik genom att lova en fördelaktig väg
- Svarthålning av trafik
- Avlyssning (MITM)
- Trafikomdirigering
  - Trafikloopar, förseningar eller överbelastning

Illasinnade aktörer

- Stater
  - Industrispionage
  - Sabotage
  - Kontroll
- Organiserad brottslighet
- Hacktivister
- Insiders

En handfull av de senare årens händelser

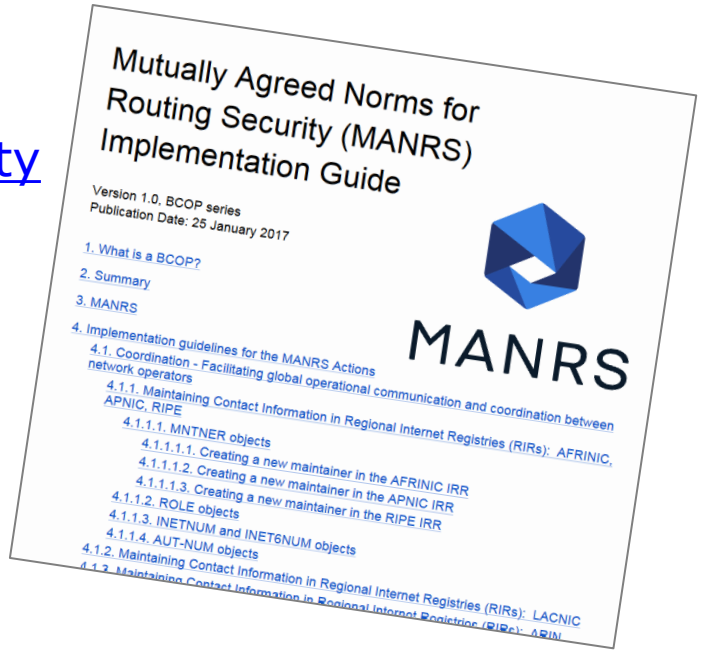
- December 2017 trafik mot Amerikanska webbsidor omdirigeras att gå via Ryssland
- April 2018 Amazon EC2 trafik omdirigeras för att stjäla tillgång till kryptovaluta
- Juni 2018 icke publikt använda IP-adresser kapas för att skapa falsk trafik mot reklamsidor
- November 2018 nationell Amerikansk trafik omdirigeras att gå via Ryssland till Kina
- Januari 2019 AS-prefix som tillhör US Dep. of Energy hamnar hos China Telecom

Vad behöver göras?

Let’s analyze

Initiativ för säker peering

- ISOC.org MANRS
- ENISA Internet Infrastructure Security and Resilience Reference Group
- RIPE NCC
- IETF BCP 194 (RFC 7454)




NO BGP
FOR YOU!
memegenerator.net

Aktivitet i tillsynsplanen 2019-2020

- Få nationella incidenter, betydligt fler internationellt
- PTS önskar att få information om hur förberedda anmälda operatörer är för incidenter relaterade till BGP
- PTS kommer under hösten 2019 att inleda tillsyn med avseende på att granska kunskap om sårbarheter i BGP och vidtagna åtgärder för att skydda information under överföring
- Skriftlig informationsinhämtning och tillsynsmöten

Frågor?

Bilder från: NASA, Cisco, Samuel Zeller, Sky News och NBC