CS558 Network Security

Lecture 6: BGP Hijacking Mitigations

BOSTON UNIVERSITY

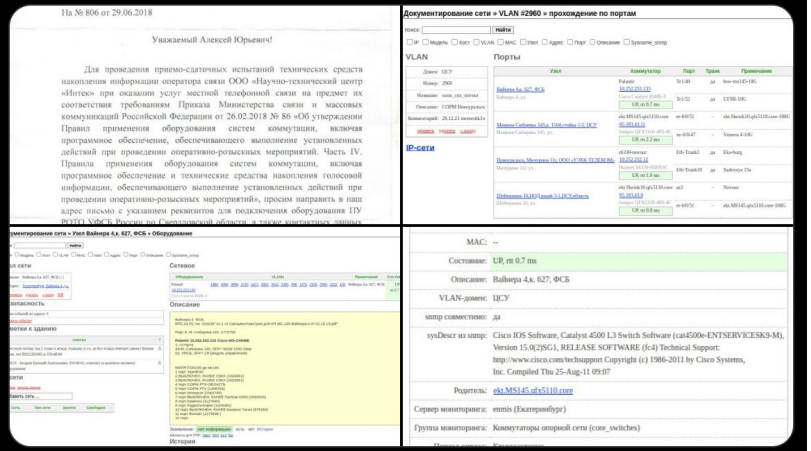
← **Tweet**

Anonymous Operations
@AnonOpsSE

#Anonymous #OpRussia convex.ru, hacked
they provide telecom services in #Russia,
internet/telephone/cable
Government, business

Green Atom project exposed and used for spying on Internet/telephone traffic under an agreement with the FSS

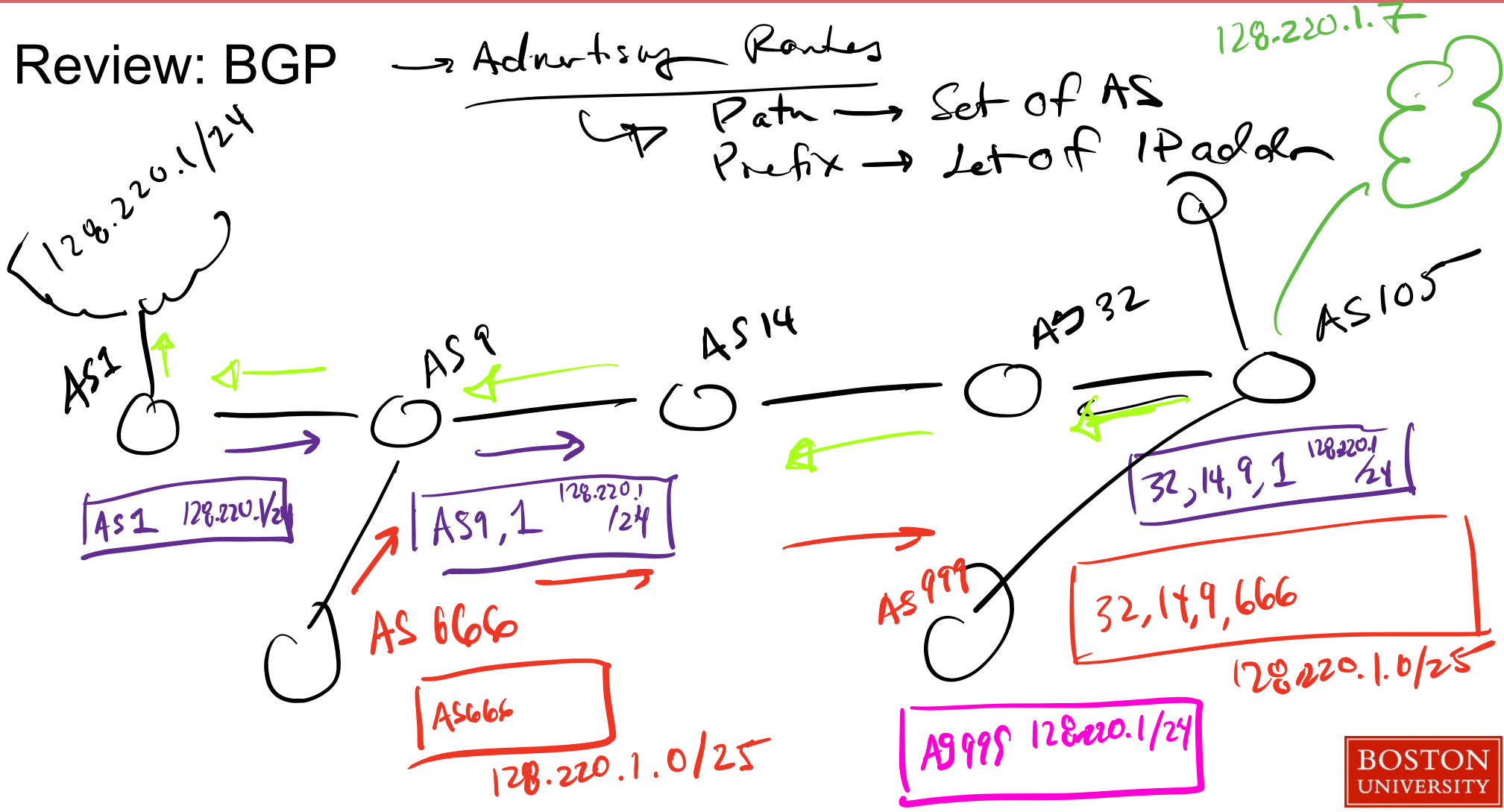
Credit- CAXXII
#Ukraine



2:02 PM · Jan 31, 2023 · **28K** Views

77 Retweets **13** Quote Tweets **276** Likes

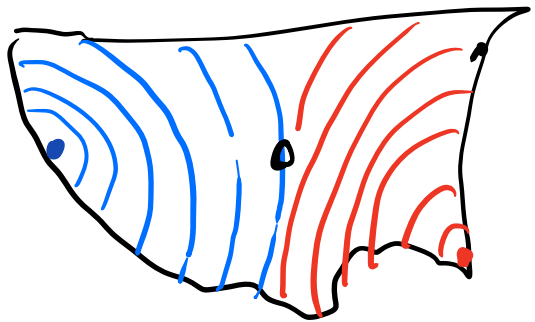
Review: BGP



Review: BGP

- Decision Criteria:
  - Best Prefix match → most Specific match wins
  - ~~AS~~ Shortest AS Path

Shorter Path Attack



Subprefix Hijack

Super Scary

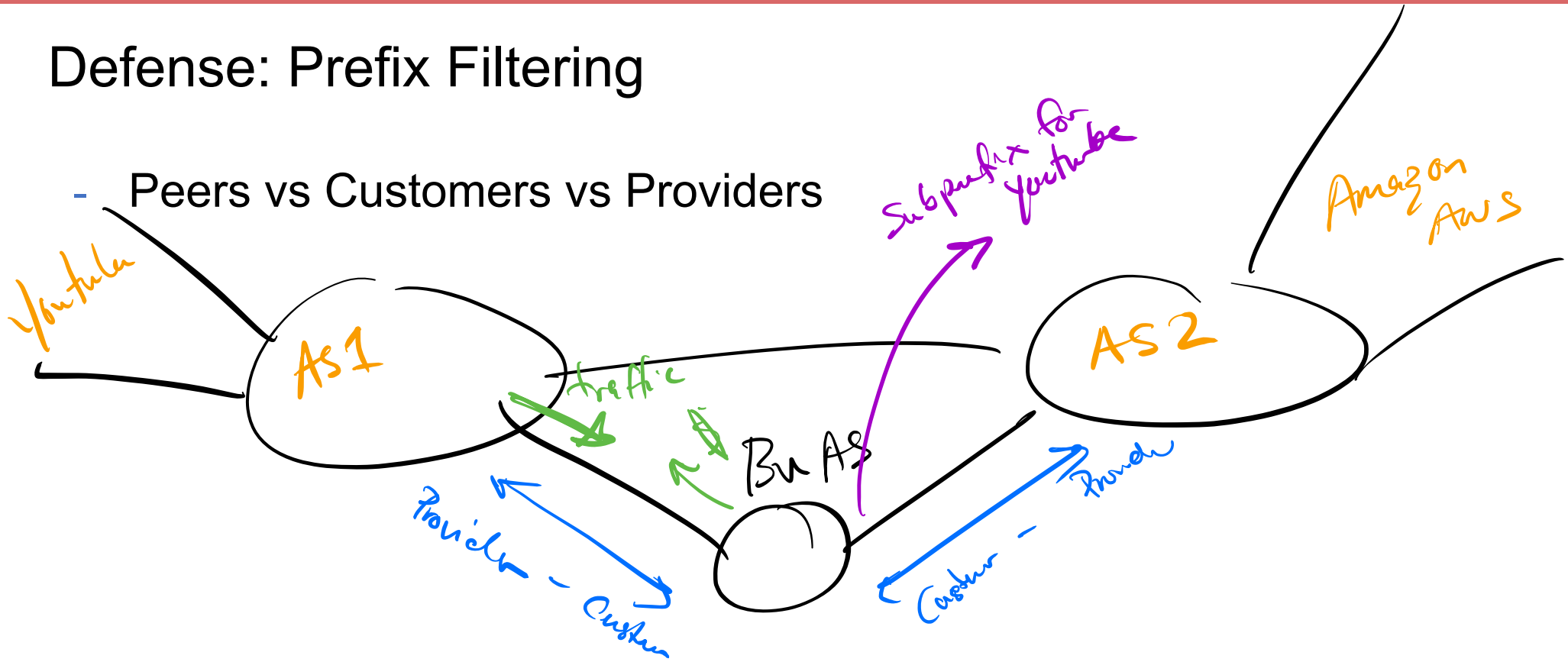
global impact

BGP Hijacking

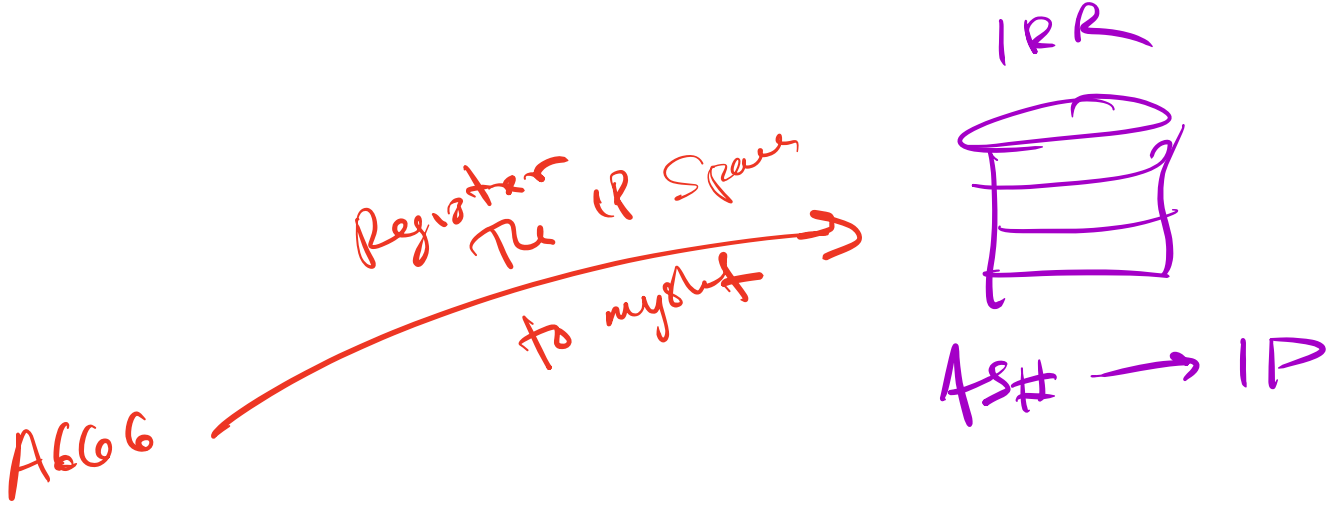
- Sub-prefix Hijack
- Hijack with Shorter AS PATH

Defense: Prefix Filtering

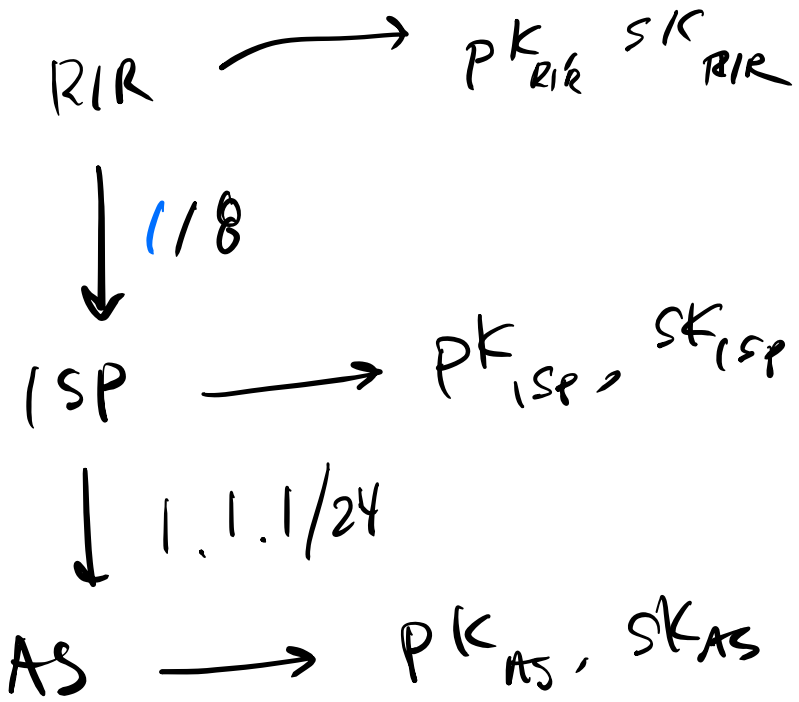
- Peers vs Customers vs Providers



Defense: IRR → Internet Routing Registry



Defense: RPKI (Resource Public Key Infrastructure)



$Sign_{sk_{RIR}}(\text{"ISP } pk_{ISP} \text{ 1/8"}) \rightarrow \sigma_{RIR}$

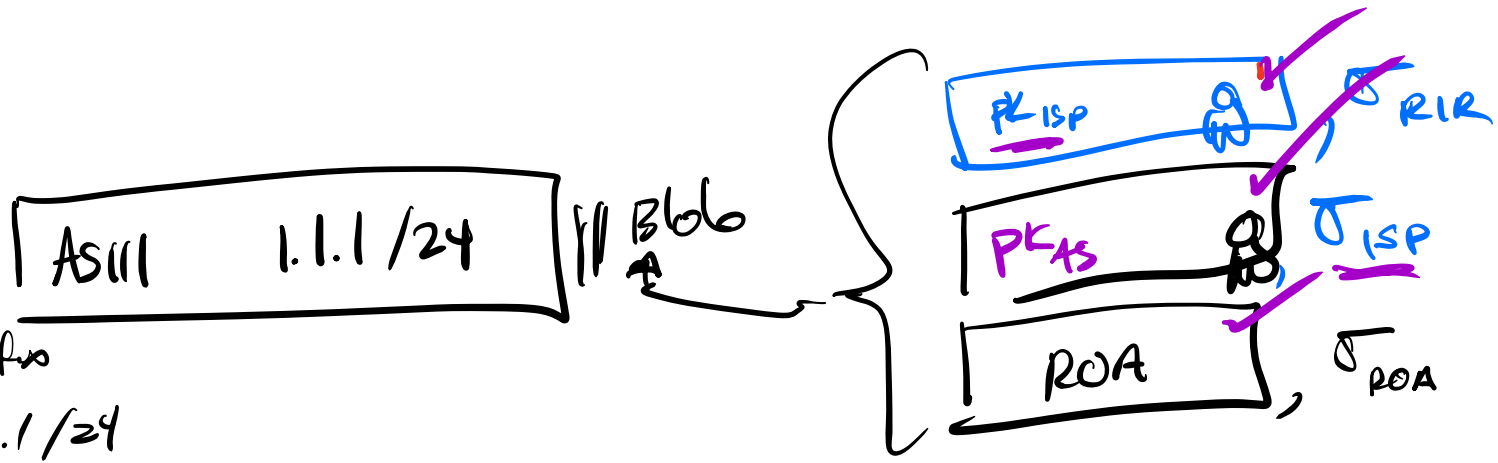
$Sign_{sk_{ISP}}(\text{"AS } pk_{AS} \text{ 1.1.1/24"}) \rightarrow \sigma_{ISP}$

ROA (Route Origin Authorization)

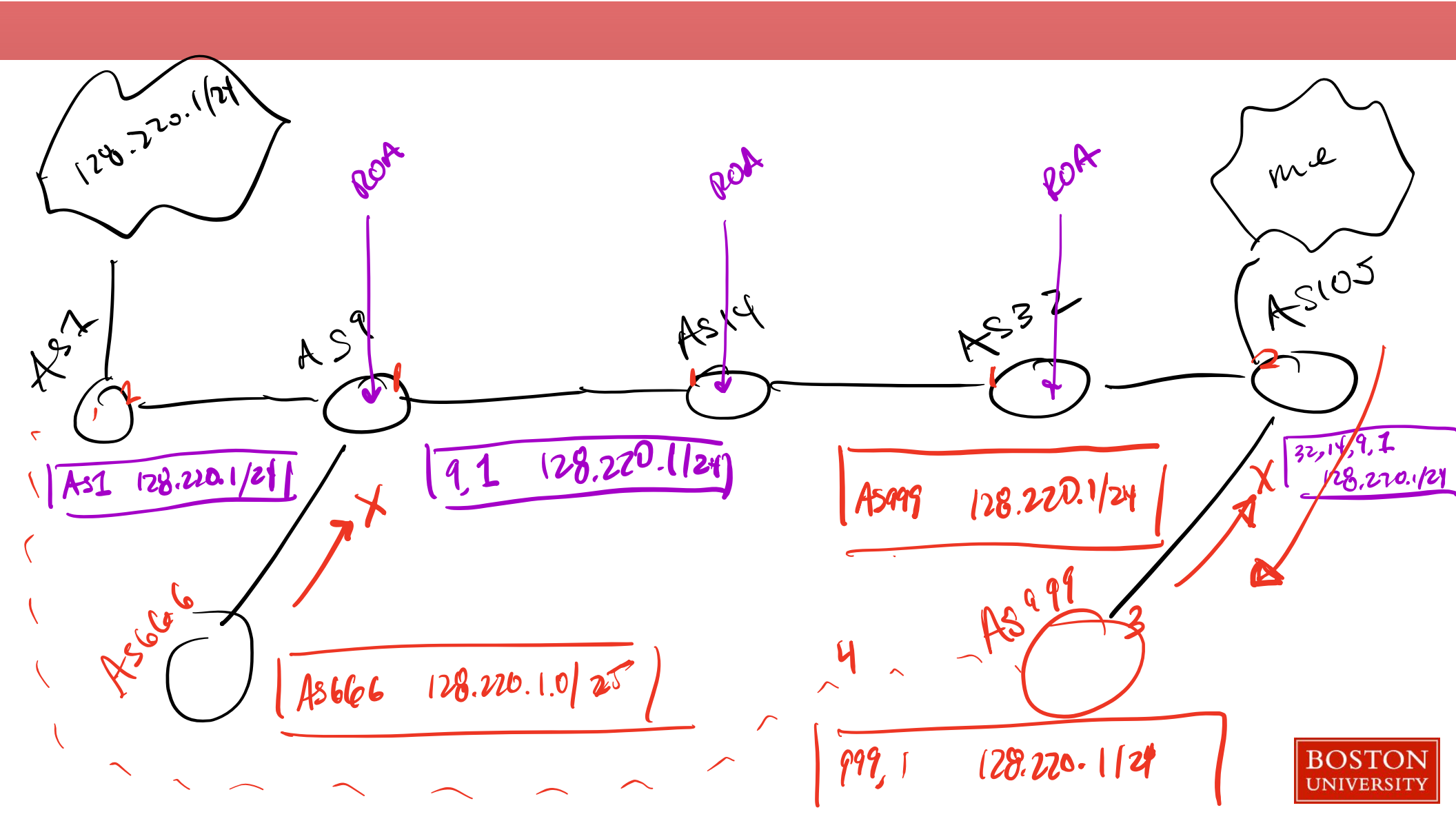
m = "[AS 111 1.1.1/24 28]"

$Sign_{SK_{AS}}(m) \rightarrow \sigma_{ROA}$

Circulate two "out of band"



AS#	IP prefixes
111	1.1.1/24
123	2.2.2/24


128.220.1/24
ROA
ROA
ROA
me
AS1
AS9
AS14
AS37
AS105
AS1 128.220.1/24
9,1 128.220.1/24
AS999 128.220.1/24
32,14,9,1
128.220.1/24
X
X
AS666
AS999
AS666 128.220.1.0/25
999,1 128.220.1/24
4

Take Aways so far

- Prefix Filtering
  - No changes to BGP
  - Takes out edge AS's from your thread model
- RPKI
  - No changes to BGP
  - Addresses sub-prefix Hijacking
  - Still allows to the one-hop attack
- Next class: BGPSec
  - What can we do if we change the protocol?