

CS558 Network Security

Lecture 6: BGP Hijacking Mitigations

hello



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

№ 806 от 29.06.2018

Уважаемый Алексей Юрьевич!

Для проведения прямо-сдаточных испытаний технических средств накопления информации оператора связи ООО «Научно-технический центр «Атлас» при оказании услуг местной телефонной связи на предмет их соответствия требованиям Приказа Министерства связи и массовых коммуникаций Российской Федерации от 26.02.2018 № 86 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-рольских мероприятий. Часть IV. Правила применения оборудования систем коммутации, включая программное обеспечение и технические средства накопления голосовой информации, обеспечивающего выполнение установленных действий при проведении оперативно-рольских мероприятий», просим направить в наш адрес письмо с указанием реквизитов для подключения оборудования ПУ

Документирование сети • VLAN #260 • прохождение по портам

Имя: **convex**

☐ IP ☐ MAC ☐ VLAN ☐ DNS ☐ DNS ☐ Адрес ☐ Порт ☐ Описание ☐ Протокол_порт

VLAN	Порт	Узел	Коммутатор	Порт	Примечание
260	1/24	10.10.10.1	10.10.10.1	1/24	10.10.10.1
260	1/24	10.10.10.2	10.10.10.2	1/24	10.10.10.2
260	1/24	10.10.10.3	10.10.10.3	1/24	10.10.10.3
260	1/24	10.10.10.4	10.10.10.4	1/24	10.10.10.4
260	1/24	10.10.10.5	10.10.10.5	1/24	10.10.10.5
260	1/24	10.10.10.6	10.10.10.6	1/24	10.10.10.6
260	1/24	10.10.10.7	10.10.10.7	1/24	10.10.10.7
260	1/24	10.10.10.8	10.10.10.8	1/24	10.10.10.8
260	1/24	10.10.10.9	10.10.10.9	1/24	10.10.10.9
260	1/24	10.10.10.10	10.10.10.10	1/24	10.10.10.10
260	1/24	10.10.10.11	10.10.10.11	1/24	10.10.10.11
260	1/24	10.10.10.12	10.10.10.12	1/24	10.10.10.12
260	1/24	10.10.10.13	10.10.10.13	1/24	10.10.10.13
260	1/24	10.10.10.14	10.10.10.14	1/24	10.10.10.14
260	1/24	10.10.10.15	10.10.10.15	1/24	10.10.10.15
260	1/24	10.10.10.16	10.10.10.16	1/24	10.10.10.16
260	1/24	10.10.10.17	10.10.10.17	1/24	10.10.10.17
260	1/24	10.10.10.18	10.10.10.18	1/24	10.10.10.18
260	1/24	10.10.10.19	10.10.10.19	1/24	10.10.10.19
260	1/24	10.10.10.20	10.10.10.20	1/24	10.10.10.20
260	1/24	10.10.10.21	10.10.10.21	1/24	10.10.10.21
260	1/24	10.10.10.22	10.10.10.22	1/24	10.10.10.22
260	1/24	10.10.10.23	10.10.10.23	1/24	10.10.10.23
260	1/24	10.10.10.24	10.10.10.24	1/24	10.10.10.24
260	1/24	10.10.10.25	10.10.10.25	1/24	10.10.10.25
260	1/24	10.10.10.26	10.10.10.26	1/24	10.10.10.26
260	1/24	10.10.10.27	10.10.10.27	1/24	10.10.10.27
260	1/24	10.10.10.28	10.10.10.28	1/24	10.10.10.28
260	1/24	10.10.10.29	10.10.10.29	1/24	10.10.10.29
260	1/24	10.10.10.30	10.10.10.30	1/24	10.10.10.30
260	1/24	10.10.10.31	10.10.10.31	1/24	10.10.10.31
260	1/24	10.10.10.32	10.10.10.32	1/24	10.10.10.32
260	1/24	10.10.10.33	10.10.10.33	1/24	10.10.10.33
260	1/24	10.10.10.34	10.10.10.34	1/24	10.10.10.34
260	1/24	10.10.10.35	10.10.10.35	1/24	10.10.10.35
260	1/24	10.10.10.36	10.10.10.36	1/24	10.10.10.36
260	1/24	10.10.10.37	10.10.10.37	1/24	10.10.10.37
260	1/24	10.10.10.38	10.10.10.38	1/24	10.10.10.38
260	1/24	10.10.10.39	10.10.10.39	1/24	10.10.10.39
260	1/24	10.10.10.40	10.10.10.40	1/24	10.10.10.40
260	1/24	10.10.10.41	10.10.10.41	1/24	10.10.10.41
260	1/24	10.10.10.42	10.10.10.42	1/24	10.10.10.42
260	1/24	10.10.10.43	10.10.10.43	1/24	10.10.10.43
260	1/24	10.10.10.44	10.10.10.44	1/24	10.10.10.44
260	1/24	10.10.10.45	10.10.10.45	1/24	10.10.10.45
260	1/24	10.10.10.46	10.10.10.46	1/24	10.10.10.46
260	1/24	10.10.10.47	10.10.10.47	1/24	10.10.10.47
260	1/24	10.10.10.48	10.10.10.48	1/24	10.10.10.48
260	1/24	10.10.10.49	10.10.10.49	1/24	10.10.10.49
260	1/24	10.10.10.50	10.10.10.50	1/24	10.10.10.50
260	1/24	10.10.10.51	10.10.10.51	1/24	10.10.10.51
260	1/24	10.10.10.52	10.10.10.52	1/24	10.10.10.52
260	1/24	10.10.10.53	10.10.10.53	1/24	10.10.10.53
260	1/24	10.10.10.54	10.10.10.54	1/24	10.10.10.54
260	1/24	10.10.10.55	10.10.10.55	1/24	10.10.10.55
260	1/24	10.10.10.56	10.10.10.56	1/24	10.10.10.56
260	1/24	10.10.10.57	10.10.10.57	1/24	10.10.10.57
260	1/24	10.10.10.58	10.10.10.58	1/24	10.10.10.58
260	1/24	10.10.10.59	10.10.10.59	1/24	10.10.10.59
260	1/24	10.10.10.60	10.10.10.60	1/24	10.10.10.60
260	1/24	10.10.10.61	10.10.10.61	1/24	10.10.10.61
260	1/24	10.10.10.62	10.10.10.62	1/24	10.10.10.62
260	1/24	10.10.10.63	10.10.10.63	1/24	10.10.10.63
260	1/24	10.10.10.64	10.10.10.64	1/24	10.10.10.64
260	1/24	10.10.10.65	10.10.10.65	1/24	10.10.10.65
260	1/24	10.10.10.66	10.10.10.66	1/24	10.10.10.66
260	1/24	10.10.10.67	10.10.10.67	1/24	10.10.10.67
260	1/24	10.10.10.68	10.10.10.68	1/24	10.10.10.68
260	1/24	10.10.10.69	10.10.10.69	1/24	10.10.10.69
260	1/24	10.10.10.70	10.10.10.70	1/24	10.10.10.70
260	1/24	10.10.10.71	10.10.10.71	1/24	10.10.10.71
260	1/24	10.10.10.72	10.10.10.72	1/24	10.10.10.72
260	1/24	10.10.10.73	10.10.10.73	1/24	10.10.10.73
260	1/24	10.10.10.74	10.10.10.74	1/24	10.10.10.74
260	1/24	10.10.10.75	10.10.10.75	1/24	10.10.10.75
260	1/24	10.10.10.76	10.10.10.76	1/24	10.10.10.76
260	1/24	10.10.10.77	10.10.10.77	1/24	10.10.10.77
260	1/24	10.10.10.78	10.10.10.78	1/24	10.10.10.78
260	1/24	10.10.10.79	10.10.10.79	1/24	10.10.10.79
260	1/24	10.10.10.80	10.10.10.80	1/24	10.10.10.80
260	1/24	10.10.10.81	10.10.10.81	1/24	10.10.10.81
260	1/24	10.10.10.82	10.10.10.82	1/24	10.10.10.82
260	1/24	10.10.10.83	10.10.10.83	1/24	10.10.10.83
260	1/24	10.10.10.84	10.10.10.84	1/24	10.10.10.84
260	1/24	10.10.10.85	10.10.10.85	1/24	10.10.10.85
260	1/24	10.10.10.86	10.10.10.86	1/24	10.10.10.86
260	1/24	10.10.10.87	10.10.10.87	1/24	10.10.10.87
260	1/24	10.10.10.88	10.10.10.88	1/24	10.10.10.88
260	1/24	10.10.10.89	10.10.10.89	1/24	10.10.10.89
260	1/24	10.10.10.90	10.10.10.90	1/24	10.10.10.90
260	1/24	10.10.10.91	10.10.10.91	1/24	10.10.10.91
260	1/24	10.10.10.92	10.10.10.92	1/24	10.10.10.92
260	1/24	10.10.10.93	10.10.10.93	1/24	10.10.10.93
260	1/24	10.10.10.94	10.10.10.94	1/24	10.10.10.94
260	1/24	10.10.10.95	10.10.10.95	1/24	10.10.10.95
260	1/24	10.10.10.96	10.10.10.96	1/24	10.10.10.96
260	1/24	10.10.10.97	10.10.10.97	1/24	10.10.10.97
260	1/24	10.10.10.98	10.10.10.98	1/24	10.10.10.98
260	1/24	10.10.10.99	10.10.10.99	1/24	10.10.10.99
260	1/24	10.10.10.100	10.10.10.100	1/24	10.10.10.100

MAC: --

Состав: UP, et 0.7 ms

Описание: Боллер 4х, 627, FCS

VLAN-дринг: ЦЕУ

http совместим: да

устройство из шпр: Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-ENTSERVICESK9-M), Version 15.0(2)SG1, RELEASE SOFTWARE (h4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 25-Aug-11 09:07

Подпись: [els MS145-05110.com](#)

Сервер мониторинга: emm (Евгений)

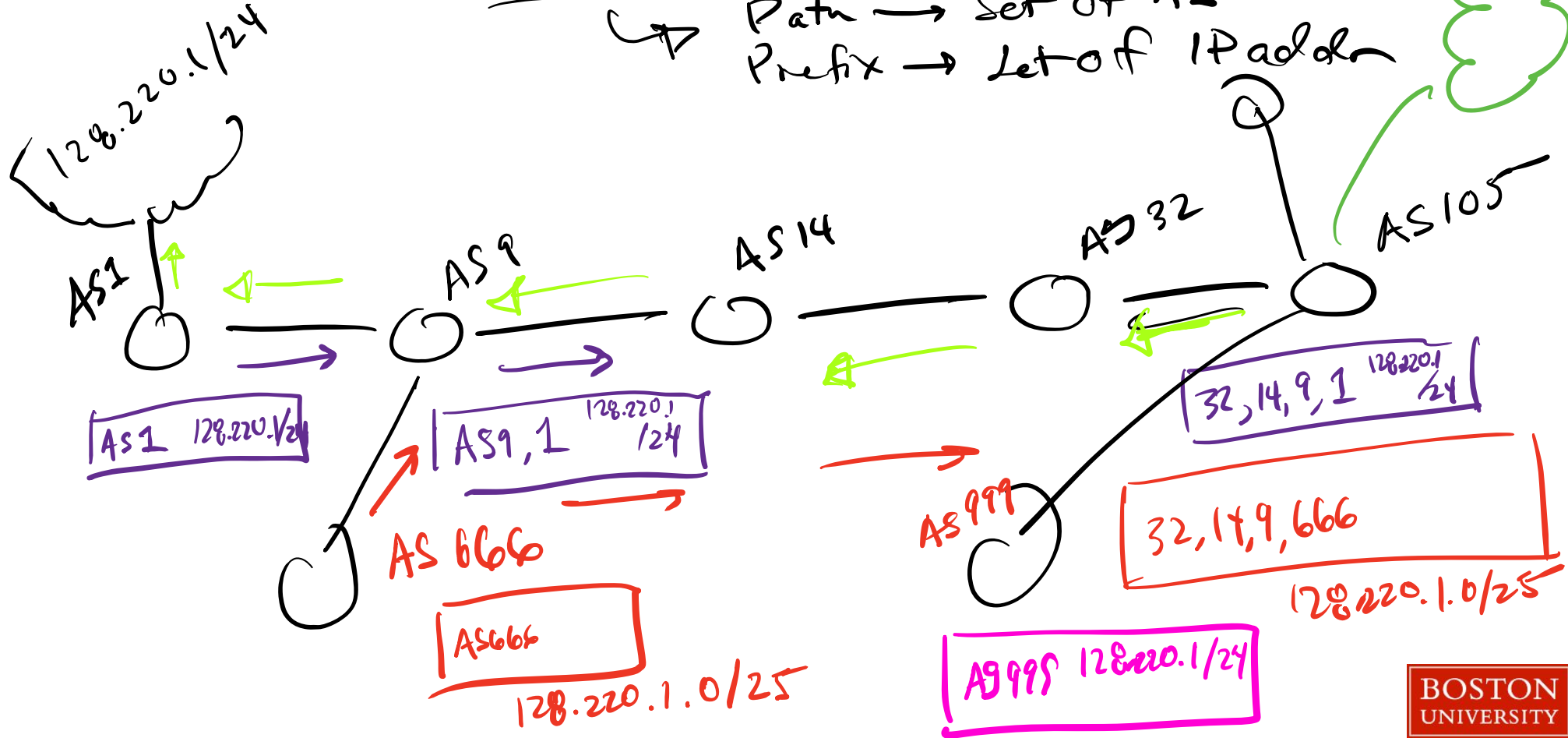
Группа мониторинга: Коммутаторы шпрной сети (core_switch)

2:02 PM · Jan 31, 2023 · 28K Views

Review: BGP

→ Advertising Routes

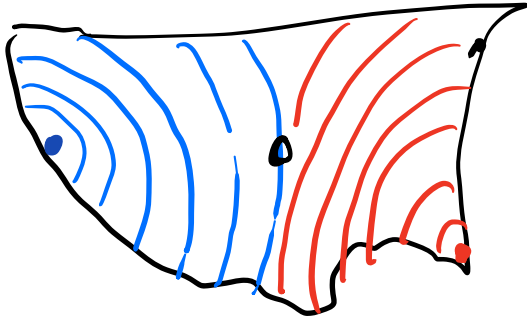
↳ Path → Set of AS
Prefix → Set of IP address



Review: BGP

- Decision Criteria:
 - Best Prefix match → most specific match wins
 - ~~As~~ Shortest As Path

Shorter Path Attack



Subprefix Hijack

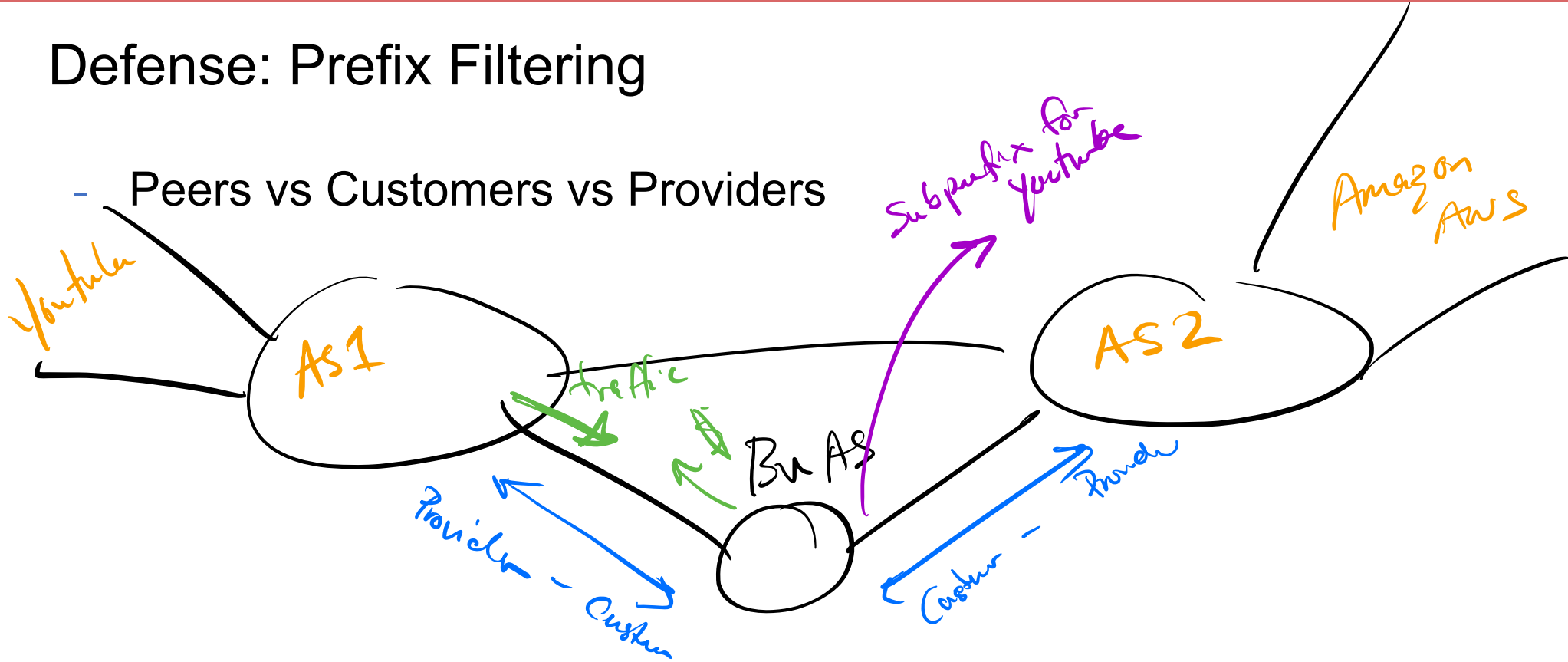
Super Scary
global impact

BGP Hijacking

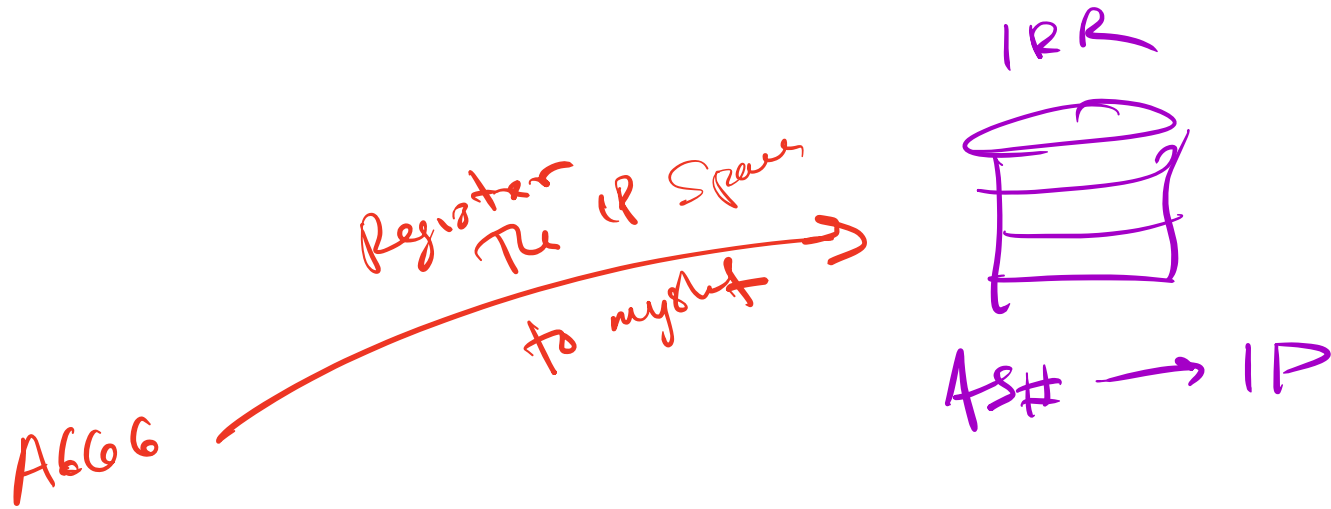
- Sub-prefix Hijack
- Hijack with Shorter AS PATH

Defense: Prefix Filtering

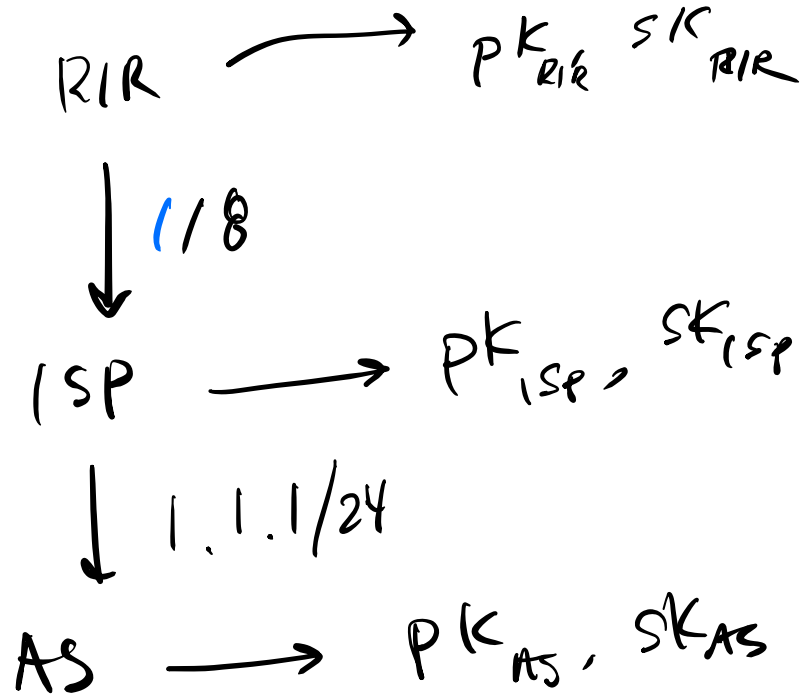
- Peers vs Customers vs Providers



Defense: IRR → Instant Reply Registry



Defense: RPKI (Resource Public Key Infrastructure)



$$\text{Sign}_{SK_{RIR}}(\text{"ISP 1/8"} \xrightarrow{PK_{ISP}}) \rightarrow \sigma_{RIR}$$

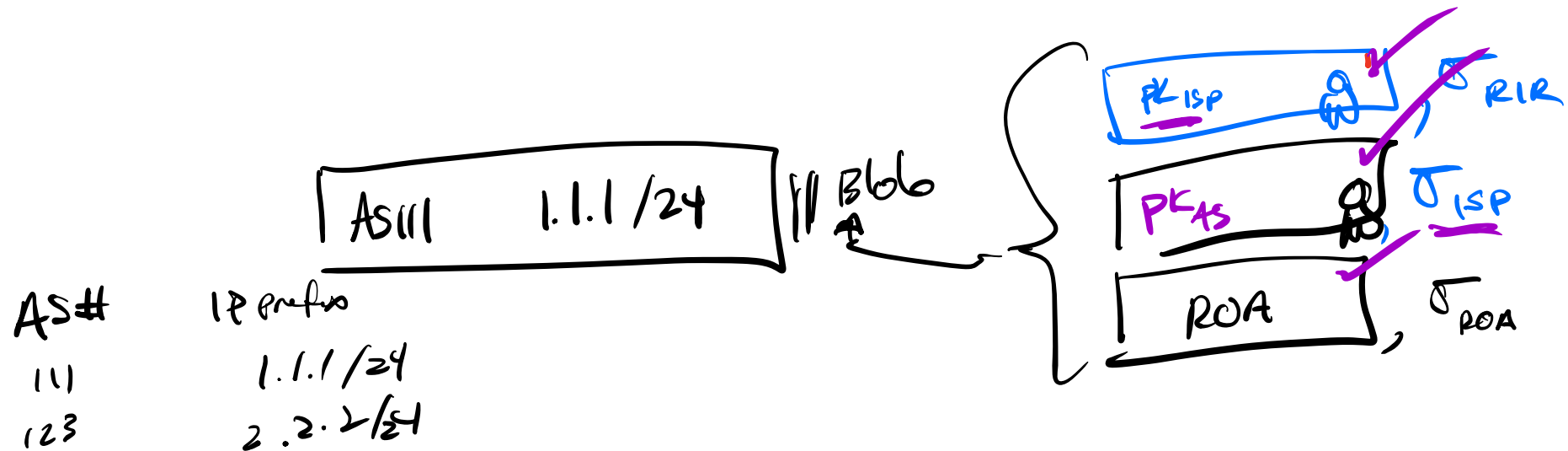
$$\text{Sign}_{SK_{ISP}}(\text{"AS 1.1.1/24"} \xrightarrow{PK_{AS}}) \rightarrow \sigma_{ISP}$$

ROA (Route Origin Authorization)

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

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

Circulate the
"out of band"



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?