Interdomain Routing Security

COS 461: Computer Networks
Michael Schapira

Goals of Today's Lecture

- BGP security vulnerabilities
- Improving BGP security
- Difficulty of upgrading BGP

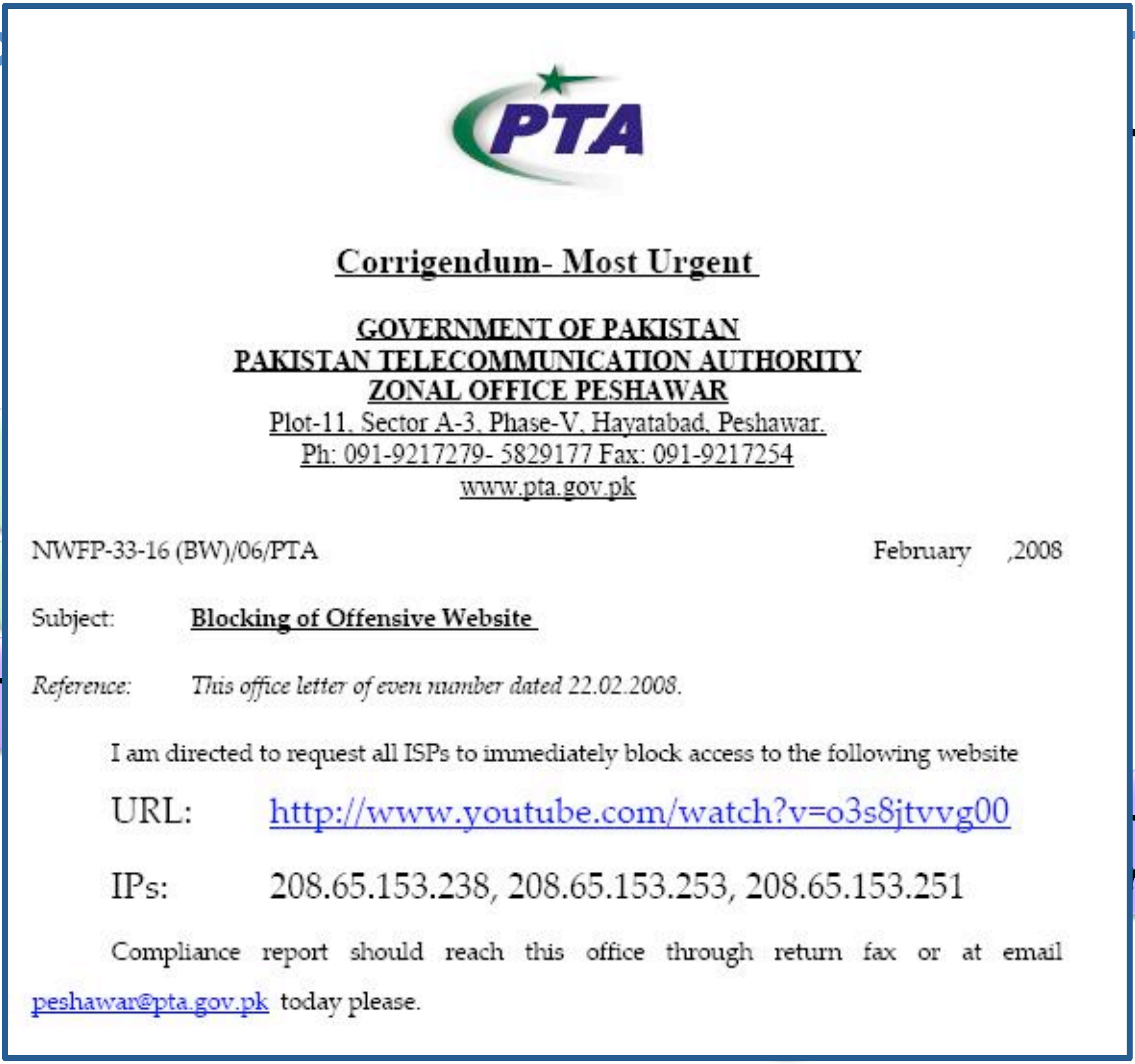
Ho ng?

Febr Tube!

You

t

n



Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

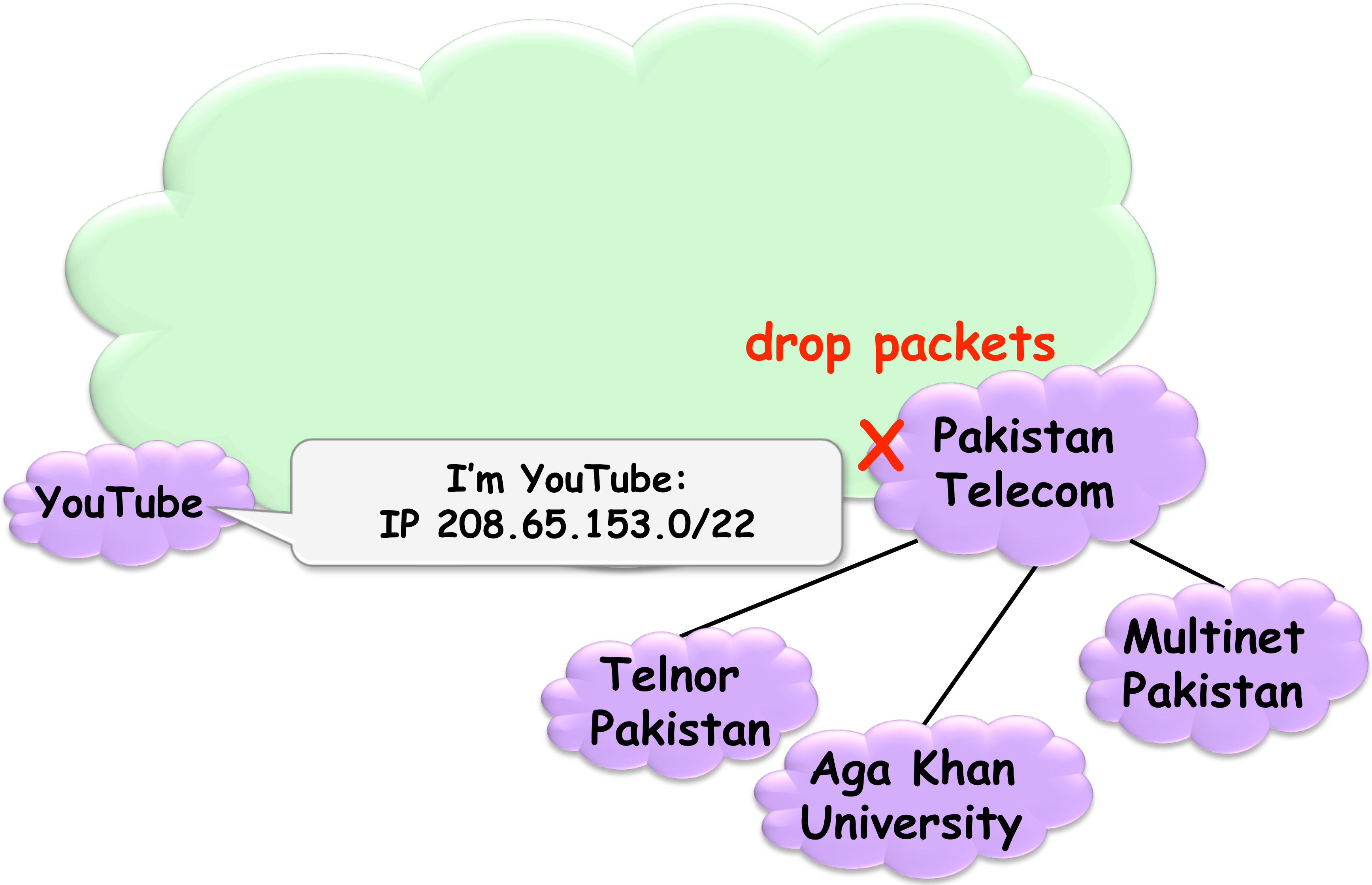
URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

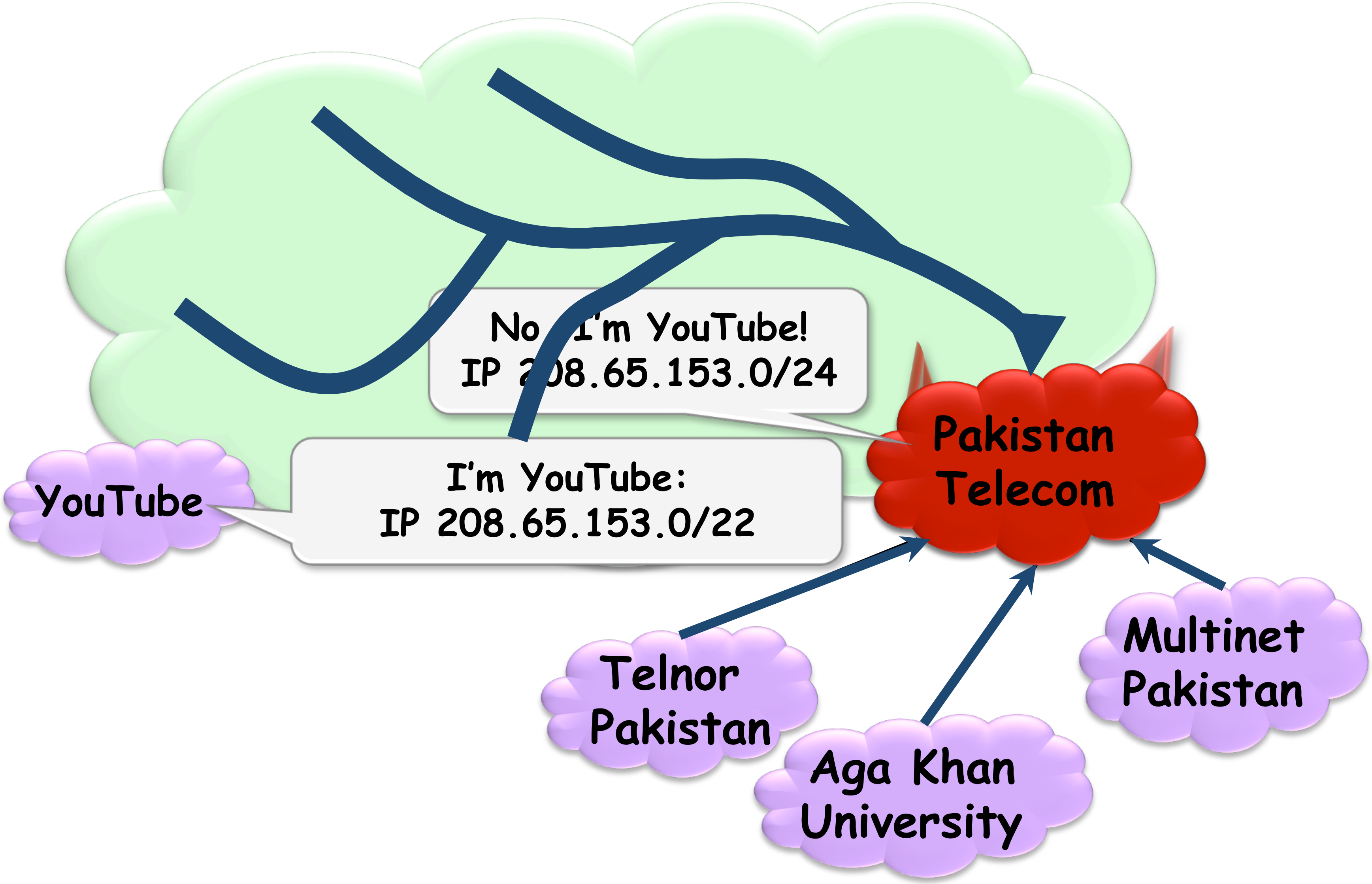
How Secure is Today's Internet Routing?

What should have happened…



How Secure is Today's Internet Routing?

What did happen…



No, I'm YouTube!
IP 208.65.153.0/24

I'm YouTube:
IP 208.65.153.0/22

YouTube

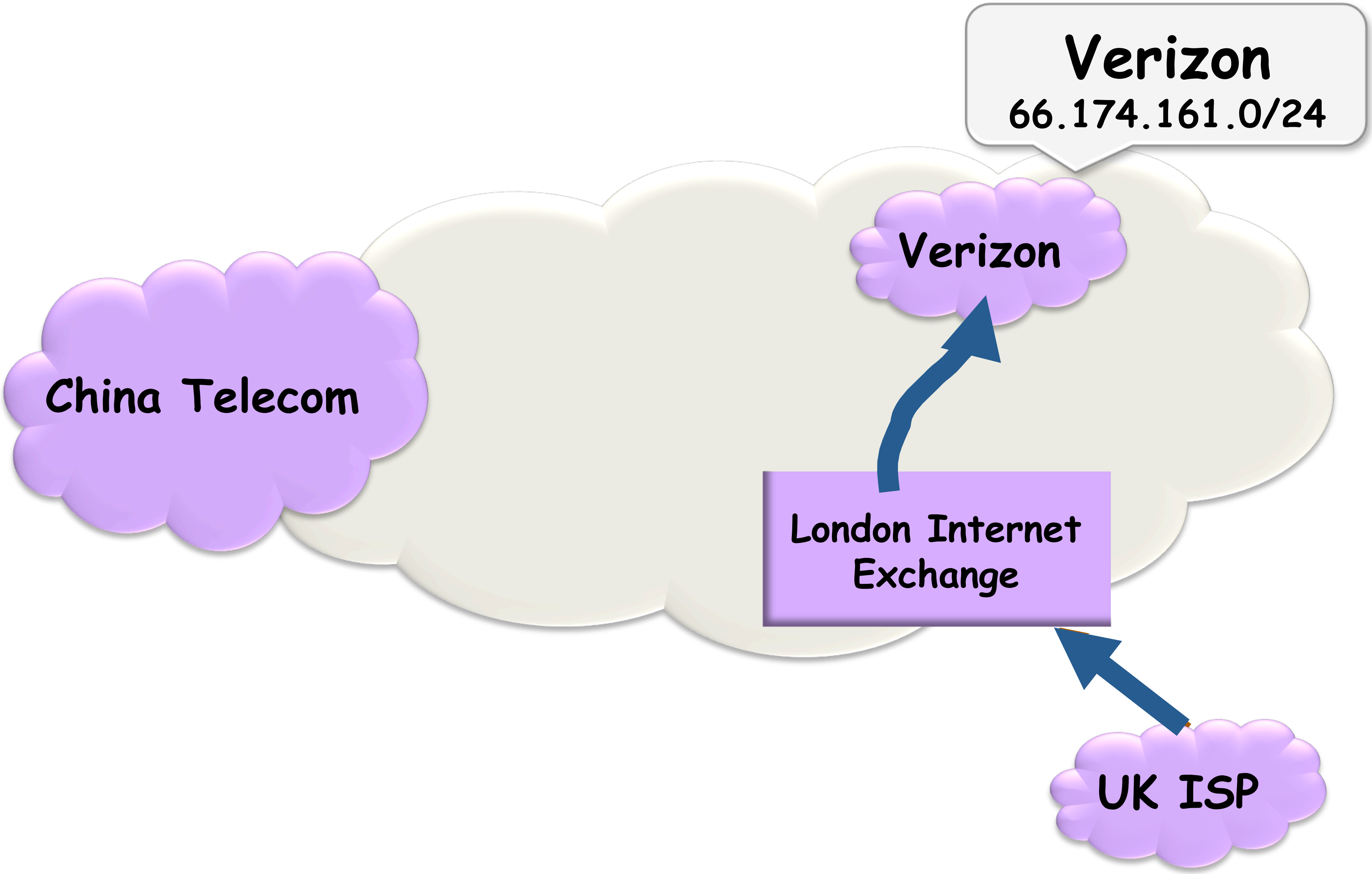
Pakistan Telecom

Telnor Pakistan

Aga Khan University

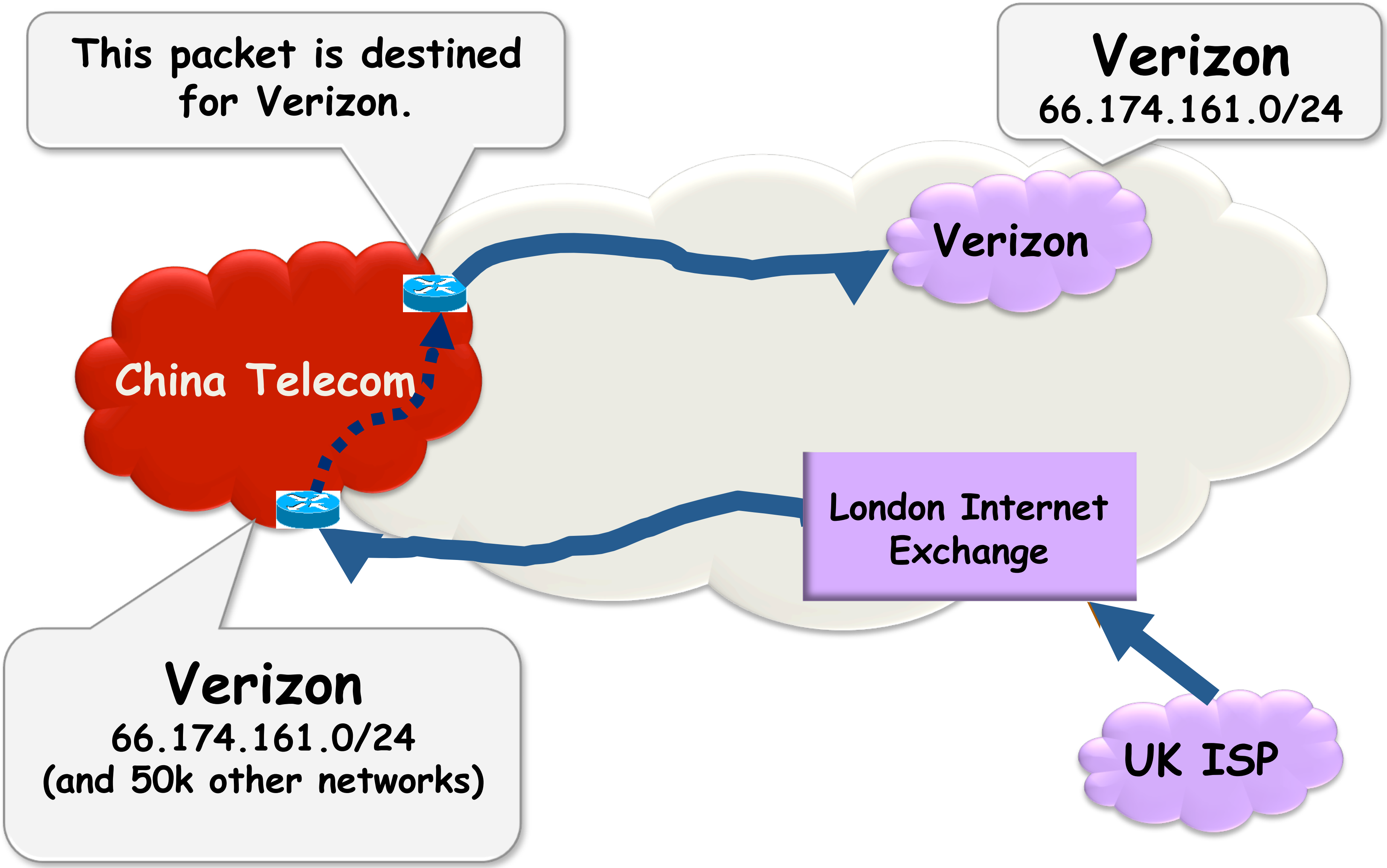
Multinet Pakistan

How Secure is Routing on the Internet Today? (2)



How Secure is Routing on the Internet Today? (2)

April 2010 : China Telecom intercepts traffic



This packet is destined for Verizon.

Verizon
66.174.161.0/24

Verizon

China Telecom

London Internet Exchange

Verizon
66.174.161.0/24
(and 50k other networks)

UK ISP

BGP Security Today

- **Applying best common practices (BCPs)**
  - Filtering routes by prefix and AS path, *etc.*
- **This is not good enough!**
  - Depends on vigilant application of BCPs … and not making configuration mistakes!
  - Doesn't address fundamental problems, *e.g.*, prefix hijacking!

Securing Internet Routing

- How to secure Internet routing?
  - Long standing agenda in the standards and research communities.

- Over the past 15 years, several secure Internet routing protocols have been proposed.

Securing Internet Routing

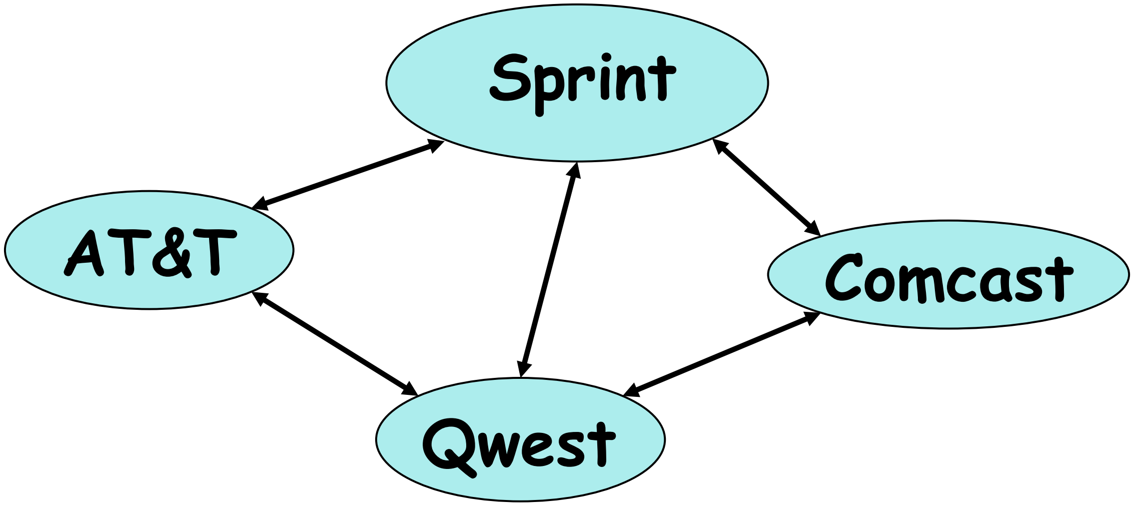
- The U.S. federal government is accelerating its efforts to secure the Internet's routing system … The effort … will secure the Internet's core routing protocol known as the **Border Gateway Protocol (BGP)**.

- "**BGP is one of the largest threats on the Internet**. It's incredible, the insecurity of the routing system."

  (Danny McPherson, CSO at Arbor Networks, Jan 2009)

The Internet

Over 35,000 **Autonomous Systems (ASes)**

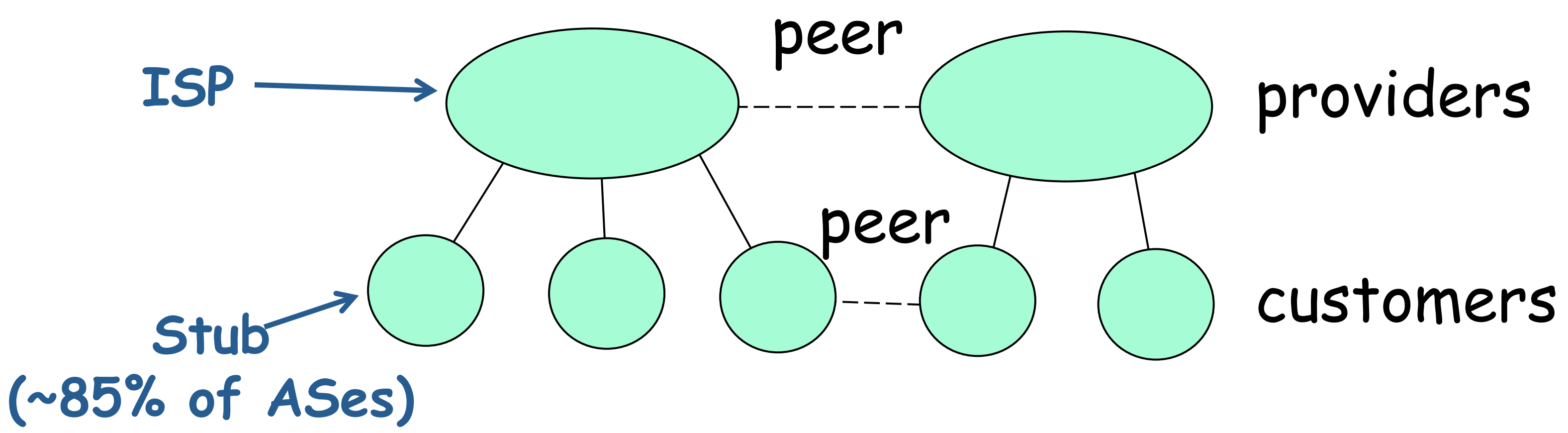


Routing between ASes handled by the **Border Gateway Protocol (BGP)**

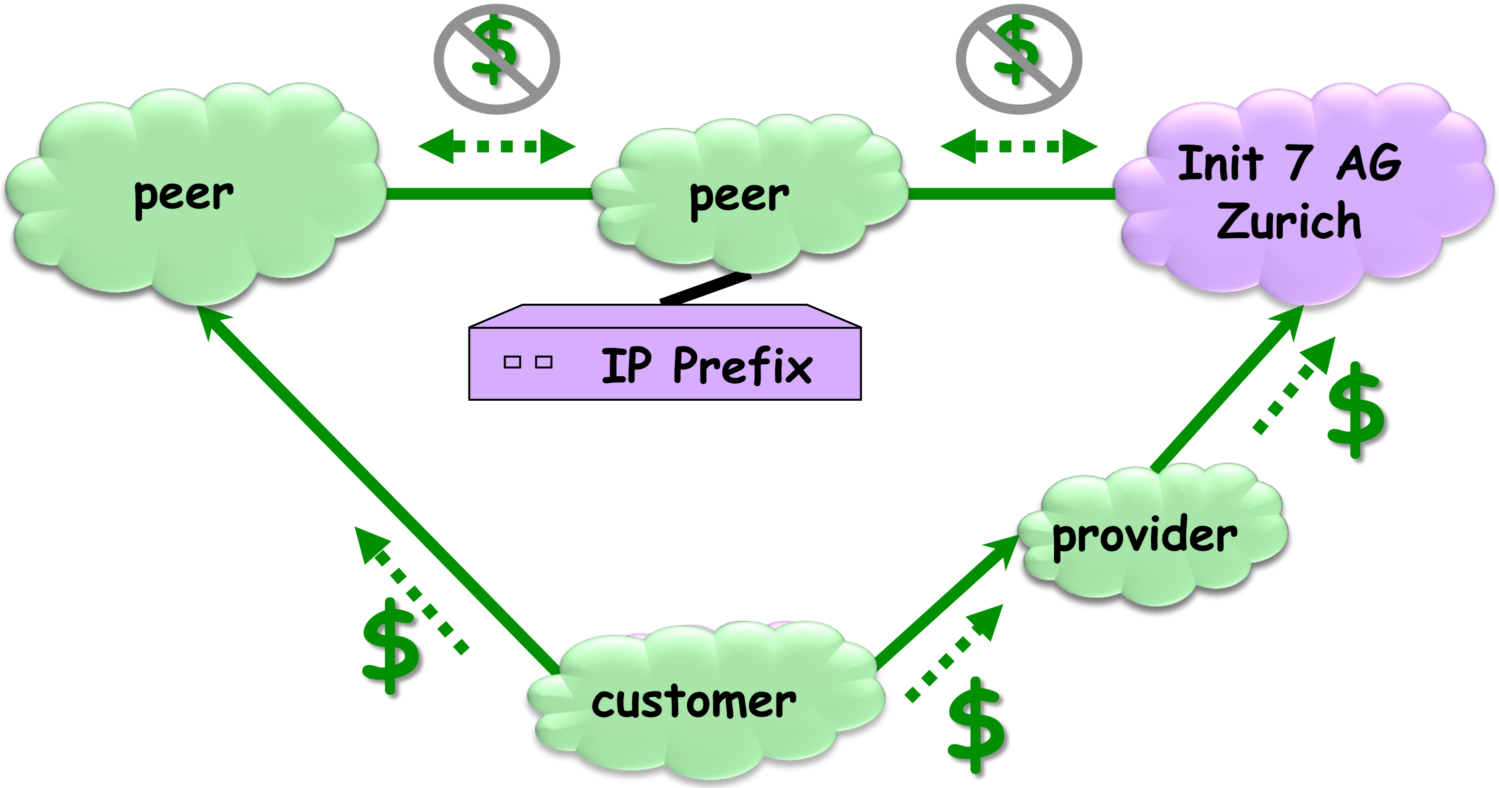
The Commercial Internet

- ASes sign long-term contracts.

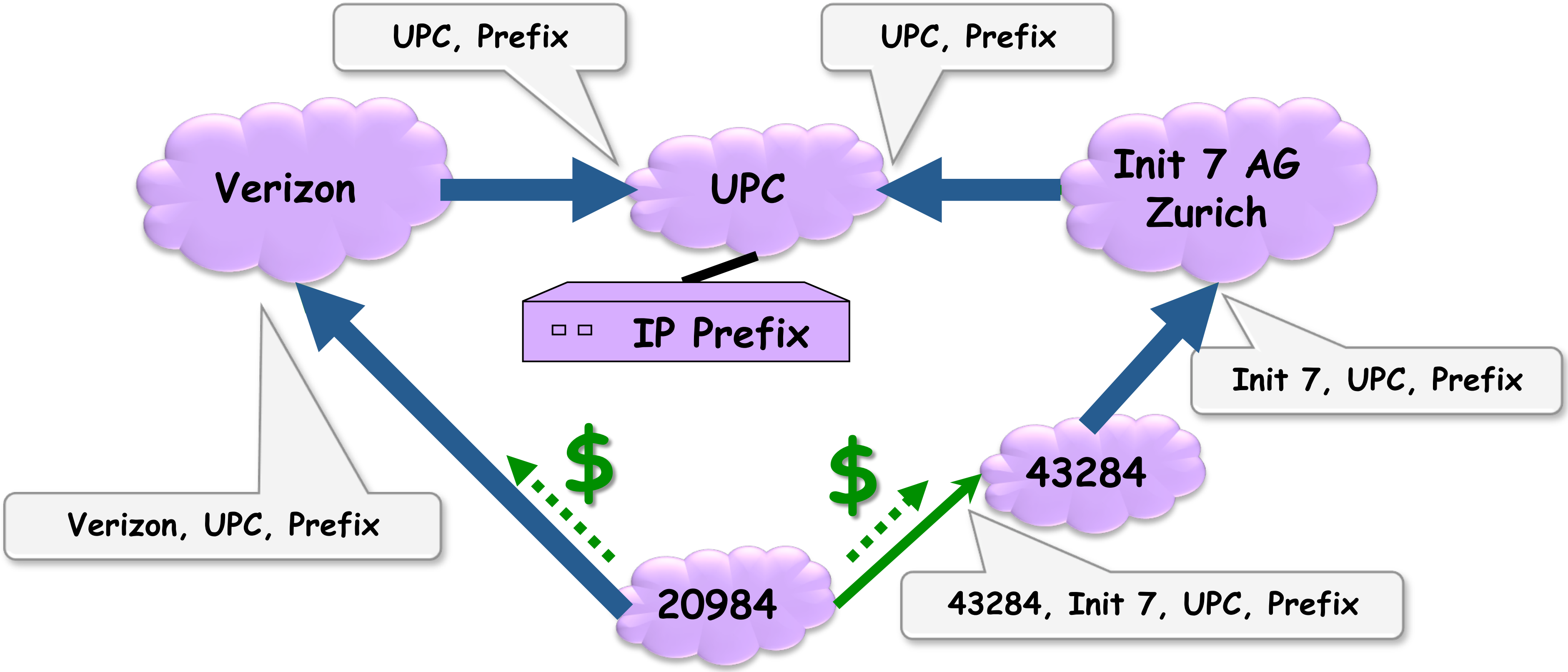
- Neighboring pairs of ASes have:
  - a **customer-provider** relationship.
  - a **peering** relationship.



Illustration

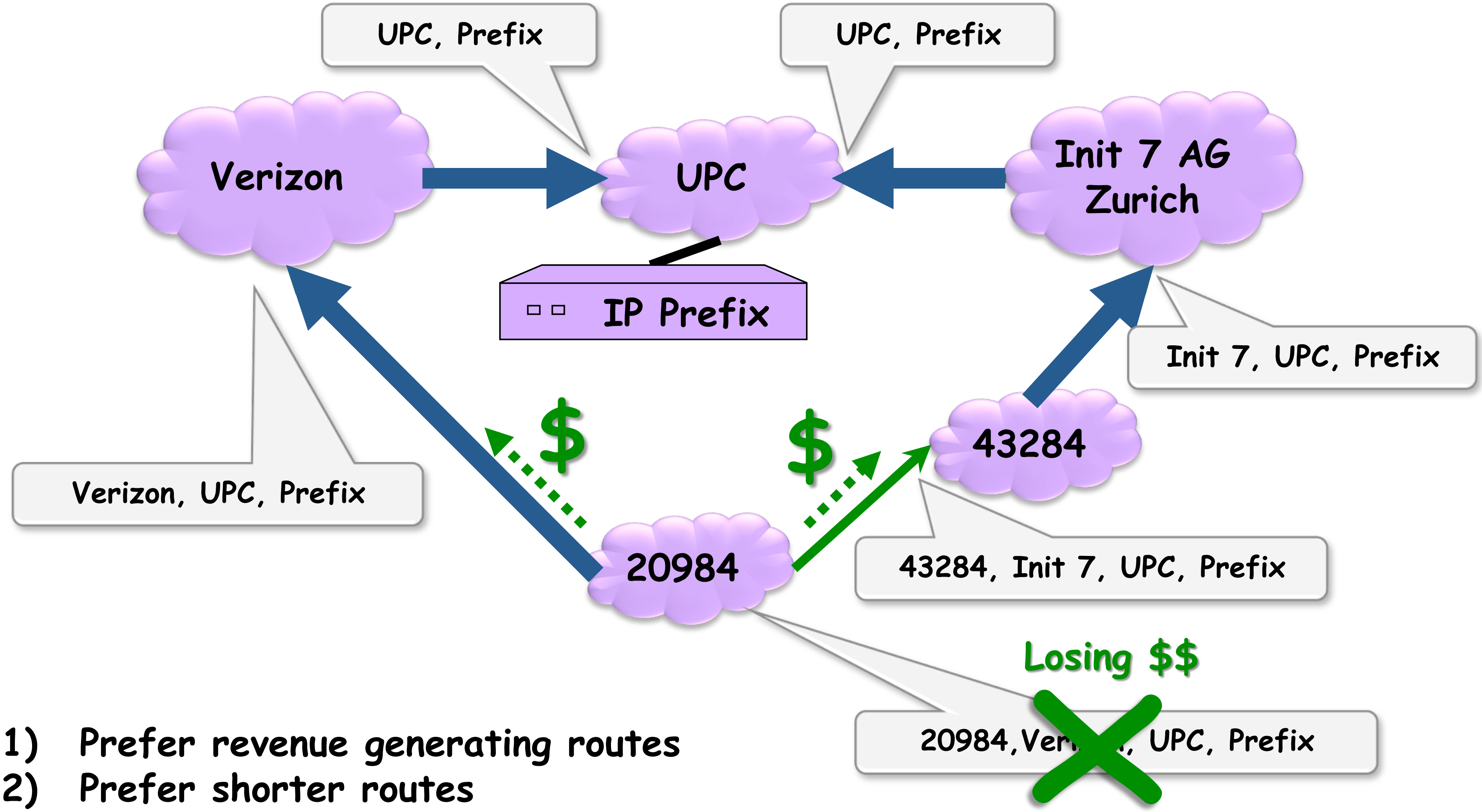


Routing with BGP



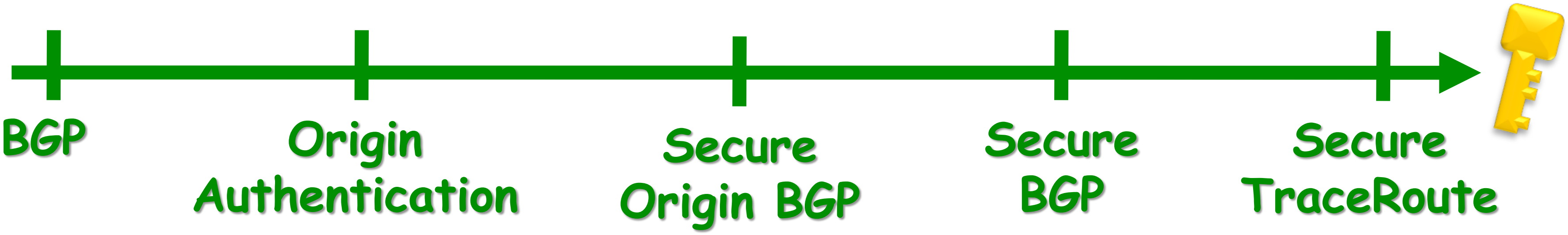
1) Prefer revenue generating routes
2) Prefer shorter routes

Routing with BGP



1) Prefer revenue generating routes
2) Prefer shorter routes
3) Do not carry transit traffic for free

Secure Routing Protocols



BGP

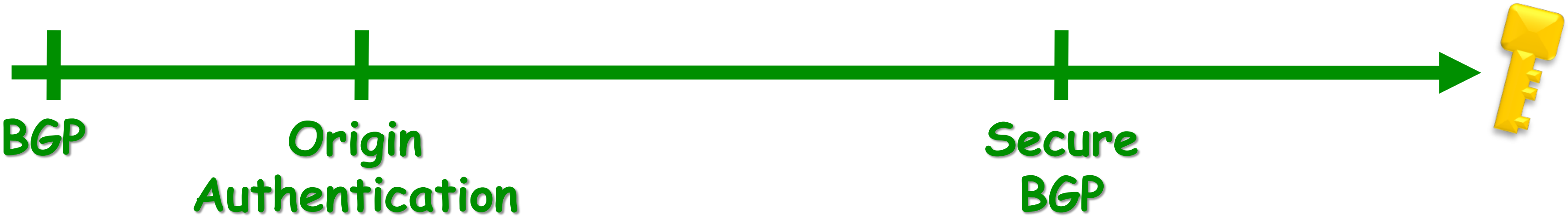
Origin Authentication

Secure Origin BGP

Secure BGP

Secure TraceRoute

In this lecture



BGP

Origin Authentication

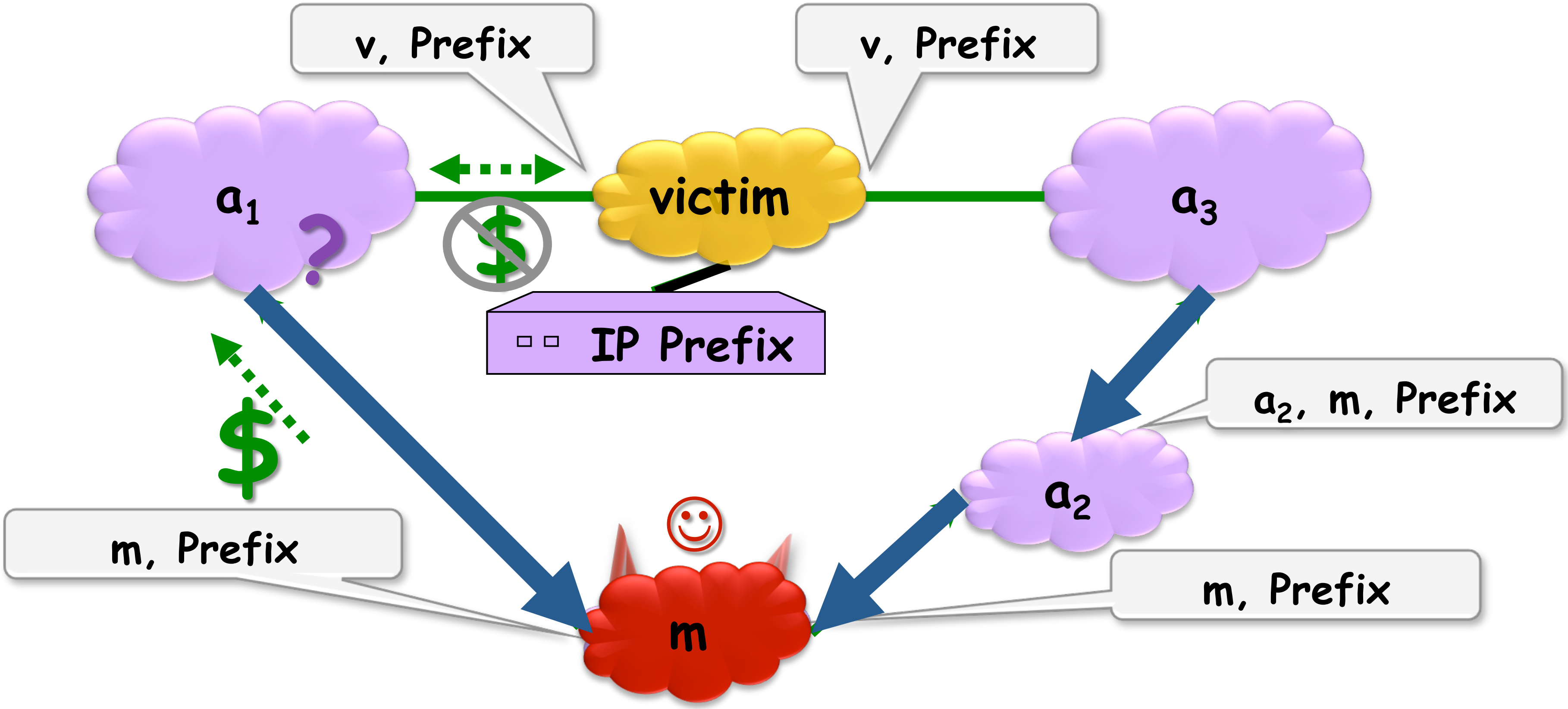
Secure BGP

Prefix Hijacking and Origin Authentication

IP Address Ownership and Hijacking

- **IP address block assignment**
  - Regional Internet Registries (ARIN, RIPE, APNIC)
  - Internet Service Providers
- **Proper origination of a prefix into BGP**
  - By the AS who owns the prefix
  - … or, by its upstream provider(s) in its behalf
- **However, what's to stop someone else?**
  - Prefix hijacking: another AS originates the prefix
  - BGP does not verify that the AS is authorized
  - Registries of prefix ownership are inaccurate

Prefix Hijacking



Hijacking is Hard to Debug

- **The victim AS doesn't see the problem**
  - Picks its own route
  - Might not even learn the bogus route
- **May not cause loss of connectivity**
  - *E.g.*, if the bogus AS snoops and redirects
  - … may only cause performance degradation
- **Or, loss of connectivity is isolated**
  - E.g., only for sources in parts of the Internet
- **Diagnosing prefix hijacking**
  - Analyzing updates from many vantage points
  - Launching traceroute from many vantage points

How to Hijack a Prefix

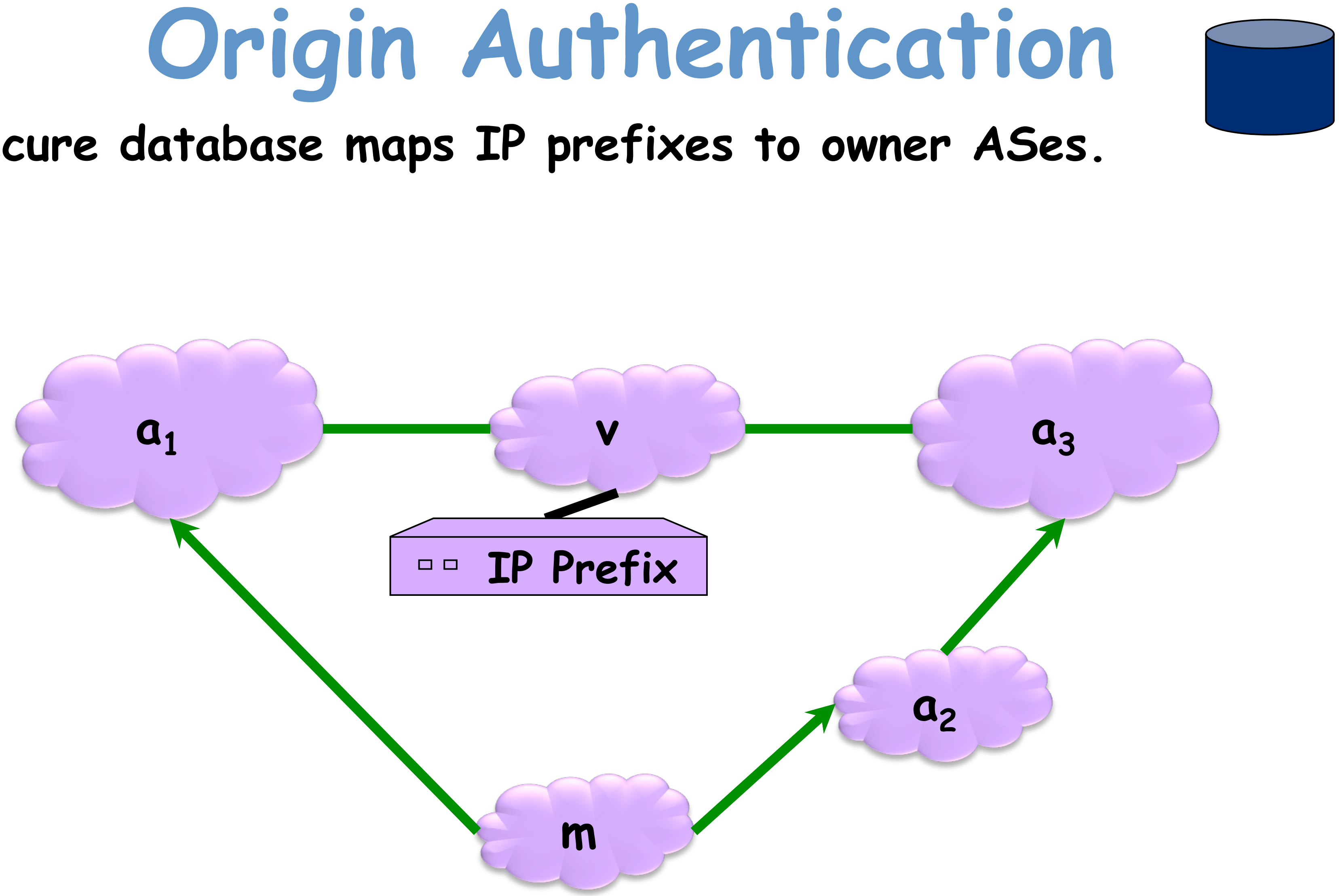
- **The hijacking AS has**
  - Router with BGP session(s)
  - Configured to originate the prefix

- **Getting access to the router**
  - Network operator makes configuration mistake
  - Disgruntled operator launches an attack
  - Outsider breaks in to the router and reconfigures

- **Getting other ASes to believe bogus route**
  - Neighbor ASes do not discard the bogus route
  - E.g., not doing protective filtering

Origin Authentication

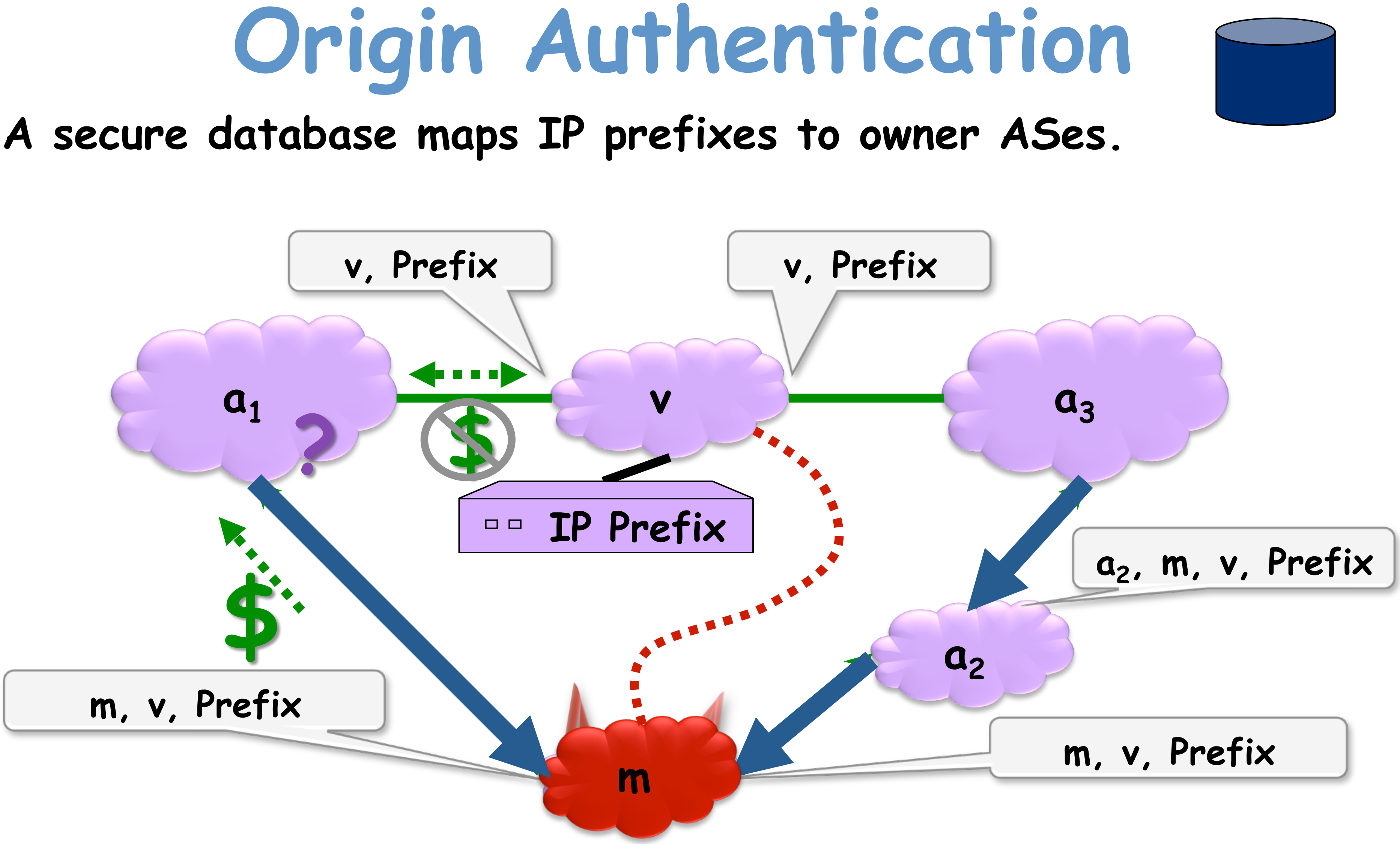
A secure database maps IP prefixes to owner ASes.



Bogus Routes and Secure BGP

Origin Authentication

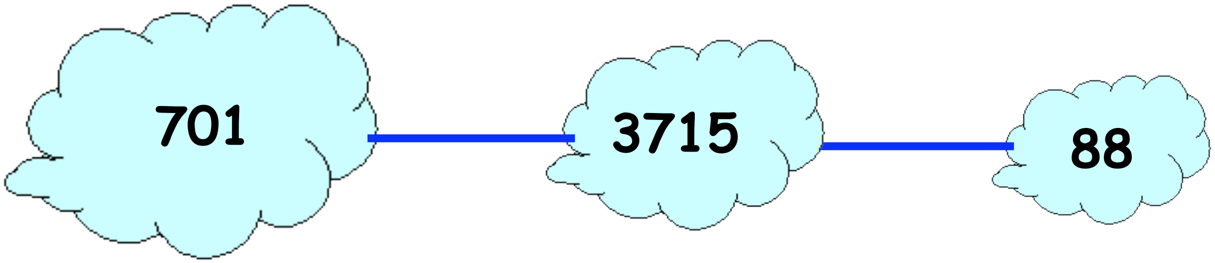
A secure database maps IP prefixes to owner ASes.



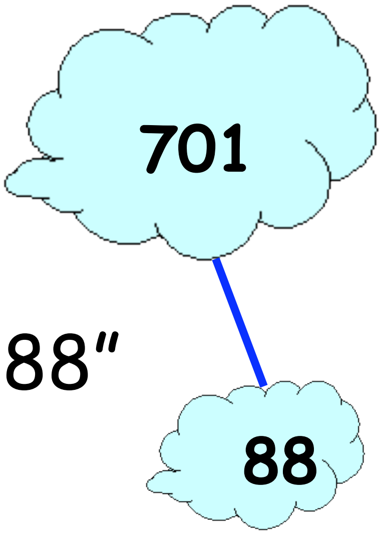
Bogus AS Paths

- Remove ASes from the AS path
  - E.g., turn “701 3715 88” into “701 88”

- Possible motivations
  - Make the AS path look shorter than it is
  - Attract sources that normally try to avoid AS 3715



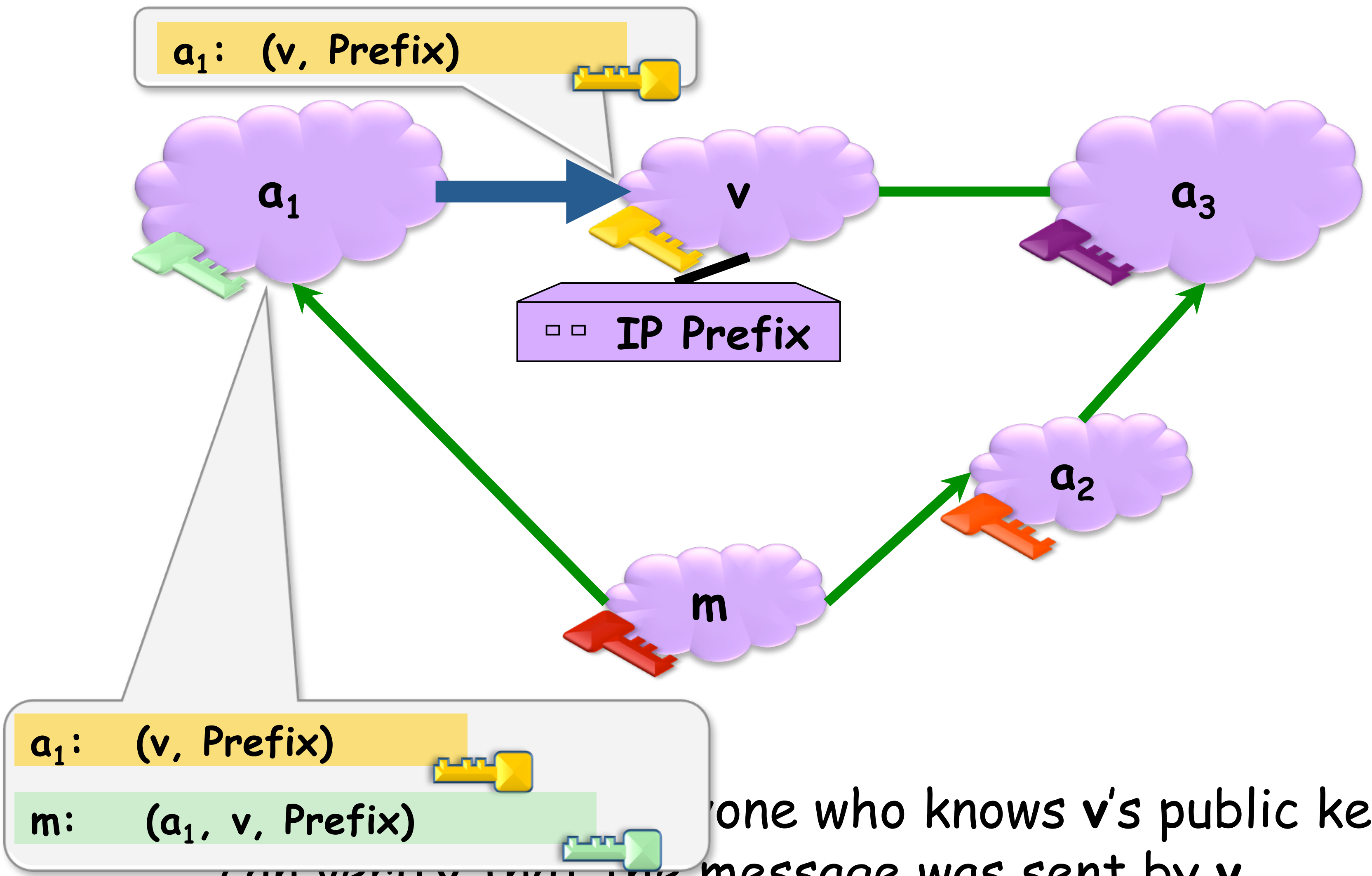
Bogus AS Paths



- Add ASes to the path
  - E.g., turn “701 88” into “701 3715 88”
- Possible motivations:
  - Trigger loop detection in AS 3715
  - Make your AS look like is has richer connectivity

Secure BGP

Origin Authentication + cryptographic signatures



a_1: (v, Prefix)

a_1: (v, Prefix)

m: (a_1, v, Prefix)

one who knows v's public key can verify that the message was sent by v.

Secure BGP

- S-BGP can validate the order in which ASes were traversed.

- S-BGP can validate that no intermediate ASes were added or removed.

- S-BGP can validate that the route is recent.

Are We There Yet?

S-BGP Deployment Challenges

- **Complete, accurate registries**
  - E.g., of prefix ownership
- **Public Key Infrastructure**
  - To know the public key for any given AS
- **Cryptographic operations**
  - *E.g.*, digital signatures on BGP messages
- **Need to perform operations quickly**
  - To avoid delaying response to routing changes
- **Difficulty of incremental deployment**
  - Hard to have a "flag day" to deploy S-BGP

Incremental Deployment?

- There is a necessary transition period.

- S-BGP must be backwards compatible with BGP

- Who upgrades first? Why?

Pessimistic View

ISPs would be the ones forced to ***upgrade all of their equipment*** *to support this initiative, but* ***how would it benefit them****? As commercial companies, if there is little to no benefit (potential to increase profit), why would they implement a potentially costly solution? The answer is* ***they won't.***

[http://www.omninerd.com/articles/Did_China_Hijack_15_of_the_Internet_Routers_BGP_and_Ignorance]

unless everyone else does?

S-BGP = IPv6?

Conclusions

- **Internet protocols designed based on trust**
  - The insiders are good guys
  - All bad guys are outside the network
- **Border Gateway Protocol is very vulnerable**
  - Glue that holds the Internet together
  - Hard for an AS to locally identify bogus routes
  - Attacks can have very serious global consequences
- **Proposed solutions/approaches**
  - Secure variants of the Border Gateway Protocol

One last thing…

Harming Internet Routing Without Attacking BGP

Attacks on TCP and Data-Plane Attacks

- **Attack TCP!**
  - A BGP session runs over TCP.
- **Do not forward traffic as advertised!**
  - Drop packets!
  - Route packets along unannounced routes!

The End