BGP route monitoring

Mar, 25, 2008

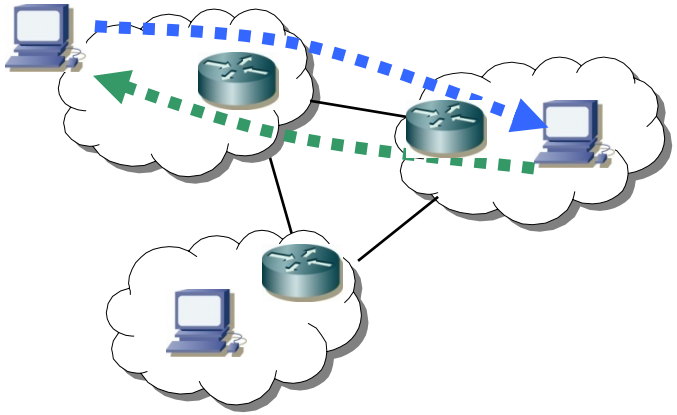
Matsuzaki ‘maz’ Yoshinobu

<maz@telecom-isac.jp>, <maz@iij.ad.jp>

abstract

- BGP prefix hijack is a serious security issue in the internet, and these events have been widely reported.
- There are several proposals of securing BGP, but it needs time to deploy.
- This paper presents a route monitoring system – Keiro-Bugyo (route-magistrate), and this system allow us to detect prefix hijacking events and take prompt action to address the problem.

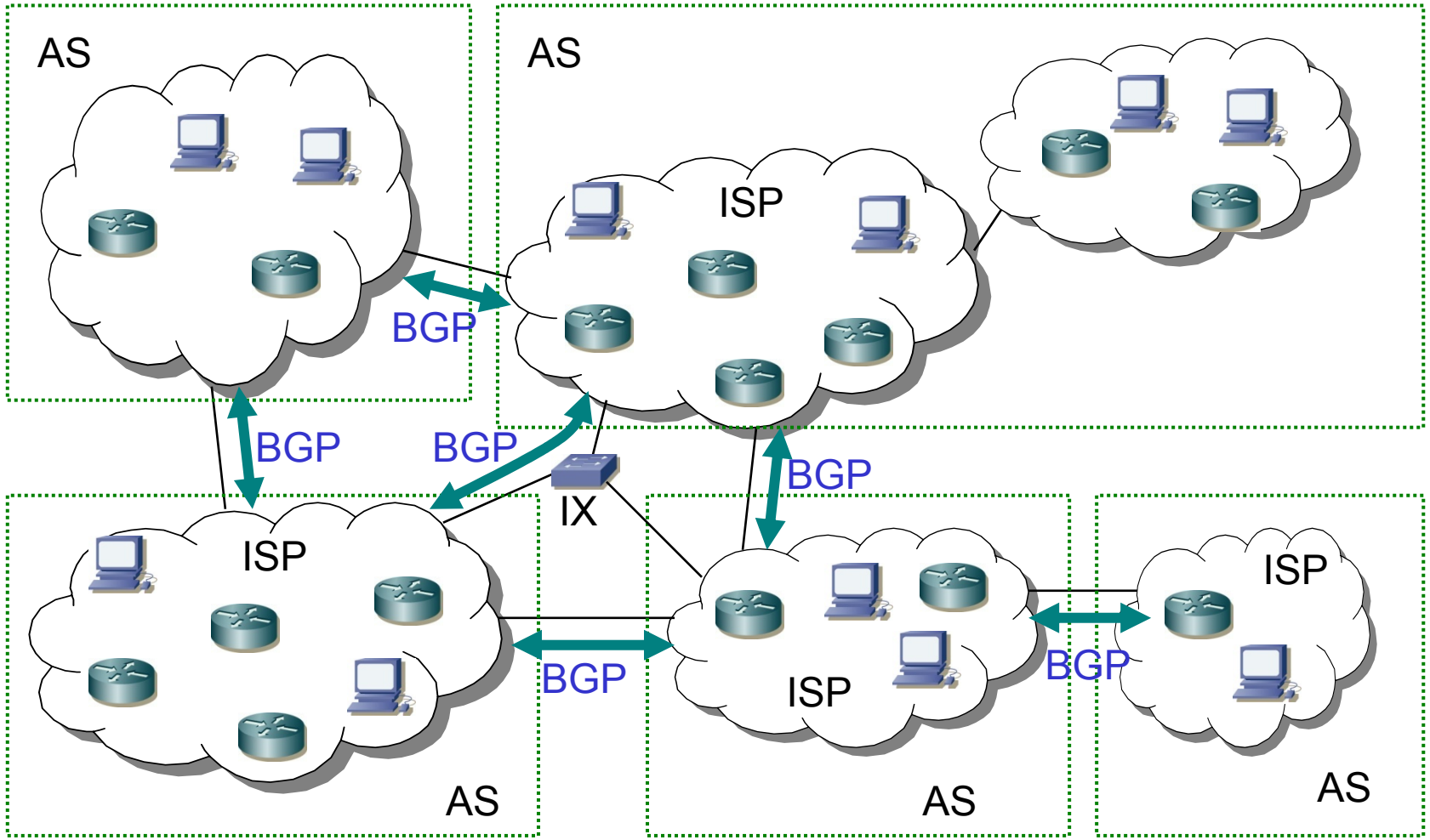
- An IP packet travel from its source to its destination across a series of routers.
- When an IP packet is forwarded, a router uses its routing information to determine which path should be used to reach the destination.



- A router shares reachability information with other routers via dynamic routing protocols.
  - A routing information is automatically managed by dynamic routing protocols reflecting a network change.
- Multiple routes to a given destination can exist.
  - A router selects the best route by tie-breaking rules.
  - A router selects the new best, if the best route to a destination becomes unusual or the router learns a more preferable route.
- A route announce is referred to as a ‘prefix’.

- Each network has unique IP blocks.
  - assigned by its *internet registry* (IR)
- An *autonomous system* (AS) exchanges routing information with its neighboring AS.
  - using the *Border Gateway Protocol* (BGP)
  - An ‘AS’ is networks under a common administration and with common routing policies, and each ‘AS’ has a unique numerical ID assigned by its IR.

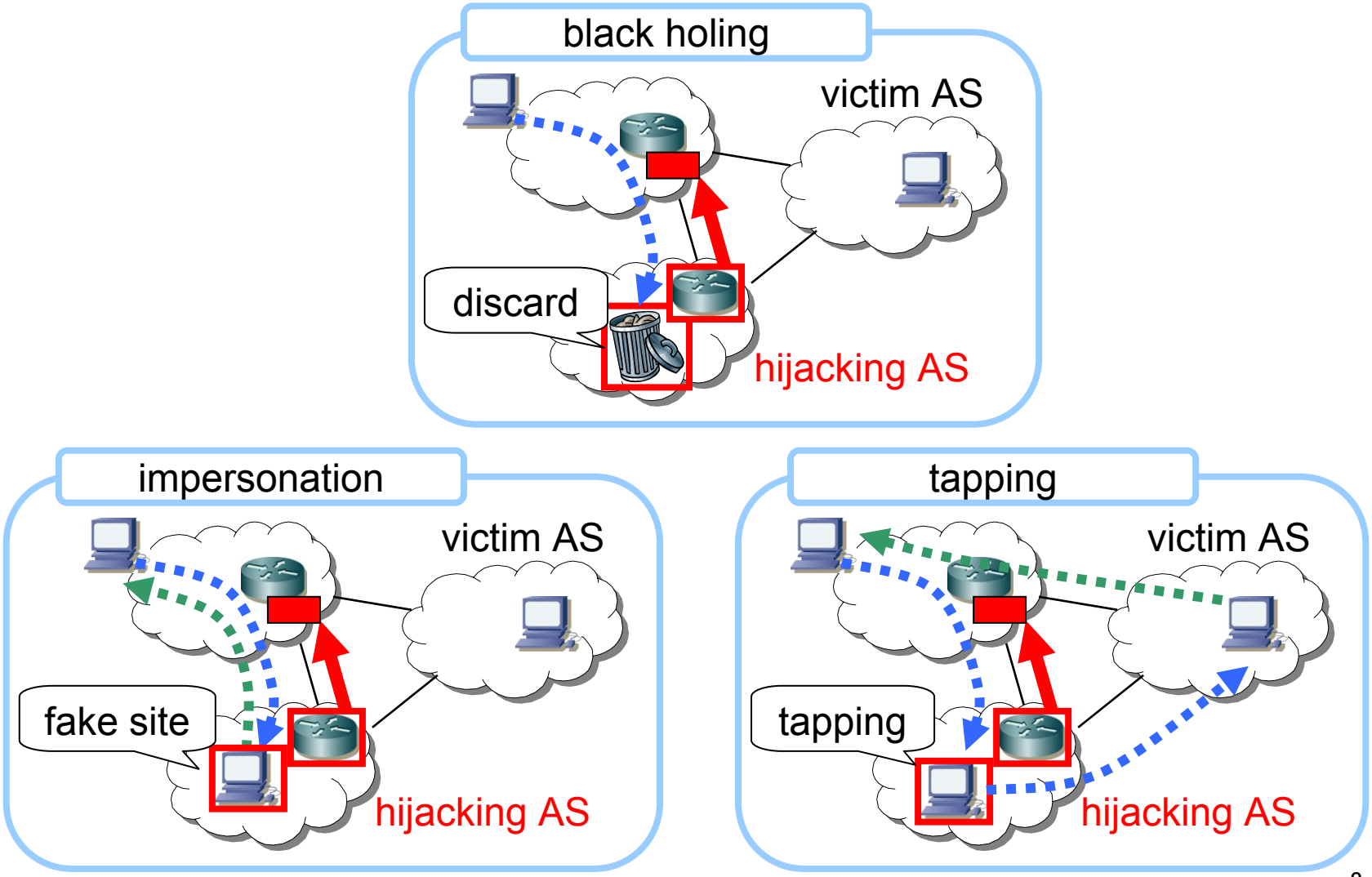
The internet architecture



ISP: internet service provider,　IX: internet exchange

- Announcing a prefix that belongs to someone else without their permission
  - These events have been widely reported, but it is difficult to detect a hijack event that is occurred outside of the ‘AS’.
  - It seems most events are explainable by misconfigurations.
    - So, the wording of ‘Hijack’ seems too strong.

possible effects of prefix hijack



- YouTube was announcing 208.65.152.0/22.
- **24 Feb 2008, 18:47(UTC)**
  - AS17557(Pakistan Telecom) starts announcing 208.65.153.0/24, and AS3491(PCCW Global) propagates the prefix.
  - YouTube traffic is redirected to Pakistan Telecom, and people can not access the YouTube.

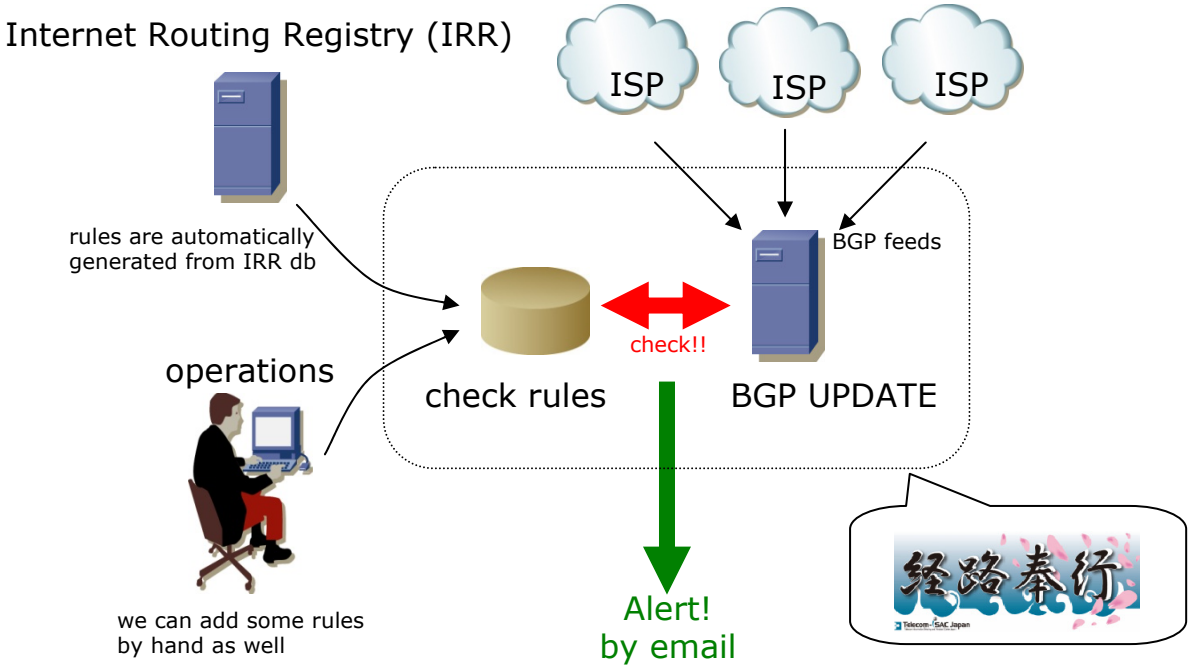
- **24 Feb 2008, 20:07(UTC) (+80mins)**
  - YouTube(AS36561) starts announcing 208.65.153.0/24 to get back the traffic. Routers that prefer this route (shorter AS Path, and so on) send traffic to YouTube.
- **24 Feb 2008, 21:01(UTC) (+134mins)**
  - AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom).
- YouTube react in about 80mins, and it takes about 2 hours to recover.

Why are these happened?

- Somebody on somewhere is accepting these unauthorized announcements.
  - They lack of a route-filter knowledge, or never check the authoritative correctness of a prefix.
- I hope we can use more secure protocol in the future.
  - soBGP, sBGP, pgBGP, and so on.
  - But it needs time to reach a consensus, and needs more time to deploy.

- I wanted to know what's going on around our ASs.
  - Are there incidents?
  - How often are they occurred?
- So we developed a route monitoring system to detect a prefix hijack.
  - This is easy to start. ☺

Keiro-Bugyo(route-magistrate)



- Monitoring BGP UPDATE
  - Receiving full BGP feeds from multiple ASs(ISPs)
  - Comparing a prefix and its BGP path attributes to the check rules
- When there is a difference between rules and BGP UPDATE, the system rapidly alerts operators by email.

- BGP UPDATE is composed of Path attributes and NLRI.
- We are checking origin AS and prefix.
  - like – 2497 { 210.130.0.0/16 }
  - This method is reasonable against a hijack caused by a misconfiguration.

maintaining the check rules

- We have to keep the strict check rules as possible, otherwise the alert becomes useless.
  - receive lots of false alerts, or
  - miss a hijack event
- We maintain our JPIRR objects to be up-to-date.
  - We automatically generates the check rules from the JPIRR DB, and this saves our time. ☺

2007 2008

	Aug	Sep	Oct	Nov	Dev	Jan
bogon	4	6	26	24	44	46
false alert	14	1	10	53	3	5
others ☹	2			1		3

- Currently the system is receiving BGP feeds from 11 major Japanese ISPs, and monitoring hijacks aimed to these 11 ASs.

detection case #1

- 2008/01
- Originated from Asian ISP
- longer prefix and invalid origin AS
  - /24 x 1
- Detected 10/11 ASs on Keiro-Bugyo
- Action
  - No action was taken, because the prefix was withdrawn soon.
- Duration : about 26 mins

detection case #2

- 2006/11
- Originated from Asian ISP
- longer prefix and invalid origin AS
  - /27 x 1
- Detected 1/7 AS on Keiro-Bugyo
- Action
  - We could not contact the hijacking AS directly, so asked for help to a upstream of the AS. They applied route filter to reject the invalid prefix and also notified the AS. After that, the hijacking AS stopped the announcement.
- Duration : about 16 hours

Assumptions

- The bgp monitoring system detects a hijack only if
  - the hijack prefix reaches the system, and
  - the system discriminates between a correct prefix and hijacked one.

- So this monitoring system has a limitation.

The system can not detect:

- A hijack prefix that does not advertise to the system
  - a local hijack in specific region/ISPs
  - a hijack prefix is filtered somewhere
- A hijack prefix that can not be discriminated from the correct one by the system
  - The define of correctness – same origin AS
  - IR/IRR DB hijacking

Is this useful?

- YES!

- The system does not solve every issues, but it is still useful for people who needs a ‘fast-food’ detection. ☺

- CJK (China, Japan and Korea) collaboration
  - Based on a government-to-government meeting about ICT Network and Information Security
  - On going project, still discussing・・・
  - Expert groups on each country will cooperate to deal with BGP prefix Hijacking.

Conclusion

- BGP prefix hijack is a serious security issue in the internet.
- To address this issue at this moment, we developed a route monitoring system, Keiro-Bugyo(route-magistrate).
- A well-maintained IRR database can be used for the route verification.
  - We recommend that AS-operators register and maintain its objects to be up-to-date.