Understanding and Mitigating Internet Routing Threats

VERISIGN // LABS

TEAM CYMRU
WWW.CYMRU.COM

John Kristoff jtk@cymru.com
Danny McPherson dmcpherson@verisign.com

One of two critical systems

Routing (BGP) and naming (DNS) are by far the two most critical subsystems of the Internet infrastructure. In the case of BGP, participation in and access to the routing system itself is generally, or rather should be, limited to a subset of trustworthy nodes and admins.

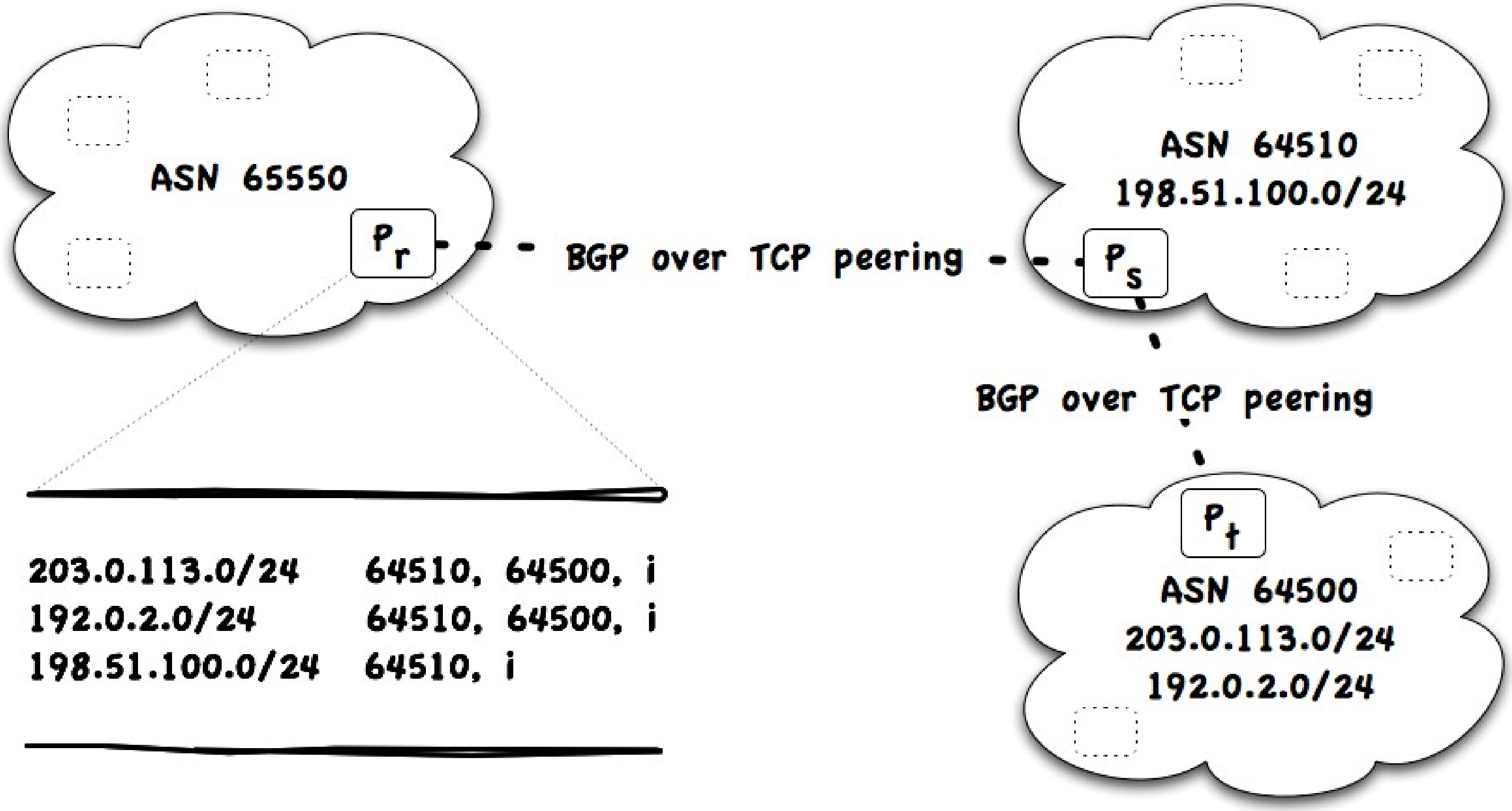
Agenda

- BGP Refresher
- Threats
- Mitigation

BGP Refresher

- Basic protocol overview
- BGP message types
- BGP path attributes
- Properties that affect BGP route decision process
- Jargon

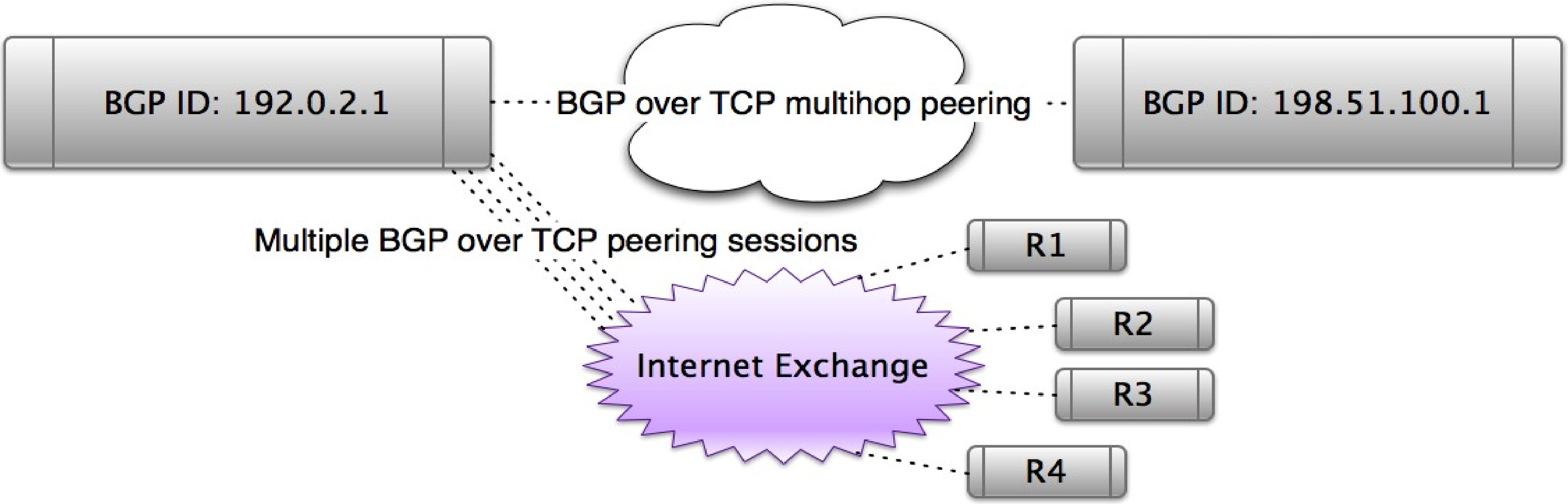
Path Vector Routing



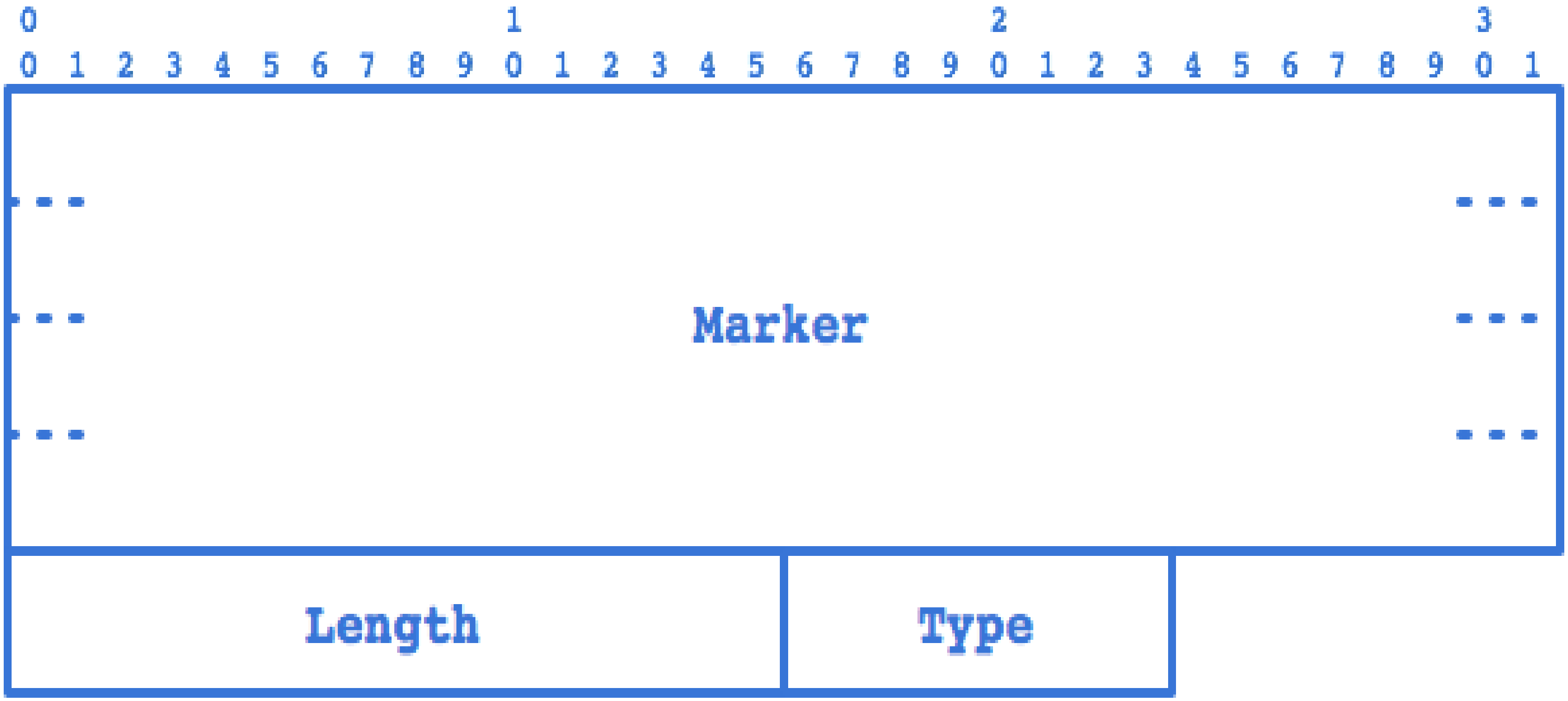
203.0.113.0/24	64510, 64500, i
192.0.2.0/24	64510, 64500, i
198.51.100.0/24	64510, i

BGP over TCP port 179

- One-to-one peering relationship
- Inherit TCP behaviors, advantages and threats


BGP ID: 192.0.2.1
BGP over TCP multihop peering
BGP ID: 198.51.100.1
Multiple BGP over TCP peering sessions
R1
R2
Internet Exchange
R3
R4

Common BGP Header



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
...                                                           ...
|                                                               |
...                           Marker                          ...
|                                                               |
...                                                           ...
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Length               |      Type     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

BGP message types

1 – OPEN

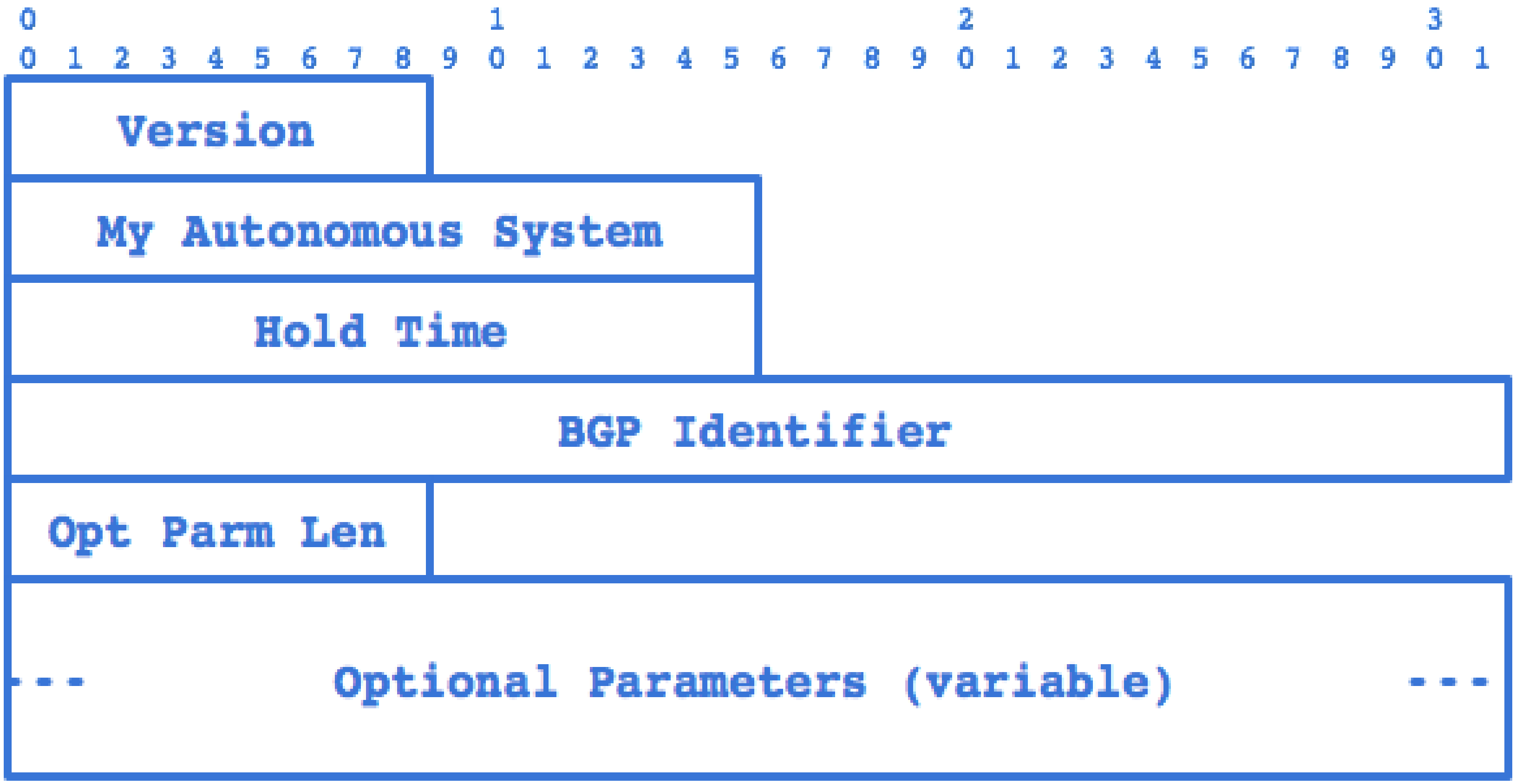
2 – UPDATE

3 – NOTIFICATION

4 – KEEPALIVE

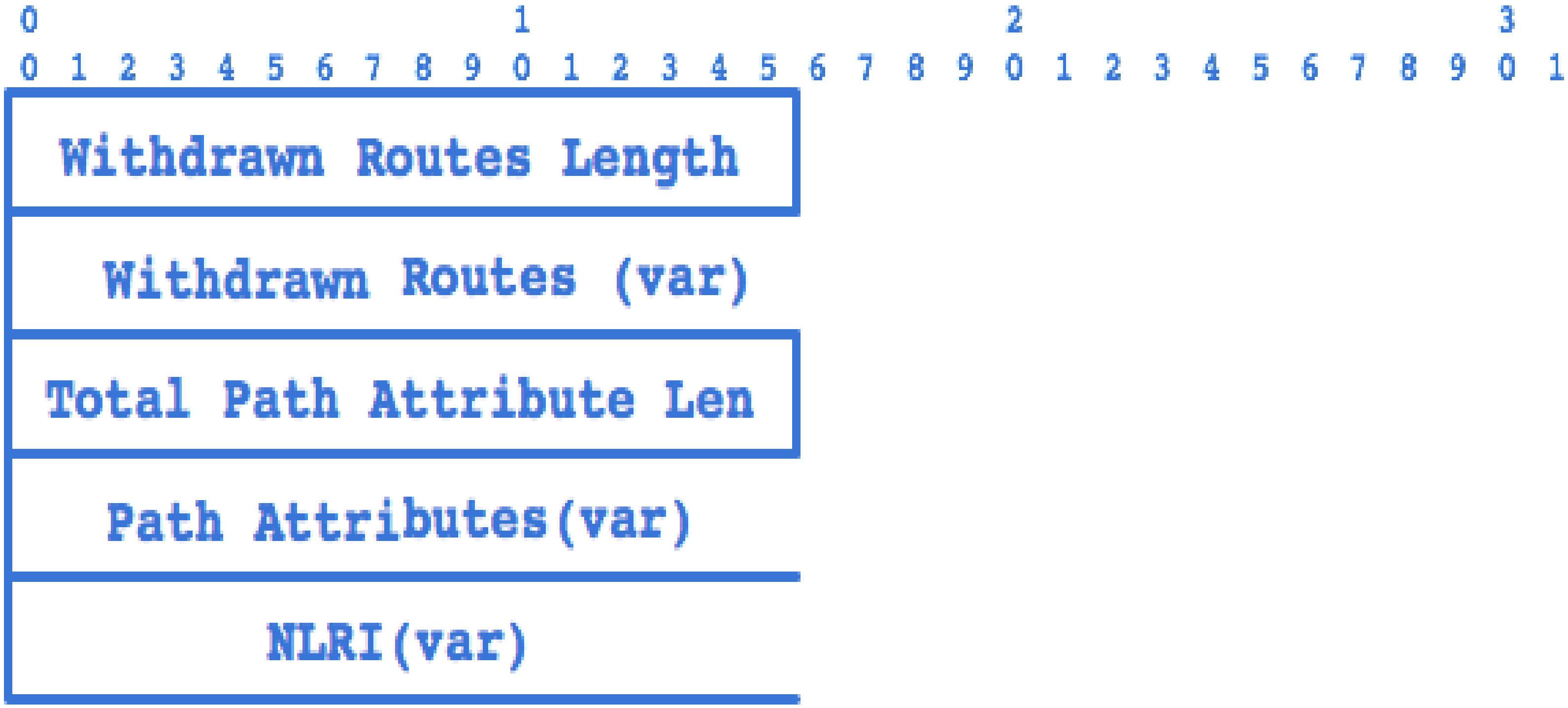
5 – ROUTE-REFRESH

BGP OPEN



0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
My Autonomous System
Hold Time
BGP Identifier
Opt Parm Len
--- Optional Parameters (variable) ---

BGP UPDATE



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Withdrawn Routes Length

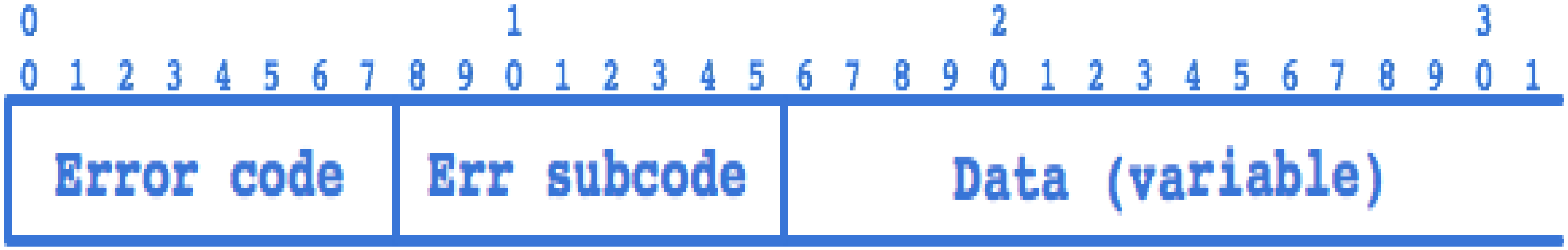
Withdrawn Routes (var)

Total Path Attribute Len

Path Attributes(var)

NLRI(var)

BGP NOTIFICATION



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Error code    | Err subcode   |   Data (variable)
```

Common BGP Path Attributes

Attribute	Well-known mandatory	Well-known discretionary	Optional transitive	Optional non-transitive
ORIGIN	**X**			
AS_PATH	**X**			
NEXT_HOP	**X**			
MULTI_EXIT_DISC				**X**
ATOMIC_AGGREGATE		**X**		
AGGREGATOR			**X**	
COMMUNITY			**X**	
MP_REACH_NLRI				**X**

Affecting BGP Route Decisions

- Prefix length
- LOCAL_PREF
- ORIGIN
- AS_PATH length
- MULTI_EXIT_DISC
- Router import and export policies
- … and more ...

BGP Operational Challenges

- Each AS operates autonomously
- Implicit trust (“routing by rumor”)
- Configuration and policy intensive
- In-band control traffic

Threats

- Availability
- Confidentiality
- Integrity

Threats to Availability

- TCP and lower layer attacks
- Packet floods and control path congestion
- Route instability and churn
- Route flap dampening
- Disaggregation and route table exhaustion
- Implementation bugs and configuration errors
- Route hijacking and black holes
- Policy disputes

Threats to Confidentiality

- Clear text communications
- Routing leaks
- Policy configuration leaks
- Route hijacking

Threats to Integrity

- Implementation bugs
- Protocol design weaknesses
- Compromised systems
- Route hijacking
- Path editing
- Overt or covert transit theft
- Divergence

A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan

- “...we have identified over 540,000 publicly accessible embedded devices configured with factory default root passwords.”
- “...range from enterprise equipment such as firewalls and routers to consumer appliances such as VoIP adapters, cable and IPTV boxes to office equipment...”
- “Vulnerable devices were detected in 144 countries, across 17,427 unique private enterprise, ISP, government, educational, satellite provider as well as residential network environments.”

Mitigation

- Protecting the transport
- Router BCPs
- Route monitoring
- Policies and Defensive filtering
- RPKI and BGPSEC

Protecting the transport

- TCP MD5 signature option and TCP-AO
  http://tools.ietf.org/html/rfc2385
  http://tools.ietf.org/html/rfc5925
- IPSec
  http://tools.ietf.org/html/rfc4301
- RFC 5082 Generalized TTL Security Mechanism
  http://tools.ietf.org/html/rfc5082

Router BCPs

- Configuration templates
  http://www.team-cymru.org/ReadingRoom/Templates/
  http://www.nsa.gov/ia/guidance/security_configuration_guides/
- Control plane protection
- Limited and protected remote access
- Current software
- Configuration management

Route monitoring

- http://bgpmon.net
- http://bgplay.routeviews.org/bgplay/
- http://puck.nether.net/bgp/leakinfo.cgi
- http://www.ripe.net/data-tools/stats/ris/
- http://www.team-cymru.org/Monitoring/BGP/
- http://bgp.he.net

Policies and Defensive Filtering

- Document policy with peers
- Internet Routing Registries (IRRs)
- Max prefix and path length limits
- Limiting disaggregation
- Remote triggered black hole filtering (RTBH)
  http://tools.ietf.org/search/rfc5635
- Dissemination of Flow Specification Rules
  http://tools.ietf.org/search/rfc5575
  http://www.cymru.com/jtk/misc/community-fs.html

RPKI and BGPSEC

- Observation:

  There is no official, and consequently, no strong association between address assignment and routing announcements

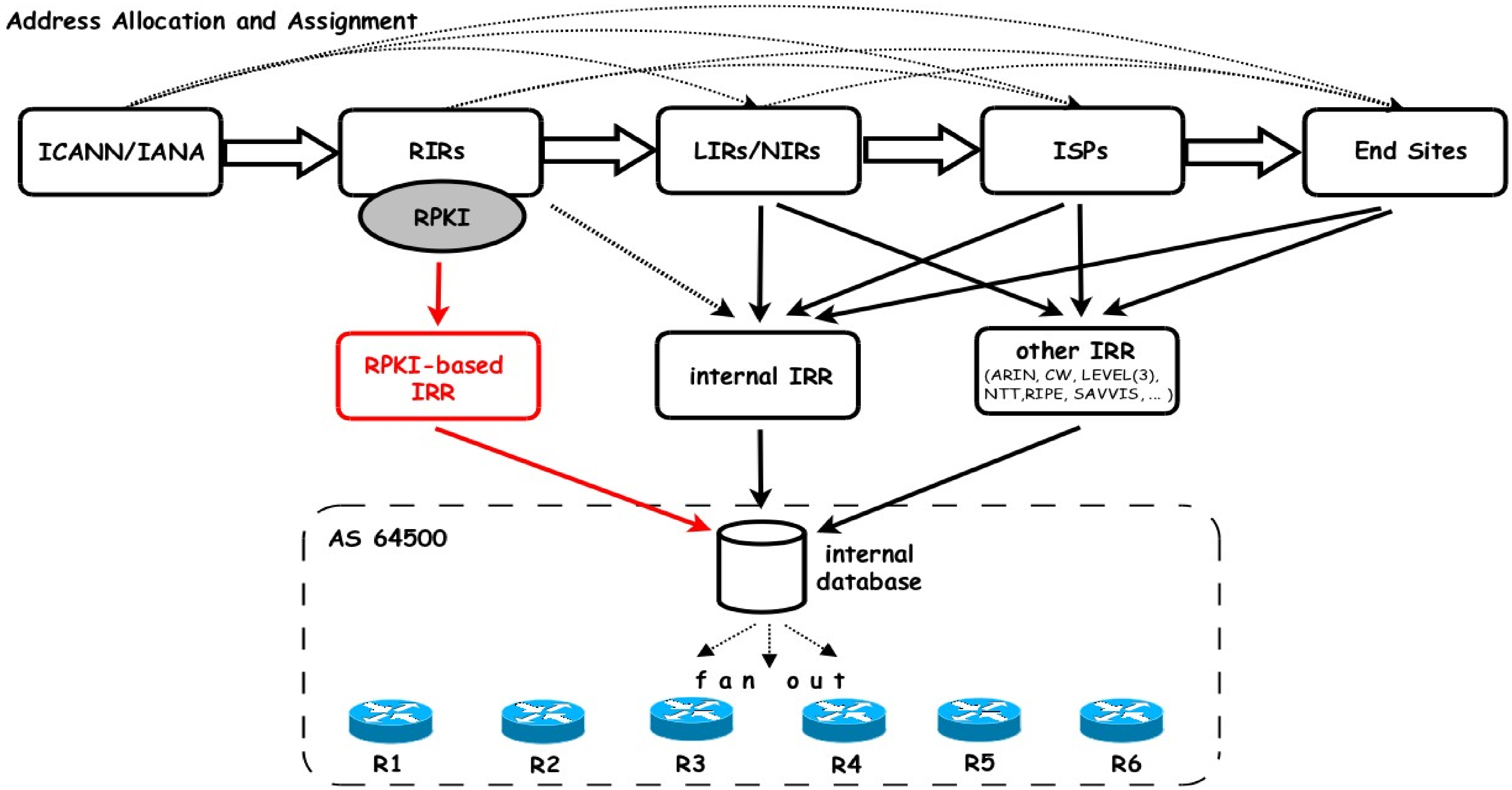
- Problem:

  How do you guard against routing threats, such as hijacks, without a means to verify the routing announcements?

Resource Public Key Infrastructure (RPKI)

- RIRs maintain RPKI infrastructure
- Prefixes linked to authorized AS
- In-band via soBGP or S-BGP
- Out-of-band for near-time validation and monitoring
- IETF SIDR WG spearheading RPKI work
  - Only for origin validation
  - BGPSEC working on path validation
- Similar in scope to DNSSEC architectural changes

A Future of IRR with RPKI



In Closing

- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4593 Generic Threats to Routing Protocols
- IETF Secure Inter-Domain Routing (sidr) WG
- Academic papers:
  - Securing BGP – A Literature Survey
  - A Survey of BGP Security Issues and Solutions
  - Securing BGP with BGPsec
- Feedback or questions to:
  - dmcpherson@verisign.com and jtk@cymru.com