Routing Security

Marco Paesani

ITNOG9 | Bologna | May, 20th 2025

Agenda

- Il valore e il ruolo della sicurezza nel routing
- La storia di MANRS
- RPKI Versione 0 (RFC 6810) e 1 (RFC 8210)
- BGPsec (RFC 8206)
- RPKI Versione 2 (ASPA)

Il valore e il ruolo della sicurezza nel routing

La sicurezza nel routing rappresenta un elemento fondamentale nelle moderne reti di comunicazione. Il routing, processo attraverso cui i pacchetti di dati vengono indirizzati da una sorgente a una destinazione, deve garantire non solo l'efficienza ma anche protezione contro possibili minacce.

- Protezione dell'integrità dei dati durante il transito
- Prevenzione di attacchi come il dirottamento di traffico
- Mantenimento della disponibilità dei servizi di rete
- Salvaguardia della riservatezza delle informazioni trasmesse
- Costituisce uno dei primi punti in cui è possibile implementare filtri di traffico e policy di sicurezza

Il valore e il ruolo della sicurezza nel routing

Il Border Gateway Protocol (BGP) riveste un'importanza fondamentale nel funzionamento di Internet, tanto da essere considerato la "spina dorsale" del routing globale. BGP è il protocollo di routing esterno che permette ai diversi sistemi autonomi (AS) di comunicare tra loro e stabilire i percorsi (path) ottimali per lo scambio di dati.

- Interconnessione globale
- Scalabilità
- Flessibilità nelle policy di routing
- Resilienza della rete

Il valore e il ruolo della sicurezza nel routing

Tuttavia, BGP è stato progettato in un'epoca in cui la sicurezza non era una priorità, e questa caratteristica rappresenta la sua principale debolezza. Incidenti come il dirottamento di prefissi IP (BGP hijacking o route leak) hanno dimostrato come vulnerabilità nel BGP possano avere ripercussioni significative sulla stabilità e sicurezza dell'intera Internet.

Per questo motivo, sono stati sviluppati miglioramenti come RPKI (Resource Public Key Infrastructure), BGPsec e altri meccanismi di sicurezza volti a ridurre i rischi associati alle vulnerabilità intrinseche del protocollo.

Il valore e il ruolo della sicurezza nel routing

BGP Hijacking

Gli aggressori manipolano gli annunci BGP per reindirizzare il traffico Internet verso la propria rete, spesso per intercettare o modificare il traffico o per ottenere l'accesso a informazioni sensibili. (types 5 and 6 RFC 7908)

BGP Route Leaks

Questo accade quando una rete annuncia accidentalmente prefissi/percorsi ad altre reti che non erano destinati a quelle destinazioni. Ad esempio, una rete potrebbe accidentalmente divulgare la propria tabella di routing interna a una rete esterna. (types 1-4 RFC 7908)

La storia di MANRS - https://manrs.org/

MANRS (Mutually Agreed Norms for Routing Security) rappresenta un'iniziativa fondamentale nel panorama della sicurezza del routing Internet, nata dalla necessità di un approccio collaborativo e condiviso per affrontare le vulnerabilità intrinseche del sistema BGP

- 2013-2014: Le origini di MANRS risalgono a discussioni all'interno della comunità tecnica di Internet, particolarmente in forum come RIPE (Réseaux IP Européens), NANOG (North American Network Operators Group) e Internet Society (ISOC).
- 2014: L'Internet Society (ISOC) lancia ufficialmente MANRS come iniziativa collaborativa per migliorare la sicurezza e la resilienza dell'ecosistema di routing globale. Il programma inizia con un piccolo gruppo di operatori di rete pionieri.

RPKI Versione 0 (RFC 6810) e 1 (RFC 8210)

Breve storia dell'implementazione:

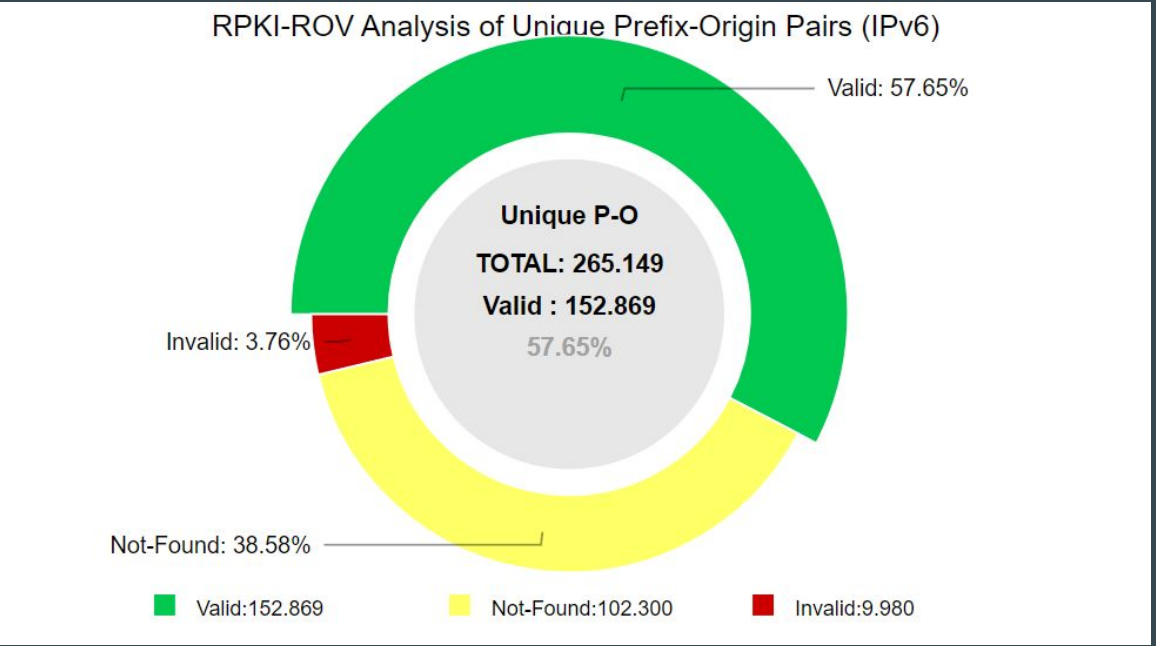
- 2006-2008: L'IETF (Internet Engineering Task Force) avvia il gruppo di lavoro SIDR (Secure Inter-Domain Routing)
- 2008-2012: Vengono pubblicati i primi RFC (Request for Comments) che definiscono l'architettura RPKI, tra cui RFC 6480, RFC 6481, RFC 6482 https://www.iana.org/assignments/rpki/rpki.xhtml Settembre 2011
- 2011: I primi Regional Internet Registries (RIR) come RIPE NCC e APNIC iniziano a implementare servizi RPKI per i loro membri
- 2016-2018: Lo sviluppo di strumenti più accessibili come Routinator, Fort e RPKI Validator 3 (EoL 2021) semplifica l'implementazione per gli operatori di rete.

RPKI Versione 0 (RFC 6810) e 1 (RFC 8210)

- 2019-2022: Inizio dell'implementazione sistematica di RPKI (Prima presentazione a ITNOG5 Maggio 2019). Accelerazione dell'adozione con grandi provider come Cloudflare, Google e altri che annunciano l'implementazione della validazione RPKI. La copertura RPKI raggiunge livelli significativi in molte regioni.
- 2023-ad oggi: RPKI è ormai considerato una best practice nell'industria, con un'adozione crescente a livello globale, anche se ancora non universale.

Oggi RPKI rappresenta un elemento essenziale nella strategia di sicurezza del routing Internet, pur essendo solo un primo passo verso un ecosistema di routing più sicuro che include anche altre iniziative come BGPsec e ASPA (Autonomous System Provider Authorization)

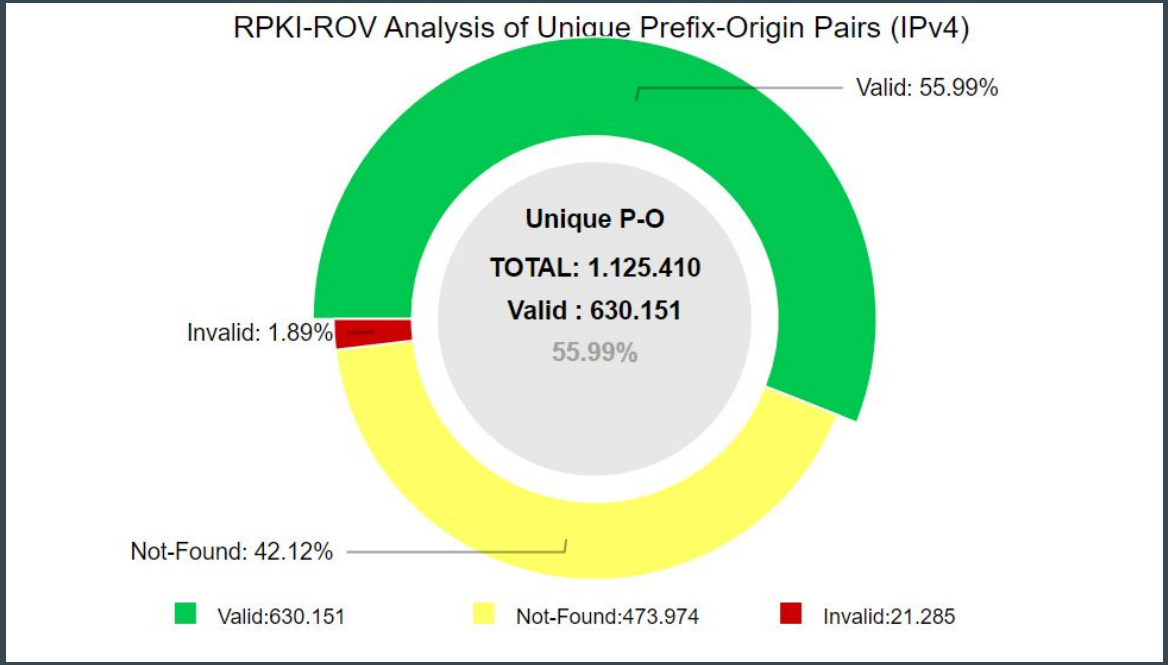
NIST
National Institute of
Standards and Technology



https://rpki-monitor.antd.nist.gov/ROV/All/6

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189r1.ipd.pdf

NIST
National Institute of
Standards and Technology



https://rpki-monitor.antd.nist.gov/ROV/All/4

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189r1.ipd.pdf

BGPsec (RFC 8206)

BGPsec

Richiede modifiche significative ai router BGP esistenti
Necessita dell'aggiornamento simultaneo di hardware e software
Rallenta la convergenza del BGP
Richiede una distribuzione quasi universale per essere efficace

ASPA

Utilizza l'infrastruttura RPKI esistente con un overhead minimo
Può essere implementato in modo incrementale
Offre benefici anche con adozione parziale con investimenti modesti
Non richiede aggiornamenti hardware significativi

RPKI Versione 2 (ASPA)

ASPA (Autonomous System Provider Authorization) è nato come risposta a una vulnerabilità fondamentale nel sistema BGP che le soluzioni esistenti come RPKI non riuscivano ad affrontare adeguatamente: gli attacchi basati sul path (percorso) BGP.

Il BGP presenta un'altra vulnerabilità critica: il "path manipulation" o "route leaks", dove vengono annunciati percorsi validi ma non autorizzati tra sistemi autonomi. Questo tipo di attacco non può essere rilevato attraverso le precedenti versioni di RPKI.

Si dovrà utilizzare sempre in abbinamento ROV Validation realizzato dalle versioni precedenti di RPKI per ottenere la massima sicurezza.

RPKI Versione 2 (ASPA)

Routinator ver. 0.14.2

Internet-Draft:
draft-ietf-sidrops-aspa-verification-22

Published: 23 March 2025

da Alexander Azimov, E. Bogomazov,

R. Bushs, K. Patel, J. Snijders, K. Sriram


```
    }],
    "routerKeys": [],
    "aspas": [{
      "customer": "AS64496",
      "afi": "ipv6",
      "providers": ["AS64499", "AS64511", "AS65551"],
      "source": [{
          "type": "aspa",
          "uri": "rsync://acmecorp.example.net/0/AS64496.asa",
          "tal": "ripe",
          "validity": {
              "notBefore": "2023-04-13T07:21:24Z",
              "notAfter": "2024-04-11T07:26:24Z"
          },
          "chainValidity": {
              "notBefore": "2023-04-18T14:32:13Z",
              "notAfter": "2023-04-20T00:00:00Z"
          },
          "stale": "2023-04-20T00:00:00Z"
        }]
    }]
}
```


https://routinator.docs.nlnetlabs.nl/en/stable/advanced-features.htm

https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification

RPKI Versione 2 (ASPA)

Esempio di configurazione statica ASPA

VRP Version 8.240 per Huawei NetEngine 8000 F1A/M4/M8/M14 and 8000E F2C

```
#
 rpki
  aspa-validation
    static record 3269 provider 6762 ipv4
    static record 3269 provider 6762 ipv6
#
```

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100408233&id=EN-US_TASK_0000001676092657

RPKI Versione 2 (ASPA)

Validazione ASPA (Autonomous System Provider Authorization)

Durante la validazione ASPA, vengono definiti i ruoli BGP che un AS può avere in relazione a un altro AS. L'AS locale si riferisce all'AS in cui risiede il dispositivo locale, mentre l'AS remoto si riferisce all'AS in cui risiede il peer (RFC 9234 - 05/2022)

- ➔ 0 - Provider: l'AS locale è il fornitore di transito dell'AS remoto e può pubblicizzare qualsiasi percorso disponibile a un cliente
- ➔ 1 - Route Server (RS): l'AS locale è un server di routing e può pubblicizzare qualsiasi percorso disponibile a un client RS (AS remoto)

RPKI Versione 2 (ASPA)

Validazione ASPA (Autonomous System Provider Authorization)

- 2 - RS Client: l'AS locale è un client RS e può pubblicizzare qualsiasi percorso appreso da un cliente o percorso originato localmente a un RS
- 3 - Customer: l'AS locale è un cliente di transito dell'AS remoto e può pubblicizzare qualsiasi percorso appreso da un cliente o percorso originato localmente a un provider.
- 4 - Lateral-Peer: se l'AS locale e l'AS remoto hanno una relazione di peer biunivoco, qualsiasi percorso appreso da un cliente o percorso originato localmente può essere pubblicizzato al peer.
- Sibling: se gli AS locali e remoti hanno una relazione full peer, possono annunciarsi reciprocamente tutti i path (sia quelli dei clienti che quelli non dei clienti).

RPKI Versione 2 (ASPA)

RIPE - RPKI Quarterly Planning

Q2 2025 Plans

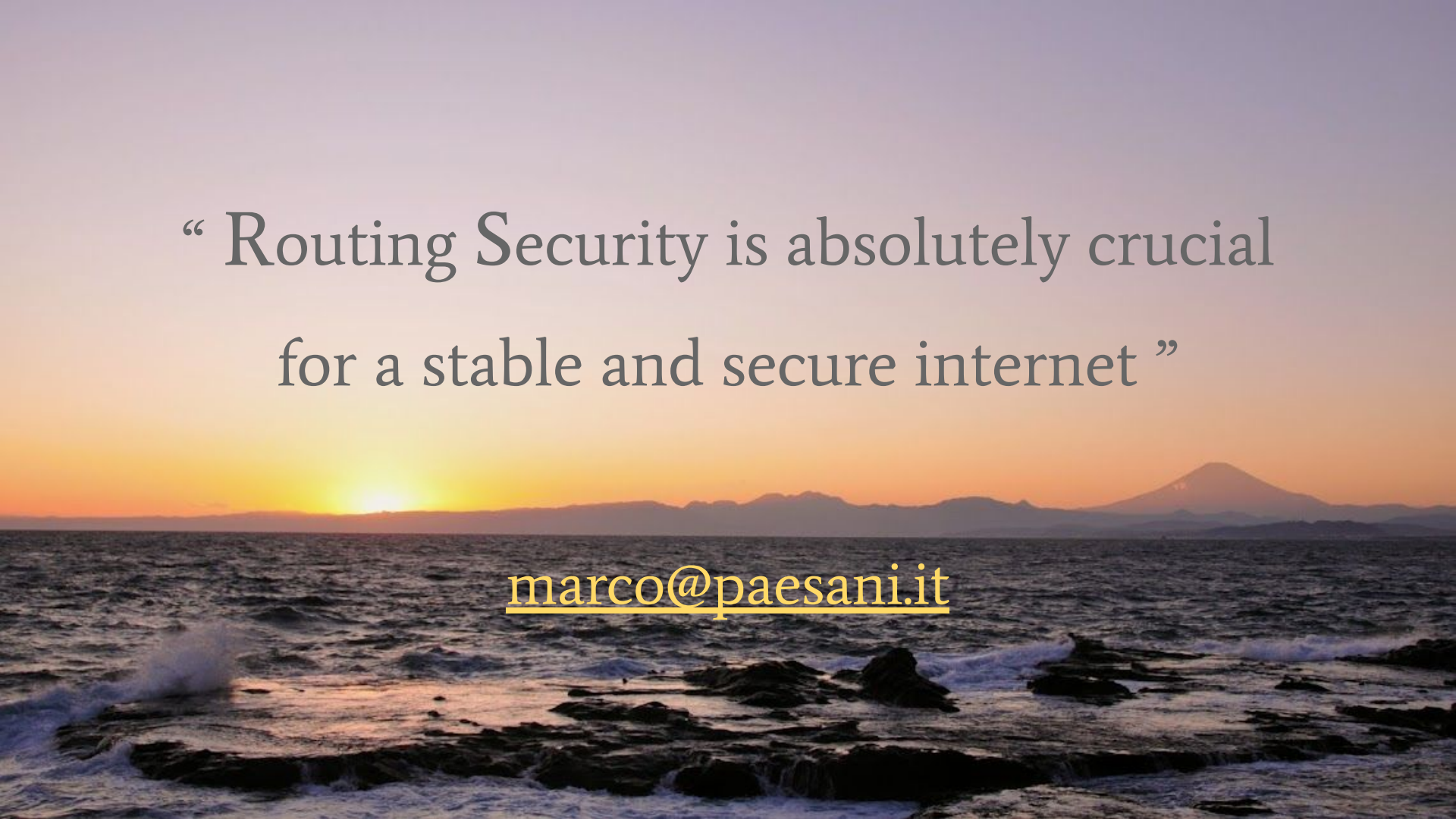
Last updated: 27 March 2025

Item #5: Support ASPA

Status: On hold (pending IETF consensus)

https://www.ripe.net/publications/documentation/quarterly-planning/rpki/

Target di implementazione globale di ASPA è il 2027


“ Routing Security is absolutely crucial
for a stable and secure internet ”
marco@paesani.it