



ROUTING SECURITY: WHAT'S THE ROLE OF POLICY MAKERS?

RIPE 85
27 October 2022

Lauren Crean
OECD Economist/ Policy Analyst – Telecommunications and Broadcasting
Digital Economy Policy Division - OECD

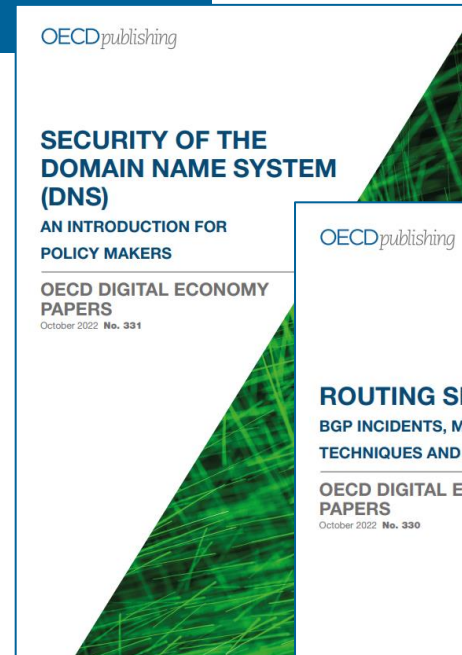


The OECD: Brief introduction

The **Organisation for Economic Co-operation and Development (OECD)** is an international organisation with 38 member countries spanning Europe, the Americas and Asia.

Provides a unique forum and knowledge hub for data analysis, exchange of experience, and advice on public policy on a range of policy topics.

OECD's work covers several topics, including the digital economy, digital security and connectivity, among others.





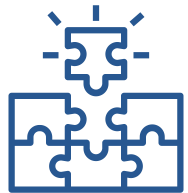
OECD Report on Routing Security



What is the **scope** and **scale** of routing incidents?



Which **security techniques** have been proposed to address them and **how effective** are they?



What is the **role of policy makers** in securing the routing system?



Routing vulnerabilities have been understood for many years, but persist



How secure is the routing system?



This Photo by Unknown Author is licensed under [CC BY-SA](#)



KLAYswap

Photo from <https://klayswap.com/>

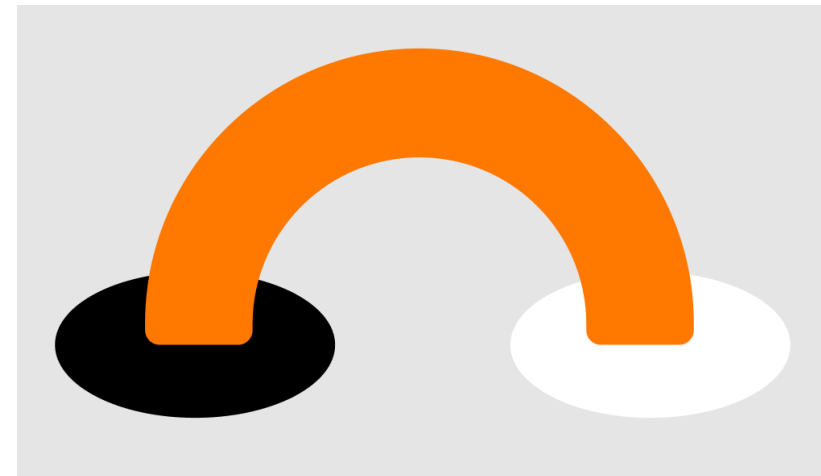
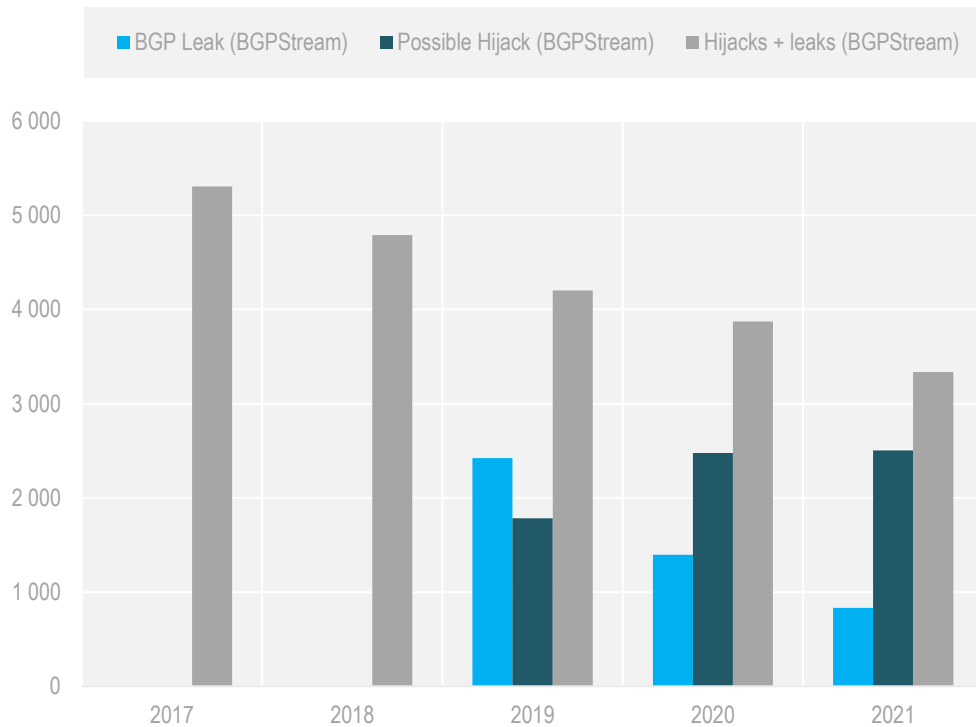


Photo from <https://www.coinbase.com/blog/celer-bridge-incident-analysis>



What is the scope and scale of routing incidents?

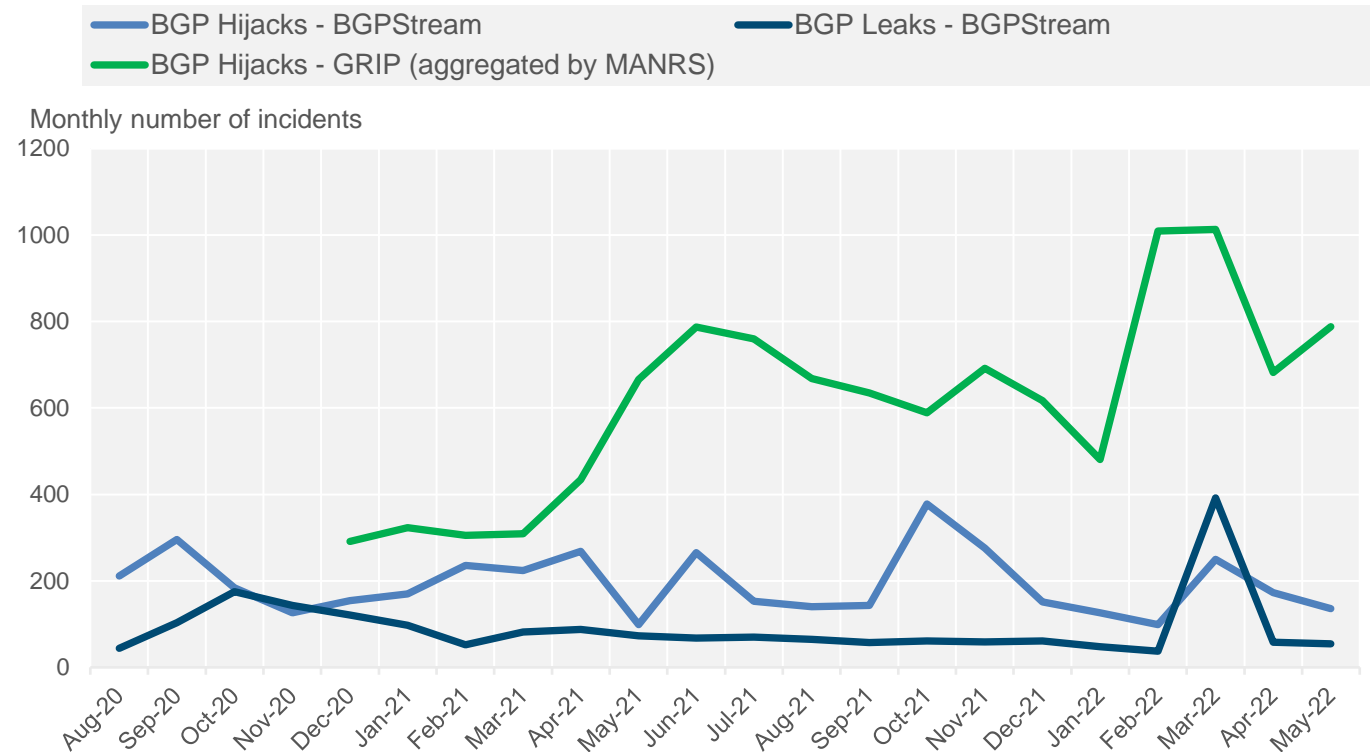
BGP events: leaks and hijacks 2017-2021



Note: Historical disaggregated data was unavailable for 2017 and 2018. BGPStream provides publicly available data on its website (bgpstream.crosswork.cisco.com) on BGP leaks and possible hijacks on a rolling 6-7 months view.

Source: BGPStream provided the underlying dataset used in all analyses (Cisco Crosswork Cloud, 2022_[21]). OECD elaboration using data collected from BGPStream (2021 data) (Cisco Crosswork Cloud, 2022_[21]). OECD elaboration using BGPStream data analysis from (Siddiqui, 2021_[22]) (for 2020 and 2019 data), (Robachevsky, 2019_[23]) (2018 data) and (Robachevsky, 2018_[24]) (2017 data).

Monthly BGP events (Aug 2020 – May 2022)



Note: GRIP data begins from December 2020 because that is the latest data available from the MANRS Observatory, which acts as an aggregator of this data to present on its website (<https://observatory.manrs.org/#/overview>). The BGPStream data for February 2022 may be underrepresented as the system appeared to be malfunctioning for a few days at the beginning of the month.

Source: OECD elaboration based on data from (Cisco Crosswork Cloud, 2022_[21]) and (MANRS, 2022_[27]). BGPStream is a free service provided by Cisco, as part of its Crosswork Cloud (Cisco Crosswork Cloud, 2022_[21]) and GRIP data (Georgia Tech, 2022_[25]) has been incorporated and aggregated by the MANRS Observatory (MANRS, 2022_[27]).



Which security techniques have been proposed to address them and how effective are they?

Origin Validation

RPKI

RPSL / IRR

SCION

BGPsec

ASPA

Path Plausibility

Path Validation



Routing security being considered by policy makers

United States Notice of Inquiry into Internet Routing vulnerabilities [2022]



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



Sweden Review of key stakeholders' treatment of Border Gateway Protocol (BGP) vulnerabilities [2020-2022]

[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

European Union ENISA's "7 steps to shore up the Border Gateway Protocol" report [2019]



[This Photo](#) by Unknown Author is licensed under [CC BY](#)



What is the role of policy makers in securing the routing system?

Policy actions to support stronger routing security

- **Promote measurement and collection of time-series data** on routing incidents, adoption of techniques and their impact to improve security
- **Lead by example** and **promote the deployment** of existing techniques and good practices
- **Facilitate information sharing** on routing incidents
- Define a **common framework with industry** to improve routing security



What is the role of policy makers in securing the routing system?

Selected policy examples around the



Promote measurement and collection of time-series data:
United States



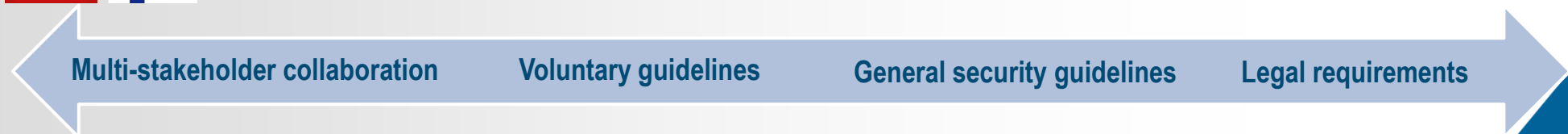
Lead by example and **promote the deployment** of existing techniques: the Netherlands



Facilitate information sharing on routing incidents
Japan



Define a **common framework with industry** to improve routing security: Brazil, Japan, Switzerland, Finland

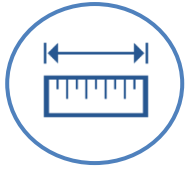




Main takeaways



Routing vulnerabilities are well-known. Many routing incidents occur that **affect the availability, integrity and confidentiality** of communications



Only **what gets measured can be improved**: The importance of **public time series data** on BGP incidents and the adoption and effectiveness of security techniques



Several ongoing efforts to improve routing security. However, **no single technique meets routing's various challenges**, either by design or in practice



There are several policy actions that governments can consider to **support the overall improvement of routing security** of the Internet



Thank you!

Access our OECD broadband data on: <https://www.oecd.org/digital/broadband/broadband-statistics/>



Let's stay in touch!

Lauren.crean@oecd.org

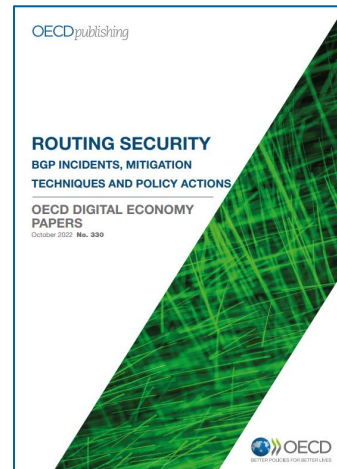


[@OECDInnovation](https://twitter.com/OECDInnovation)

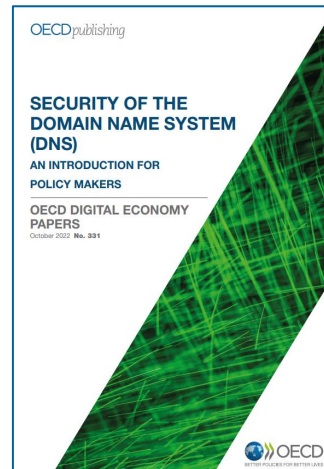


[Lauren Crean](https://www.linkedin.com/in/laurencrean)

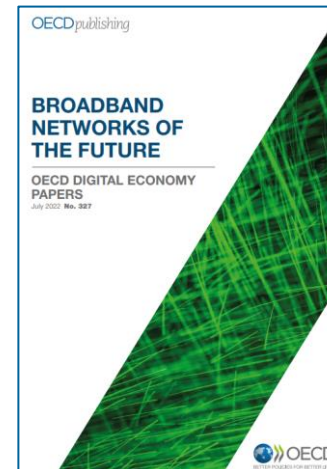
Further reading



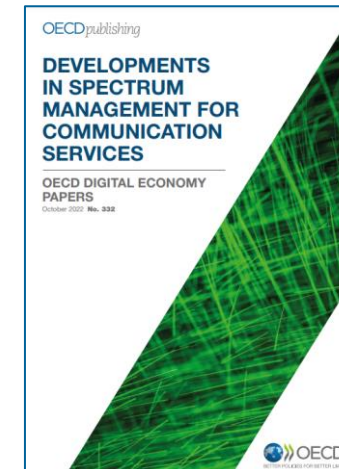
Routing Security (2022)



Security of the DNS (2022)



Broadband Networks of the Future (2022)



Developments in Spectrum Management for Communication Services (2022)



Bridging Digital Divides in G20 Countries (2021)