AIによるOpen Source Routing Protocol実装のSecurity Checkとzebra-rsのパフォーマンス測定

ENOG89
Kunihiro Ishiguro

オープンソース成功の代償 CVEへの対応

・FRR
ultrathink. We want to find potential crash issue regarding packet parser. Please take a look into previously found issue in here:
https://www.cvedetails.com/vendor/17227/Frrouting.html
And investigate other issue in codes.

・gobgp
ultrathink. Please investigate potential buffer overrun or crash issue

・zebra-rs
ultrathink. Please investigate potential buffer overrun or crash issue in @crates/isis-packet and write down the result into markdown file.

isis-packet Security Audit: Buffer Overrun and Crash Issues

Summary

Found **9 issues** across the crate. The most common patterns are unchecked `split_at()` calls with untrusted TLV lengths, unchecked slice indexing in checksum code, and u8 cast truncation in length calculations.

Critical (CRASH/Panic from malformed packets)

1. Unchecked buffer indexing in checksum validation

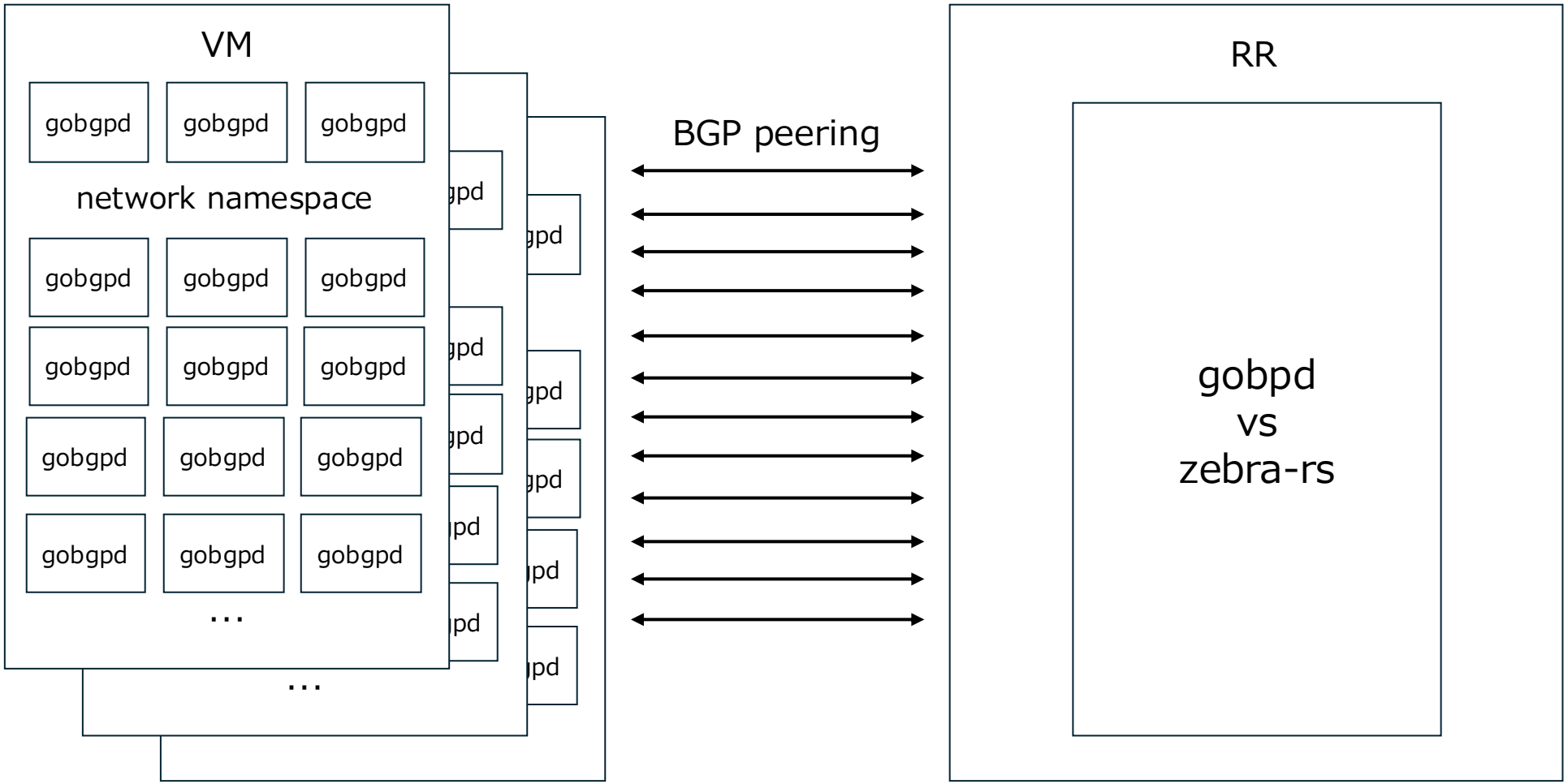
- **File:** `src/checksum.rs:2`
- **Code:**

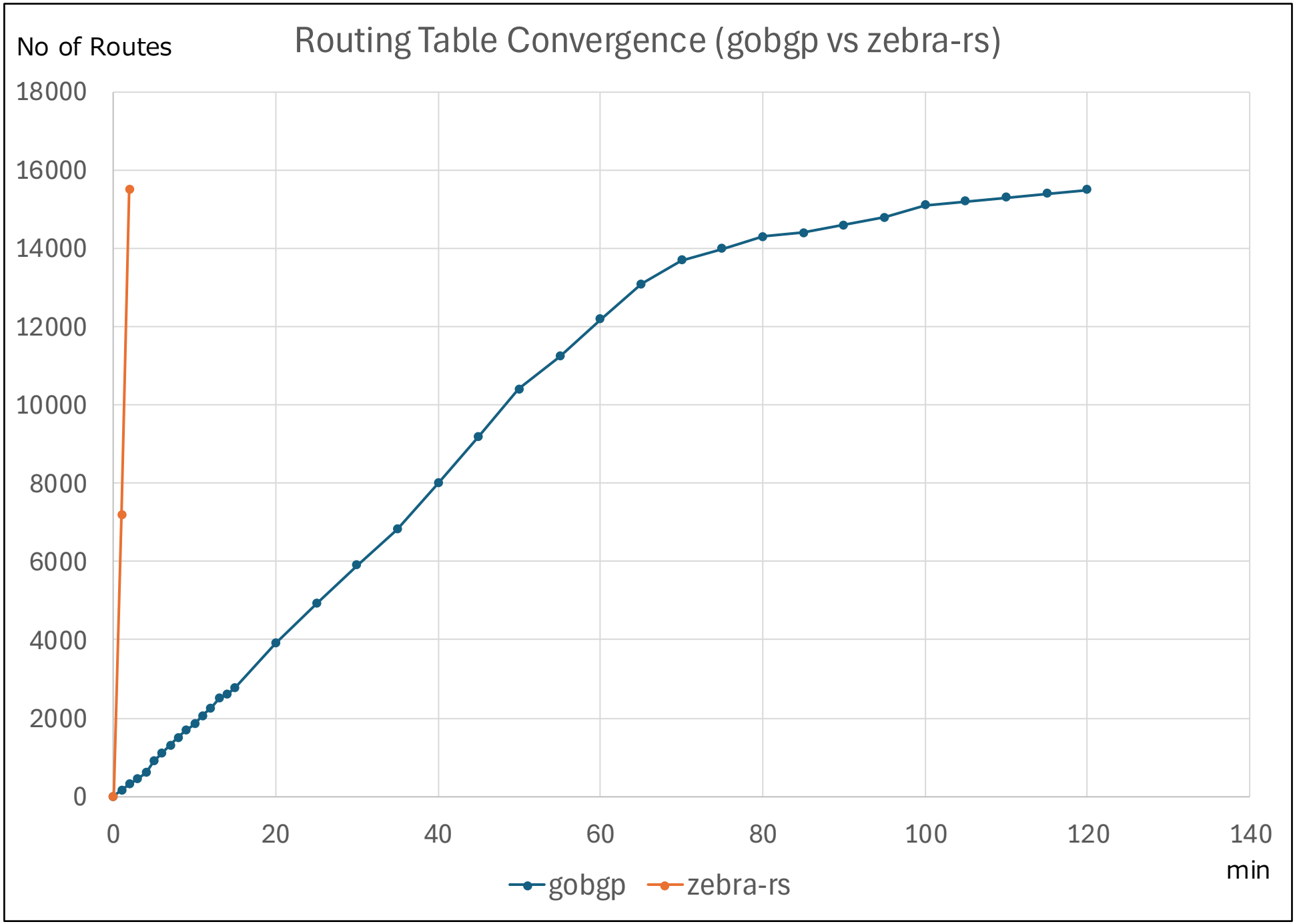
```
pub fn is_valid_checksum(input: &[u8]) -> bool {
    fletcher::calc_fletcher16(&input[12..]) == 0
}
```

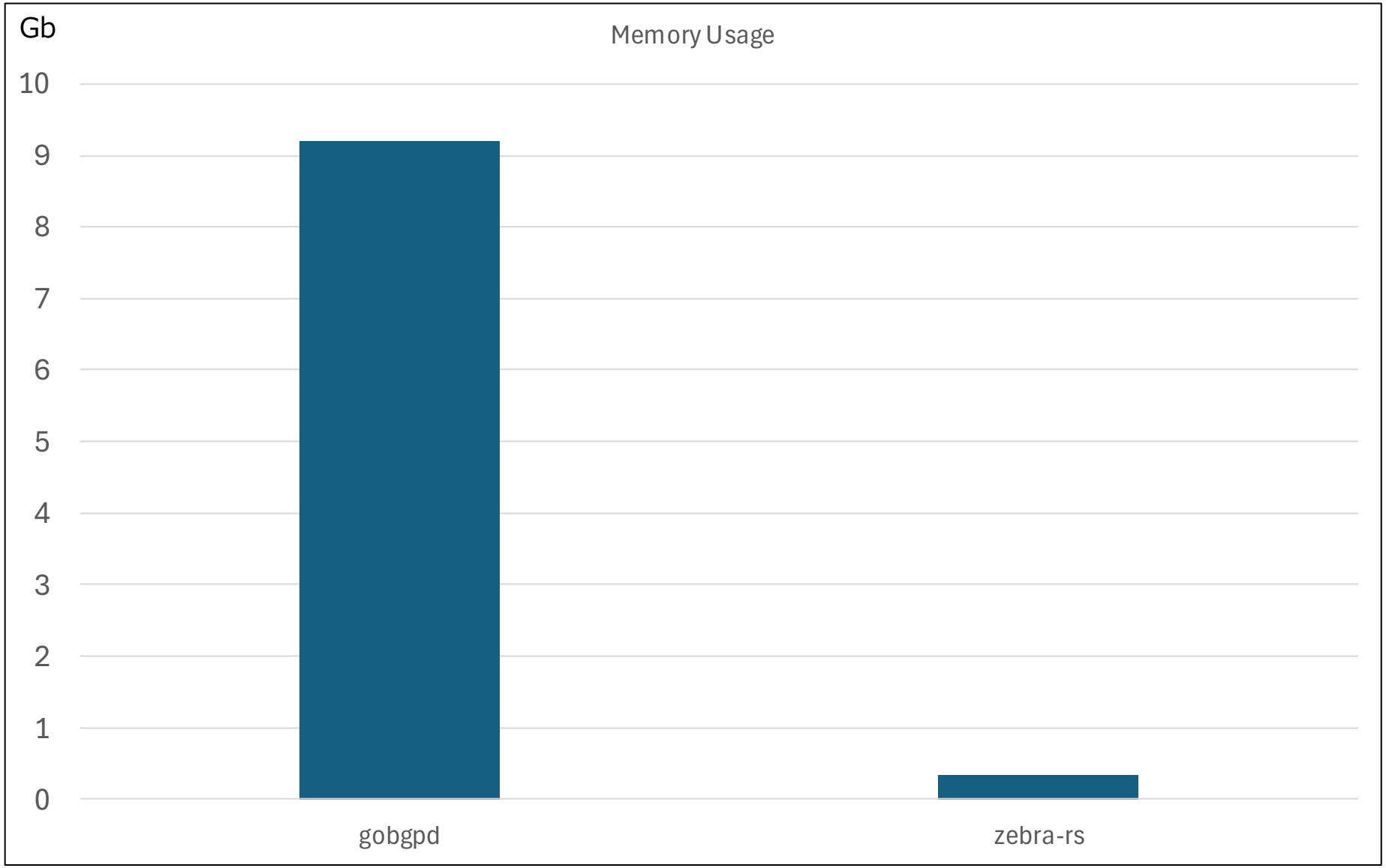
- **Problem:** Direct slice index `input[12..]` panics if `input.len() < 12`.
- **Trigger:** Any IS-IS packet smaller than 12 bytes.
- **Fix:** Return `false` if `input.len() < 12`.

Performance Measurement

RR1の経路をエミュレート: Peer: 1799, Routes: 15073




No of Routes
Routing Table Convergence (gobgp vs zebra-rs)
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
0
20
40
60
80
100
120
140
min
gobgp
zebra-rs


Gb
Memory Usage
10
9
8
7
6
5
4
3
2
1
0
gobgpd
zebra-rs

Async implementation of BGP