RPKI off the beaten happy path

Koen van Hove
University of Twente

Ties de Kock
RIPE NCC

Tim Bruijnzeels
NLnet Labs
Partial RPKI data

• CA 1 has a ROA for AS1 1.1.0.0/16
• CA 2 has a ROA for AS2 1.0.0.0/8
• CA 3 has a ROA for AS3 1.2.0.0/16
• CA 4 has a ROA for AS4 1.2.3.0/24
• Not considering the data of one of these CAs can result in a route changing from valid to invalid (instead of not found)
• Case: there is no current publication point set available for CA 3 (repo down - no cache in RP, CA down and MFT/CRL expired, etc.)
  • What to do when resources are missing?
  • When should an RP report ready to RTR?
Exponential PP spread

- Several RPs limit the depth of the chain (12, 32, 100)
- One can go wide and deep:

```
E
/   \
E-1  E-2  E-3  E-4  E-5  F  E-7  E-8  E-9
|     |     |     |     |   |     |     |     |
F-1  F-2  F-3  F-4  F-5  F-6  G  F-8  F-9
|     |     |     |     |   |     |     |     |
N-1  N-2  N-3  N-4  N-5  N-6  N-7  N-8  N-9
```

- Questions:
  - What should the RP software/operators do?
  - What should the CAs do when it happens?
  - Should CAs prevent it from happening?
  - How should false positives be dealt with?
File system capacity

• Create many folders and overflow the amount of inodes
• rsync client will happily create all folders
  • /001/002/003/../00A/00B/../00Z/00a/../../../zzz/zzz/etc
• As folders are 0 bytes in size, it will bypass normal size restrictions
• Max path length is ~4096, above comes to ~1024
• Applying this to the RIPE NCC PP results in 17,964,612,606 folders (as of 2022-01-29)

• How should an operator prevent this?
Router capacity

• Case: a /48 has been delegated to me
• I can create $\sum_{i=0}^{80} 2^i = 2^{81} - 1 = 2417851639229258349412351$ prefixes
• I can pair those prefixes to $2^{32}$ ASNs
• This creates $2^{133} - 2^{32} = 10889035741470030830827987437812287799296$ pairs
• RPs accept this and pass it on via the RTR protocol
• No router can handle so many entries

• At which level should this be solved? Router/RTR/RP/PP/CA?
Reporting

• Case: targeted attack based on IP address
  • In the case of rsync folders it can also be done as MITM

• Can an operator effectively stop the attack with the current tools?
• If not: how to report malicious behaviour to the (parent) CA so that they can stop it?
  • How does one prove who the perpetrator was? Is that even possible?
  • How can a CA know that their behaviour is viewed as malicious?
    • Does the publication protocol need to be extended?
Discussion

• Partial RPKI data
• Exponential PP spread
• File system capacity
• Router capacity
• Reporting

• RFC:
  • (How) should these problems be dealt with?
  • Who (CA/PP/RP software/operator/router) should solve them?
  • Proactively or reactively?