Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols

(draft-gont-numeric-ids-history &

draft-gont-numeric-ids-generation)

Fernando Gont
Iván Arce

IETF 105
Montreal, Canada. July 20-26, 2019

Introduction

- For the last 30 years, many protocol specifications and/or implementations got numeric identifiers wrong
- **Examples:**
  - Predictable TCP Initial Sequence Numbers
  - Predictable transport protocol numbers
  - Predictable IPv4 or IPv6 Fragment Identifiers
  - Predictable IPv6 IIDs
  - Predictable DNS TxIDs
  - Predictable TLS session tickets/IDs
- Lessons learned about numeric identifiers in one protocol were not leveraged/applied in others
- New protocols/specifications specified/built with the same flaws

Document Roadmap

- **draft-gont-numeric-ids-history**
  - Targets PEARG
- **draft-gont-numeric-ids-generation**
  - Targets PEARG
- **draft-gont-numeric-ids-sec-considerations**
  - Targets AD-sponsored RFC

draft-gont-numeric-ids-history

- Analyzes the timeline of some sample numeric identifiers
- Targets PEARG to work on this item

draft-gont-numeric-ids-generation

- Categorizes numeric identifiers based on interoperability requirements and failure modes
- Analyzes the security and privacy implications of each numeric identifier type
- Proposes some sample algorithms to generate each numeric identifier type
- Targets PEARG to work on this item

draft-gont-numeric-ids-sec-considerations

- Requires protocol specs to do a proper assessment of their numeric identifiers
- Points to the previous two documents
- Targets AD-sponsored RFC

Moving forward

- Adopt
  - draft-gont-numeric-ids-history
  - draft-gont-numeric-ids-generation

  as RG work items?