Large Record Sizes for TLS and DTLS

draft-mattsson-tls-super-jumbo-record-limit-02

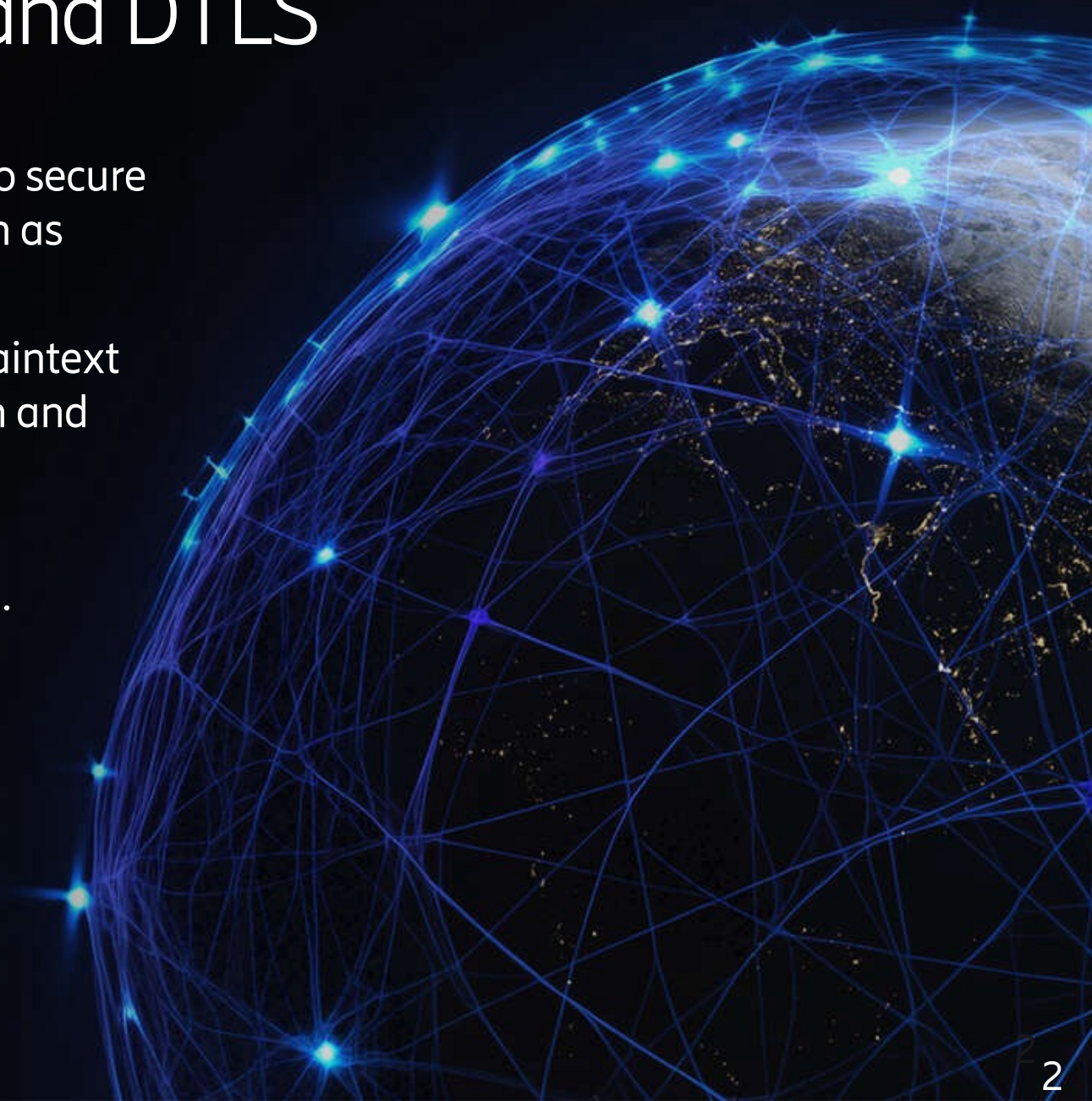
John Preuß Mattsson
Ericsson

Hannes Tschofenig
Siemens

Michael Tüxen
Münster Univ. of Applied Sciences

Large Record Sizes for TLS and DTLS

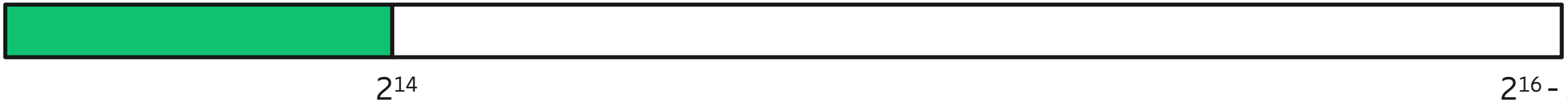
- TLS-based protocols are increasingly employed to secure long-lived interfaces in critical infrastructure, such as telecommunication networks.
- In some infrastructure use cases, the 2^{14} bytes plaintext limit in TLS leads to more frequent fragmentation and results in more CPU/memory consumption.
  - In some of these use cases, 2^{16} bytes records would eliminate the additional fragmentation.
- In RFC 6083 (DTLS over SCTP) the 2^{14} bytes limit is a severe limitation.
- Agreement in the TSVWG "DTLS for SCTP Design Team" that "Large Record Sizes for TLS and DTLS" would improve performance in several of the proposed solutions.



Large Record Sizes for TLS and DTLS

- TLS has an uint16 length field that could theoretically allow records of $2^{16} - 1 = 65535$ bytes in size.
- RFC 8449 defines a “record size limit” extension for TLS and DTLS allowing endpoints to negotiate a maximum plaintext record size smaller than the protocol-defined maximum record size (2^{14} bytes).
- “Large Record Sizes for TLS and DTLS” specifies a "large record size" flag extension to be used in combination with the “record size limit” extension allowing endpoints to negotiate a maximum plaintext record size of up to $2^{16} - 257$ bytes in TLS 1.3.
- An alternative would be a separate extension instead of a flag extension.

“Record size limit” extension:



“Record size limit” extension + “Large record size" flag extension

Summary

- New proposed flag extension "large record size" used in combination with the “record size limit” extension allowing maximum plaintext record size of up to $2^{16} – 257$ bytes.
- Larger TLS records would improve performance and reduce limitation in some use cases of TLS-based protocols in infrastructure interfaces.
- **TLS Adoption?**

Summary by Nick Youngson CC BY-SA 3.0 Alpha Stock Images