IOTEROP
PUSHING IOT BOUNDARIES

# IoT Security Protocols

## A Comparison of TLS, DTLS, OSCORE and Solution Design Considerations.

by Loïc DALMASSO, PhD and Yohan Boyer, PhD

# What are the eventual consequence of poor IoT security?

## CHAOS • LEGAL • REPUTATION • FINANCIAL

IOTEROP

02

# Table of Contents

## Topics Covered

Introduction

TLS and DTLS

OSCORE: A New Approach

Summary

About IoTerop

Get full whitepaper

IOTEROP

"98%

of all IoT device traffic is unencrypted, exposing personal and confidential data on the network."

—Palo Alto Networks Unit 42 research team

IOTEROP

"IoT without security equals the Internet of threats."

—Stephane NAPPO, Global CISO of the Year FINSEC Awards 2018, Société Générale

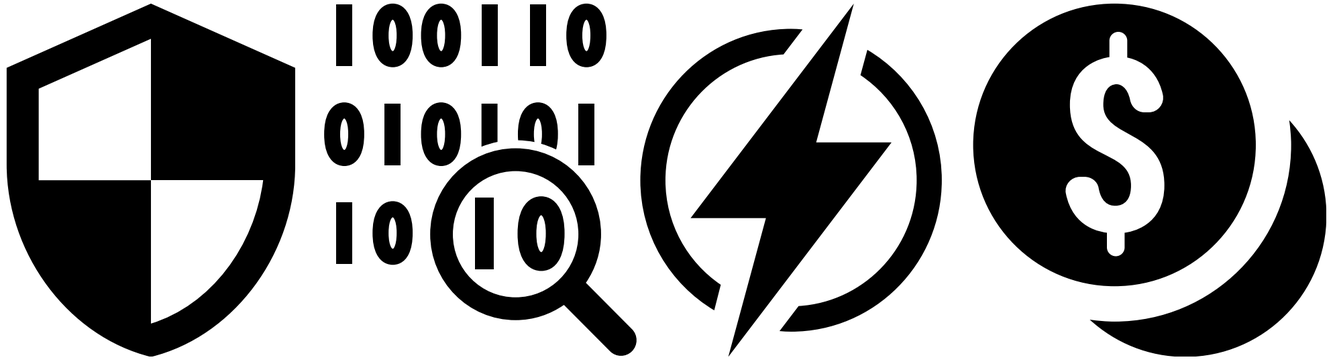
## Introduction

Connected devices create value by collecting, acting upon, and reporting data. Former Intel CEO Bob Swan says, "We see a world where everything increasingly looks like a computer." However, unlike computers, IoT is defined by constraints, use-models that limit human intervention, and devices expected to be numbered in the tens of billions ubiquitous at a scale never seen before in human history.

It is no understatement to declare IoT will create unprecedented security challenges. Rationality argues we should do our utmost to secure the devices that will increasingly become inseparable from the services and products we need to survive like healthcare, energy, and food.

Legacy security approaches TLS and DTLS face challenges in constrained environments where computing power, memory, bandwidth, and energy are all in short supply. These approaches, perfected to secure the internet, quickly reveal themselves to be both too cumbersome, technologically ill-adapted, and economically impractical for constrained nodes and networks, like IoT.

The OSCORE protocol, a lightweight security alternative explicitly designed for constrained nodes and networks as IoT, increasingly attracts various interested parties' attention and efforts. This document compares TLS, DTLS, and OSCORE protocols emphasizing the design implications of different approaches.



"IoT must be secure, but it is also about finding the right balance between security, efficiency, and functionality."

—David Howard, Senior Solution Architect, Itron

IOTEROP

"We measure smart metering solution efficiency in bytes, picoamps, and pennies."

—David Roe, EDMI, Smart Water Metering

## TLS and DTLS

TLS and DTLS are two proven, well-accepted protocols used to secure the internet. Never the less TLS used in conjunction with TCP and DTLS, often used with UDP to transfer data securely, were not designed for IoT but the internet. As a result, each approach may contribute to subpar solution performance, wasted resources, and inadequate security.

TLS over TCP requires a "connection" to establish security and transfer data. This connection is problematic in massive IoT use-cases that depend on high-latency, low-power wide-area (LPWA) networks, especially if the device is battery-powered as devices use power in wake mode. This approach also leads to inefficient use of network and server resources, negatively impacting operational costs.

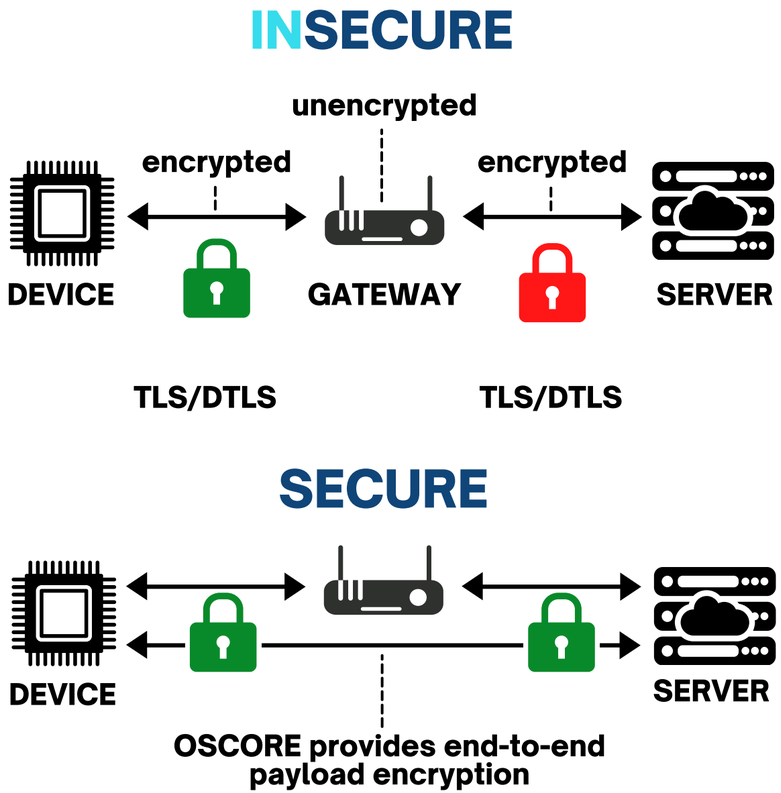
DTLS over UDP improves LPWA IoT solution performance. However, DTLS over UDP relies on a broadcast approach. As a result, data may be lost, requiring re-transmission—each re-transmission consuming precious resources.

Cellular LPWAs such as NB-IoT and LTE-M provide robust encryption raising the question are TLS and DTLS even necessary? Whereas alternative LPWA topographies may require data to travel through one or more gateways. Notably, TLS and DTLS only protect data from hop-to-hop or device to gateway and not end-to-end.

# Important OSCORE Advantages

## OSCORE answers the hop-by-hop security challenge.

**Efficient end-to-end security.**




IOTEROP

"OSCORE is a new lightweight IoT security protocol designed specifically for constrained nodes."

—Ericsson, OSCORE: A look at the new IoT security protocol

## OSCORE: A NEW APPROACH

OSCORE, like CoAP for transport, was designed specifically for IoT's constraints and the security challenges of distributed computing.

Unlike TLS and DTLS, which work well respectively with TCP and UDP for the internet where resources are more plentiful, OSCORE is transport-independent, securing data from end-to-end at the applicative level.

OSCORE's security approach minimizes resource constraints by encrypting only the data payload, not the entire message. Devices can have smaller processors and less memory. Network traffic is reduced. Less data throughput, requires fewer server resources to receive, process, and forward.

OSCORE's approach ensures only pre-authorized endpoints may unencrypt data eliminating the previously mentioned hop-by-hop network vulnerabilities.

In use cases where security is paramount and resources less constrained, OSCORE may be combined with TLS and DTLS to enhance security even further.

# Important OSCORE Advantages

## Protocol overhead comparison single message request-response.

| | TLS | DTLS | OSCORE |
|---|---|---|---|
| Response-request | 42 bytes | 58 bytes | 24 bytes |

Transmission Time

-29%

Computational Time

-50%

Memory Utilization

-15% RAM
-15% ROM

Message Size

-45%

Energy.

-30%

IOTEROP

# Efficiency.

"Application developers and device OEMs should consider LwM2M, among other standards, to simplify and unify their application and product development, particularly in the cellular landscape."

—Gartner,Hype Cycle for IoT Standards and Protocols, 2020,

## SUMMARY

Secure, efficient IoT solutions are challenging to build with poor choices leading to undesirable outcomes.

Encryption, although important, is just one aspect of IoT security. IoT security, although important, is just one aspect of efficient IoT solutions.

Proper IoT security begins during the design and development phases. OSCORE is part of Lightweight M2M (LwM2M), a device management standard. LwM2M provides IoT solutions with a complete, standardized security framework, including device commissioning, certificate-key distribution, device authentication, and secure firmware updating mechanism (FOTA).

To learn more about OSCORE, click to download the full whitepaper.

To learn more about integrating OSCORE into your IoT solutions and how LwM2M can unlock your IoT strategy, contact IoTerop.

"EDMI chose IoTerop after a detailed market analysis because IoTerop provides us with the perfect, implementable version of LwM2M."

—David Roe, EDMI, Smart Water Metering Business Unit Manager

IOTEROP

**"Building metering solutions with IOWA's LwM2M services improves our ability to control operational costs and provide end-to-end security, two key business objectives."**

—Erik Wikstrom, Chief Sales Officer, Elvaco

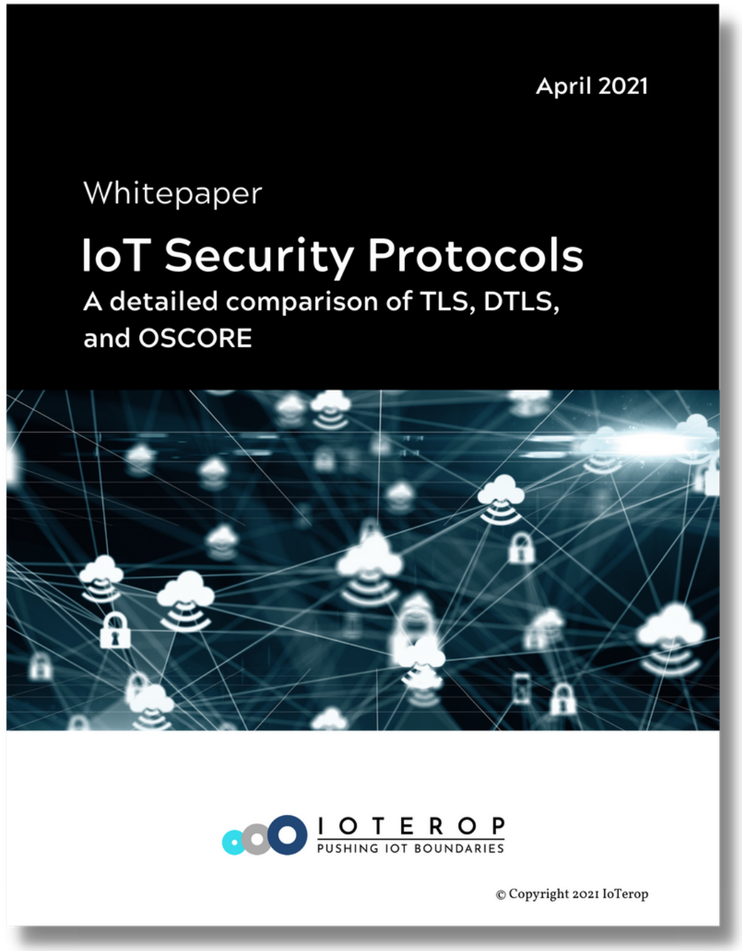
## ABOUT IoTEROP

IoTerop is an award-winning provider of IoT device management solutions whose services reduce the challenges of creating and operating economically disruptive IoT solutions.

IoTerop's co-founder David Navarro is an Open Mobile Alliance SpecWorks board member along with representatives from AT&T, Ericsson, T-Mobile, ARM, Itron, and Qualcomm and a significant contributor to the LwM2M standard since 2011.

IoTerop was founded in 2016 and is headquartered in Montpellier, France.

www.IoTerop.com




**Get the full whitepaper.**

IOTEROP