



DAVID BALBÁS

Imdea Software Institute

JUEVES 27 de FEBRERO

13:00 to 14:15 hrs

(snacks and refreshments afterwards!)

SALÓN DE GRADOS DE LA EPS, Auditorio Padre Soler

Unraveling end-to-end encryption: what, why, and how?



Abstract

End-to-end encryption (E2EE) stands as the gold standard for digital privacy. But how does this cryptographic shield truly work—and why does it matter for businesses and individuals alike? In this session, we will unpack why E2EE isn't just a buzzword but a necessity in a world full of challenges such as AI-driven surveillance, sophisticated malware, and data breaches.

We will explore the meaning of E2EE in cryptography, presenting why simple mechanisms to achieve authenticity and confidentiality do not suffice. We will borrow examples from cloud storage and secure messaging to understand how protocols can self-heal after breaches, ensuring past and future data stays locked even if current keys are stolen.

Finally, we will walk through the architecture of the Signal Protocol -- the backbone of WhatsApp, Facebook Messenger, Signal, and others. We will build its "double ratchet" system from scratch, understanding how its ephemeral keys and resilience against device compromise set the benchmark for modern secure messaging.



uc3m