

ROS Cipherer

Publishing & consuming of encrypted topics

Robotics Group
University of León

Jesús Balsa

Carmen

Alexis

Ángel Manuel Guerrero



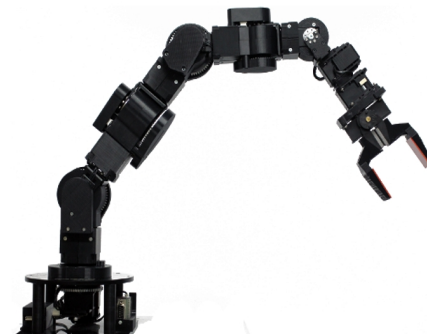
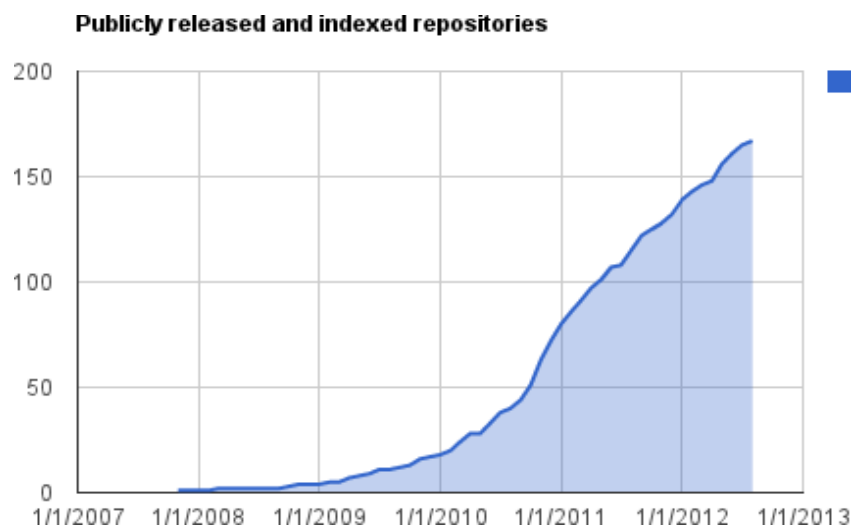
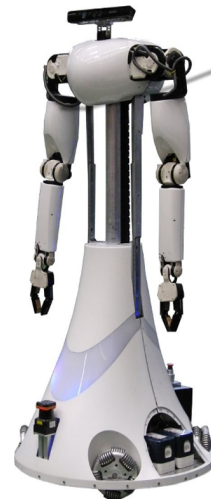
¿Por qué nosotros?

- Robótica asistencial
- Dispositivos hápticos
- **Seguridad en sistemas autónomos**



¿Por qué ROS?

- Open source
- Popular
- Estándar de facto

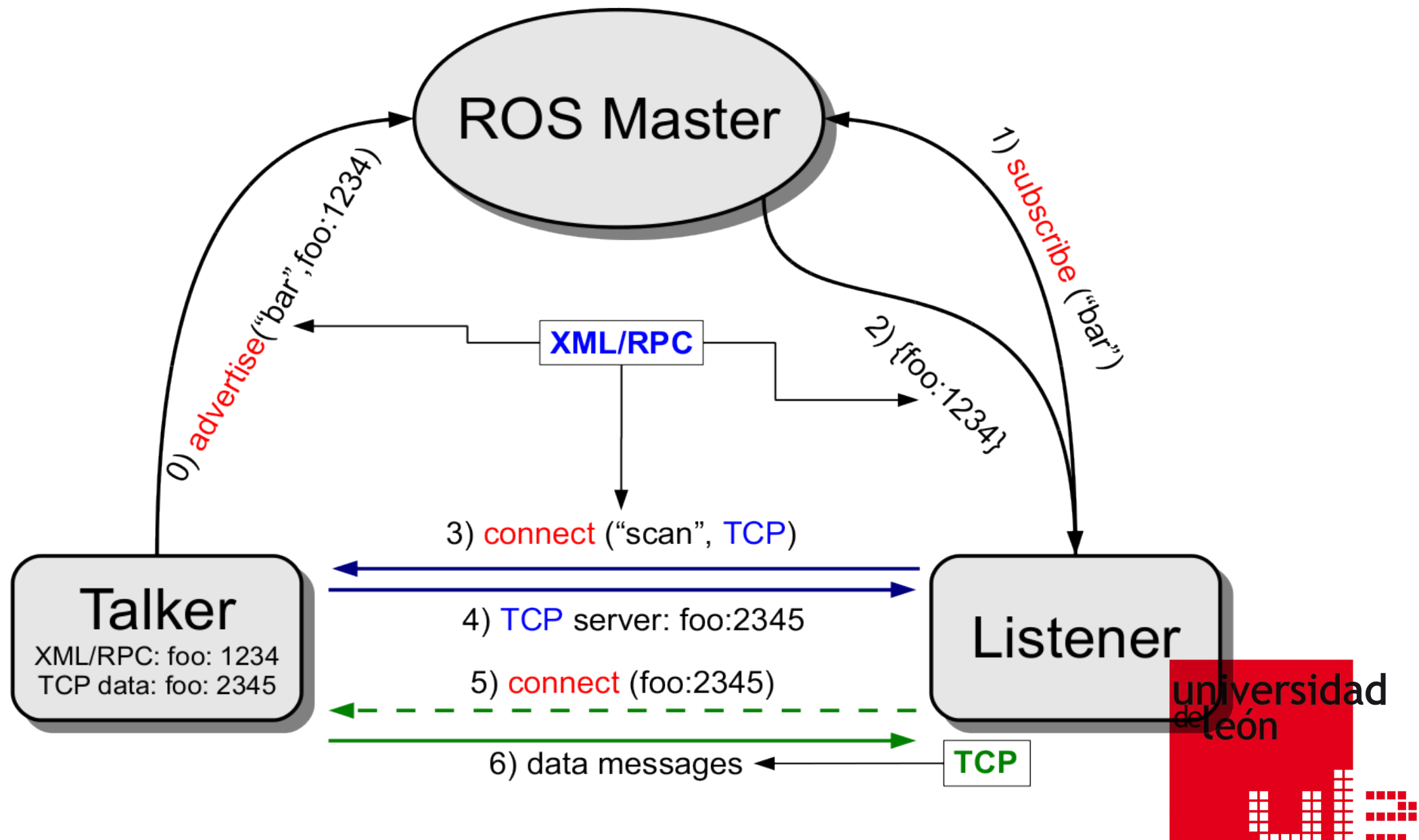


GRUPO DE ROBÓTICA

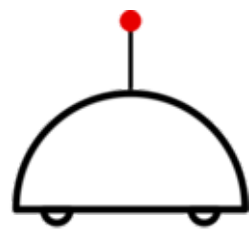
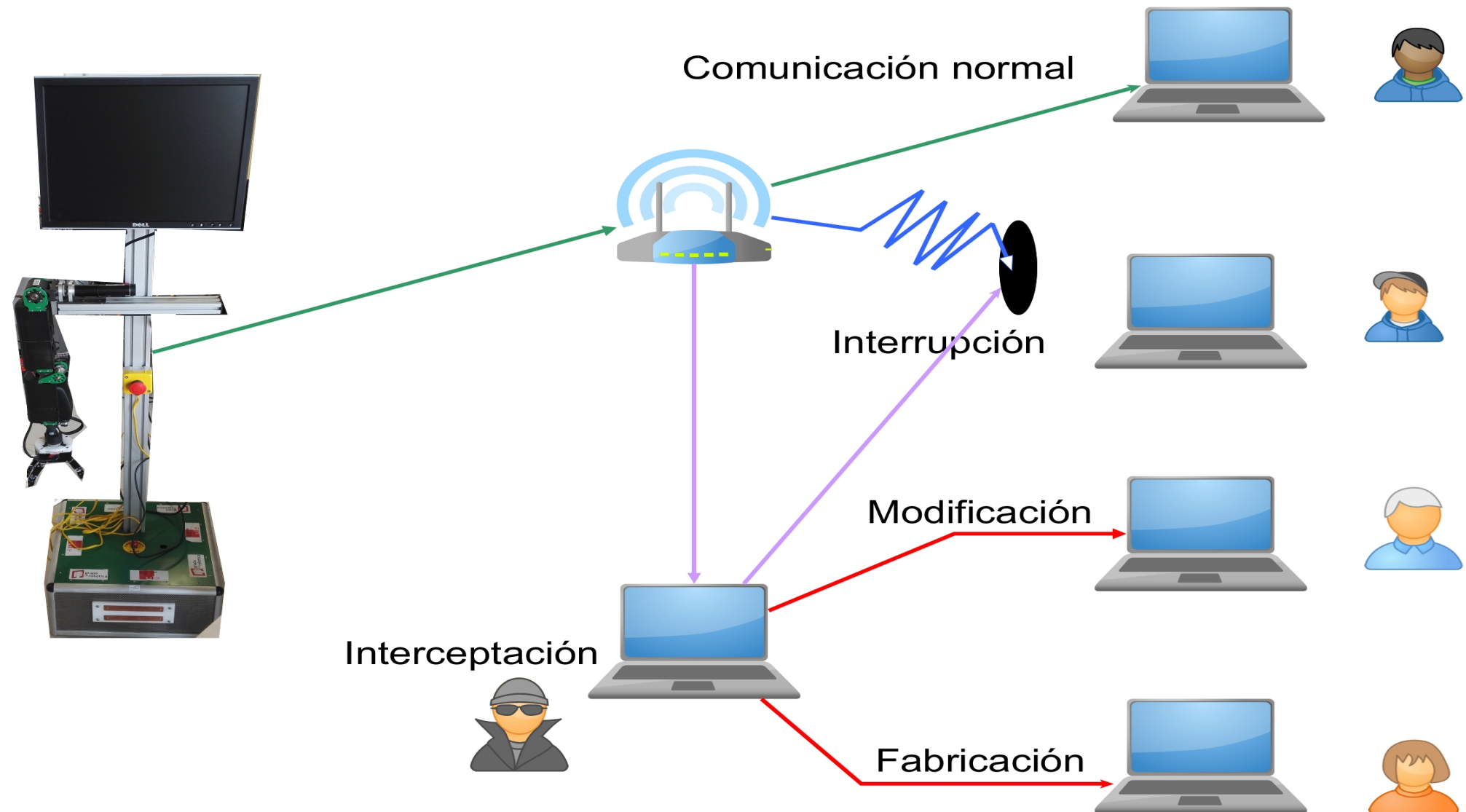


¿Como funciona ROS?

- Framework distribuido que



Seguridad en ROS



GRUPO DE ROBÓTICA



¿Que aporta ROS Ciphered?

- Cifrado de topics con **AES** o **3DES**
- **PyCrypto**
- Cada mensaje tiene su propio IV que viaja junto al mensaje cifrado
- La cola de mensajes solamente tiene capacidad para 1 mensaje
- El mensaje se cifra junto a un número de secuencia
- El consumidor comprueba la validez del número de secuencia

