

# ROS Cipherer

Publishing & consuming of encrypted topics

Robotics Group  
University of León

Jesús Balsa Comerón  
M<sup>a</sup> Del Carmen Calvo Olivera  
Alexis  
Ángel Manuel Guerrero Higuera



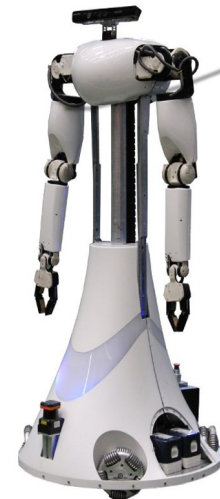
# ¿Por qué nosotros?

- Robótica asistencial
- Dispositivos hápticos
- Seguridad en sistemas autónomos

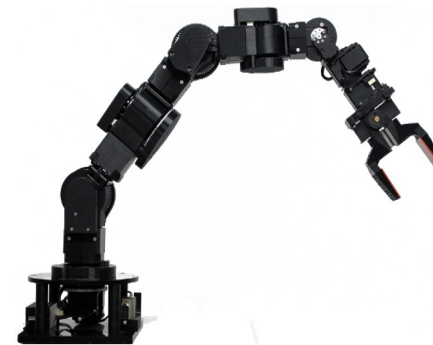
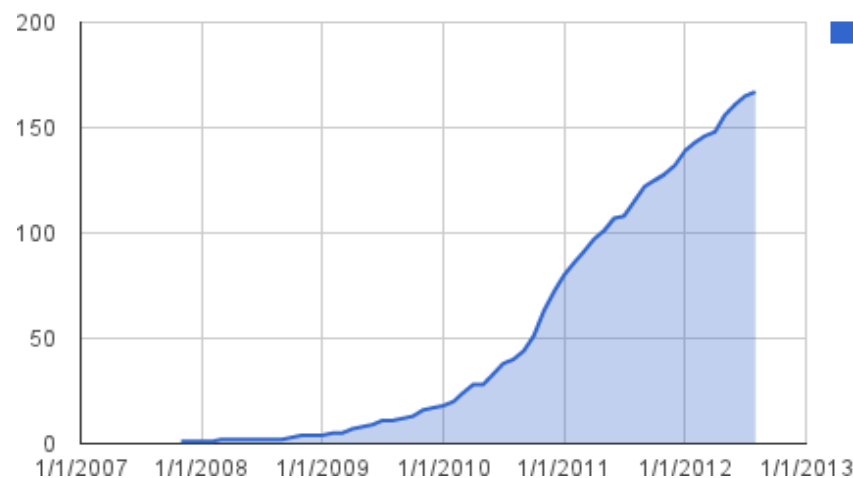


# ¿Por qué ROS?

- Open source
- Popular
- Estándar de facto

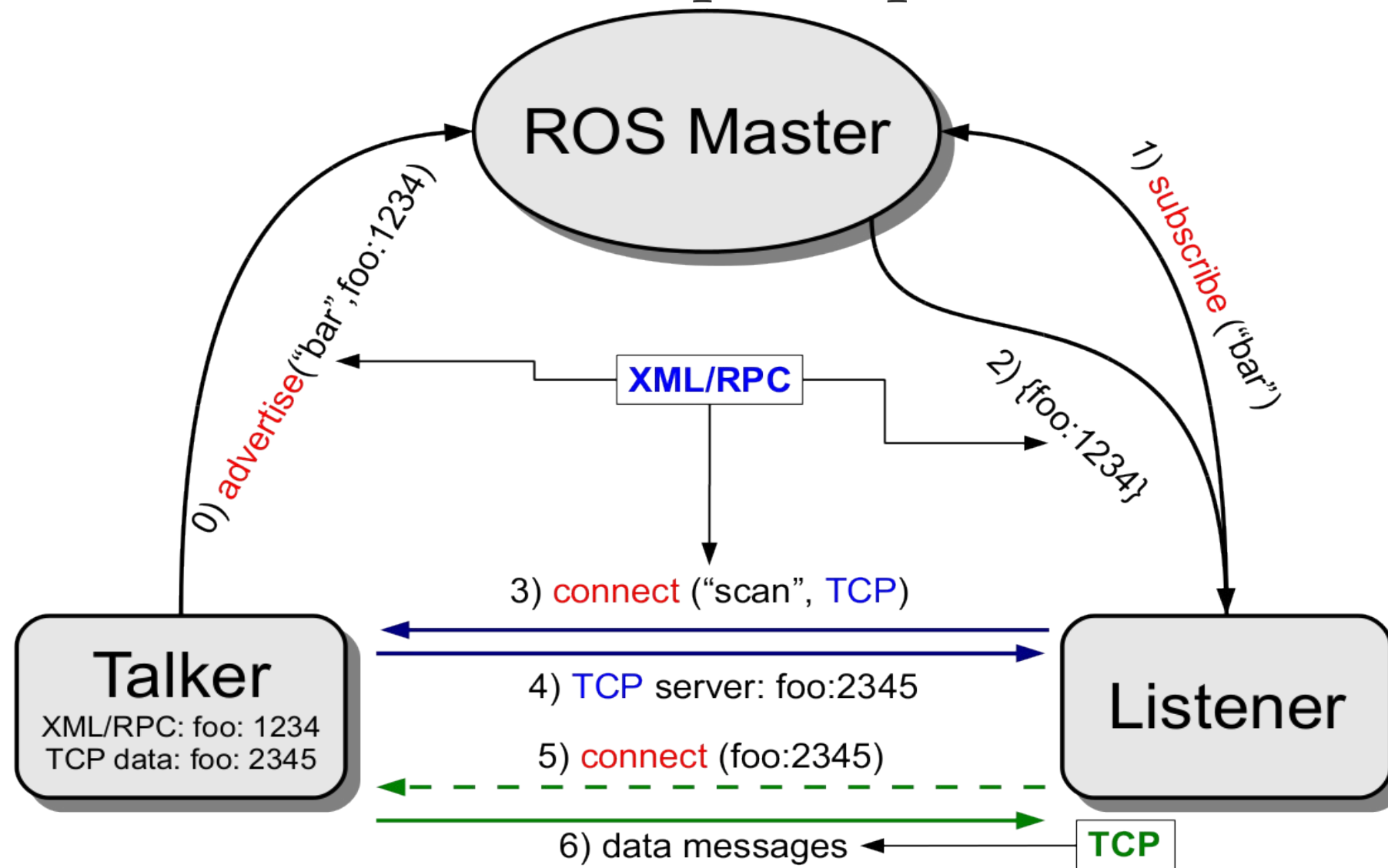


Publicly released and indexed repositories

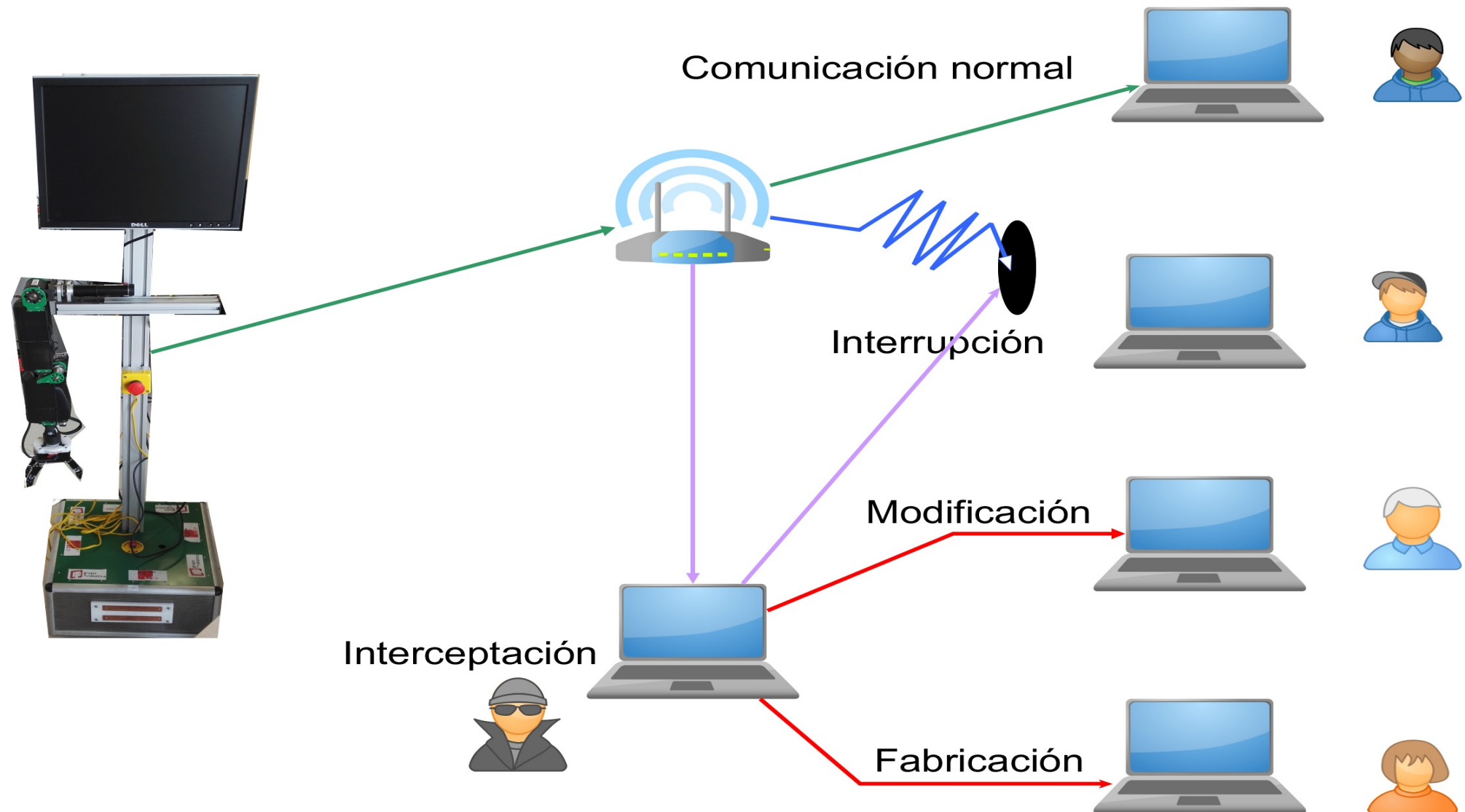


# ¿Cómo funciona ROS?

- Framework distribuido donde unos procesos (nodos) publican información (topics) que otros consumen



# (In)seguridad en ROS





# ¿Que aporta ROS Cipherer?

- Topics cifrados 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 nodo **publisher** cifra el mensaje junto a un número de secuencia
- El nodo **suscriber** descifra y comprueba la validez del número de secuencia



# Trabajos futuros

- Intercambio de clave segura
- Paquete *startup* que permita elegir que topics cifrar

