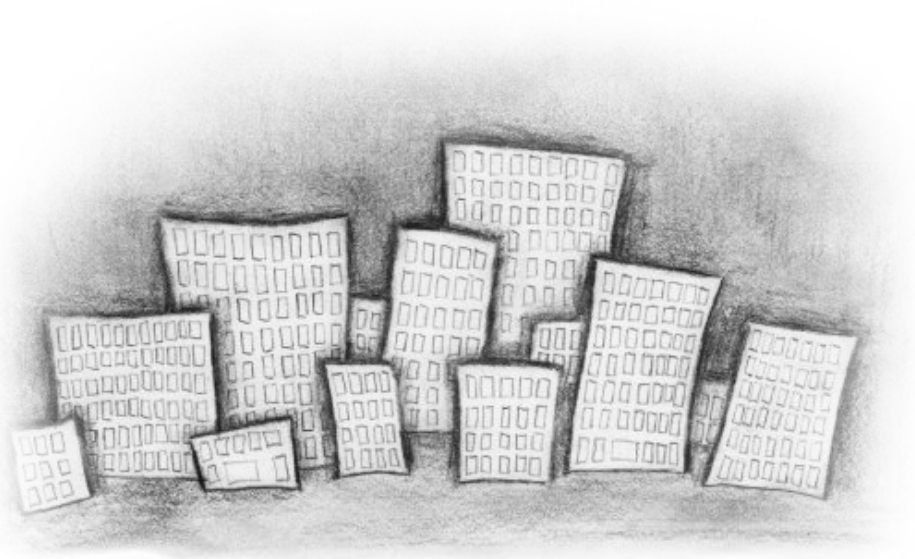
El Futuro de la Seguridad Informática

Miguel Angel Astor Romero

15 de mayo de 2019

Seguridad en las Ciudades Inteligentes

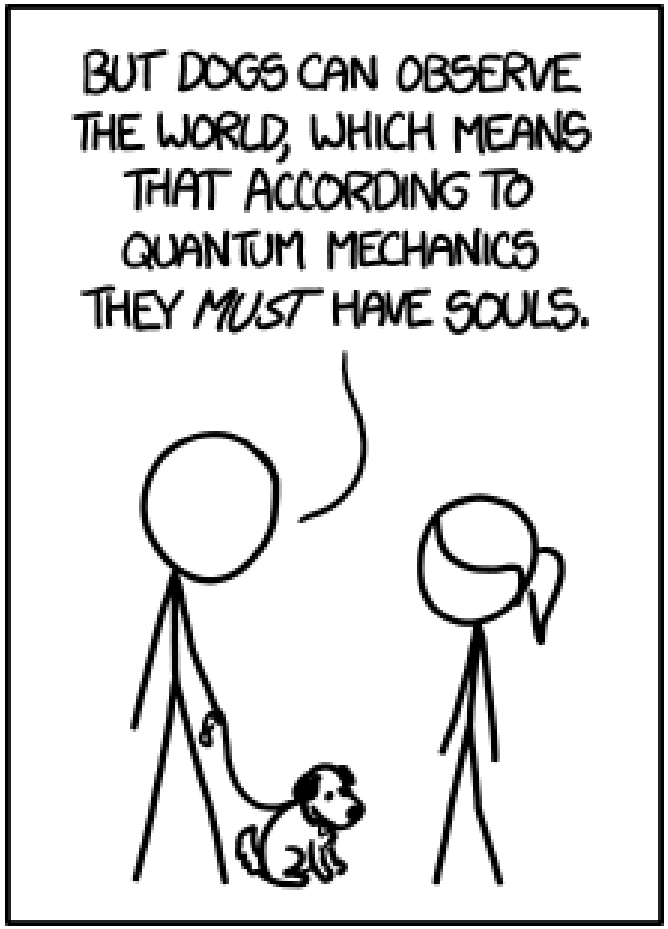
- La conectividad y las redes son transversales a todo en las CI.
- Enormes cantidades de dispositivos y sensores conectados a Internet.
  - Pueden pasar mucho tiempo desatendidos.
- La seguridad y la confianza cobran especial relevancia.



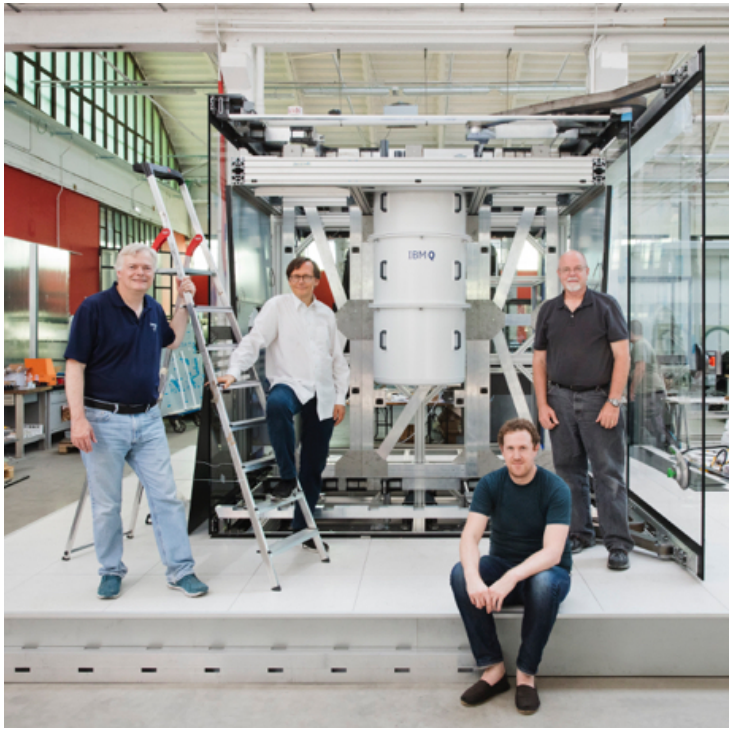
La seguridad y la confianza cobran especial relevancia en todo el ámbito de las CI.

Tendencias en Seguridad Informática

- Redes vehiculares e IoT.
- Cómputo confiable.
- Descentralización y confianza.
- Protección a la privacidad.
- Guerra cibernética.
- Educación.
- Criptografía post-cuántica.


BUT DOGS CAN OBSERVE THE WORLD, WHICH MEANS THAT ACCORDING TO QUANTUM MECHANICS THEY MUST HAVE SOULS.
PROTIP: YOU CAN SAFELY IGNORE ANY SENTENCE THAT INCLUDES THE PHRASE "ACCORDING TO QUANTUM MECHANICS"

Computación Cuántica



- Un nuevo paradigma de computación.
- Basado en mecánica cuántica.
- Qubits, superposición, teletransportación cuántica, decoherencia...
- Algoritmos cuánticos más eficientes.

Tópicos de Investigación

- Reducción de ruido cuántico.
- Ventaja y supremacía cuántica.

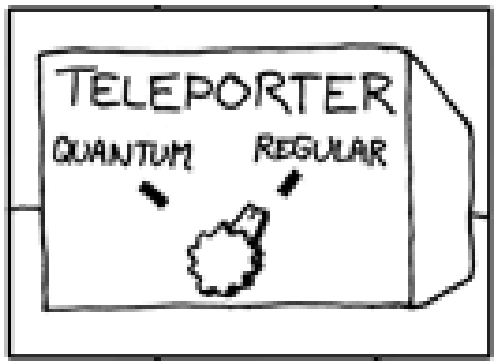
Amenazas a la Criptografía de Clave Pública

- Problemas intratables en la computación clásica pueden ser tratables en la computación cuántica.
- Shor, P., " *Algorithms for quantum computation: discrete logarithms and factoring* ", 1994.
- Factorización de enteros en tiempo polinomial.

La criptografía asimétrica y de curva elíptica dependen de que la factorización de enteros sea muy difícil de resolver.

Criptografía Post-Cuántica

Hay que desarrollar y evaluar nuevos algoritmos criptográficos resistentes a los algoritmos de Shor.



Clases de criptografía post-cuántica

- Basada en funciones *hash*.
- Basada en códigos.
- Basada en rejillas[a].
- Basada en ecuaciones cuadráticas multivariable.
- Criptografía simétrica.

[a] *Lattice* en inglés.