ID de aportación : **221** Código de aportación : **Eje 3_2, TUE 26 - #221** Tipo: **2. Presentación Oral**

Rastreo Digital de Proximidad para COVID-19: seguridad y privacidad

martes, 26 de julio de 2022 16:15 (15 actas)

Uno de los factores decisivos para detener la epidemia de COVID-19 ha sido la aplicación de controles de una epidemia clásica, como son el aislamiento de casos, el seguimiento de contactos y la cuarentena, así como el distanciamiento social y las medidas higiénicas. Rastrear los contactos de las personas infectadas es una de las principales estrategias. Sin embargo, el rastreo manual de contactos es un proceso lento, proclive a errores y omisiones y vulnerable en términos de seguridad y privacidad.

Dadas las altas tasas de contagio, que dificultan el rastreo manual de contactos, surgieron iniciativas para desarrollar tecnologías de rastreo digital de proximidad (RDP). La utilidad de una aplicación de RDP radica, principalmente, en su capacidad para detectar contactos en riesgo mediante el uso de dispositivos móviles. Desde el comienzo de la aparición de las tecnologías RDP se instaló a nivel internacional un interesante debate entre especialistas en el campo de la seguridad y la protección de datos personales. En particular diferentes equipos de investigadores señalaron potenciales riesgos de seguridad y privacidad.

El proyecto PROTECT (PRivacy Oriented TEchniques for the assessment of Contact Tracing solutions), financiado por el Programa CSIC "Conocimiento especializado para enfrentar la emergencia planteada por el COVID-19 y sus impactos", se enfocó en estudiar los desafíos de seguridad y privacidad en el diseño e implementación de soluciones de RDP, aportando a identificar y definir con precisión, lo que una aplicación de RDP como la CoronavirusUY podría, o no, garantizar al respecto. Se analizó en profundidad los requisitos de seguridad y protección de datos personales que deben satisfacer estas soluciones, los modelos de infraestructura subyacente y las tecnologías utilizadas, relevando aplicaciones implementadas a nivel mundial. En particular, se identificaron amenazas potenciales que podrían socavar la satisfacción de los requisitos analizados, violando normas hegemónicas de protección de datos personales.

Palabras clave

rastreo digital de proximidad, privacidad, datos personales

Características de la colaboración

Este trabajo se generó a partir de autor/es y coautor/es clave que comenzaron a colaborar a consecuencia de la pandemia

Interinstitucionalidad

Si

Interdisciplina

Si

Autores primarios: Dr. BETARTE, Gustavo (Facultad de Ingeniería, Universidad de la República); CAMPO, Juan Diego (Facultad de Ingeniería, Universidad de la República); DELGADO, Andrea (Instituto de Computación, Facultad de Ingeniería, Universidad de la República); EZZATTI, Pablo (Instituto de Computación, Facultad de Ingeniería, Universidad de la República); FORTEZA, Álvaro (Departamento de Economía, Facultad de Ciencias Sociales, Universidad de la República); GONZALEZ, Laura (Instituto de Computación, Facultad de Ingeniería, Universidad de la República); MARTÍN, Álvaro (Instituto de Computación, Facultad de Ingeniería, Universidad de la

República); MARTÍNEZ, Rodrigo (Instituto de Computación, Facultad de Ingeniería, Universidad de la República); MURACCIOLE, Bárbara (Centro de Derecho Informático, Facultad de Derecho, Universidad de la República); RUGGIA, Raúl (Instituto de Computación, Facultad de Ingeniería, Universidad de la República)

Presentador: CAMPO, Juan Diego (Facultad de Ingeniería, Universidad de la República)

Clasificación de la sesión: Eje 3_2 Ciencia de datos II. Presentaciones orales

Clasificación de pistas: .