Università
della
Svizzera
italiana

Facoltà
di
scienze
informatiche

Privacy, is there any in IoT?

Malicious Software and Hardware in Internet of Things Panel: IoT and pervasive computing: are new definitions of security and privacy needed?

***Alberto Ferrante* - alberto.ferrante@usi.ch**

*«There is plenty of room for people to **knowingly** divulge personal information in exchange for a service»* [1]

- 43 apps (23 paid and 20 free) for mobile health analyzed [2]:
  - Apps with no privacy policy: 26% of free and 40% of paid
  - Apps that send data to someone not disclosed in the privacy policy: 39% of free and 30% of paid
  - Apps that encrypt all data transmission: 13% of free and 10% of paid

- Even with encryption in place, specific IoT devices and/or their behavior can be identified, thus revealing potentially sensible information:
  - The presence of a specific medical device, reveals potential health problems of the owner
  - Some devices send messages only when specific events occur

[1] Gilad Rosner, *Privacy and the Internet of Things*. O'Reilly Media, 2016.

[2] Linda Ackerman, Mobile Health and Fitness Applications and Information Privacy. Privacy Rights Clearinghouse, 2013.

Privacy, is there any?

- Most used technique to collect data and protect privacy: data anonymization
- Is anonymization effective?
  - By using known characteristics of a user, data can be de-anonymized, e.g.:
    - By locating four times an user in one year, it is possible to extract complete user location information from an anonymized database of 1.5 million mobile phone users [3]
    - By using data emitted from accelerometers of different devices, it is possible to correlate multiple persons and use the location of one of them to compute the location of the others [4]

[3] Yves-Alexandre de Montjoye; César A. Hidalgo; Michel Verleysen; Vincent D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility," Scientific Reports, March 2013, No. 1376.

[4] Jun Han, E. Owusu, L. T. Nguyen, A. Perrig and J. Zhang, "ACComplice: Location inference using accelerometers on smartphones," 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, 2012, pp. 1-9.

Privacy protection need to be redefined

- Local data preprocessing (on node or fog device)
  - No need to send raw data
  - Preprocessing level should be related to the desired level of privacy
  - Challenging:
    - Limited power and computational resources
    - Cloud algorithms need to be redesigned to accept preprocessed data
      - Different levels of preprocessing and/or data provided
    - Data is part of the business for companies

- Users need to be able to verify which data are sent:
  - Especially challenging for IoT devices that have limited or no capabilities to display information