УДК 004.9

Є.В. Горобець
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МОДЕЛЬ БЕЗПЕКИ ДАНИХ В «РОЗУМНИХ МІСТАХ»

Y.V. Horobets

DATA SECURITY MODEL IN «SMART CITIES»

Конфіденційність і безпека - це дві взаємозалежні задачі, які тісно пов'язані з одна з одною, що їх можна розглядати як єдину проблему, яка повинна бути вирішена в контексті розумних міст. [1, 2].

Конфіденційність, з одного боку, не тільки суб'єктивна, але й ситуаційна проблема. Очікується, що сервіси міста будуть працювати на гнучких фреймворках [3, 4] і пропонувати різні варіанти конфігурації [5]. З іншого боку, почуття безпеки від фізичних, спільних та кіберзагроз підвищує впевненість у конфіденційності та сприяє введенню комп'ютерних технологій у повсякденне життя [6]. В «розумному місті» користувачі мають можливість зберігати різні види даних в своїх смартфонах. Щоб моделювати проблему безпеки для різних даних, дані користувачів діляться на кілька рівнів безпеки. Найбільш приватні дані користувачів мають найвищий рівень безпеки, стандартні дані - середній рівень безпеки, а публічні або загальні дані - найнижчий рівень. Приватні дані в основному включають особисту інформацію, таку як місце розташування, контакти, листи, повідомлення та деякі оригінальні фотографії. Публічні або загальні дані, які мають самий низький рівень безпеки, представляють дані, які користувачі завантажують з публічних серверів або публікуються на їх сторінках в соціальних мережах. Інші дані класифікуються як середній рівень безпеки, який містить дані додатків, тимчасові обчислювальні дані та інші [7]. Після поділу на різні рівні безпеки дані користувачів необхідно зберігати в хмарі з використанням різних сервісів. Дані з найнижчим рівнем безпеки зберігаються в найпростішому сховищі, яке забезпечує слабкі засоби безпеки і складне шифрування, але споживає найнижчий обчислювальний ресурс. Дані з більшим рівнем безпеки зберігаються з більшим дозволом безпеки і складнішим шифруванням. Дані з найвищим рівнем безпеки можуть використовувати найскладніші службу шифрування і використовують найбільші обчислювальні ресурси[8].

Література

1. Making Sense of Smart Cities: Addressing Present Shortcomings / R. Kitchin/ Cambridge Journal of Regions, Economy and Society 8:1 (2014) 131–136

2. Privacy Concerns in Smart Cities/ L. van Zoonen/ Government Information Quarterly 33: 3 (2016) 472–480.

3. Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia/ Townsend/ New York & London: WW Norton & Co, 2013.

4. Smart Cities, Ambient Intelligence and Universal Access/ N. Streitz/ in C. Stephanidis, ed., Universal Access in Human-Computer Interaction: Context Diversity Berlin, Heidelberg: Springer, 2011 425–432

5. Smart Cities Applications and Requirements/ Net!Works Expert Working Group / White Paper, Net!Works European Technology Platform 2011 Accessed January 23, 2012

6. Smarter Cities: Making Societies Smarter/ P. J. McNerney and N. Zhang,/ ACM XRDS: Crossroads 18: 2 2011 48–48.

7. Fear and the city: role of mobile services in harnessing safety and security in urban use context/ J. Blom, D. Viswanathan, M. Spasojevic, J. Go, K. Acharya, and R. Ahonius, / in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010, pp. 1841–1850.

8. Security and privacy in smart grid demand response systems/ Paverd, A. Martin, and I. Brown,/ in Smart Grid Security. Springer, 2014, pp. 1–15.