International Journal of Combinatorial Optimization Problems and Informatics, 14(2), May-Aug 2023, 1-2. ISSN: 2007-1558.

www.editada.org

A Brief Panorama of Cybersecurity's complexity into Smart Cities

Alejandro Fuentes-Penna, Raúl Gómez-Cárdenas, Juan de Dios González-Ibarra
[1] El Colegio de Morelos, México.
E-mail: alexfp10@hotmail.com

Cities have been incorporating new technologies into their management by adapting technologies to accelerate their modernization and becoming smarter. These technologies allow optimizing resources, saving money and providing better services. Smart cities allow citizens to interact with it in a multidisciplinary way and adapts in real time to their needs, offering open data, solutions and services to solve the effects of the growth of cities in public and private spheres, through integration of infrastructures with intelligent management systems. Smart cities seek to take advantage of the multiple intelligences of the urban environment regarding quality of life, economic competitiveness and sustainability.

However, the interconnection of all the elements of a city (Internet of Things) and the use of all possible information (big data) implies new cybersecurity risks, which has created particular interest from governments, manufacturers and the researchers:

- A vulnerable device can create an entry point to the entire smart city environment.
- Access to information systems has more vulnerabilities within the organization than remotely.
- The saturation of servers and bandwidth is a critical point because several devices connect to share information.
- There may be vulnerabilities in Cloud, Big Data and IoT devices.

Cybersecurity comprises three large areas: confidentiality – privacy; integrity, and availability of information and services. Security is very important in smart city infrastructures, because networks are prone to a wide variety of attacks. The goals of a smart city will not be achieved if the information is not properly secured. In addition, the privacy of the systems that collect data and trigger emergency responses should be considered.

In smart cities, many devices are wireless, which makes deployment easier; but they are also more susceptible to being hacked. Every new technology brings new problems. Any city, whether or not it is considered smart, can experience cybersecurity incidents. Smart cities have a low tolerance for damage caused by cyberattacks due to the impact it would have on their technology-based infrastructure. With the increasing complexity and interdependence of information, it is difficult to know what is exposed and to what extent.

The smarter a city is, the more systems it will incorporate, increasing the risk and impact of an attack. This requires greater control and better visibility. Other factors that increase complexity in smart cities is the integration of solutions from different providers, especially during phases of rapid technological transformation. Most vendors have little or no experience with security issues, especially in the areas of IoT and industrial systems.

The ICT systems that supervise and control a smart city need to be designed considering cybersecurity, robustness, privacy, information integrity and, above all, resilience. Understanding a city's pressure points and the interdependencies between critical infrastructures can help test the limits of a city's defenses and find ways to mitigate vulnerabilities in technologies that optimize services but lack cybersecurity. Any city can become a safe city by incorporating threat intelligence analysis and networked operation centers, as well as conducting regular exercises and simulations, and initiating a robust penetration testing regimen. A pragmatic approach opts for a middle path: it consists of identifying solutions that allow the deployment of smart city technologies, but in a way that is not harmful to citizens.

On the one hand, that they actively minimize data breaches and address cybersecurity issues. On the other hand, that they work during the entire life cycle of the solutions (from provisioning to retirement) and extend throughout the ecosystem (all components and all interested parties).

The attack surface of smart cities is extensive and completely exposed. It is a real and immediate danger. The more technology a city uses, the more vulnerable it will be.

Thus, smart cities have the highest risks. Now is the time to act to make cities safer and protect them from cyberattacks. It is essential to properly audit the security of all technologies used in cities before implementing them. The huge amount of data that feeds the systems of a smart city, blindly entrusted to the city, can be easily manipulated and the systems are easy to 'hack' ; this is how smart cities become dumb cities. Risk management is related to gray areas. There is a need to use adaptive frameworks to continually assess risk-related benchmarks; This allows security gaps to be identified over time and addressed appropriately. Cybersecurity is practically absent from strategic plans and evaluation methods on smart cities. This is so even despite the fact that smart city systems are directly related to critical infrastructures, such as transport, energy, water, administration, ICT or health. Due to interdependencies and chain reactions, failures can affect other critical and non-critical infrastructures. It is about building smart cities around cybersecurity and not the other way around. To achieve this, it is essential to introduce the security requirements from its conception (security by design), at the time of design.