KNOWLEDGE PARTNER

THE RISE OF THE SMART CITY

Vincent Dupart, President of SPAC and Anne-Isabelle Parodi, General Secretary of SPAC discuss smart city security challenges

More and more of us are living in cities – the UN predicts that 68% of the world's population will live in urban areas by 2050. And this means our cities are facing growing environmental, societal and economic challenges. By making cities smarter, we can overcome some of these challenges and make cities better places to live

The smart city is a necessity, but we must solve security challenges to make it successful. Vincent Dupart, President of SPAC and Anne-Isabelle Parodi, General Secretary of SPAC explain.

What is a smart city and what are the security needs?

Vincent Dupart: A smart city is one that leverages technology to increase efficiencies and improve the quality of services and life for its residents. Smart city initiatives can cover anything from building management, power distribution, transport systems, streetlights and rubbish collection. The idea is to use data and technology to make everyday life easier and better for the people who live and work in the city, while maximising the use of resources.

IoT sensors, video cameras, social media, reader access control, security hardware and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions.

These sensors and connected devices collect and analyse data. This data is used to optimise city operations, manage resources and improve the everyday life of citizens.

Our interest today is to focus on the physical security of these Smart cities. The choice of devices and of communication protocols is crucial for the security success of a Smart City.

This is the mission of the SPAC Alliance.

With so many more layers of technology, sensors and data, smart cities are open to many potential risks. Smart city security is a big area of focus as there are a number of potential risks and challenges involved in these urban landscapes.

One area of risk comes from the level of interconnected information technology (IT) systems and operational technology (OT) systems. The integration of the digital and physical environment creates a large layer of connected endpoints. This results in more opportunities for attackers.

Even if smart cities offer a whole new world of efficiency, innovation and improved community systems, they also involve the widespread movement of data and information. These communications can clearly pose a threat to smart city security - an area that needs particular focus in order for smart cities to function well.

Before we go any further, what is the SPAC Alliance?

Vincent Dupart: Cities or companies contain infrastructures and are increasingly subject to physical attacks by intrusion into buildings or data centres and logical attacks by the Internet vector. Cybersecurity and physical security should go hand in hand as both notions are increasingly intertwined.

In addition, connected objects are more often present in the premises of cities or of the companies that are located there and they communicate on the same communication protocol as the security devices. All the devices are more interconnected than ever before.

In light of these serious physical threats, we decided to create SPAC.

SPAC is an Alliance whose goal is to build a strong and open physical security solution including connected devices. Our members offer different security solutions and IoT solutions.

We choose to promote strong security solutions, resistant to all cyberattacks, open and scalable.

Our actions and choices adapt to the smart city. That's why SPAC will be a key player in the success of the smart city.

What are the assets used by SPAC and which are adaptable to the smart city?

Anne-Isabelle Parodi: Following the hybrid attacks for instance against sensitive infrastructures, the European Commission and European agencies like the ANSSI have defined regulations to fight against these attacks.

These Directives like the NIS Directive define requirements to be implemented in our security solutions in order to secure sensitive infrastructures and to be resistant to all cyberattacks.

And the role of S.P.A.C. is to promote these strong solutions to prevent our ecosystem from choosing weak physical security solutions.

One of the important requirements that we recommend is security certifications of the connected or not connected devices. Using certified devices ensure the usage of trusted solutions. In addition, protocols must be security certified to allow the provision of a complete trusted security solution.
In addition, to secure a smart city, the security certified protocol must offer the possibility to communicate on wired and wireless links.

> "A smart city is one that leverages technology to increase efficiencies and improve the quality of services and life for its residents."

The SSCP communication protocol is the answer to all these requirements and is the solution for the smart city.

What is this protocol?

Anne-Isabelle Parodi: The SSCP Protocol is an Industrial Standard allowing integrity and confidentiality by the encryption of sensitive data. It is the first protocol for our security market to have been security certified by the ANSSI to be resistant to all cyberattacks. In addition, this protocol allows communicating on wired or wireless links (RS485, USB, TCP/IP, etc.), meaning that it is interface agnostic.

And it offers the possibility to communicate with different hardware objects which can be connected or not connected to offer a global trusted security solution with the same security.

And this Industrial Standard is completely open to be evolutive and is future-proofed for any new requirements of the smart city. This evolution is carried by the SPAC Alliance.

With these assets, we meet the expectations required to secure a smart city and to enable its success.

For more information about SPAC, please contact Anne-Isabelle Parodi - ai.parodi@sp-ac.org - https://en.sp-ac.org/