Cyber-security, data protection and cyber-resilience in Smart Sustainable Cities

ITU Forum on Smart and Sustainable Cities
Abu Dhabi 3-4 May 2015

Giampiero Nanni
Leaders of the “Technical report on cyber-security, data protection & cyber-resilience in Smart Sustainable Cities”

Source and references

- This document presents a brief summary of the “Technical Report on Cyber-security, Data protection & Cyber-Resilience in smart sustainable Cities” that is being developed by the ITU-T’s Focus Group on Smart Sustainable Cities (FG-SSC).

- Please also refer to the following documents submitted to ITU-D SG2, as contributions: 26, 27, 28, 29, 30 and 34.

Overview

Smart and sustainable city deployments will be carried out by a diverse ecosystem of providers in innovative domains, involving state-of-the-art technology, including critical and complex ICT implementations.

- These deployments can address different components and city systems, like Intelligent Transportation, Connected Healthcare, Public Safety and Security, Emergency Services, Smart Grid and Smart Metering, Intelligent Buildings, etc.
- Increasing ICT complexity, hyper-connectivity, namely through 'Internet of Things' environments, as well as the generation of significant amounts of data, will also mean increasing vulnerability, both to malicious attacks and unintentional incidents. By conceiving interconnected urban systems with Cyber-Security and Data Protection in mind, city administrators will be able to ensure service continuity, safety and well-being for citizens and businesses alike.
- This draft Technical Report details these Cyber-Security and Data Protection considerations in Smart and sustainable city developments. It will explore the requirements and challenges of creating a secure, reliable and resilient smart and sustainable city. It will consider how administrations and the overall city ecosystems will need to provide innovative, resilient 'smart' solutions that leverage digital information while protecting against malicious violations, unintentional damage and natural disasters.

Definition of SSC

"A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects".

The SSC cyber-equation

- "Smart and Sustainable Cities" have ICT as key enabler
- This implies:
  - Highly complexity of the ICT systems
  - Highly interconnected components
  - High volume of data generated

A resilient Smart and Sustainable City…

…needs to be designed, from inception, with…

- Cyber security
- Privacy
- Integrity
- Compliance
- Reliability
- Resilience

…in mind.

Definitions: resilience and cyber-resilience

Resilience

- ITU-T SG17 defines resilience as the "Ability to recover from security compromises or attacks."
- Complementing this focus, a recent ITU report on 'Resilient Pathways' defines resilience as "The ability of a system or a sector to withstand, recover, adapt, and potentially transform in the face of stressors such as those caused by climate change impacts".

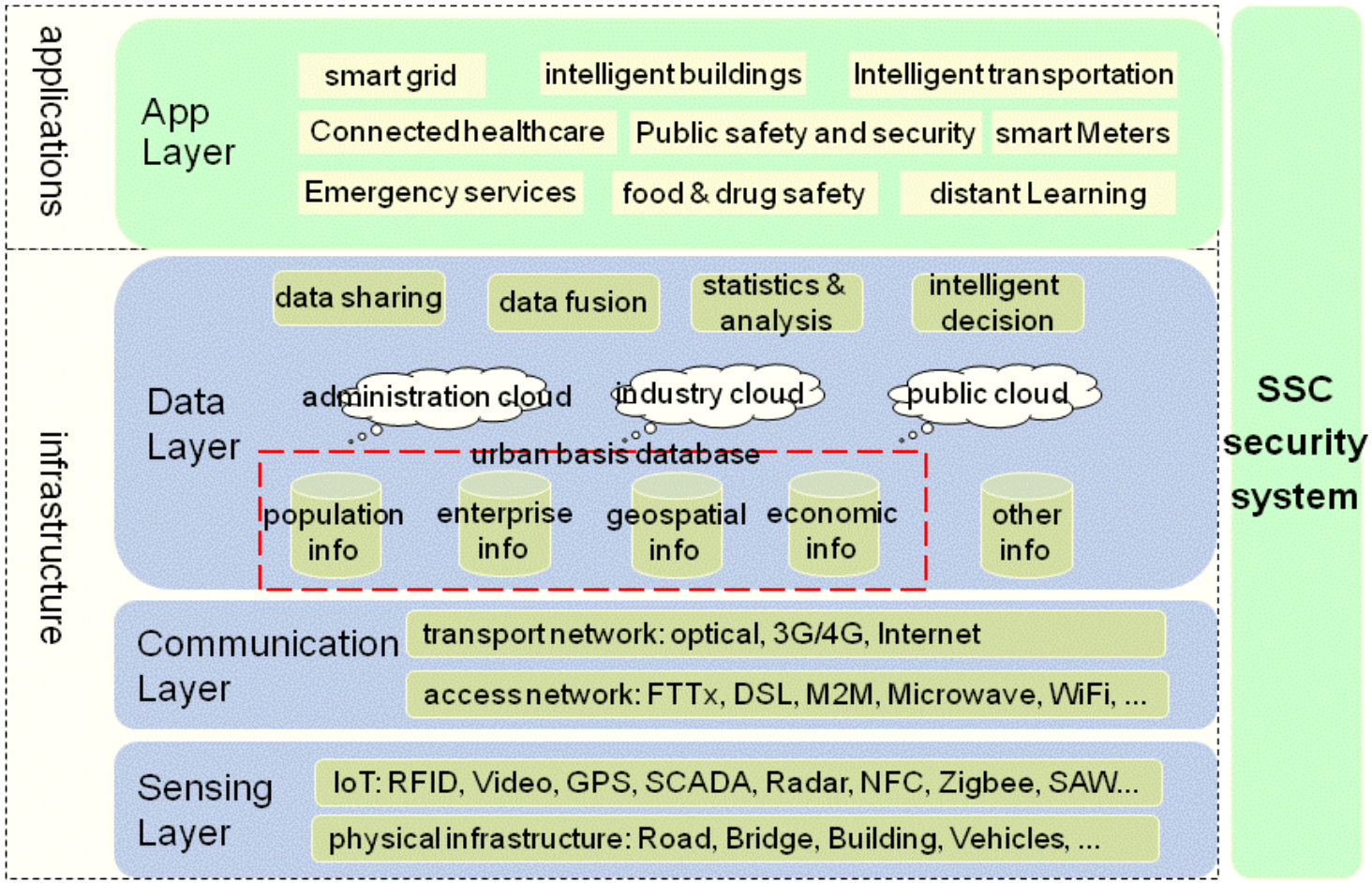
b. Cyber –security

- This concept refers to the discipline of ensuring that ICT systems are protected by attacks and incidents, whether malicious or accidental, threatening the integrity of data, their availability or confidentiality, including attempts to illegally 'exfiltrate' sensitive data or information out of the boundaries of an organisation.

c. Data protection

- This notion refers to the tools and processes used to store data relevant to a certain ICT system or environment, as well as recover lost data in case of an incident - be it fraudulent, accidental or caused by a natural disaster.

Layered view, and architecture…

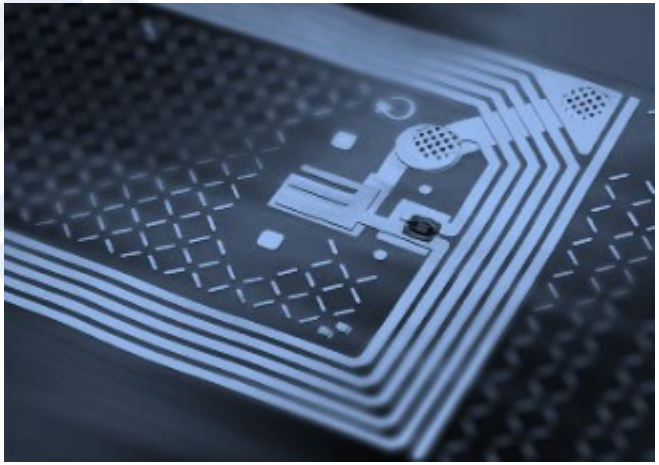


Smart grids and energy efficiency

- Cities consume between 60 and 80% of world's energy
- Smart Grid, smart metering with IP address and sensors allow monitoring and adjust generation and delivery based on consumption models
- Reduce cost and environmental impact

Intelligent transportation

- Real-time traffic flow information
- Telco, Global Positioning Systems (GPS)
- M2M communication, Wi-Fi and RFID technologies
- Data analytics and prediction techniques



Connected Healthcare

- Secure collaborative access for authorised medical services, to Electronic Patient Records, in a way, at any time, from anywhere, from any accredited device
- Telemedicine solutions for remote areas or in case of natural disaster
- Ageing population: assisted living and monitoring service for independence at home
- All require privacy, identification and cyber security

Public safety and security

- Protecting against crime, natural disasters, accidents or terrorism.
- Tele-surveillance systems to help emergency services
- First respondents to benefit from secure connectivity
- Secure data access and sharing

Wireless communications & hotspots

- Increasingly popular service, with increasing vulnerability
- Unsecure access to sensitive and personal data (online banking, social network, etc.)
- Younger population particularly exposed
- Cyber-crime increasingly active in these environments

Technologies involved & vulnerabilities

- Network Infrastructure
- Cloud Computing (availability, security)
- Internet of Things (sensors, RFID, M2M, Standards…)
- Data and Big Data (embed security with data, confidentiality, integrity, authentication, availability)
- Legislation increasingly prescriptive, nationally and EU

Ensuring continuity of critical services

- City governance to ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy
- Technology to enable policy
- City CIOs increasingly part of strategic policy discussions
- Systems/IoT, need to be standardised, interoperable and open, but also secure
- Cyber-security and resilience to be embedded from inception
- Cyber-security + backup and recovery systems for mission-critical administration data (& Big Data)
- Legislation increasingly prescriptive, nationally and EU

Recommendations (1)

- Establish Governance - Identify and organise key stakeholders
- Governance, Risk and Compliance (GRC) - Fulfil through policies and processes, enabled by ad hoc IT suites: stay compliant and mitigate risks
- Service continuity - Solutions and methodologies on Cyber-security, backup, data loss prevention, archiving and disaster recovery.
- Protect information proactively
- Information-centric approach
- Embed security within data
- Utilise encryption
- Authenticate users with Strong Authentication
- This also prevents from accidental disclosing of credentials and from attaching unauthorised devices to the infrastructure.

Recommendations (2)

- Threat intelligence - In order to understand the major trends in terms of potential attackers, through analysing trends on malware, security threats, and vulnerabilities
- Managed security services - Outsourcing security services to providers. The ICT leadership can in that way focus on their functional duties of running the city systems
- Rely on their national Computer Emergency Response Teams (CERT), in order to be aligned with national coordination on cyber-incidents and security, and benefit from the international visibility this provides these entities provide.
- Protect the infrastructure by securing endpoints, messaging and web environments.
- Ensure 24x7 availability of the critical infrastructure
- Develop an information management strategy

Links & Additional Information

- ITU-T and Climate Change
  itu.int/ITU-T/climatechange
- ITU Focus Group on Smart Sustainable Cities
  itu.int/en/ITU-T/focusgroups/ssc/
- ITU Symposia & Events on ICTs and Climate Change
  itu.int/ITU-T/worksem/climatechange

Thank you

- tsbfgssc@itu.int
- giampiero_nanni@symantec.com