ROKE

Cyber resilience and the UK's evolving Smart City ecosystem

Exploring the potential for cyber-attacks to generate systemic risk to the UK's evolving smart cities

ROKE

1 INTRODUCTION

This paper explores the potential for cyber-attacks to generate systemic risk to the UK as our cities evolve into smart cities.

By 2050, about 68% of the world's population is expected to live in cities. The inherent interconnectivity and transparency of smart cities make them highly vulnerable to security attacks. Roke would naturally advocate that Cybersecurity or to be more precise Cyber Resilience be designed in from the start for all smart city initiatives.

Cities in the UK and indeed across the developed world are rapidly adopting IoT and related low power communications and AL/ML technologies to transform themselves into Smart Cities. There are significant socio economic drivers ensuring this transformation is occurring rapidly. The complex evolving system of systems that are in the process of being built today are bringing with them rapidly growing threat surfaces and associated vulnerabilities.

However finding and funding the cyber security expertise to provide the cyber resilience in this context is challenging given the growing skills shortages relative to the growing scale and complexity of the task. A 2018 UK government sponsored study found that that more than half of all businesses and charities (54%) have a basic technical cyber security skills gap, falling to 18% in public sector organisations. Smart cities typically involve a mixture of public and private partnerships, so this is a significant systemic risk in itself.

This white paper is designed to help our customers gain insights into the potential smart city cyber chain reactions that can be exploited by threat actors to attack not just components of a smart city, but potentially the entire smart city ecosystem to generate a systemic risk to the UK economy.

The goal of this paper is to help inform cyber security experts on the systemic cyber security risks associated with Smart Cities and federated Smart city eco-systems. Roke can also help our customers develop operational services associated with providing cyber resilience to smart cities.

Smart Cities are a growing multi-billion £ market and are related to aspects of UK CNI such as Energy, Transport, Public Safety and Surveillance. The opportunities here are international including with Roke target markets such as the US. One of the innovation proposals in this paper is the concept of the 'Cyber Twining' of cities to share cyber expertise and threat intelligence.

2 SMART CITIES: THE CONCEPT

In very broad terms the concept of a smart city is designed to improve the provision and development of urban services through the use of digital technology. This covers aspects such as public safety, mobility, governance and health. As shown by the simplistic Roke model in Figure 1 our concept of a smart city spans both the socio technical domains and the physical infrastructure domains that comprise that city.

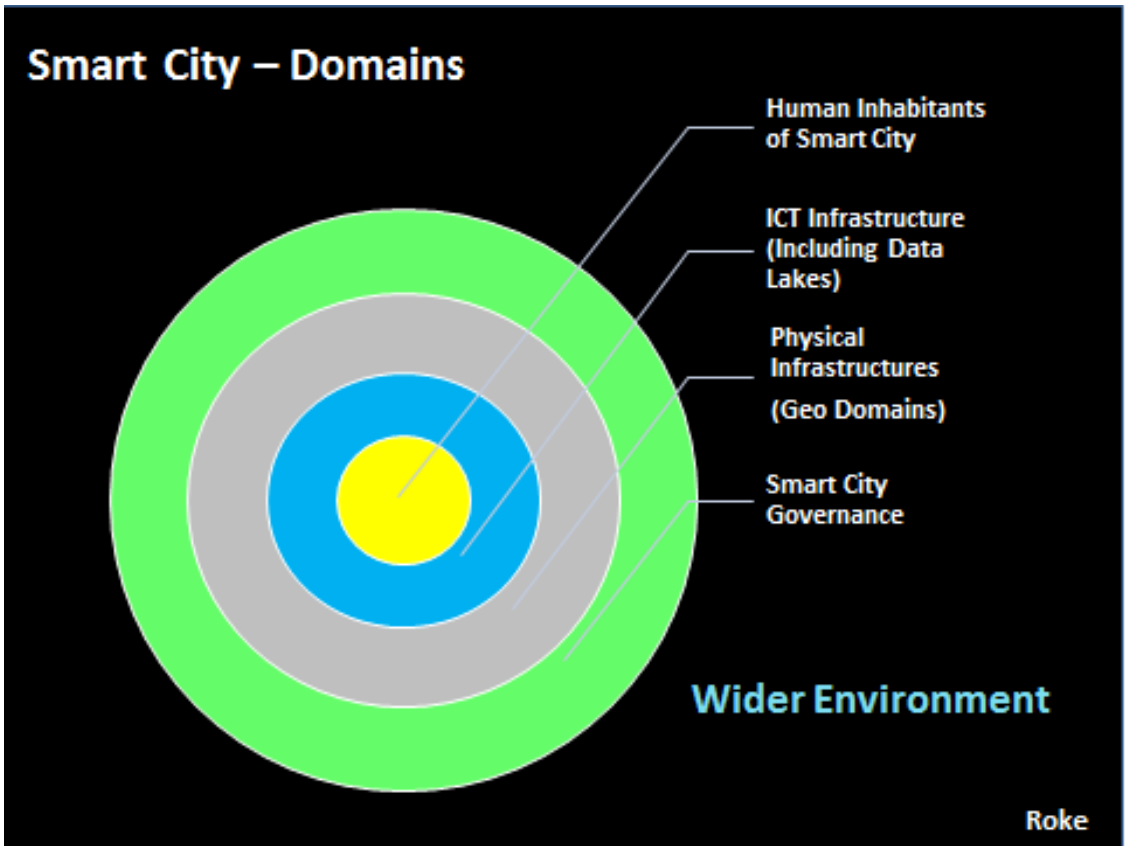


Figure 1 – The basic domains of the Roke smart city model

The Roke model places the Human inhabitants at the very heart of the smart city concept as it is designed to transform the lives of the city's population through improved socio technical services. In our model we are looking at a portfolio of smart city services including those aimed at human socio services such as smart real time health monitoring and psychological support as well as improved IT and kinetic services such as smart mobility.

The Human interaction with the smart city is through the ICT infrastructure domain comprising the many diverse forms of sensors, devices and communications networks that form the IoT saturating the geo physical domains over which the city is spread.

The smart city's IoT include kinetic physical devices such as autonomous vehicles. The huge typically cloud based data lakes, associated with the cities IoT are also a part of this ICT infrastructure layer.

The smart city ICT infrastructure is typically modelled logically in terms of edge components (devices, sensors), a core (cloud or IoT platform) and communication networks connecting the edge devices to the core platform.

The physical infrastructure in our model is comprised of the static physical structures such as roads, buildings and cable ducts that span the geo domains of a given city.

The smart city Governance layer in our model is comprised of a combination of public and private organisations working together within a coherent framework to provide the strategic socio-economic, cyber security and technical direction as well the day to day secure operations of the smart city.

We should highlight here the challenges associated with creating a coherent smart city governance framework. Although it sounds simple in principle in practice it is very difficult to move from the historic silo model of vertical sectors to a coherent integrated model of the smart cities where verticals such as energy and mobility and environment operate in real time together to optimise their efficiency in a truly smart way.

There are also significant challenges in operating public private partnerships in a smart way to ensure the diverse vested interests work together for the common good of the city's human population. Finally the smart city governance layer faces challenges in managing the data lakes of the smart city and the benefits they can bring whilst also complying with the regulatory regimes they fall under especially data protection laws such as GDPR.

The G20 Global Smart Cities Alliance on Technology Governance (Ref 1) unites municipal, regional and national governments, private-sector partners and cities' residents around a shared set of principles for the responsible and ethical use of smart city technologies. The Alliance establishes and advances global policy standards to help accelerate best practices, mitigate potential risks, and foster greater openness and public trust.

The typical features of a smart city may include: sensors which dim public lighting if there is no one around; IoT fleet management of automated waste collection; weather monitoring (including e.g. flood or storm damage risk). The intelligent / smart delivery of water, electricity and other vital supplies are the most central tenets of many of today's smart city projects.

In an article on Smart Cities by Dorota Sikora-Fernandez and Danuta Stawaszat University of Lodz (Ref 4) they state that cities can be defined as smart if they have the following dimensions:

1. **Smart economy** - cities should have high productivity based on the use and combination of means of production using knowledge, the climate of innovation and flexible labour market; economy should be characterised by the utilisation of innovative solutions and flexible adaptation to changing circumstances. In this sense, the term is also related to "smart" ICT industries, as well as to business and technological zones.

2. **Smart mobility** - owing to the ICT sector, a city becomes a huge network of connection between all of its resources. Both traditional transport and digital communication should be based on advanced technologies needed for the rational utilisation of existing infrastructure.

3. **Smart environment** - a smart city optimises its energy consumption by using renewable energy sources and other means, strives to minimise waste emissions and bases its waste management policies on the principles of sustainable development. Environmental activities also require a high level of environmental education.

4. **Smart people** - a learning society. All changes in the city should be initiated by the inhabitants who, when provided with appropriate technical support, are able to prevent excessive energy consumption and pollution, and try to improve their quality of life.

5. **Smart living** - friendly environment, especially by the provision of wide access to public services, technical and social infrastructure, high level of security, an expansive cultural and entertainment offer, as well as proper care for the environment and greenery.

6. **Smart governance** - development in this regard requires the formation of a proper governance system, the development of procedures that require the cooperation of local authorities and other users of the city, and the use of new technologies in running the city.

As we have started earlier the achievement of these smart services requires a coherent cross sector integrated framework.

Many of the early Smart City initiatives have taken a silo vertical sector approach treating verticals e.g. like urban, transport, energy, water and waste supplies as separate independent domains. Smart Cities need however to have an integrated approach to generate value. The EU has recently identified (Ref 2) the following common features associated with high value-added integrated Smart Cities & Communities (SCC) solutions:

- **Data-driven transformation:**
    - An aspect common to most integrated solutions is the emergence of data centres and, more generally, they use of data to steer integrated solutions, personalise services and manage the solution. Data enables both the creation and provision of entirely new Smart City services, and the integration of siloes across city government structures.

- **A fast-growing "sensor environment" across cities:**
    - Most of the SCC solutions mapped share the common feature of an increasing number of sensors being deployed. Although it is only in a limited number of cases that these devices are collecting personal information, there is still a missing overall regulatory framework in place to govern them. As a fundamental part of a Smart City's

Internet of Things infrastructure, these sensors should be subject to city guidelines on the type of data they collect and how this is used.

- **Open standards**
    - To avoid vendor lock-in and enable the procurement of the best technologies available, many cities employ open standards both on the technological and on the business level.

To this we add the coherent Governance layer that we introduced earlier in our Roke model. Smart Cities evolve along with new modes of value creation through the intermediation of public-private partnerships, cross-sectorial collaboration, city-led "open innovation marketplaces" and other forms of governance.

3 THE CURRENT STATE OF SMART CITIES TODAY (2019)

In this section of our white paper we summarise the current state of smart cities as we approach the start of the 2020's. We focus on the UK Smart city eco-system but begin by putting it in context of the worlds most advanced smart cities.

3.1 THE MOST ADVANCED SMART CITIES IN THE WORLD TODAY (2019)

Forbes in 2019 views Singapore as the top city for technology (placing first on this dimension), as well as occupying position 4 in international outreach. In Singapore, everything revolves around technology: it has a fibre optic network the length and width of the island and up to three mobiles for every two residents, and it has robot hospitals (with human staff and robots), autonomous taxis (with no driver), and vertical gardens and farms that regulate the temperature by absorbing and dispersing heat while collecting rainwater.

If we look where the investment is China is where we should look. China is developing 500 smart cities – almost half of the world's total and more than 10 times that of the United States. The smart cities in the United States that are getting the most investment are New York, Los Angeles, Washington, D.C., and Chicago.

5G significantly improves the functioning of smart cities by providing fast data transfer speeds, low latency, and better connectivity for smart devices. The roll out of 5G is therefore of great significance in the Smart City context and again it is China that is in the lead in terms of roll out and patents, way ahead of the United States and Europe. This is complicated in the UK case by the high profile security concerns currently surrounding the use of Chinese 5G suppliers such as Huawei in UK 5G networks.

China has named Wuzhen the country's first '5G town' which has which boasts super-fast internet connection pervasively. The 5G network in Wuzhen was launched jointly by Huawei and state-run provider China Telecom.

3.2 CURRENT STATE (2019) OF THE UK SMART CITY ECOSYSTEM

Bristol was chosen as Britain's smartest city in the UK Smart Cities Index, published by Huawei and Navigant Consulting in October 2017, based on its pioneering approach to open data, energy innovation and community engagement.

Key initiatives include a high-speed fibre optic network that connects smart traffic lights and police and emergency services to improve response times and safety. The city's big data is available on a free, open-data website and analysed and visualised on a giant screen in a converted planetarium. A commitment to cut emissions by 40% by 2040 led the council to set up its own energy company and pump significant investment into renewable power. And "citizen sensing" projects have highlighted the benefits and drawbacks of data and sparked the development of new apps.

Bristol's powerful data capability is underpinned by a fibre optic test network that functions as a springboard for IoT sensors mounted on 2,400 smart street lamps and a city-wide wireless zone.

Bristol's Smart City Operations Centre connects with the council's Emergency Control Centre, Traffic Control Centre and Community Safety Control rooms, plus services for telecare, alarm and security monitoring and lone-worker support.

3.3 GROWTH OF IoT ONE OF THE DRIVERS OF SMART CITY EVOLUTION

Gartner, Inc. forecasts that the enterprise and automotive Internet of Things (IoT) market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019. By the end of 2019, 4.8 billion endpoints are expected to be in use, up 21.5% from 2018.

Utilities will be the highest user of IoT endpoints, totalling 1.17 billion endpoints in 2019, and increasing 17% in 2020 to reach 1.37 billion endpoints. Electricity smart metering, both residential and commercial will boost the adoption of IoT among utilities, according to the Gartner report. They also state that, physical security, where building intruder detection and indoor surveillance use cases will drive volume, will be the second largest user of IoT endpoints in 2020.

Building automation, driven by connected lighting devices, will be the segment with the largest growth rate in 2020 (42%), and followed by automotive and healthcare, which are forecast to grow 31% and 29% in 2020, respectively.

In healthcare, chronic condition monitoring will drive the most IoT endpoints, while in automotive, cars with embedded IoT connectivity will be supplemented by a range of add-on devices to accomplish specific tasks, such as fleet management.

4 SMART CITY REFERENCE ARCHITECTURES

Smart Cities are evolving and in order to build in cyber resilience we need to consider how the associated cyber threat landscape is likely to change over time. To explore this we introduce a simple Roke Manor Research Ltd conceptual model of a Smart City as shown below in Figure 3

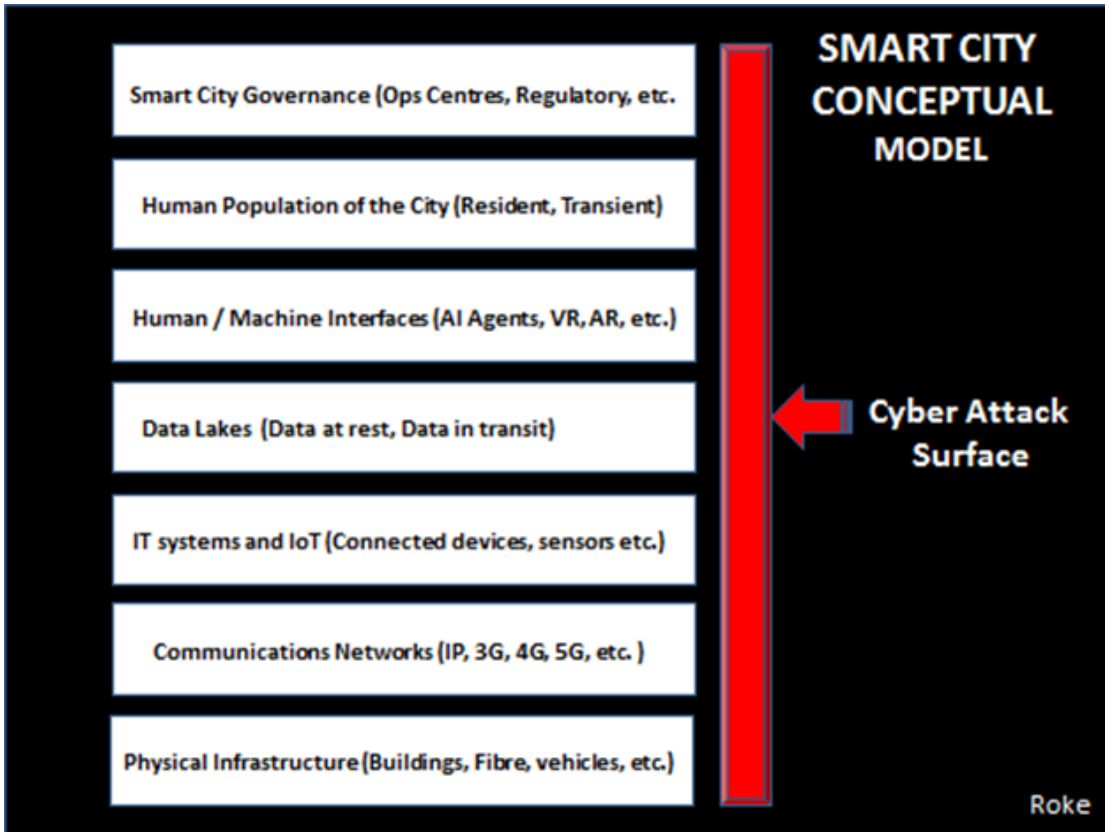


Figure 3 – A Conceptual Model of a Smart City © Roke Manor Research Ltd

The different layers of this conceptual model span the physical, technical and socio domains that comprise any Smart City eco-system. As is highlighted in Figure 3 the Cyber Attack surface also spans across all of these layers.

If we look at the communications layer we can highlight the way in which dynamic slices of the 5G network can be used to underpin many of the smart city services. For example through:

- An enhanced mobile broadband slice with high data rates, high security, and high
  mobility for sporting events, customer data, payments, and fleet management

- A massive IoT slice with high scalability and big data sets for street lights, traffic
  management, smart meters, and water/waste management

- A mission-critical services slice with high reliability, low latency, and high security for
  first responders, autonomous emergency vehicles, and emergency healthcare

- A private smart factory slice with high reliability, low latency, high security and high
  data rates for automated production.

However in the short term there are also other communication services in smart cities that currently compliment the evolving 5G communications infrastructure. A prime example of this is LoRaWAN.

This technology shares some of the strengths of 5G in that it leverages an open standard and a thriving global ecosystem, managed by the LoRa Alliance®.

In contrast to 5G, LoRaWAN is a relatively simple networking protocol that has been designed from the ground up to serve distinct use cases. The prototypical use case for LoRaWAN is a battery-operated device that transmits several bytes of data at intervals of 15 minutes to an hour, and needs to last in the field for 10+ years without wires.

The communication range can easily reach more than 10km, which is much longer than Bluetooth®, Wi-Fi, and millimetre wave 5G. LoRaWAN is not the right choice for applications that require streaming of video or voice calls, nor is it optimal for ultra-low latency applications. However, it is the optimal choice for what it was specifically designed to do and it accomplishes this efficiently and cost-effectively.

LoRaWAN serves a well-defined technological use case which can be utilized by many applications. Some of the most obvious applications are water, gas metering and smart parking where devices must be battery-operated, low cost, and last in the field for 10+ years.

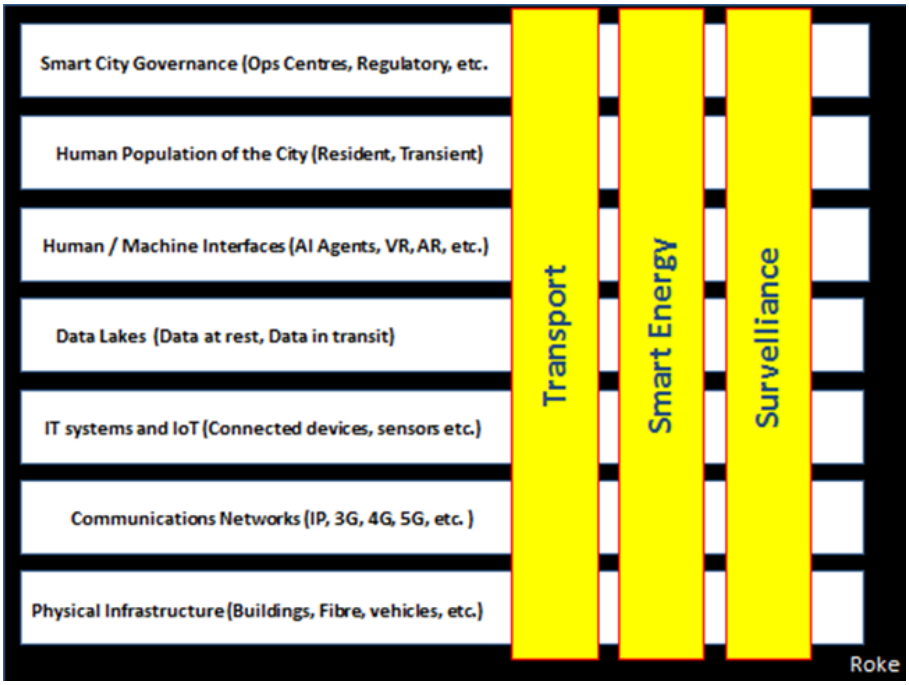


Figure 4 – Smart City Conceptual Model – including examples of vertical domains

The key point to note here is the hybrid and complex nature of the communications layer of the Smart City framework. This complexity is typical of each of the layers shown in Figure 4. From the perspective of cyber security this complexity leads intrinsically to increased vulnerability.
There is a reference architecture for smart cities that has been produced by the EU known as FIWARE.

The FIWARE Foundation is targeted to boost creation of an ecosystem around the FIWARE platform, which provides a simple yet powerful set of Application Programming Interfaces (APIs) that ease the development of smart applications in multiple vertical sectors. FIWARE API specifications are public and royalty-free.

Supported by an open source implementation, this enables multiple FIWARE providers to emerge more quickly in the market with a low-cost proposition. The FIWARE context management API has been adopted by more than 75 cities to support real-time open data.

The FIWARE Foundation aims at contributing to the definition of an open-source reference architectural framework for smart cities that it can then help implement and promote.

This is shown below in Figure 5.

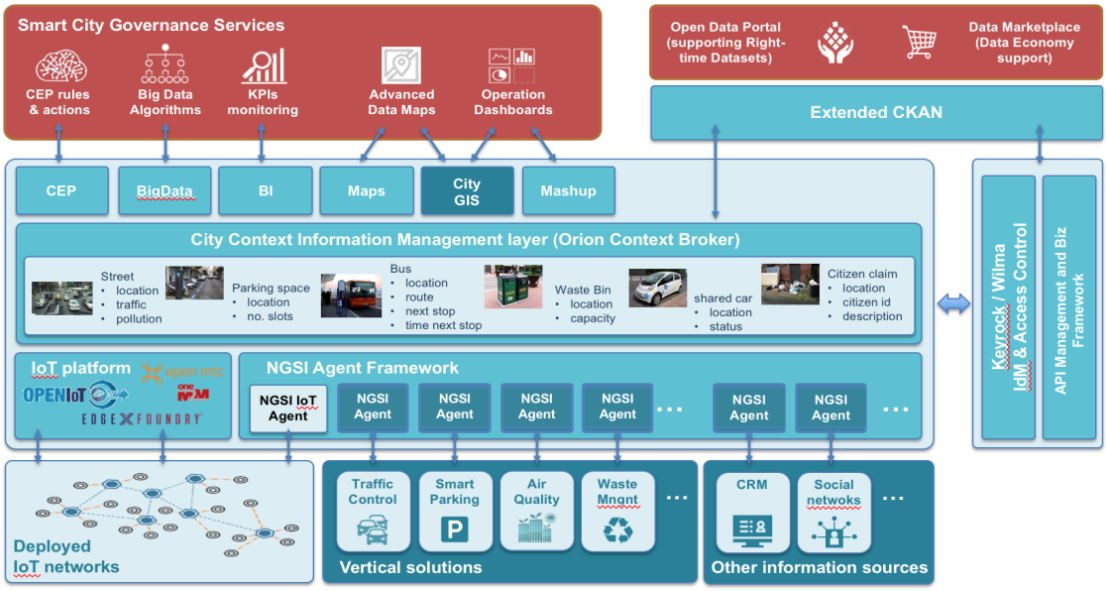


Figure 5 – The FIWARE the EU's Smart City Reference Architecture

The cornerstone component in the proposed Reference Architecture is a FIWARE-compliant Context Broker component. This component supports interfaces:

- Southbound: to IoT networks and different vertical smart city services management solutions deployed by the city, as well as to other information sources such as the city's CRM (Citizen Relationship Management) systems or social networks (Twitter, Facebook, …), thus gathering valuable context information from them. These systems may, in turn, also consume context

information published by the Context Broker in order to trigger different actuations.

- Northbound: providing context information to smart city governance systems. These systems may, in turn, enrich context information through this interface (e.g., making insights derived from big data analysis available as context information).

- Eastbound: to other cities and third parties for the exchange of context information.

Context information managed through the Context Broker provides a holistic picture of what is going on in the city at any time. The Context Broker exports the FIWARE Next Generation Service Interface (NGSI) v2 API through all these interfaces, enabling it to gather updates on, or get access to, context information in real-time. This API is experiencing a growing adoption.

Multiple implementations of the Context Broker component can exist as far as they provide an API that is in compliance with the public and royalty-free FIWARE NGSIv2 API specifications. The FIWARE Community has developed and evolves an open-source reference implementation of the Context Broker named Orion.

Multiple products can be plugged and played together with the Context Broker component in a smart city reference architecture powered by FIWARE. They interface with the Context Broker using the FIWARE NGSI API.

Members of the FIWARE Open Source Community contribute open-source platform products implementing several functions (big data analysis, complex event processing, business intelligence analytics, etc.) that come with modules enabling an easy integration with any FIWARE-compliant Context Broker product. Some of them rely on well-known open source platform products (e.g., Hadoop, Spark, etc.).

These platform products are then considered FIWARE Generic Enablers supported by the FIWARE Community. Connection to the IoT can be implemented through FIWARE Generic Enablers provided by the FIWARE Community or by using alternative IoT platforms for which modules implementing integration through FIWARE NGSI are available.

The FIWARE Community has developed FIWARE Generic Enablers enabling enforcement of policies for controlling access to context data resources through the FIWARE NGSI API.

Extensions to CKAN (one of the most widely used open-data publication platforms) have also been developed to bring support to the publication of real-time context information resources and related access control policies, thus enabling the transition from

Open Data to real-time Open Data. Additional CKAN extensions, combined with FIWARE Generic Enablers supporting accounting and rating of FIWARE NGSI API calls, enable the monetization of city context data, enabling the transformation of cities into platforms for the data economy.

ROKE

5 SOCIO CYBER VULNERABILITIES OF SOCIO-TECHNICAL SMART CITIES

As we stated earlier in this paper the human inhabitants are at the very heart of our Roke smart city conceptual model. So what do Humans need in this context? We adopt Maslow's hierarchy of needs, which is a motivational theory in psychology comprising a five-tier model of human needs, often depicted as hierarchical levels within a pyramid. Needs lower down in the hierarchy must be satisfied before individuals can attend to needs higher up.

Figure 6 - Maslow's hierarchy

In essence then as well as addressing smart infrastructure services we need to consider these aspects if we claim to be genuinely providing human centric smart services. A recent paper (Ref 8) introduces the concept of People-Centric Service Intelligence for Smart Cities.

People-centric service intelligence in smart cities has to support the realization of people's needs within urban and social domains, for example, physiological, safety, love/belonging, esteem, and self-actualization needs according to Maslow's theory.

A smart city provides critical resource services (i.e., environments, techniques, and infrastructure) to people, while society supports the mental needs of interaction, ethic, and culture. Both of them need to be designed and constructed with an appropriate level of service intelligence suitable to developed or developing cities.

However there is always the dark side to consider and there is a risk that smart cities will be designed more to control than to serve their human populations.

Mass surveillance through big data acts in a manner that reduces urban anonymity,[due to the breadth of information and potential uses which can be extrapolated when multiple data streams are analysed together by a single governmental entity. Advocates of smart cities (such as Vince Cerf) state that this is akin to the level of privacy experienced in small towns.

In contrast, critics state that information sharing in smart cities has shifted from horizontal information flows between citizens to a vertical, unilateral process between citizen and government, reflecting concerns about panopticism.

The Panopticon, an architectural design put forth by Jeremy Bentham in the mid-19th Century for prisons, insane asylums, schools, hospitals, and factories. The Panopticon offered a powerful and sophisticated internalized coercion, which was achieved through the constant observation of prisoners, each separated from the other, allowing no interaction, no communication. This modern structure would allow guards to continually see inside each cell from their vantage point in a high central tower, unseen by the prisoners. Constant observation acted as a control mechanism; a consciousness of constant surveillance is internalized.

Whereas the panopticon is the model for external surveillance, panopticism is a term introduced by French philosopher Michel Foucault to indicate a kind of internal surveillance. In panopticism, the watcher ceases to be external to the watched. Rather than external actions, the gaze of the watcher is internalized to such an extent that each prisoner (economic agent/worker) becomes his/her own guard.

For Foucault, the real danger was not necessarily that individuals are repressed by the social order but that they are "carefully fabricated in it" (Foucault, 1977), and because there is a penetration of power into the behaviour of individuals.

So the risk here is that smart surveillance can be used in a smart city context for socio political engineering and control of target populations. However the nuance here is best illustrated by the case of pervasive social media enhancing the more obvious role of CCTV surveillance.

Social media is a good example of a system that enforces panopticism, since it is a context where each individual chooses carefully what to say on a social media site and what to visit in fear of suffering consequences. We emphasise this since it is also in my view an interesting and potentially very powerful vulnerability for state actors launching PsyOps against population clusters target states.

There are however two types of risk associated with panopticism

- The inherent risk associated with emergent socio psychological behaviours in a dense cyber hive type smart city environment. Complex system of systems produce emergent behaviours that cannot be predicted, some of these may be constructive other destructive, e.g. flash mob type events. The governance layer is not really in control of this rapidly evolving complex system of system, even though it might think it is. Even new benign services introduced in this complex context may lead to encounters with the law of unintended consequences.

- The cyber PsyOps risk associated with hostile threat actors especially those controlled by nation state threat source. This is similar to the current risk of socio political, religious and other fault lines in a countries population being manipulated through e.g. social media channels to create civil unrest and socio economic instability. However in the smart city context this risk is

increased in magnitude by the increased depth, speed and dependency on cyber based human interaction in the smart city context.

In some countries the vertical control of their populations will be more of a concern. In a smart city context where real time monitoring of location, what you watch, facial expression and soon even real time biometrics like blood pressure and mood, the vertical governance layer to human population panopticon will be a key factor in determining the physiological behaviours of the smart city population. You might want to ensure your smart city population is safe, and also you may way want to enforce politically correct behaviours. Leaving aside the inherent Orwellian concerns, there is also a cyber risk here associated with threat actors exploiting such vertical panopticon control channels.

China's implementation of their social credit system shows how AI and ML can be deployed in just such a panopticon controlling vertical mode. Using facial recognition technology to identify individual citizens, their system will be able to identify behaviours such as not paying for train or bus tickets, jaywalking, speaking rudely, or causing a commotion.

Rule violations would result in points being subtracted from a citizen's social credit score. Initially, each government department and city agency will have their own social credit system — the parking authority will dock credit points for a parking violation, while the transit system will dock points for an infraction on public transportation.

But China's goal is to join these systems to a Universal Social Credit System — where violations in one area could result in loss of opportunity in society in another area. If you don't bag your trash correctly or pay your taxes on time, you could lose work or educational opportunities, travel rights, or vacation time. The implications are frightening.

The role of AI and ML needs to be considered here in order to understand the associated cyber risk to the socio eco-system of a smart city. Ai and ML systems in the smart city governance layer operating on the real time data lakes enable not only for autonomous monitoring of the human population in real time but to make decisions based on how each of these elements behave, how behaviours change over the course of each day or over time, and how elements are responding to city systems.

In short, AI will understand how cities are being used and how they are functioning and could assist city planners in understanding how the city is responding to various changes and initiatives.

there is a definite dark side to the potential for AI in urban planning — and that is the prospect of using AI monitoring of residents to control behavior through fear of punishment.

6 SMART CITY EVOLUTION – THE CYBER VULNERABILITIES

If we look at the EU's Smart City Reference Architecture that we introduced earlier in section 4 (Figure 5) there is more a focus on smart city core services, business intelligence and surveillance as distinct to the People-centric service intelligence of the Roke model.

From a cyber-security perspective the attack surface associated with the Human / socio domain is not really considered. We have however explored these socio PsyOps vulnerabilities in section 4. So here we shall focus on the technical framework.

As smart cities evolve they will go through a number of distinct phases as they incorporate the new enabling technologies such as 5G. Cities taking the smart city route often need to integrate new technologies with legacy systems. This kind of integration creates significant challenges. Most legacy systems don't allow for live updates or data encryption.

Merging disparate technology platforms can create "holes" in the security perimeter. That's how actors attacked a wastewater treatment plants in Australia. The attackers discovered vulnerability, and used it to disrupt the Supervisory Control and Data Acquisition system (SCADA).

In the next section (6.1) we will explore some of the vulnerabilities associated with the smart city deployed IoT networks and platforms and the associated low power communication networks. In subsequent section (6.2) we will highlight the associated cyber vulnerabilities in the smart city 5G infrastructure.

In the subsequent section (6.3) we will then explore vulnerabilities associated with the context broker of the EU FIWARE framework. In particular we will look at the EU FIWARE framework in the context of a federation of EU smart cities (i.e. the Synchronicity initiative) and explore the cyber vulnerabilities that exposes in federated trust in the governance layer.

Finally in section (6.4) explore the vulnerabilities associated with the AI and ML algorithms and their potential systemic impact.

6.1 BASIC CYBER VULNERABILITIES OF THE CURRENT STATE

Industrial Internet of Things (IIoT) made up of industrial control systems (ICS) are at the heart of our Smart Cities. As we showed earlier in section 3.3 the IoT is growing rapidly across smart city sectors. The IIoT controls critical infrastructure such as smart transport systems, smart energy grids and CCTV surveillance networks, The ICS comprising the IIoT of a smart city can range from the smallest sensors to large scale industrial equipment.

It is well known that IoT devices have significant cyber security vulnerabilities typically associated with risk cost balance working against security in many low end commodity markets and long lasting legacy embedded physical end points. So given their role in our rapidly evolving smart cities there are obvious concerns. We will

highlight here recent significant vulnerabilities of particular relevance to core smart city services including dependent on IoT and 5G.

Let us consider VxWorks a simple operating system that has a big footprint in the IIoT. VxWorks is designed as a secure, "real-time" operating system (RTOS) for continuously functioning devices, like medical equipment, elevator controllers, or satellite modems.

The research form Armis Labs (Ref 6) has found this year (2019) a cluster of 11 zero day vulnerabilities impacting VxWorks, six of which could give an attacker remote device access, and allow a worm to spread the malware to other VxWorks devices around the world. Roughly 200 million devices appear to be vulnerable; the bugs have been present in most versions of VxWorks going back to version 6.5, released in 2006.

Armis has maned these URGENT/11 i.e. the group of 11 zero day vulnerabilities they have so far discovered in the IPnet TCP/IP stack implemented by various RTOSs, and primarily by VxWorks, a widespread RTOS used by over 2 billion devices including critical devices, such as industrial, medical and enterprise.

The vulnerabilities impact IPnet versions from the last 16 years, and thus affect a wide range of devices. URGENT/11 is serious as it enables attackers to take over devices with no user interaction required, and even bypass perimeter security devices such as firewalls and NAT solutions. These devastating traits make these vulnerabilities ‘wormable,’ meaning they can be used to propagate malware into and within networks.

Such an attack has a severe potential, resembling that of the EternalBlue vulnerability, used to spread the WannaCry malware. For a Smart city designed to exploit its IIoT to provide the majority if not all its critical services this is a significant risk. It is also capable of spreading between cities creating the smart city equivalent of a malware pandemic.

The most common IIoT cyber vulnerability perception is that of massive DDoS botnets able to deliver huge attacks -- like Mirai -- from thousands of compromised IoT devices. However a new survey by Irdeto Global i.e. The Connected Industries Cybersecurity Survey (Ref 5) now shows that direct cyber-attacks against IIoT have already started and that DDoS is no longer the main concern.

The survey questioned 700 security decision makers across Connected Health, Connected Transport and Connected Manufacturing, and the IT and technology firms that manufacture devices. Data was gathered in March and April 2019 from China, Germany, Japan, the UK and the U.S. Eighty percent of these organizations experienced a cyber-attack against their IoT over the last 12 months. The highest rate was in the UK at 86% (three other regions had attacks against more than 80% of respondents), with Japan at the relatively low 60%.

We go down a level now and look at the cyber vulnerabilities associated with the low power networks associated with a smart city IIOT. We will start by introducing LoRa.

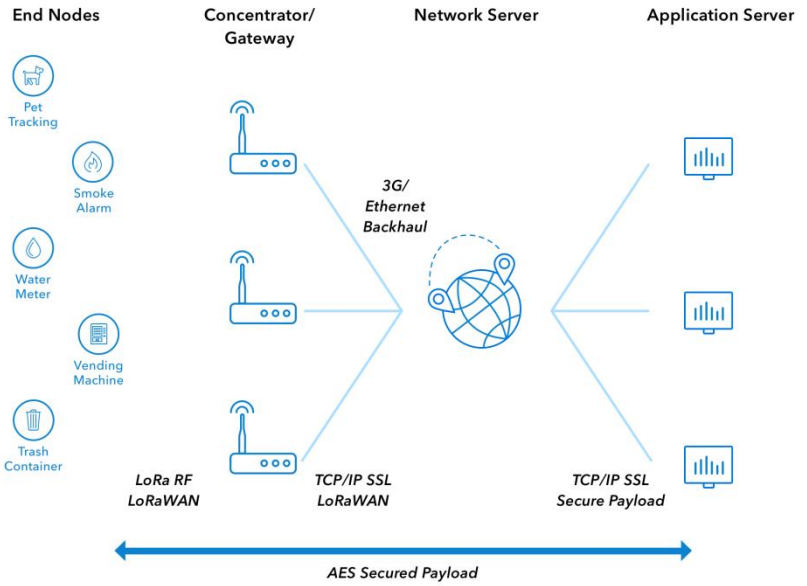


Figure 7 – LoRaWAN Architecture

LoRa short for long range (acronym overkill, but also a trademark) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology. LoRa (along with its upper layers definition—LoRaWAN) is one of the most promising Low Power Wide Area Network (LPWAN) technologies for implementing Internet of Things (IoT)-based applications.

It is becoming increasingly prevalent in smart cities in providing low power, low cost, and long-range radio communication. The vulnerabilities associated with the architecture shown in Figure 2 include end-device physical capture, rogue gateway and replay attacks.

Significant risks associated with the latest version (1.1) of LoRaWAN include:

- Device Cloning or Firmware Replacement (critical risk for authentication and access control, major risk for confidentiality and integrity and minor risk for availability)

- Self-Replay Attack (critical risk for availability and minor risk for the rest)

- Rogue End-Device Attack (critical risk for authentication and access control availability and minor risk for the rest)

LoRaWAN is used in smart cities for example in the context of enabling Smart Meters so the potential loss of availability would have a significant impact in this example on services such as smart energy management.

As we can see through illustrative examples there are already plenty of current cyber vulnerabilities in the IoT infrastructure layer of the smart city framework.

6.2 CYBER VULNERABILITIES IN FEDERATED SMART CITIES

In this section we explore the cyber vulnerabilities associated with the Federated Smart Cities Trust Model.

SynchroniCity (Ref 9) represents the first attempt to deliver a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones - 8 European cities & 3 more worldwide cities - connecting 34 partners from 11 countries over 4 continents.

It builds upon a mature European knowledge base derived from initiatives such as OASC, FIWARE, FIRE, EIP-SCC, and including partners with leading roles in standardization bodies, e.g. ITU, ETSI, IEEE, OMA, and IETF.

SynchroniCity is intended by the EU to deliver a harmonized ecosystem for IoT-enabled smart city solutions where IoT device manufacturers, system integrators and solution providers can innovate and openly compete.

We explore the EU SynchroniCity Federated Smart City Trust Framework from a cyber-security perspective.

In Figure 8 below we depict the basic context in which the federated trust framework operates.

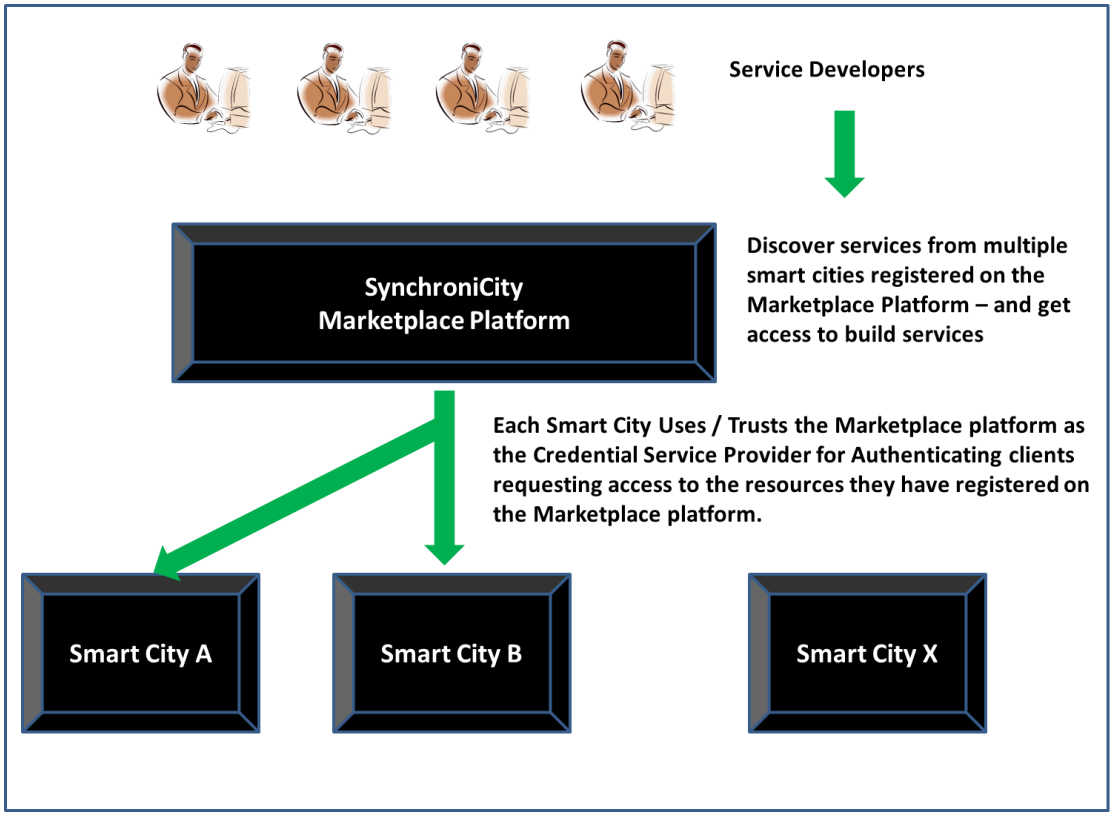


Figure 8 – The Basic Trust Model Context of the SynchroniCity Platform

As shown in Figure 8 the set of multiple smart cities are configured in a hub and spoke topology with the SynchroniCity Marketplace platform forming the hub. Each

Smart City has its own autonomous platform that features data resources and services. Each Smart City can selectively choose to register some of these resources on the Marketplace platform so they can be made available to (paying) external clients, shown here simply as service developers.

Rather than have each of the service developers registering their identity and roles multiple times i.e. once for each of the N Smart cities the model simply requires them to register once with the Identity Management service provided by the Marketplace Platform.

In order for this to work operationally this requires each Smart City to Trust the Marketplace platform to provide it with services for authenticating service developers requesting access to any of the resources it has registered on the Marketplace Platform. So how will they establish this Trust?

Trust amongst members of an identity federation is foundational to its operation and is established through a set of agreements and associated rules that are specific to that community. Such rules for a federated identity management arrangement are known as its trust framework.

As we know Trust frameworks serve as the basis for the multilateral agreements that enable the trust and governance of a federation's operations among all of the federation's members.

In our Federated Smart City context this has implications for the operation of the SynchroniCity Marketplace Platform in terms of the roles and responsibilities associated with administering the federation and acting as the Credential Service Provider.

In order to explore the Identity Management, Authentication and Authorisation flows in this context we need to go down a level of detail and introduce the key XACML architecture components. Applying this to the basic Trust Model Context of the SynchroniCity Platform that we introduced earlier in Figure 8 we arrive at the more detailed view shown in the following Figure 9.

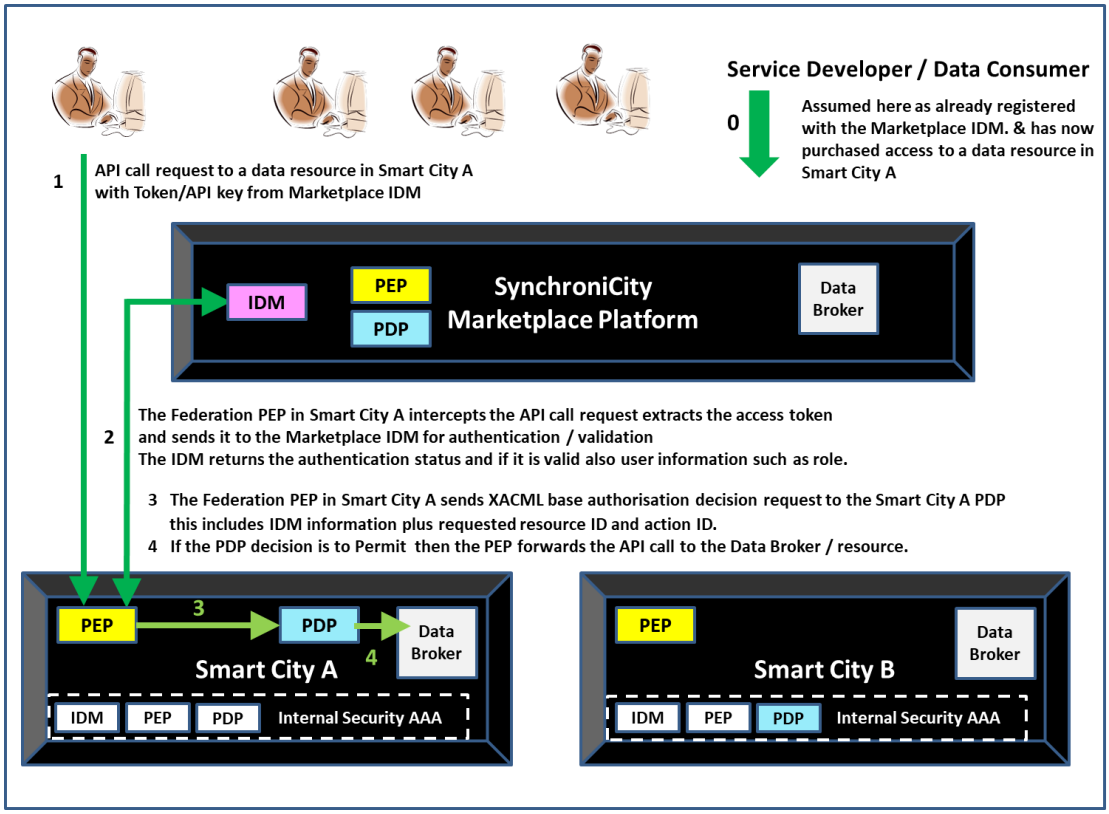


Figure 9 – Federated Trust Model Logical Architecture for accessing Data Resources.

A key feature of this model as shown in Figure 9 is that each Smart City augments its internal Security AAA components (IDM, PEP, PDP) with a dedicated PEP instance for intercepting all API calls from the SynchroniCity Marketplace Platform. These Smart City (Federated) PEPs are registered with and trust the SynchroniCity Marketplace Platform IDM for authentication services.

In exploring cyber security vulnerabilities we assume here in our analysis that each Smart City platform complies (at a vendor neutral logical level) with the EU FIWARE (that we introduced earlier in section 4 of this paper), which provides a complete Reference Architecture for Smart Cities

Below we illustrate a particular implementation of PEP, IDM and PDP using Wilma, KeyRock and AuthZForce respectively. However any vendor implementation can be used provided that they comply with the OATH2 flows that we have described.

Among the FIWARE GEs, the identity management GE relies on standard protocols, such as SAML and OAuth, to provide authentication and authorization features, which allows managing users' access to networks, services, and applications.

The IdM GE is also responsible for the user profile management, as well as SSO and identity federation across different service domains. Keyrock is an open source implementation of the IdM system defined in FIWARE. Keyrock relies on the OpenStack IdM implementation called Keystone.

The FIWARE PEP proxy GE is WILMA. Earlier in Figure 9 we showed the Authentication and Authorisation flows associated with a data consumer accessing a data resource, we show these again in the FIWARE GE context in Figure 10 below, as the flows 2, a, b, c.

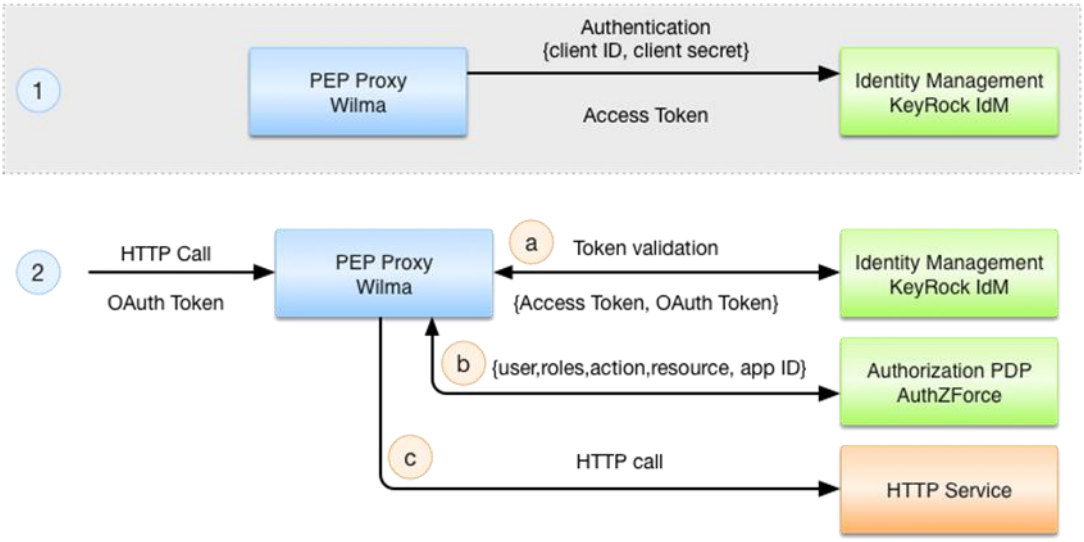


Figure 10 - High Level FIWARE System Architecture for accessing Data Resources.

The FIWARE Authorisation PDP in FIWARE is AuthZForce as is shown in Figure 10. We look next at the interaction between the Wilma PEP proxy and the KeyRock IDM i.e. flow a in Figure 3, so that we can explore Token Authentication in this context. After authentication, a client presents its access token with each HTTP request to gain access to protected resources. Validation of the access token is required to ensure that it was indeed issued by the trusted identity provider (IDM) and that it has not expired.

The OAuth 2.0 core specification (RFC 6749) does not specify a format for access tokens. However in the real world, there are two formats in common usage:

- JSON Web Token (JWT) as defined by RFC 7519
- Opaque tokens that are little more than a unique identifier for an authenticated client

So from our cyber security perspective we highlight here the fact that the OAuth Bearer tokens can be passed just like session cookies. You can pass an Opaque token around and you're good to go, it's not cryptographically bound to the user. Using JWTs helps because they can't be tampered with. However, in the end, a JWT is just a string of characters so they can easily be copied and used in an Authorization header!

However the real vulnerabilities in this federated trust model are in the governance layer. To see this consider first the fact that the Permission PolicySet we define in

the PDP of Smart City X associated with a role determines what the role holder can and cannot do with the data resources they are granted access to in Smart City X.

However the IDM responsible for registering users and associating them with roles is the Wilma IDM of the Marketplace Platform. As was shown in Figure 9 flow 2 the IDM sends authentication status and user information such role to the PEP, which send it on along with resource ID to the PDP for an authorisation decision (Flow 3).

This means that the definition of each Role in terms of its associated permission etc. needs to be agreed as part of the ongoing governance of the identity federation across the multi-Smart-City Trust framework. Initially this would be the responsibility of Federation Administrator to facilitate.

Roles will be associated with many different forms of Trust relationships across the federation. For example commercial trust associated with the payment for, use and protection of data from data sources. There will also be regulatory and legal relationships associated with each role, for example roles associated with Police or Emergency services may have permissions that give access to sensitive data including personal data in a Smart Cities.

This is an important consideration for the Marketplace Platform operators since in this model that organisation is responsible for registering Users and part of that is appropriate proof of identity relative to the roles being granted to those users.

As the IDM responsible for the authentication of these data consumers the Market Platform operating company is thus also accountable in terms of trust, commercial and legal consequences. All of these trusts, commercial and legal terms and conditions need to be defined as part of the governance layer of the Federated Trust Framework.

A consideration for trust framework legal rules is the allocation of risk and liability of federation members. Authentication transactions involve data exchanges between a user, a Relaying Party (RP) such as the PEP in our model, and a CSP.

There are then clearly cyber risks at the governance layer associated with the execution of these transactions and subsequent access authorizations that may present consequent risks to any of the parties involved. For example, the CSP may have erred in the enrolment information or credentialing of the user, users may be denied service due to a disruption in system services, or relying parties may have allowed unauthorized access to protected resources due to identity theft or fraud.

The result of any of these circumstances is that a federation member or user may feel that they have suffered a loss (e.g., financial, exposure of personal information, exposure of restricted resources).

In a federation of smart cities these risks could be systemic given the potential for state actor to exploit opportunities for unauthorised access to read and control the resources in the shared market place platform.

6.3 CYBER VULNERABILITIES IN SMART CITIES 5G INFRASTRUCTURE

5G networks in smart cities will underpin many new services such as:

- real-time augmented/virtual/mixed reality smart city experiences
- Autonomous vehicles, for smart delivery
- Surveillance drones
- Critical infrastructure operations: enhanced management and monitoring systems for traffic, energy and water facilities
- Real time emergency and healthcare services

5G brings with it significant cyber security vulnerabilities. It introduces smart services and infrastructure providing better visibility, efficiency and performance to smart cities. However in doing so it is making non-critical infrastructure critical to the populations of those smart cities.

We can illustrate this by observing that much of Huawei's commercial networking equipment is known to run the VxWorks RTOS whose significant cyber vulnerabilities we explored earlier in section 6.1 of this white paper.

As we know VxWorks is used for mission-critical systems for the enterprise, including SCADA, elevator, and industrial controllers, as well as healthcare equipment including patient monitors and MRI scanners. It is also used for networking equipment, including that often found at the perimeter of networks, such as firewalls, routers, and satellite modems, as well as VOIP phones and printers.

Huawei hardware contains third-party software VxWorks, including security-critical components that will cease long-term support in 2020, even though the Huawei products in question will be in service for much longer.

Security problems in mobile networks are nothing new, but the risk of attack is increasing. the distributed nature of 5G is a major risk.

Smart city networks are especially vulnerable to advanced persistent threats (APTs), which are complex attacks involving a combination of techniques. For example, an APT campaign can combine involve zero-day exploits and malware with multiple access points.

Researchers from Threatcare and IBM X-Force Red joined forces to test several smart-city devices that are widely deployed, with the specific goal of investigating “supervillain-level” attacks from afar. The research, presented at Black Hat and DEF CON 2018 (Ref 3) , delved into three categories of devices: Intelligent transportation systems, disaster management and industrial IoT.

Potential implications:

"Attackers could manipulate water level sensor responses to report flooding in an area where there is none — creating panic, evacuations and destabilization," Crowley said, adding that the same could be true for radiation monitors at nuclear power plants and similar critical infrastructure. "Conversely, attackers could silence flood sensors to prevent warning of an actual flood event [or other catastrophe], whether caused by natural means or in combination with the destruction of a dam or water reservoir."

Or, an attacker could control a few square blocks worth of remote traffic sensors, to create a gridlock effect as is often seen in the movies.

"Those gridlocks typically show up when criminals needed a few extra minutes to evade the cops or hope to send them on a wild goose chase," Crowley said. "Controlling additional systems could enable an attacker to set off a string of building alarms or trigger gunshot sounds on audio sensors across town, to further increase panic."

6.4 CYBER VULNERABILITIES IN SMART CITIES AI / ML

To do this, they formulated a master attack methodology using various established frameworks for vulnerability, threat and exploit analysis that represent the anatomy of an attack's "when", "where", "what" and "how".

The phasing sequence of the attack, or what we call the "when", leverages Lockheed Martin's cyber kill chain . The surface area of where the attack could occur, or what we call the "where", references the OpenWeb Application Security Project's (OWASP) attack surface areas.

The actions required to successfully accomplish the given phase of attack, or the "what", is represented by both MITRE's Common Attack Pattern Enumeration and Classifications (CAPEC) and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. Finally, the tools used to execute the actions, or the "how", are represented by both Kali Linux tools [14] and known exploit tactics by MITRE's ATT&CK Matrix. Each framework occupies a level in the traditional attack tree format as seen in Figure 10 below.

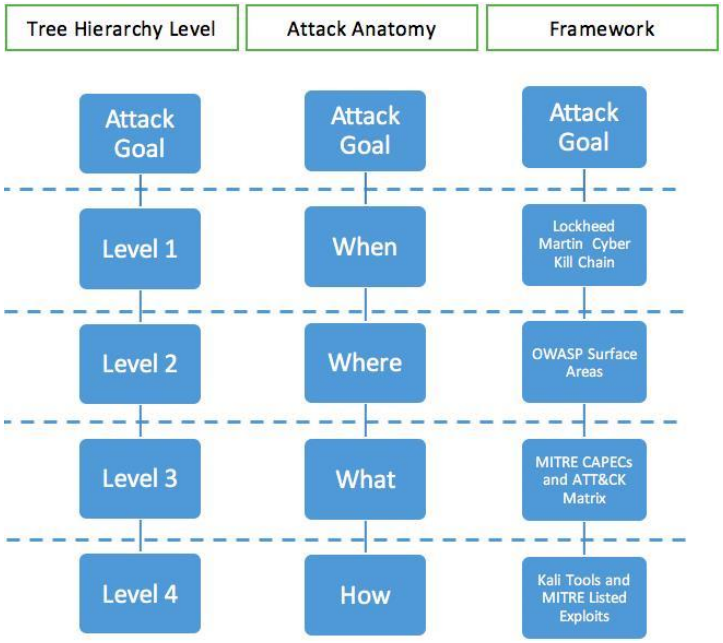
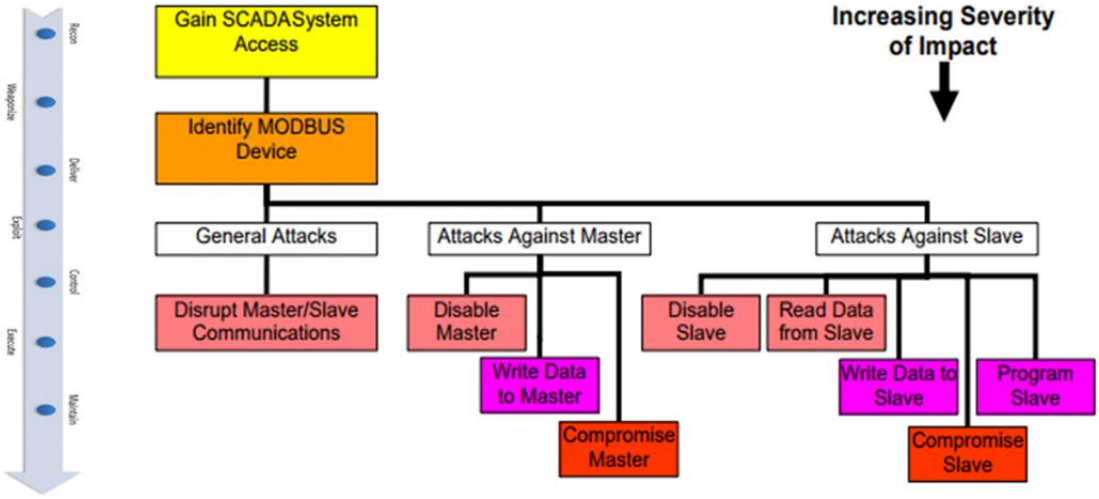


Figure 10 - Attack Tree Framework Mapping by Gregory Falco and team from MIT

The



The proposed master attack methodology deployed for an AI planning system can be useful for public administrators to understand cyber risks for their smart cities. By using an attack planner auditing tool to evaluate smart city digital asset risk, defensive measures can be taken to mitigate the potential cyberattacks and their associated financial damages.

Many publicly available security tools that are intended for good can also be used by malicious actors. The master attack planner proposed would be no different. Potential attackers ranging from novice script kiddies to nation states seeking to wage advanced persistent threats against a smart city can leverage this tool to plan out their attack.

The tool can theoretically help them to determine their most effective and efficient attack options to penetrate and disrupt city operations. We can take solace knowing that the master attack methodology alone will not sufficiently help a malicious actor plot a cyberattack against a smart city.

7 DATA PROTECTION ISSUES ASSOCIATED WITH SMART CITIES

Government authorities implementing smart cities regimes are at risk of violating privacy laws if appropriate safeguards are not taken. The European Court of Human Rights has held that surveillance mechanisms (including those implemented in smart cities technologies) can violate the right to privacy, especially where domestic legislation does not define the scope or manner of surveillance. Conversely, individuals may find that their data has been used illegally in the implementation of smart cities technology.

In the United States concerns around safety, security and data privacy are prominent. Several US cities are banning or considering bans on use of citizen data such as mobile location and facial recognition. Contrast this with nation states such as China where the state has much more control over personal data.

As much smart city technology is based on open platforms that are often outsourced to private citizens and corporations, there are massive risks that PII may be unlawfully shared to third parties. Compounded with the relative opaqueness of data storage by governments, critics argue that individual privacy can be curtailed massively through residence in a smart city with little recourse for individuals.

ROKE

GLOSSARY

DARPA	Defense Advanced Research Projects Agency
DASA	Defence and Security Accelerator
DHS	Department of Homeland Security
FIWARE	Future Internet – ware
IIOT	Industrial Internet of Things
ITAR	International Traffic in Arms Regulations
JAIC	DARPA – Joint Artificial Intelligence Centre
JFC	Joint Forces Command
LPWAN	Low Power Wide Area Network
NSA	No Such Agency (otherwise known as the National Security Agency)
NGSI	Next Generation Service Interface
NSTC	National Science and Technology Council
OSTP	White House - Office of Science and Technology Policy
SCC	Smart Cities & Communities
SIGINT	Signals Intelligence
STEM	Science, Technology, Engineering and Mathematics
USCYBERCOM	US Cyber Command

ROKE

REFERENCES

1. The G20 Global Smart Cities Alliance on Technology Governance https://globalsmartcitiesalliance.org/

2. EU - Analysing the potential for wide scale roll-out of integrated SCC solutions - June 2016 29 https://ec.europa.eu/energy/sites/ener/files/documents/d2_final_report_v3.0_no_annex_iv.pdf

3. Black Hat USA 2018 https://www.blackhat.com/us-18/briefings/schedule/index.html

4. THE CONCEPT OF SMART CITY IN THE THEORY AND PRACTICE OF URBAN DEVELOPMENT MANAGEMENT https://www.researchgate.net/publication/304570582_THE_CONCEPT_OF_SMART_CITY_IN_THE_THEORY_AND_PRACTICE_OF_URBAN_DEVELOPMENT_MANAGEMENT

5. Irdeto Global Connected Industries Cybersecurity Survey https://go.irdeto.com/connected-industries-cybersecurity-survey-report/

6. Armis Labs VxWorks Urgent 11 Zero Days https://www.armis.com/urgent11/

7. EU report - coordinated risk assessment of 5G networks security https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

8. People-Centric Service Intelligence for Smart Cities file:///C:/Users/cfox/Downloads/smartcities-02-00010.pdf

9. EU SynchroniCity project https://european-iot-pilots.eu/project/synchronicity/

ROKE

ANNEX A - NOTES

Future state – Rotterdam Port – example of Cyber Resilience approach for smart cities

The city uses systems to collect data from users and sensors. A dedicated platform analyses and processes this data. The city then uses this data to improve the services for its residents. At every step, at any connected point, there's an opportunity for attackers.

The technology infrastructure of a smart ecosystem consists of three layers:

- Edge—The front end of the smart city. Consists of connected devices such as sensors, actuators, smartphones, smart lights and smart trash collection. This layer gathers the data from IoT devices, then sends it through the communication layer to the core.
- Communication—connects the core and the edge by a network system, such as WiFi, Bluetooth, or LAN. The components of the ecosystem connect through this layer.
- Core—a cloud or IoT data platform that processes data and generates outputs that make sense of the data streaming from the edge.

Most smart cities add IoT solutions into their existing infrastructure. For example, water companies might deploy smart water meters while keeping the existing pipes. These meters usually have minimal security protocols, which makes them highly vulnerable to attacks.

Smart cities can't function without IoT devices, which rely on information security. Unfortunately, IoTs are notoriously vulnerable. Today's threat actors can launch sophisticated attacks, such as advanced persistent threats (APTs), to breach smart cities and cause critical damage.

Cyber Vulnerabilities

Smart city technologies permeate all aspects of city life, blurring the lines between physical and digital. Residents, choice locales, and devices are connected via information technology (IT) systems and operational technology (OT) systems. These systems monitor events, devices and processes, and then compute the data to adjust city operations. This level of interconnectedness presents a heightened level of risk.

Every endpoint presents a potential gate for attackers. The more connected endpoints your network collects, the more vulnerabilities attackers can exploit. Such attacks can disrupt operations and compromise a city's critical systems.

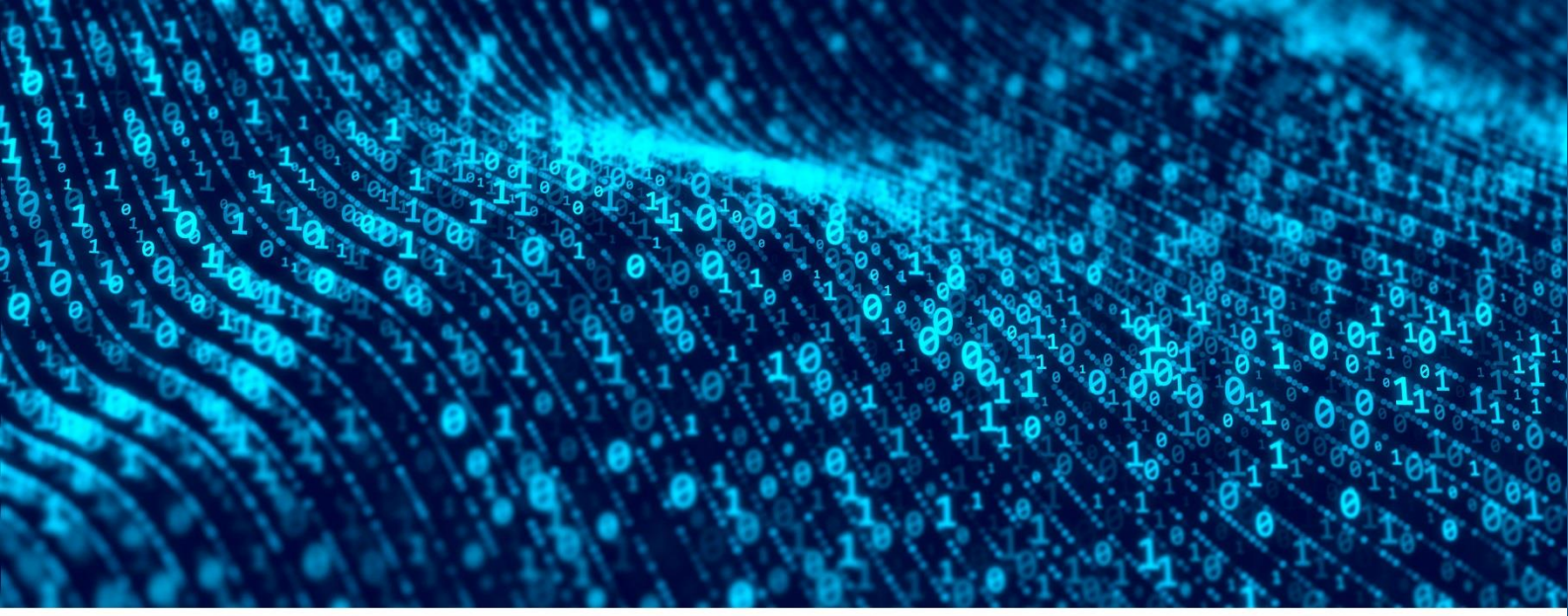
Convergence of legacy and new technologies

Cities taking the smart city route often need to integrate new technologies with legacy systems. This kind of integration creates significant challenges. Most legacy systems don't allow for live updates or data encryption.

Merging disparate technology platforms can create “holes” in the security perimeter. That’s how actors attacks a wastewater treatment plants in Australia. The attackers discovered a vulnerability, and used it to disrupt the Supervisory Control and Data Acquisition system (SCADA).

Security Risks That Threaten Smart Cities

Smart city networks are especially vulnerable to advanced persistent threats (APTs), which are complex attacks involving a combination of techniques. For example, an APT campaign can combine involve zero-day exploits and malware with multiple access points.



ROKE

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk