SECURING
SMART
CITIES

The Smart Cities Internet of Access Control, opportunities and cybersecurity challenges

Sept 25, 2017

Authors

Mohamad Amin Hasbini, Senior Security Researcher, Kaspersky Lab

Martin Tom-Petersen, CEO, Smart City Catalyst

Contributors

David Jordan, CISO, Arlington County Government, Virginia, USA

Alan Seow, Cybersecurity Practitioner

TOC

Introduction

The Smart city is a fast advancing zone in urban planning and aged cities of today. This concept is based on the application of connected various systems in managing a city effectively. Some of the major aspects that the smart city emphasizes are energy and water supply, transport and access control, public health and safety management. The ambition of building and modernizing cities with connected infrastructures is to provide better public services, seamless high-speed communication and a better-quality living environment.

The development of the smart city significantly relies on the Internet of Things (IoT) technologies. The IoT can be applied in a great variety of environments ranging from energy saving systems, traffic monitoring, connected vehicles, building management and access control to smart-home devices. The expansion of IoT devices, is expected to grow beyond 50 billion devices in the next decade, providing the technological backbone for smart cities development. To a large extent, the adoption of IoT technology in the smart city development focuses on two aspects: energy and communication efficiency. These two attributes can also be achieved through effective, well-planned and integrated access control management.

In this perspective, a smart city can allocate its resources economically as well as limit excessive access of vehicle and people. Hence, this paper emphasizes the centralized access control management of the smart city (service centered, cloud based or similar). IoT based access control systems are composed of connected structures with incorporated sensors. They can modernize and improve traditional access control efficiency via decision-making algorithms. As a result, time and monetary resources can be optimized for both the city authority and citizens. Nevertheless, the underlying technology of IoT presents security concerns, the collaboration of IoT vendors and access control technologies may provoke a series of incompatibility issues and thus open the way for weaknesses and vulnerabilities.

This document introduces the concept of the “Internet of Access Control”, a futuristic concept of connected access control systems distributed over an urban ecosystem, part of its critical infrastructure. Even though highly worrying and controversial concept to look at with current technological standards in addition to cybersecurity and privacy occurrences, if perfected, it could progress some of the current world’s most alarming complications like traffic jams, crime, terrorism...

This research consists of three parts. The first section contextualizes the background of access control systems in urban planning. Since discussions around internet based access control are not well developed online, traditional and IoT-based access control systems will be analyzed comparatively. The second section provides a comprehensive review on the advantages of adopting IoT-based access control systems in various scenarios of the smart city. The third section illustrates cybersecurity issues of deploying IoT-based access control systems in the smart city context.

Challenges of traditional access control

Access control systems, whether traditional or IoT-based, always serve the purpose of selectively restricting access to a physical location and/or electronic resources. The enhanced adoption of smart devices further emphasizes the access control need in varying circumstances. More importantly, in a mix of cyber and physical world today, new access control systems having embedded connectivity can enormously contribute to centralizing access control management on a city level, each system can function independently while sharing data seamlessly for a centralized operation coordinating different access control components of the entire smart city.

Resources waste in traditional traffic access control

Cities were built and developed prior to the existence of the Internet, access control systems were therefore established in a decentralized structure where each of its systems functions separately without coordination. Take the cases of traditional traffic management as an example, the traffic of one area of the city does not reflect what is happening in other regions of the city. It is therefore inevitable to cause inefficiency in access control management on a city-wide scale.

The Texas A&M Transportation Institute and INRIX 2015 Urban mobility scorecard (1) details figures regarding the impact of traditional access control in the urban areas of the United States. For example, the travel time delay in the United States was of 6.9 Billion hours in 2014, an increase from 6.8 Billion hours in 2013 and 6.5 Billion hours in 2010. The relative congestion cost is 160Billion $ in 2014, 156Billion $ in 2013, and 149Billion $ in 2010. These stunning figures show a glimpse of the wasted resources in the developed world due to inefficient access control in urban areas. The same study further suggested the cost of traffic congestion would mount from $160 billion (in 2014) to $192 billion in 2020. From an average. From an average commuter’s perspective, in 2020 congestion cost will amount to $1,100, 47 hours and 21 gallons of fuel. These numbers expose the incompetence of traditional access control systems in managing always evolving cities, from the traffic management point of view.

(1) https://static.tti.tamu.edu/tti.tamu.edu/documents/mobility-scorecard-2015-wappx.pdf

Resources waste in traditional physical access control

The initial acquisition cost of most traditional access control devices may be much lower vis-à-vis the new ones having embedded connectivity or advanced biometrics. For example, compare one standalone door with a mechanically-operated lock (average cost $200 to $400) with an entrance system having biometrics recognition (up to $10,000), the upfront installation cost is undoubtedly higher than a basic access control setup. However, it is important to consider the total cost of ownership (TCO) in a comprehensive perspective. The support, technical maintenance and other hidden costs of traditional access control systems, given a specific fixed time period, may eventually surpass those of the innovative ones. The same comparison example between a mechanical and biometric locking system can justify this argument. Adding the costs of personnel (security guards, administrative and technical support) to supervise a building of 200 mechanically operated doors, the entire operation workflow and costs are multiplied by 200 times, not to mention the training costs involved in the renewal of personnel. On the contrary, the same building with 200 biometrically operated doors will require one centralized monitoring system as well as a handful of maintenance officers, limited training and on-demand technical support. In this point of view, the high upfront costs of smart access control systems can be an offset as the operation and maintenance costs diminish in short to medium terms. The same principle can notably be applied in customs control. Some Asia-Pacific cities such as Dubai, Seoul, Sydney, Taipei and Hong Kong have been successful in installing automatic smart gates to register and authorize entry of tourists in the airport, ports and other land borders checkpoints. This significantly reduces the human resources costs and improves the efficiency of monitoring the departure and entrance of citizens.

Rationale of a city-scale centralized access control in a Cyber-Physical Realm

Centralized access control can contribute to the smart city city resources optimization. It allows one or more sites to be managed securely, remotely or locally through a large variety of-technology readers such as RFID, NFC, biometrics and smartphones. Furthermore, instead of distributed and separated access control systems, centralized IoT-based access control devices can be installed city-wide to provide support to and complement all subsystems ranging from video management, access control, video analytics, intrusion detectors and other connected equipment. These new access control solutions facilitate the monitoring and management of smart cities.

From a centralized operation center, operators have the ability to coordinate from a single point, issue and handle access requests of an employee, a guest, a group of guests, a vehicle, or even a flying object (aircraft or drone). The fundamental argument to centralizing the resources in a control management system is to reduce the administrative costs and highly manual processes incurred in traditional access control management, notably the interdepartmental approvals and procedures. Moreover, centralizing the access control devices under one coordination point of service/contact optimizes business recovery when it comes to technical issues, the concerned technical support personnel will only need to access centralized physical servers to conduct remediation work. They can also be authorized to verify and modify the pertinent of specific access control policies from their smartphone or tablet. In this way, they can acknowledge the state of a technical issue immediately. The access request or problem such as access device refusal, door locks and other technical failures can also be addressed through interacting with other networked systems (sensors, video surveillance, intrusion alarm and monitoring devices) and other databases.

One competitive edge of using centralized access control systems is the straightforwardness of redeploying the same security and access restrictions as the data can have multiple backups, even-though grouping and coordinating a large number of connected devices to serve the city is not a simple task. This process requires considerable work in selecting and adopting the appropriate and compatible policies and devices. In this context, many encryption and authentication protocols and methodologies are employed to ensure secure and efficient communication among different systems and platforms. As multi-technology readers play a major role in access, it is important to mention the popular industry protocol: Open Supervised Device Protocol (OSDP)(1). It provides the framework for standardizing, scaling and managing the interoperability of card readers, biometric recognition and other authentication control functions.

(1) www.osdp-connect.com

Despite the numerous advantages of employing centralized access control devices and systems in managing smart cities, we should not neglect the risk of the single point of failure. The implementation of a connected access control infrastructure and service is highly demanding from a smart city cybersecurity perspective and should only be considered when the city possesses a level of maturity which can guarantee and assure safe operations of its critical infrastructure. The entire city’s access control will be at stake in case the centralized operations are interrupted, therefore special technological, organizational and national requirements need to be matched in order to maintain stable operations. The worst scenario could be no access request and approval processed to all registered connected access control objects. Consequently, the entire city could be paralyzed. In addition, such a centralized access control center can have considerable impact on performance if its resources are not sufficient to manage all access requests equally and efficiently.

Connected access control, applications in smart cities

The concept of centralized operations permits IT and security personnel to administer and monitor access control from centralized locations (virtual, cloud-based). The IoT architecture makes it possible to grant or revoke access remotely in a timely manner via standardized authentication policies and centralized management tools.

Access control for city-wide access control and emergency management

Smart gates in sensitive access points of the city, notably, airports, are already being adopted globally, with smart integrations happening in between different countries. It is one example of how centralized operation centers can contribute to public security and access control. The supplementary examples of similar access control systems can also be extended to baggage storage and train station lockers. Smart locks can register the identity of users and inform relevant parties in case of suspicious items or behavior.

In terms of emergency management, a lot could be done from an access control perspective to enable the most efficient response to wildfires or earthquakes… Connected smoke/fire sensors can send data to the centralized operation center immediately on fire source, fire extent, fire propagation; relevant personnel can react fast to stop the spreading and protect humans and assets. In case of emergencies, gates unlock decision in a building or a location could be made to allow evacuating populations faster than in traditional standalone monitoring systems.

Access control for roads access and traffic control

Effective traffic management is a top challenge in numerous urban areas. Using centralized access control systems ensures real-time control and thus significantly improves road safety and traffic congestions. The access priorities and rights of pedestrian and vehicles can be regulated according to live traffic situations. In this aspect, access points using badges, smartphones, and other RFID technologies can be set up according to user profiles and thus notifies them continuously about their access rights. Moreover, during days of severe air pollution or major road maintenance, smart access control systems can moderate or throttle vehicle entry to relieve traffic jams of the city more efficiently. Vehicles causing more pollutants could be forbidden to circulate.

Smart safety mechanisms are increasingly integrated in connected vehicle designs to advise on safety regulations to the driver attitude (location tracking, speed limit, safety, misbehavior...). Such valuable data can be used to relate to the drivers’ license point system. It can also contribute automatically towards detecting irresponsible or unaware drivers (under influence of alcohol...) or drivers on the road before they can cause accidents or tragedies. Hence, road and public safety can be exceptionally enhanced.

In addition, traffic control aligned with the centralized operation center can receive great network orchestration effects. One convincing example is the traffic and road lighting systems networked with live accidents and traffic situations. Even street lighting colors can be dimmed when the usage is low at night to reduce energy consumption. Most importantly, they can switch to different colors to facilitate operations for emergencies as police, ambulances and firemen intervention in case of incidents. Vehicles can then manually or automatically slow down to give way to officers.

Access control for smart home, vehicle or other personal belongings

A compelling neighborhood or a housing group access control system stops unauthorized intrusions and trespassing as well as provides valuable forensic data in case of unpleasant incidents. Smart homes can react collectively to certain events during the day and trigger a succession of commands calling for external intervention. Connecting outdoor security systems, cameras or heat sensors to the local police stations can also save the time for investigation, minimizing unnecessary field operations and sourcing witnesses. If all houses are equipped with such access control systems to inform local authorities, it will greatly reduce the time cost and manpower on a city level. Such technologies can be extended to attribute identifying rights to smart devices, in particular valuable ones like vehicles. The most compelling authentication method in this case is biometrics access control system which can be stored on centralized databases allowing the user to access his own properties (multiple houses, offices, warehouses and vehicles) with the same set of biometric attributes (similar techniques already used by airports for identity verifications...).

Access control for government institutions and business premises

Terrorism in its different forms has been a troubling issue across the planet. Cities having diverse ethnic groups are exposed to political risks, which are provoking spontaneous offenses against local government institutions. Using access control systems together with security staff (or robots) to restrict the entrance of *persona non-grata* in government offices and buildings is a preemptive measure to protect government assets and personnel. The electronic records can also categorize visitors so as to better cater to their needs. One important characteristic of using access control systems is that they can cross-reference the number of visitors in relation to sensitive events to detect abnormal crowd gatherings or motion. Having such technologies to monitor/analyze the crowds enables better security options.

Similar precaution can be applied in private institutions, especially when it comes to employee dismissal and insider threats. A smart access control, both for physical entrance and office desktops, can be used to manage employee clearance and real-time monitoring of hardware and facility access. Modifying and disabling access cards, passwords and even elevators control can stop undesirable and unauthorized access, thus enabling better prevention from insider threats, ex-employee revenge or outsiders tailgating.

Additionally, from a safety point of view, a centralized access control system plays a significant role in responding to accidents. For example, in the case of a fire, the system can activate all evacuation exits fast, unblock access rights and locate unidentified personnel with geo-identity enabled access cards or utilities. This advantage helps personnel to leave the fire scene fast and safely but enables rescuing units to offer immediate aid to missing personnel.

Access control for tourists

Touristic sites and customs deal with a high volume of domestic and international visitors. Automated access control systems, notably smart gates, add value to touristic spots by creating a safe, comfortable and relaxing environment. The smart gates connected to the centralized access control operation centers can be used to identify, register, authorize entry and exit. Tourists can be advised to install applications on their smartphone as to be informed with live traffic and tourism data accordingly to optimize their sojourn time. The city authority can install connected devices to monitor live capacity of touristic facilities such as hotels, car rentals, theaters, theme parks, beaches and hiking trails. The information is then shared via the application to help tourists reserve their tickets and plan their hang-outs more comfortably without having to stand in queue for hours. Such types of applications can also help resolve another problem that tourists constantly face in foreign countries which is getting lost from friends or close ones.

One additional benefit of managing tourists via centralized access control centers is the ability to cross-reference and match both the domestic populations and tourist needs. Many major touristic cities in the world like Venice, Dubrovnik, Paris, Barcelona and Hong Kong suffer from tourism mismanagement that the domestic population protest against the over-reception of tourist causes deterioration of life quality and public infrastructure efficiency. The centralized access control operation center can reconcile the differences and pacify deception of both the domestic population and international travelers. A combination of smart gates and live information sharing via touristic spot monitoring sensors will make a city more live-able and ‘travelable’.

Access control for national security and public order

A centralized access control operations center will contain considerable valuable data for law enforcement units to conduct missions such as surveillance, site audit and raids. In such situations, traditional field practice would require a further deal of planning to study the operation site with limited data sources. The sites’ civilians can also be informed or barred from certain access points simultaneously as the operation goes on. This measure facilitates the field agents to capture criminals and save hostages/humans effectively.

Robots and drones are also gaining fame in fighting crime and monitoring terrorist activities. Access rights are therefore equally important in managing the unmanned devices. They can be given special access rights and coordinated by the same access control operations center using wireless technologies (Bluetooth, NFC and Wi-Fi) to carry out the missions. In addition, unmanned devices can be used as counter-intelligent tools. In particular, the variety of drones represent a severe risk for privacy (illicit filming and recording) and security (shoplifting and remote assault). They are difficult to monitored without a centralized surveillance system, a citywide access control operation is indispensable in such cases.

Access control for standard sites: public parks, schools, companies, hospitals etc.

In the same perspective, access control systems can be installed or retrofitted to different buildings and places serving public or private functions. The profiles of the users and visitors are constantly updated with the latest access control policies on the databases as well as law enforcement units' records. Access rights will therefore be lively monitored and processed. Individuals representing a threat can be denied access in various scenarios. For example, parks can automatically enforce/limit access of visitors with animals and inappropriate items (skateboards, kites, drones, etc.) according to new regulations of the city or nation; schools can also synchronize the data of their students with police record and parental guidance to prevent unauthorized items (drugs, pornography, weapons, etc.) to enter the premises; hospitals can react faster in referencing the incoming patients' medical record and offer immediate and personalized medical care.

Apart from the perspective of filtering existing undesirable individuals from entering certain premises, smart access control systems can also serve an anticipatory purpose. One example is restricting underage access to nightclubs, alcohol/substance selling points and gambling sites. In a more futuristic perspective, deep machine learning will potentially be able to analyze a variety of applications and security systems regarding suspicious activities of a particular individual across the city such as unusual driving speed, facility entry and exit irregularities, etc.

All these examples are existing issues and demands of cities and their citizens. Nevertheless, using innovative access control systems elevates the service quality of a city to higher levels. As discussed, individual access control systems can be coordinated by a centralized operation center to maximize the network orchestration effect. Each of the access control components works as if they are part of a bigger ecosystem instead of coping with their own tasks.

Cyber Security Issues

One main concerns of traditional access control systems is their exposure to physical security weaknesses, notably, infrastructure vandalism, operation site break-ins and other unauthorized entries. These same risks, though still exist, are reasonably mitigated in the case of IoT based access control systems. Remotely monitoring and control of unmanned facilities can provide more responsive maintenance and replacement support. However, new technology comes with new challenges in addition to the traditional ones. The complexity of IoT technology in access control systems, to a large extent, involves plenty of cybersecurity threats.

Protection of communication

Access control systems are built with extensive networks of connected devices. Managing such a huge number of devices is no simple task. It is worth pointing out that these networks are also likely to come from different vendors and manufacturers. The technical issues, in particular the interoperability of these connected networks and devices, demand considerable manpower and resources to operate and maintain. More importantly, the vast data generated every second by these devices grows endlessly. In the connected world, data is the new gold mine and it inevitably attracts malicious attention. On the other hand, data theft is a highly lucrative business. The accessed data of individuals, vehicles, flying objects and other valuable devices can enable physical tracking of users and pose a real threat to their lives. On the other hand, the interoperability between different groups of devices may cause difficulties in the data transmission processes and in securing such transactions. Technical problems ranging from incompatible data formats, encryption protocols to storage and response capacity can be problematic to solve, thus, exploitable by cyber attackers. For example, intentional or unintentional data transfer, processing or security of data transmissions on a single highway could cause outdated and inappropriate traffic information, lowering systems efficiency and endangering the safety of road users. Large scale DDoS attacks are notorious in their effectiveness and low cost of deployment. Furthermore, as discussed in section one, the concentration of access control operation center’s activities under specific services unavoidably centralizes the information security risk in one specific virtual location. In case of a cyberattack targeted against such a coordination access control center, the whole city can fall apart within hours and provoke public chaos.

The security of connected devices is therefore at stake. According to the connectedness nature of IoT based access control systems, a security event may threaten the entire network. In this perspective, it is essential to focus on the network security aspects to ensure that in case of security incidents, the communication interruption between the connected devices and coordination center will be minimal and optimal service will be restored in the least time. Communication protocols on the network and transport layers of connected devices such as TLS/SSL and IPSec should be regularly reviewed and audited to ensure the data integrity, authenticity and confidentiality. Network encryption solutions such as WPA, TKIP, AES, PPPoE should be implemented and embedded in the product design as well as in the operation wireless environment (WiFi and cellular network). In addition, the identity of devices/authorized personnel is equally important in the communication protection process. Fabricated data and fraudulent identities can be manipulated to disguise cyberattacks.

Protection against tampering and spoofing

Both the software and hardware aspects of the access control connected systems are exposed to the risk of being tampered and spoofed. As discussed, the connectedness of the access control system is a double-edged sword. It can revolutionize the traditional access control management and enhance significantly its efficiency in a great variety of scenarios as demonstrated in section four. Delivering fake or deliberately-altered signals to millions of connected devices in city-wide is no longer a movie scenario, but a feasible scheme. Hijacking an entire access control operation center may seem unlikely to take place, nor does it attract cyber-attackers without abundant resources, though it is not impossible and a city is definitely a considerable target. Replacing or eavesdropping the access control systems with altered devices in the network, though, can also be a 'profitable' suggestion for attackers, though other options pose less risk on the attackers, such as reselling intercepted data, selling access to compromised devices taking over the control of a subdivision of the entire access control system… Nevertheless, a combination of different city-wide access control and monitoring systems would help agencies identify such types of attempts from earlier stages.

Secondly, the security and authentication certificates, knowns as keys, are in the main spoofing attack target. Using a high-quality key management system (KMS) to generate, exchange, store, and replace keys as needed for devices and applications. a KMS is tailored to specific use-cases such as secure software update or machine-to-machine communication. The KMS is aspired to provide a specific comprehensive key distribution scheme for wireless sensor networks according to practical contexts. It is in particular suitable for the IoT technology.

Finally, inappropriate and legacy routing protocols will lead directly to the collapse of the entire network. Besides, the end node problem in cloud computing and IoT architecture is another challenging issue to manage. The ecosystem of IoT-based access control systems is vast and peripheral devices are constantly connected to the entire network, in particular with wireless sensors and networks. It is difficult to determine the security level of these devices because most of them do not have the most updated security standards and software comparable with the centralized network's security level. Meanwhile, this regular data exchange is inevitable in the operation of connected devices, and it has to be able to identify trustworthy devices so as to operate safely.

Enforcement of multiple biometric verification systems in sensitive locations

The security issues mentioned in the previous sections are highly related to data exchange on the network level, which can be intercepted, altered and manipulated via imitating the authentic data set. Moreover, traditional and non-traditional access control systems rely on mechanical locks and keys, passwords and access cards to process access request. The duplicable characteristic of these items is similar, even identical, to data duplication. These identification methods can be lost and forgotten, causing additional recovery costs and risk of exploits. Hence, the attacker can take advantage of this vulnerability as they do in manipulating duplicable technical data on the network level to attack the access control systems.

Biometrically-enabled access control systems can effectively counter this vulnerability. Biometric devices permit machines to intelligently recognize the unique biological attributes of humans such as face, iris, handwriting, voice and fingerprint. The complexity of duplicating such data is then higher than reproducing an intercepted set of data to fool the system, nevertheless still possible. Besides, both the stored biometric data and the authentication methods (basically the individual himself) are highly mobile and duplicable without the security concerns of using third-party items such as keys, passwords, access cards, etc. In addition, biometrics are non-intrusive, accurate and cost-effective. Even though the attacker manages to steal his target's biometric data, it is unlikely to be duplicated on another person's body, or it may incur extraordinary costs.

A biometric access control system can be deployed in two models. One is the enrollment model (offline) and the other one is the verification model (online). In the offline model, biometric data is scanned and pre-installed on the access control server. This model is suitable for facility with low personnel turnover rate and regular access control request. It can operate without constantly connected to a centralized operation center to stay cost-effective. In the online verification model, the stored biometric data is taken a step forward to ensure real-time authentication and register new users. This model perfectly matches the operational strengths of a centralized access control, where biometric data is located in a single location (virtual location, e.g. cloud...). Thus, an individual requesting access in multiple access locations during different hours of the day might not need to have their biometrics data registered on all different locations. The centralized access control center can handle his requests and rights referring to one single point of biometrics data storage. Such systems are highly regarded to be applied in the entrance of sensitive locations, in particular government buildings, medical care establishments and schools. Not only does it discourage *persona non-grata* to try their luck, but also the law enforcement can track individuals efficiently, upon need.

Biometrics data of individuals attempting to cross the borders to initiate malicious endeavors can be transferred via the Internet to international law enforcement parties. In this era, with which radical ideas may encourage transnational terrorist attacks, biometrics can be the ultimate solution to the perfection of connected access control systems beyond an individual city to the international community.

Conclusion

Today, there are more people living in cities than in the countryside. Vehicles and energy consumption in cities are skyrocketing. The domestic and international mobility of citizens is significantly improved and tourists are travelling extensively from one city to another. Under such circumstances, many metropolitan cities are dealing with challenges such as overpopulation, waste management, massive energy consumption and pollution as a result of dramatic increase of migrants and travelers.

Traditional access control systems, therefore, can no longer effectively deal with such multidimensional challenges, traffic jams and long queue waiting times should not be accepted as the norm. Cities have to innovate themselves with better and smarter access control systems to track and manage their populations, vehicles, buildings and touristic sites. The IoT architecture plays a significant role in shaping this wave by establishing smarter access control systems in cities to address the new challenges. Smart and connected devices can be applied in a great variety of scenarios in the city. Connecting them to a connected access control operation center significantly contributes to effective management of the city. Nevertheless, it is crucial to be aware of the cybersecurity dangers as there are multiple points of entry in such a large network of devices. In conclusion, the trend of adopting smarter access control systems and connecting them to a centralized network is going on in many big cities in the world. More research in perfecting the security of smart access control devices is expected in the near future.