Cyber Security Challenges in smart city

Safety, Security and Privacy

Shivam Shrivastava

Dr. Shakuntala Misra National Rehabilitation University, Mohan Road, Lucknow.
shivamkhunkhun@gmail.com

Abstraction

The world is experiencing an evolution of Smart Cities. These emerge from innovations in information technology that, while they create new economic and social opportunities, pose challenges to our security and expectations of privacy. Humans are already interconnected via smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on their path to the full connectivity known as the "Internet of Things." Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. We examine two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. We also present a model representing the interactions between person, servers and things. Those are the major element in the Smart City and their interactions are what we need to protect.

Keywords

Smart City
Internet of Things
Security
Privacy protecting systems
Security and privacy models

Introduction

The benefits of Information and Computing Technologies (ICT) in a Smart City and of the Internet of things are tremendous. Smart energy meters, security devices, smart appliances for health and domestic life: these and more offer unprecedented conveniences and improved quality of life. City infrastructures and services are changing with new interconnected systems for monitoring, control and automation. These benefits must be considered against the potential harm that may come from this massively interconnected world. Technical, administrative and financial factors must be weighted with the legal, political and social environment of the city

Methodology

Several paradigms and categorical structures may be applied in analysing the benefits and detriments of this data environment. An applicable paradigm used for this analysis is that of IBM that the Smart City, its components and its citizens are

- Instrumented
- Interconnected
- Intelligent

This is denoted as "IN3."

"Instrumented" gives city components and citizens devices, at varying levels of features that,

at a minimum, respond to a sensor network. These are, in turn, "interconnected" as to pass information into a network. That information is computationally available for analysis and decision-making, making the Smart City "intelligent" in its operations. Security and privacy concerns rest on how the information within IN3 is used. The core of the technology is the information. A full examination of any system of the Smart City may categorize information as to sources, types, collections, analytics and use

(Fig. 1, Fig. 2, Fig. 3, Fig. 4,)

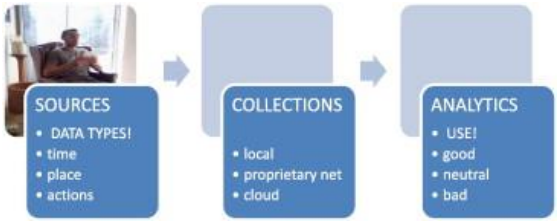

Figure 1

Data sources feed data collections feed data analytics for knowledge

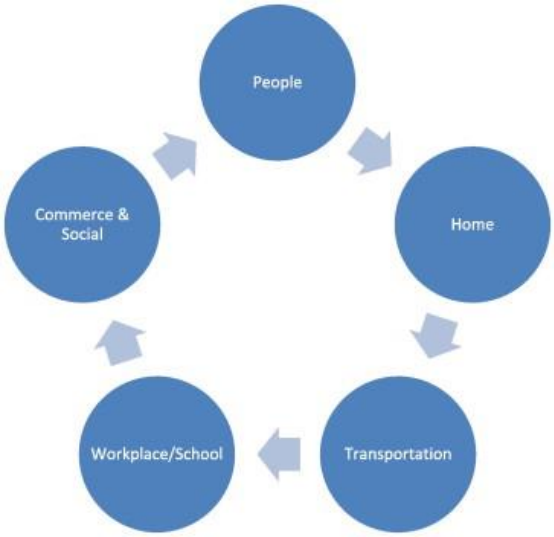

Figure 2

The production loci of data in the Smart City.

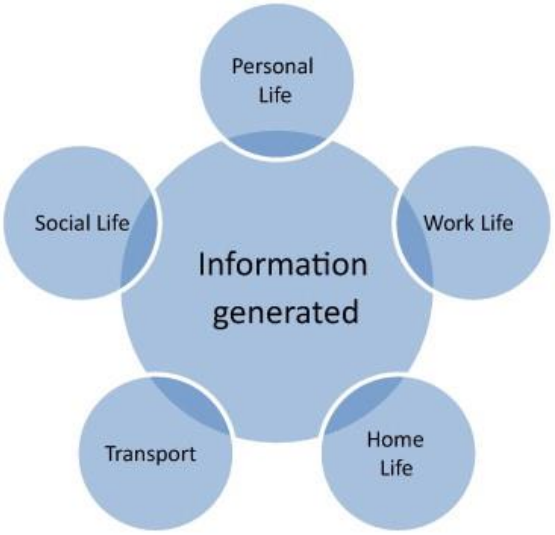

Figure 3

Source nodes of activities and services producing data.

Figure 4

The recursive cycle of data in the Smart City information generated is information used is information generated is information used.

The instrumented source may have particular rights or risks associated with particular types of information, such as a person's location or actions. The collections of that information, such as on the device or on a cloud aggregator, similarly invoke issues of rights, duties and risks. From those collections analytics can build services of varied sophistication which, in turn may be used for good or ill.
The loci of activity nodes may be categorized in relation to people, workplace, transportation, homes and social/commercial interactions.

An additional way to categorize within this space is to consider information source nodes as the activities and services of social and civic life, people, work, home, transport and social life.

In all of the interactions the information generation and exchange is at least bilateral and communicative. Actions often call and use information which, in turn, generates new

information related to the services, including bettering those services on analysis.

IN3 is brought together in the commercial culture of search, recommender services and locational apps for devices that suggest services based on a person's location, characteristics and historical preferences.

More fundamental civil services at greater efficiency and reduced cost are possible for a Smart City. Citizen safety is a paramount civil responsibility. After the murder of a social worker making a home visit, computer engineering students devised an app package for smartphones that would track via GPS and provide panic button notification to supervisors and police via direct activation and timed cancelation. This support was only possible with this instrumented, interconnected and intelligent system. Similarly, every police officer on patrol may be monitored as to his or her precise location in relation to other activity in the city.

Yet this is subject to abuse. Various apps subvert the instrument, such as a smartphone, and turn it into a spy and tracking device for a jealous spouse, obsessed former associate or malicious voyeur.
The first major instrumented/interconnected/intelligent case before the U.S. Supreme Court involved a GPS tracking device. The Supreme Court of the United States found the placement and monitoring of a GPS tracking device on a person's automobile while it travelled on public roads to be illegal absent sufficient evidence relating the vehicle to criminal activity as determined by a neutral magistrate . This was an "unreasonable search" even though it would have been completely permissible for police agents to follow the automobile in their own vehicle and log the movements.
Although a prevailing rationale was that the placement of the tracking device without permission was a trespass, Associate Justice Sonia Sotomayor in a concurring opinion addressed the growing risks pervasive computing and communications technologies, such as GPS-enabled smartphone presented for traditional notions of privacy. Electronic surveillance may still be improper "when the government violates a subjective expectation of privacy that society recognizes as reasonable" and she agreed with Justice Alito that long-term GPS monitoring would impinge on those expectations.
In cases involving even short-term monitoring, … GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations … ("Disclosed in [GPS] data … will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment centre, the strip club, the criminal defence attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future and because GPS monitoring is cheap in comparison with conventional surveillance techniques and, by design, proceeds surreptitiously, The knowledge of such surveillance could have a negative impact on freedoms of speech and association with others as well as provide the government with immense private information subject to misuse.

Security is a global idea tied to safety, an assurance that a person may go about his or her life without injury to life, property or rights. Cyber security is a subset that focuses on computing systems, their data exchange channels and the information they process, the violations of which may be sanctioned under criminal law. Information security and assurance intertwine with cyber security with a focus on information processed.

Representation and Modelling

We can represent the whole domain as some Sets and relations as follows:

The sets are mainly, the Persons (P), the Servers (S), and the Things (T) which are elements of the Internet of Things. Essentially, we have :P={pi,p2,…,pL}S={s1,s2,…,sM}T={t1,t2,…,tN}where: M < L ≪ N since there are less servers than persons and much less persons than thing in the emerging Internet of Things.
The traditional Security and Privacy concerns are focused on protecting the vertices of the following within graphs:Gp={P,EP};whereEP={(pi,pj)}suchthati,j=1,2,…,LGS={S,ES};whereES={(si,sj)}suchthati,j=1,2,…,M
The within graph of Things as listed here is currently ignored as it is not the focus of attacks GS={T,ET};where ET={(ti ,tj)}such that i, j=1,2,…,N
The external relation graphs representing interactions such as between persons-servers and person-things are represented below:GPS={P,S,EPS};whereEPS={(pi,sj)}suchthati=1,2…L,,j=1,2,…,MGPT={P,T,EPT};whereEPT={(si,sj)}suchthati=1,2…L,,j=1,2,…,NGST={S,T,EST};whereEST={(ti,tj)}suchthati=1,2…M,,j=1,2,…,NWith the growing number of interconnected Things, G_{PT} and G_{ST} are becoming extremely important and almost intractable. Our focus in the near future will be on protecting the varices of

these graphs to create secure and privately acceptable Smart Cities.

Result and Discussion

Our first discussion is the impact of these issues relating to transportation. Intelligent transportation, public and private, has access to a web of interconnected data including financial, GPS, vehicle state (within various parameters), weather and traffic updates.

Though legal and social expectations of privacy are less in public, mobile and regulated environments, people still have expectations as to rights of privacy and information security in those environments. Those security and safety concerns may be enhanced because of danger from misuse or accident, misconduct of others.

As in other areas of social instrumentation, the evolution of the Smart City and computational transportation networks is evolving and growing. We examine and discuss those components within the IN3 and the Source-to-Use structures and the issues of security and privacy each presents as to the system of automobile transportation in the United States. Automobiles are data sources from a variety of subsystems within them that produce different types of information. These data are collected locally but may also be transmitted and collected in central repositories where it ay analysed and used for a variety of purposes.
Other types of system instrumentation came into wider use. Event data recorders (EDR), sometimes referred to as "black boxes," are data recording devices that record and preserve various information on automobile recorded activities including OBD data. The National Highway Traffic Safety Administration of the United States (NHTSA) mandated the types of data EDRs must collect including the format of the data and its survivability

Security and Privacy Issue

For such instruments the privacy concerns relate to the data kept in them. Locational data can detail much about a person's life they do not wish revealed, as Justice Sotomayor discussed as to medical, political or social contexts. GPS systems can track destination and origination points when used and may even store the actual route taken. Access to contact lists and messages tells much that may need to be kept private for personal, professional or commercial reasons.

Locational data can be a key security concern. Many set the GPS originating address from their homes. Access to these data details that home location. If the automobile is away from home, that home may be a better target for burglary. If the driver is avoiding a stalker, now the stalker knows where they live.

The OBD II systems are open access without sufficient security. OBD II Bluetooth dongles may be surreptitiously installed, allowing external monitoring. Vehicles with native Bluetooth access may also be compromised.
The Event Data Recorders raise several issues. Vehicle manufacturers have used EDR data in their defence against claims their vehicles were at fault in crashes. Claims of surreptitious data collection as an invasion of privacy have been rejected. *Id*.
Legally these data are within the control of the vehicle owner who controls access to that data absent a judicial order to produce it to third parties, including the government. Accessing these data without consent or a judicial order is unauthorized access to a computing device that carries both criminal and civil penalties.

With these data from these sources, the next step is to collect that data via systems that offer remote viewing and remote analysis for many different purposes.

But security and privacy are also vital to the personal safety and security of people and their families. The security issues with information in the Smart City extend to relations between the people of the city and their own personal safety. General crime theory is another way to consider these issues for the Smart City. One criminological theory for examining meta-security issues in the Smart City is Routine Activities Theory. Routine activities theory in crime control can map to information security and suggest vulnerabilities and solutions for enhanced IT security.

This privacy violation is a major security risk. Once the motivated offender has a profile and location on the victim/target at all times he or she knows when that victim/target would be most vulnerable to a physical attack.

These systems and their use must consider what capable guardian services can mitigate these risks. Technical hardening of such systems is important, even as some early implementations do not seem to have anticipated these risks from even such vulnerabilities as open Bluetooth access ports. System implementation that both locks the data collected by these systems and notifies a vehicle user that the information is being transmitted/accessed are important security features. Capable guardians may include those who do vehicle maintenance or other instrumented data recipients who may alert the victim/target to compromise in the system that may appear in their data. And it must also include the user/target, who should not be left ignorant of these issues but should be informed of the vulnerabilities, risks and proper responses.

Conclusion

Matching the daunting security vulnerabilities Smart City systems may present in the hands of unwitting users is the absence of a clear theory of law and rights to define what can and should be done with the power these systems represent.

Justice Sotomayor suggested in her concurring opinion in the *Jones* GPS tracking case that a reevaluation of the concept of privacy and third party data collection should be undertaken in this new age of electronic data collection and analysis [19]. Her concern, as seen simply in GPS data collection and analytics, was that:
The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society".
The good and the bad of this altered relationship may be seen in investigation of the 2013 Boston Marathon terrorist bombing in United States. The quick and wide distribution of information via social media and other multimedia systems aided in public engagement and the swift identification of the suspects, an association with possible motives and the apprehension of one suspect . But it also led to false leads and injudicious actions by some wrongly accusing individuals and groups of the crime. Some have come to question whether or not the untrained use of these interconnected, instrumented and unmediated social relations may have risks that outweigh the benefits.
These concerns are present in the discussions over the proper role of state security in legal monitoring and analysis of telecommunications transactional data, such as that over the proper role of the U.S. National Security Agency.
In sum, the benefits do and will far outweigh the risks when the rights and liberties in a democratic society are observed and protected. The Smart City offers us much. But we must not let it take that which makes us who we are. Difficult and concerted debate on these issues is needed.

References

1. https://www.forcepoint.com/cyber-edu/cybersecurity
2. https://economictimes.indiatimes.com/definition/cyber-security
3. https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
4. https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html
5. https://reolink.com/cyber-security-tips/
6. https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-fundamentals/top-20-security-awareness-tips-tricks/]
7. https://www.reveantivirus.com/en/computer-security-threats/cybercrime
8. https://cybersecurity.att.com/blogs/security-essentials/how-to-avoid-becoming-a-victim-of-cybercrime-5-tips