Cyber security challenges in Smart Cities: Safety, security and privacy

- Researched by Syed Kazim

**Main Idea**

The author, in the article, says that although there are numerous benefits of technology in the sectors of education, healthcare etc. and during emergency situations and disaster recovery, there are various disadvantages of Information and computing technologies. Thus, technical, administrative and financial factors must be weighed with the legal, political and social environment of the world (Elmaghraby, 2014).

**Context**

Smart cities face a huge challenge in today's world. When it comes to Intelligent transportation, public and private, has access to a web of interconnected data including financial, GPS, vehicle state, weather and traffic updates. The security concern can increase because this information can be misused.

GPS systems for location and store three types of information, event data recorders, Handsfree telephone and messaging and GPS navigation systems, which stores trip data.

There are various privacy issues. Locational data reveals a lot of information about a person’s life that he may not wish to reveal. Many people keep the originating address from their homes which might make it easier for burglary.

**Methods**

In order to find vulnerability and suggest solutions for IT security, Routine activity theory in Crime Control can be helpful. There are three elements that can promote any criminal activity. 1. A motivated offender, 2. A suitable target and 3. Absence of a capable guardian. Similarly, information security addresses three general domains of 1. prevention, 2. detection and 3. recovery from a security compromise which applies to information systems, computer network and the Internet (Elmaghraby, 2014).

**Conclusion**

Data privacy and security is going to be a huge concern at each stage of the process of turning cities into smart cities. Thus, we need to take some serious steps to ensure that this is controlled and avoided and that it does not allow the disadvantages to overcome the advantages.
Social Media & Privacy: A Facebook Case Study
- Researched by - Syed Kazim

Main Idea
Everyday, we upload a lot of personal information on Facebook and provide others an easy access to our data. Most Social Media users are unaware as to how their information is vulnerable to information-aggregation and reselling activities (Haumann., 2015). Social harassment, state intrusions, corporate surveillance and commodification and reduction in our ability to control how others may perceive us are some disadvantages of social media. The author also talks about how we can reclaim our privacy rights.

Context
Although Facebook’s privacy settings were very minimal at its founding, with users’ profiles fully visible to all other users on the Harvard University campus, the corporation gradually introduced some more settings (boyd, 2010). Through a series of rather complicated steps, one can limit what those in one’s network can see of your profile and how deeply Facebook and its advertising partners can change one’s profile for their benefit. Facebook’s current data policies indicate that they collect information on the content users upload as well as information related to the social networks users connect their profiles to. Facebook generates revenue by gathering and selling information related to and produced by their users to third-party advertisers.

In addition to commodification, there have been other consequences too. Firstly, it is possible to exploit the gaps in Facebook’s protection of its users’ personal information for social activities. Secondly, state agencies in the United States have collected information on Facebook users’ profiles, regardless of the privacy measures users may have implemented to protect their profiles. Furthermore, police and government officials have utilised Facebook profiles and histories to crack down on activities ranging from underage drinking to criticisms against ex-President George W. Bush. (Haumann., 2015)

Methods
It can be reduced using some steps. Firstly, Facebook, for example, currently forces its users to go through a series to opt out of privacy invasions for corporate profit. In contrast, an alternative, more privacy-friendly approach to Web 2.0 policies would offer users the choice to sell their information to third parties. we should create more groups that act as watchdogs against privacy violations. Thirdly, if we had social networking websites that were primarily created for social networking rather than the generation of corporate profits, our private information would not be viewed as virtual commodities. (Haumann., 2015)

Conclusion
Thus, we can conclude that social media can lead to serious privacy issues. The necessary steps must be taken to protect the personal information of the users. Personal information should not be used to generate ads and private information should not be viewed as virtual commodities.
Bibliography

