UDK 351.851:004
https://doi.org/10.18485/fb_ic4hs.2018.21

USAGE OF MODERN WIRELESS TECHNOLOGIES FOR CHILDREN'S PRESENCE AND LOCATION ANALYTICS AT EDUCATIONAL INSTITUTIONS - TECHNICAL, SECURITY AND LAW DILEMMAS

Milenko MARKOV[*], Nenad PUTNIK[**], Mladen MILOŠEVIĆ[***]

Abstract: One of the basic tasks in the management of educational institutions is to create and realize a security policy aimed at the protection and safety of students, staff and material resources. Formulating a security policy is a form of proactive action that minimizes risk materialization and prevents harmful consequences.

Information and communication technology (ICT) is used in the educational system for performing technical and administrative tasks and teaching activities. However, its range of use is broadening with a view to increasing students' safety. In recent years, for example, US educational institutions have been using software tools to monitor students on social networks in order to prevent electronic peer violence. It is necessary to monitor students effectively, not only in the virtual but also in the physical world, where the management of an educational institution is responsible for the safety of its students within the school perimeter.

In this paper, we will discuss the possibility of using various modern wireless technologies for presence and location calculation in order to increase the security of children (or people and goods in general) in open spaces and around public venues such as schools. The paper will discuss technical, ethical and legal challenges related to the implementation of such solutions.

We will consider GSM/GPS-based tracking, tracking of Wi-Fi and user devices such as mobile phones and tracking of BLE (Bluetooth Low Energy) or IEEE 802.15.4 enabled devices and passive and active tags in detail. In addition to a thorough technical overview and the working principle of these technologies, the paper will discuss the potential pitfalls

[*] BScEE, Technical Consultant at Hewlett Packard Enterprise, milenko.markov@hpe.com

[**] Associate Professor, PhD,University of Belgrade Faculty of Security Studies,Serbia, nputnik@fb.bg.ac.rs

[***] Associate Professor, PhD, University of Belgrade Faculty of Security Studies,milosevic@fb.bg.ac.rs

and drawbacks of the analyzed solutions such as battery life, range limitation, and precision.

In the era of Big Data, IoT and analytics, we would like to compare these technologies from the perspective of reliability of collected data, reporting and alarming systems, legal compliance (e.g. the latest GDPR legislation), security of collected data (risks related to data misuse) as well as other legal, ethical and security dilemmas about how justified it is to apply new technologies, which arise as a consequence of the need to protect personal privacy on the one and increase the safety of individuals, especially children, on the other hand.

Keywords: child security, risk prevention, presence/location analytics, ICT, GDPR legislation

1. INTRODUCTION

Contemporary information and communication technologies play a special role in the life of students, fulfilling their cognitive, value-related, cultural, and general socio-psychological needs.

But for parents, schools, and security experts, new technologies are viewed as a source of new potential problems because they require a broader scope of prevention measures and the addressing of security challenges, risks and threats in order to protect the students' psychophysical integrity, both in the physical and virtual space. (Milošević, Banović & Putnik, 2014; Kovačević & Nikolić, 2015). Consequently, Schwartz and associates recognize twelve types of technologies for school security, the most important of which are: access control, video surveillance, metal detectors, alarm systems, alerting and warning systems, and social networks monitoring (Schwartz et al., 2016: xii).

However, each technology is neutral in value; it can be useful, but also misused. In this paper, we examine the possibilities of implementing modern wireless technologies with the aim of controlling students' presence and determining their spatial location in educational institutions.

2. GPS-BASED TRACKING

GPS-based location services rely on the ability of the end-user device to receive a radio signal from multiple positioning satellites at the same time and calculate its coordinates based on the received signal. Since it is the most popular, we are going to discuss the Navstar GPS system. The Navstar GPS system (or simply GPS) is used by almost all currently available mobile devices such as mobile phones, tablets, car tracking systems, etc. (Norton, 1982).

The Navstar system consists of 24 main satellites, orbiting the Earth every 12 hours and sending a synchronized signal from each individual satellite. As the satellites are moving in different directions, users on the ground receive the signals at slightly different times. When at least four satellites get in touch with the receiver (or when at least four of them are visible to it), the receiver can calculate where the user is – often achieving one-meter accuracy for civilian use.

The calculated data represent geographical latitude, longitude, and altitude. Additionally, the end-user device can be an accurately synchronized precise time source. The Navstar GPS system is unidirectional in its essence, meaning that the end device (the receiver) is by definition able to calculate its location, but the system is not aware of the location of its receiver. In terms of its implementation, this arguably means that user location information should be communicated and processed by some other means, such as GSM, GPRS or a Wi-Fi network.

The fact that it is the most popular positioning system has influenced its price, features, and availability. The cost of receiving a module with an integrated antenna is relatively low (~ 5USD), its precision is high (~1m), it has a high percentage of coverage without additional infrastructure, and low power consumption, so battery-operated devices are commercially available. Major drawbacks of GPS-based systems are that they do not support indoor operation (there must be 'radio visibility' between the satellite and the receiving device), they are affected by weather conditions (cloudy weather), there is a delay in initial location calculation ('time to first fix'), and the system needs an additional channel of communication in order to determine client location (to share the client's location), like Wi-Fi or 3G/4G/LTE, etc.

3. WI-FI-BASED TRACKING

When discussing Wi-Fi-based tracking in this paper, we will focus on Wi-Fi as defined in the IEEE 802.11 standard, which provides wireless connectivity to mobile devices. In a typical environment, we would have a set of Wi-Fi access points (each of them covering approximately 100 square meters) that transmit the signal to and receive it from mobile devices. Wi-Fi access points have a wired connection to the rest of the network. Wi-Fi systems can be implemented to have both indoor and outdoor coverage.

Wi-Fi systems can be (and usually are) implemented in such a way that all access points act as a part of the same Wi-Fi infrastructure, so that end-users have seamless *roaming* between access points when moving around the object (hotel, shopping mall, school, warehouse, etc.). In order to achieve this, a Wi-Fi system must constantly measure the client's radio signal level, in order to determine the optimal access point that will provide the connection service to the specific client.

In order to uniquely represent themselves to the system, Wi-Fi devices (clients) use a 48-bit long unique identifier called a MAC address. The same MAC address is usually used even if the client is not connected to the system (in some cases there is a process called randomization, that randomizes the MAC address of a non-connected client). When this information (the MAC address) is combined with the signal level of each station, two pieces of information can be extracted: a) client presence – if (and when) the client is seen in the range (area around) of an access point and b) approximate location of the client within the infrastructure.

The signal level of a specific client is usually streamed from the wireless infrastructure using a RTLS (real time location service) protocol to the location engine that is aware of the physical infrastructure, so that exact presence and location information can be

extracted. Presence information is extracted from the fact that AP is reporting that it "sees" the specific client with the given signal level. Combining the presence information from at least three sources (access points) using triangulation, location information can be extracted. It can be provided in absolute coordinates (latitude, longitude, floor (level)). Usually, the timestamp (exact time) of the provided data is also provided (*Aruba Analytics and Location Engine API Guide*, 2018).

The Wi-Fi tracking system provides relatively inaccurate position data (approximately 5 meters, depending on the implementation) but exact presence data. These systems can be implemented by using the existing infrastructure (if the infrastructure supports a RTLS service) and they do not require separate end-user devices (existing mobile phone/terminals could be used). There are also dedicated battery-operated "Wi-Fi" tags. Wi-Fi tracking systems can be used both indoors and outdoors. Since the position is calculated by the system and not by the end-user device, their location is easily shared by other components of the infrastructure.

4. BLE BEACONS AND MICRO-LOCATION SERVICES

As previously discussed, GPS systems rely on the radio visibility between the receiver and the satellite, and therefore have limited operation indoors. In order to overcome this limitation, the industry is working hard on a solution for this problem.

One of the approaches is to use BLE beacons to provide location services to clients. BLE (Bluetooth Low Energy) or Bluetooth 4.x technology is slightly different from previous Bluetooth versions, at least as far as the following is concerned: a) it does not require 'pairing' so some information can be exchanged between devices without previous negotiation ('connectionless communication') b) BLE is of such low power consumption that the battery-powered beacon emitter can last for years without battery replacement.

A BLE beacon is a device that constantly emits the same radio message at a constant rate, usually once per second. This message consists of the unique beacon identifier and, optionally, the battery level of the beacon. On the client's side (usually a mobile device), there is a receiving process, which accepts beacon messages, measures the radio level of the received signal, and sends this information (via Wi-Fi or 3G/4G/LTE) to a location server that calculates and returns the client's position. In that way, both the location server and the client are aware of the client's location.

BLE beacon systems can be used for both presence (e.g. student presence in the class) and location services (e.g. indoor navigation). Having been developed with GPS's limitations in mind, it provides location information in such a way that seamless switchover from GPS to an indoor service is possible (e.g. it uses GPS while the client is outdoors and switches over to the beacon positioning system when the client does not have GPS coverage).

BLE beacon systems, if implemented appropriately, have high location accuracy (1m). They require clients (e.g. smart phones) with a specific service/application that supports the BLE positioning service. They work in both indoor and outdoor environments and are conservative in energy use. The BLE beacon positioning system requires specific

infrastructure (beacons and a location processor) in order to provide location services. By its nature, the location information is available to both the clients and the system (*Google Beacon Project*, https://developers.google.com/beacons/; *Aruba Location Services*, https://www.arubanetworks.com/products/location-services/).

5. PASSIVE AND ACTIVE TAGS AND ID CARDS (RFIDS).

In this paper, we will classify them in the same group although they are significantly different from the perspective of the technology used. The concept behind them is that, by using active 'gates' (doors or passages), the system controls access to specific regions, so that the information about someone's presence can also be extracted. For example, by using a passive RF tag (a tag that does not have a power source or a battery but would rather use radio-inducted power in order to communicate with the gate), the system could control access to a specific region of an object. As every RF tag could have a unique identifier, by pulling information from the gate, the system could determine information such as presence, time and a people count for every specific region of an object.

These systems cannot provide location but provide presence information. This information is available to the system only (in the case of passive tags) and to both the system and the client (in the case of active tags). Their power consumption is relatively low, but the system requires dedicated gates and door control. This creates additional challenges as the system must address other safety requirements (e.g. the behavior of doors in case of fire or another emergency).

6. CONCLUSION

Cases of peer violence outside schools and the continuous increase in crime rates among young people clearly point to the need for students to be monitored with a view to preventing unfortunate events and their consequences. Every type of surveillance and control suggests a number of other questions and dilemmas – technical (what logical and technical means and tools to use to control access and successfully ensure prevention) and ethical (the necessity of monitoring, application limitations, privacy rights), but also legal, psychological, etc. (Putnik & Milošević, 2016).

As with many other technologies, there is no ideal solution for all implementations. For example, the GPS system provides high accuracy and a low cost of implementation, but does not provide indoor operation. On the other hand, Wi-Fi tracking could provide almost no cost of operation for indoor coverage (as the system already provides a connectivity service), but has low accuracy. BLE beacons-based systems offer high precision but bring additional costs of operation. There is high probability that RFID systems are already being implemented, but they are usually isolated from other systems and are not used for presence/location services.

Preventive action is neither simple nor is it possible is only logical and technical means are employed. The implementation of modern wireless technologies with the aim of access control can certainly bring results. However, we believe that a wider approach must be taken to combat peer violence and prevent accidents outside the school perimeter, which

would include not only logical and technical tools, but also the harmonization of national legislation with international standards in this field, consultations with ethics experts, as well as the education of students, parents, teachers and non-teaching school staff.

However, the usage of modern wireless technologies for children's presence and location analytics introduces numerous legal issues, especially those concerning privacy rights. The need for improving national, local or corporate security (or, in this case – the security of educational institutions) often violates the inalienable human right to privacy. The balance between human rights and security is hard to achieve and maintain, but a lack of this balance brings serious concerns. In the light of the General Data Protection Regulation (GDPR), which has finally been approved by the EU Parliament on 14 April 2016 (after four years of preparation and debate) and came into force on 25 May 2018, those concerns look even greater (Directive 95/46/EC). The GDPR replaced the Data Protection Directive 95/46/EC and it can be seen as a step forward in the protection of the rights to privacy (Blackmer, 2016). The regulation has established rules which are designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy and change the way all institutions and organisations deal with privacy issues. The GDPR norms are a challenge for every organisation, including schools, because it is not an easy task to comply with the regulation and meet its demands. The GDPR rules will present serious hurdles in the usage of contemporary technologies while the need for balance in the relation between security and law is increasing and becoming more of a challenge.

The creation and development of ethical standards and principles concerning the use of information and communication technology for security purposes is of great importance. Questions of privacy, democracy, property rights, and others can be included in such issues. The establishment and development of these norms and principles is of paramount importance because they could find application in all those cases of security violations that do not violate the law, but are perceived as socially unacceptable behavior. In the historical sense, unfortunately, the field of computer ethics has been reactive in relation to technology – computer ethics have followed technological development and only subsequently reacted to it (Johnson, 2006).

The challenge faced by the educational institutions that apply or intend to implement measures of control over their students include an approach to solving the problems of crime, violence and other abuses, and the issue of preventing the application of technical measures and resources and strategies from eroding the confidence of students in the institution.

The primary and also the best protection against peer violence and other forms of bullying or crime is – knowledge. In the Enlightenment, the motto was *sapere aude* (dare to know). This term implied that if the detection of something is not unequivocally dangerous, then at least it presents a challenge and requires great work. This maxim is still valid today and is applicable to the process of acquiring knowledge in the sphere of information and communication technologies. The constant growth of innovations in the field of technology and virtual communications requires continuous education on both their purposefulness and safe use.

7. REFERENCES

Aruba Analytics and Location Engine API Guide. (2018). https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/30756/Default.aspx, retrieved 03/09/2018

Aruba Location Services, https://www.arubanetworks.com/products/location-services/, retrieved 03/09/2018

Blackmer, W.S. (2016). GDPR: *Getting Ready for the New EU General Data Protection Regulation*, Information Law Group, InfoLawGroup LLP.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 1995.

Džonson, D. (2006). *Kompjuterska etika*. Beograd: Službeni glasnik.

Google Beacon Project, https://developers.google.com/beacons, retrieved 03/09/2018

Kovačević, A. & Nikolić, D. (2015). Automatic Detection of Cyberbullying to Make Internet a Safer Environment. In: Cruz-Cunha, M.M. & Portela, I.M. (Eds.) (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. Hershey: International Science Reference, pp. 277-290.

Milošević, M., Banović, B., Putnik, N. (2014). Nasilje i drugi oblici ugrožavanja bezbednosti u obrazovno-vaspitnim ustanovama i mogućnosti krivičnopravne i prekršajne zaštite. U: Popović Ćitić, B., Đurić, S. (urednici), *Modeli unapređenja bezbednosti u obrazovnovaspitnim ustanovama*. (str. 37-55). Beograd: Fakultet bezbednosti

Norton, J.H. (1982). Navstar Global Positioning System, *International Hydrographie Review*, Monaco, LIX (1), pp. 23-30

Putnik, N., Milošević, M. (2016). Smernice za izradu politike bezbednosti informaciono-komunikacionih resursa i njihovih korisnika u obrazovno-vaspitnom sistemu. U: Popović Ćitić, B., Lipovac, M. (urednici), *Bezbednost u obrazovno-vaspitnim ustanovama: osnovna načela, principi, protokoli, procedure i sredstva* (str. 97-116). Beograd: Fakultet bezbednosti

Schwartz, H.L. et al. (2016). *The Role of Technology in Improving K-12 School Safety*. Santa Monica: RAND Corporation