Varna interoperabilna infrastruktura za pametna mesta
/
Secure Interoperability Infrastructure for Smart Cities

Blaž Ivanc
Institut »Jožef Stefan«
Jamova cesta 39
1000 Ljubljana
+386 41 304 013
blaz.ivanc@ijs.si

Dušan Gabrijelčič
Institut »Jožef Stefan«
Jamova cesta 39
1000 Ljubljana
+386 1 477 3757
dusan@e5.ijs.si

Borka Jerman Blažič
Institut »Jožef Stefan«
Jamova cesta 39
1000 Ljubljana
+386 1 477 3408
borka@e5.ijs.si

POVZETEK

V tem prispevku opisujemo vidike varnosti in zasebnosti interoperabilne infrastrukture za organizacije javne varnosti v povezavi s pametnimi mesti.

ABSTRACT

In this contribution we describe security and privacy aspects of the data interoperability infrastructure for public safety organizations in relation to smart cities.

1. UVOD

Izredni dogodki z vplivi na varnost prebivalcev bodo čedalje pogostejša stalnica v večjih mestih prihodnosti in eden izmed ključnih problemov [1]. Koncept pametnega mesta odgovarja na probleme modernih mest, med katerimi je vprašanje varnosti osrednjega pomena [2]. Koncept pametnega mesta omogoča nadzor ključne infrastrukture in nadzira varnostne vidike z namenom zagotovitve visoke varnosti prebivalcem [3].

Z vidika zagotavljanja javne varnosti bodo pametna mesta z množico senzorjev zagotavljala številne prednosti. Zbiranje prej nedosegljivih podatkov, deljenje in ponovna uporaba ter sprejemanje odločitev na podlagi podatkov, pridobljenih v realnem času, so zgolj nekatere od njih.

Službe javne varnosti, kamor med drugimi spadajo policija, nujna medicinska pomoč, civilna zaščita, protiteroristične enote in drugo, so in bodo ključnega pomena pri zagotavljanju varnosti. Med omenjenimi službami še posebej prevladujejo potrebe po dostopu do podatkovnih baz, senzornih sistemov in kamer. S konceptom pametnih mest bodo pridobljene številne nove prednosti. Te prednosti bodo v primeru odziva ob nesreči oziroma incidentu vplivale na učinkovitejši in bolj kakovosten odziv. To pa se bo zgodilo, če se bo zagotovila varna in dovolj prilagodljiva infrastruktura za povezovanje različnih virov podatkov.

V tem prispevku je predlagan koncept interoperabilne infrastrukture, kakršna se razvija v okviru projekta REDIRNET, s poudarkom na zagotavljanju informacijske varnosti kot ene od nujno potrebnih sestavin za zagotavljanje nemotenega delovanja ključne infrastrukture pametnega mesta, varovanja prebivalcev in ne nazadnje njihove zasebnosti.

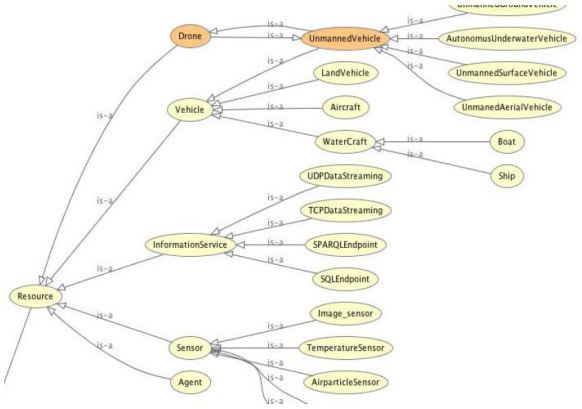
2. VARNA INTEROPERABILNA INFRASTRUKTURA

Kot smo že omenili v uvodu, je naš predlog razvoj varne infrastrukture za izmenjavo meritev, podatkov in informacij med službami javne varnosti. Namen takšne infrastrukture je povezati različne senzorne sisteme, kar bo razširilo zmogljivosti komandno nadzornih zmogljivosti omenjenih služb. S tem bosta zagotovljeni večja učinkovitost in kakovost odziva ob incidentu ter kasnejših analiz. Rešitev ima tudi stroškovni učinek.

Interoperabilna infrastruktura je decentralizirano ogrodje za interoperabilnost sistemov. Infrastruktura temelji na javnem metapodatkovnem prehodu, ki bo nadzorovan s strani posameznih lastnikov podatkovnih virov preko strokovnega družbenega omrežja. To bo omogočilo povezovanje partnerskih organizacij glede na njihove želje in operativne potrebe, hkrati pa omogočilo določanje obsega takšne interoperabilnosti. Podpora s semantičnimi spletnimi metodami bo v pomoč za vzpostavitev takšnega povezovanja.

Obravnavana infrastruktura bo službam javne varnosti zagotovila medsebojno povezovanje komunikacijskih sistemov in izmenjavo informacij. Takšna komunikacijska rešitev bo omogočila izmenjavo in deljenje podatkov, slik, videa, CCTV in informacij z oddaljenih senzorjev.

Namenska ontologija bo zagotovila temeljne koncepte in podatkovne strukture podatkovnega modela platforme. Njen namen je prevzeti vlogo pri odkrivanju razpoložljivih virov določene organizacije in podpirati semantično interoperabilnost med organizacijami z različnimi podatkovnimi viri in informacijskimi sistemi. Slika 1 prikazuje del osnutka osrednje ontologije v okviru projekta REDIRNET, slika 2 pa rezultate poizvedbe na podlagi testnega primera varnostnega incidenta.



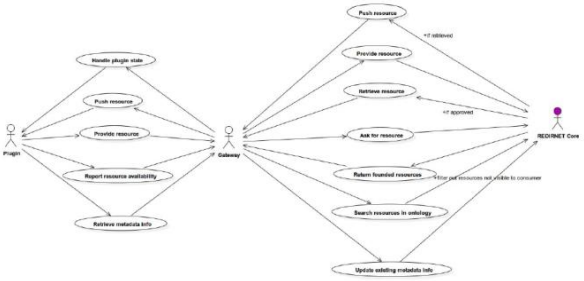
Slika 1. Del osrednje ontologije.

agency	operator	resource	capability	event
BelgianPolice	BrabantWallon_Command	CCTV_Waterloo_Lion13	video_stream	WaterlooLionFire
Waterloo_Police	BrabantWallon_Command	CCTV_Waterloo_Lion13	video_stream	WaterlooLionFire
BelgianPolice	BrabantWallon_Command	Hero4	video_stream	WaterlooLionFire
Waterloo_Police	BrabantWallon_Command	Hero4	video_stream	WaterlooLionFire

Slika 2. Rezultati poizvedbe.

Organizacije javne varnosti in tudi druge poslovne entitete bodo imele občutne koristi z dostopom do podatkovnih virov partnerskih organizacij. Za ta namen se bo treba registrirati v strokovno družbeno omrežje in preko ontološkega iskalnika poiskati želene podatkovne vire ter vzpostaviti partnersko povezavo.

V fazi integracije pri končnem uporabniku je treba prenesti izvirno kodo prehoda in ustvariti virtualnega uporabniškega agenta za podatkovne vire. Slednji bo implementiral abstrakten vmesnik, ki bo služil kot vtičnik za prehod, ki bo omogočal komunikacijo med podatkovnimi viri in infrastrukturo oziroma njenim sistemom.



Slika 3. Obratovalni model prehoda.

Prehod je vmesni sloj med jedrom sistema in vtičniki. Obratovalni model prehoda ima z vidika delovanja dva načina – porabniški in ponudniški.

3. ZAHTEVE VARNOSTI IN ZASEBNOSTI PAMETNIH MEST

Informacijska tehnologija, glavni pospeševalnik koncepta pametnih mest, ustvarja številne ekonomske in družbene priložnosti. S tem pa prinaša tudi dodatne izzive na področju varnosti in zasebnosti. Z vidika zasebnosti lahko, na primer, lokacijski podatki, vezani na posameznika, predstavljajo velik poseg v zasebnost, če se ti podatki analizirajo in predstavijo v različnih kontekstih [4]. Avtorji v [3] predstavijo varnost in zasebnost kot eno od treh dimenzij IKT-infrastrukture pametnih mest. Naštejejo naslednje izzive: grožnje s strani hekerjev in vsiljivcev, grožnje s strani zlonamerne programske kode, varovanje osebnih podatkov ter visoke stroške varnostnih aplikacij in rešitev.

Eden izmed ključnih dejavnikov, s katerimi se bodo soočila pametna mesta, je razvoj zaupanja vrednega ogrodja, ki bo zagotavljal storitve brez prikritih, škodljivih namenov [5]. Sem lahko uvrstimo kršitve varnosti in zasebnosti, ki se nanašajo na osebne podatke prebivalcev, prepoznavanje skritih vzorcev in izvajanje drugih analiz podatkov, kot so vzorci uporabe storitev in podobno. Nadalje se zastavljajo vprašanja o pravilnosti zaznanih podatkov, skladnosti obdelave podatkov z zakonodajo, dostopu do podatkov in kontroli nad deljenjem le-teh. Ta in še mnoga druga vprašanja zadevajo ponudnike storitev in prebivalce.

Danes se med drugim srečujemo s sledečimi problemi, za katere ne sme biti prostora pri razvoju interoperabilnih infrastruktur pametnih mest:

- Varnostne pomanjkljivosti pri zasnovi sistemov, ki ustvarjajo mnoge, še neznane ranljivosti.
- Nameščanje že kompromitirane informacijsko-komunikacijske opreme.
- Pomanjkljiva znanja na strateški in koordinacijski ravni upravljanja z informacijsko varnostjo.

Informacijska varnost je temelj zagotavljanja zasebnosti. V povezavi z vseprisotnim internetom znotraj koncepta pametnih mest se tako srečujemo s številnimi informacijskimi komponentami in njihovimi vmesniki, katerih površna varnostna zasnova odpira vrata posegom v zasebnost.

V pobudi predlagamo uporabo kompetenc na področju modeliranja napadov in vzpostavitev ustreznega okolja z naborom temu primernega kadra za izvajanje varnostnih presoj IK-tehnologij, ki bodo imele ključno vlogo v pametnih mestih z vidika zagotavljanja varne interoperabilnosti.

Modeliranje napadov je eden izmed najpomembnejših načinov, kako najti šibke točke. Pomembno je za dvig zavedanja o realni situaciji, ki se nam lahko zgodi. Modeliranje napadov pripomore k temu, da se pripravimo na možne scenarije, ki jih v praksi ne želimo preizkusiti. Če se nanje pripravimo, lahko ustrezno zaščitimo sistem, da do dejanskega incidenta ne pride [6].

Predpogoj za modeliranje napadov je zagotoviti okolje, ki obravnava varnostna vprašanja z vidika agentov grožnje in spremlja ter analizira nove tehnike napadov. Slednje pomeni, da je treba zagotoviti dostop do ustreznih laboratorijskih sistemov.

4. PROJEKT REDIRNET

V okviru EU FP7 projekta REDIRNET[1] nastaja panevropska platforma, namenjena izmenjavi meritev, podatkov in informacij med službami javne varnosti. V projektu sodeluje devet partnerjev iz sedmih držav. Med partnerji je tudi Laboratorij za odprte sisteme in mreže na Institutu »Jožef Stefan«. Konzorcij sestavljajo še: Združenje strokovnjakov s področja informacijskih in komunikacijskih rešitev za službe javne varnosti (British APCO), razvijalci profesionalnih komunikacijskih rešitev in druge raziskovalne institucije.

Ključni cilji projekta so:

- Vzpostavitev registra interoperabilnih problemov in potreb s strani končnih uporabnikov.
- Priprava interoperabilnega ogrodja, skladnega s postopkovnimi in tehnološkimi standardi.
- Zagon interoperabilne platforme.
- Integracija prvih končnih uporabnikov.
- Vzpostavitev vseevropskega sodelovanja in zavedanja o projektu REDIRNET s ciljem standardizacije koncepta.

Poleg partnerjev v projektu Laboratorij za odprte sisteme in mreže na Institutu "Jožef Stefan" sodeluje z Generalno policijsko upravo ter Upravo za zaščito in reševanje. Namen sodelovanja je prepoznati potrebe končnih uporabnikov in s pomočjo raziskav poiskati ustrezne rešitve.

Na tem mestu velja pozvati industrijske partnerje v Sloveniji, naj aktivno sodelujejo pri pametni specializaciji z možnostjo smiselne uporabe rezultatov dela v projektu.

[1] Spletna stran projekta: www.redirnet.eu

5. ZAKLJUČEK

Varna interoperabilna infrastruktura bo pomembno orodje za službe javne varnosti pri zahtevni nalogi zagotavljanja varnosti pametnih mest in njihovih prebivalcev. Informacijska varnost bo imela ključno vlogo v konceptu pametnih mest tako z vidika neprekinjenega delovanja ključnih sistemov kot tudi z vidika zasebnosti.

6. REFERENCES

[1] Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., Portugali, Y. 2012. Smart cities of the future. *Eur. Phys. J. Special Topics* 214, 481–518.

[2] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D. 2014. Sensing as a Service Model for Smart Cities Supported by Internet of Things. Trans. *Emerging Tel. Tech.*, 1-12.

[3] Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., Scholl, H. J. 2012. Understanding Smart Cities: *An Integrative Framework. 45th Hawaii International Conference on System Sciences*, 2289-2297.

[4] Elmaghraby, A. S., Losavio, M. M. 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research* 5, 491-497.

[5] Khan, Z., Pervez, Z., Ghafoor, A. 2014. Towards cloud basedsmart cities data security and privacy management. *International Workshop on Smart City Cloud*, (London, 8-11 December 2014). IEEE, London, UK, 806-811.

[6] Ivanc, B. Klobučar, T. 2014. Attack modeling in the critical infrastructure. *Elektrotehniški vestnik*, 81, 285-292.

Rešitve Iskratela za pametno mesto in skupnost / Smart City and Community Solutions by Iskratel

Ana Robnik
Iskratel, d.o.o., Kranj
Ljubljanska c. 24a
SI-4000 Kranj
+38642072686
Ana.Robnik@iskratel.si

Gorazd Novak
Iskratel, d.o.o., Kranj
Ljubljanska c. 24a
SI-4000 Kranj
+38642072382
Gorazd.Novak@iskratel.si

Boštjan Mešič
Iskratel, d.o.o., Kranj
Ljubljanska c. 24a
SI-4000 Kranj
+38642072382
Bostjan.Mesic@iskratel.si

POVZETEK

Podjetje Iskratel, d.o.o., Kranj je s svojo lastno blagovno znamko, lastnim razvojem in lastno proizvodnjo tradicionalno prisoten na področju infokomunikacijskih omrežij, storitev in aplikacij. V skladu s strateškimi usmeritvami podjetja ponuja - in bo tudi v bodoče nadgrajevalo - napredne rešitve s področja železniškega in cestnega prometa, javne varosti in energetike za javni in industrijske sektorje.

Usmerja se tudi na področje zahtevnejših infrastrukturnih projektov, kjer je skupaj s partnerji in podizvajalci ponudnik celovite rešitve s področja prometa, javne varnosti, širokopasovnih omrežij in informacijske infrastrukture, vse bolj pa se usmerja tudi na področje energetike. Vsa zgoraj omenjena področja so tudi pomembna domenska področja pametnih mest, ki vključujejo poleg najprimernejše izbranih rešitev tudi celovit pristop k izvedbi tako zahtevnih projektov.

ABSTRACT

The company Iskratel, d.o.o., Kranj, with its own brand, its own development and its own production, is traditionally present in the area of info-communication networks, services and applications. In accordance with its strategic guidelines, the company offers—and will continue developing—advanced solutions in the fields of rail and road transport, public safety, and energy for public and industrial sectors.

It focuses on complex infrastructure projects and offers, in cooperation with its partners and subcontractors, comprehensive solutions for transport, public safety, broadband networks and IT infrastructure, increasingly focusing on the energy sector as well. All the above-mentioned areas are also important domains of Smart Cities, which include not only the most appropriate solutions, but a comprehensive approach to the implementation of such complex projects.

1. INTRODUCTION

Iskratel, d.o.o., Kranj is a high-tech enterprise and the leading European manufacturer and provider of info-communication solutions in the Central European area. It stands out with its own research and development department, production, 65 years of experience and local presence in over 30 countries, and with more than 70% of exports in 2014. Iskratel leverages solution development and ICT expertise in delivering integrated solutions across telco, transportation, public safety and energy industries. Its solutions help people and communities, ensure safety, increase efficiency and business innovation. In collaboration with its partners, Iskratel provides a comprehensive project approach: from consulting, design, equipment supply and implementing complete solutions to training, maintenance and after-sales support. This approach is also used in infrastructure projects in the above fields, which are important components of Smart Cities and Communities.

Iskratel is developing its Smart City and Community solution based on the Safe City comprehensive solution. Broadband network and IT infrastructure services are added to that solution, ensuring advanced user experience. It enters the transport domain with comprehensive solutions for rail and road transport, which include equipping stations and stops, adding to them solutions for the energy efficiency of the Smart City.

2. ISKRATEL SOLUTIONS IN THE AREA OF SMART CITY AND COMMUNITY

2.1 Safe City

2.1.1 Safe City - a step-by-step comprehensive approach

Ensuring the safety and security of citizens in smart cities is one of the key challenges for governments, mayors and policy makers. “Safe City” is an open and reliable solution that provides a variety of integrated operational services for a highly complex operational chain and effective deployment, not only at the level of an individual municipality, but also allowing integration into a single federal structure. This solution also supports the smart integration of services for safety and security at the city level into federal infrastructure. With this approach, local characteristics and global trends are equally important; they slightly differ on our markets (i.e., the European market and the market of Common Independent Countries - CIS, especially Russia).

Providing a large-scale centralized system for all the above-mentioned areas in one step is unrealistic; there are usually considerable problems with the budget and the lack of appropriately trained and experienced staff. As a result of such an approach, very often the autonomous, not-interoperable systems are introduced, each of which essentially solves private, local problems.

City authorities develop and introduce urban mission-critical/monitoring centres, centralized urban systems like 911/112, alarm and notification systems and evacuation in the city, secure telecommunications/communications systems. All the above-mentioned systems incorporate centrally-managed areas of life in the urban environment such as:

- City management and its administration;
- Law enforcement and its support for policy features;