Arhitektura in varnost interneta stvari

Conference Paper · June 2014

CITATION
1

READS
571

2 authors:

Muhamed Turkanović
University of Maribor
39 PUBLICATIONS **1,198** CITATIONS
SEE PROFILE

Marko Hölbl
University of Maribor
63 PUBLICATIONS **1,717** CITATIONS
SEE PROFILE

ARHITEKTURA IN VARNOST INTERNETA STVARI

Muhamed Turkanović [a], Marko Hölbl [b]

[a] CEI-Systems OG, Fakulteta za elektrotehniko računalništvo in informatiko, Univerza v Mariboru, Maribor, Slovenija
[b] Fakulteta za elektrotehniko računalništvo in informatiko, Univerza v Mariboru, Maribor, Slovenija

[a] m.turkanovic@cei-systems.eu, [b] marko.holbl@um.si

Povzetek: *Zaradi hitre evolucije tehnologije smo vedno bolj obdani z vseprisotno inteligentnimi, med seboj povezanimi napravami, ki nam ponujajo nov vidik našega vsakdanjega življenja. Koncept Interneta stvari (angl. Internet of Things) je uporaba standardiziranih komunikacijskih protokolov in omrežne infrastrukture z namenom razširjanja navidezno prostorskih meja interneta na heterogene naprave, ki imajo sposobnost samostojne konfiguracije in medsebojnega sodelovanja. Kot končni uporabniki bomo prav tako del obogatenega internetnega prostora (tj. internet stvari). Zaradi vseobsežne in vsesplošne medsebojne povezanosti različnih naprav ali »stvari« se poraja vprašanje varnosti in zasebnosti. V prispevku bomo obravnavali osnovne principe in se osredotočili na arhitekturo in varnost Interneta stvari.*

1. UVOD

Internet stvari (angl. Internet of Things) je pojem, ki predstavlja nov pojav in se lahko karakterizira kot steber interneta prihodnosti. Zaradi hitre evolucije tehnologije smo vedno bolj obdani z vseprisotno inteligentnimi, med seboj povezanimi napravami (npr. pametni telefoni, pametne hiše, RFID, senzorji, itd.), ki nam ponujajo nov vidik našega vsakdanjega življenja.

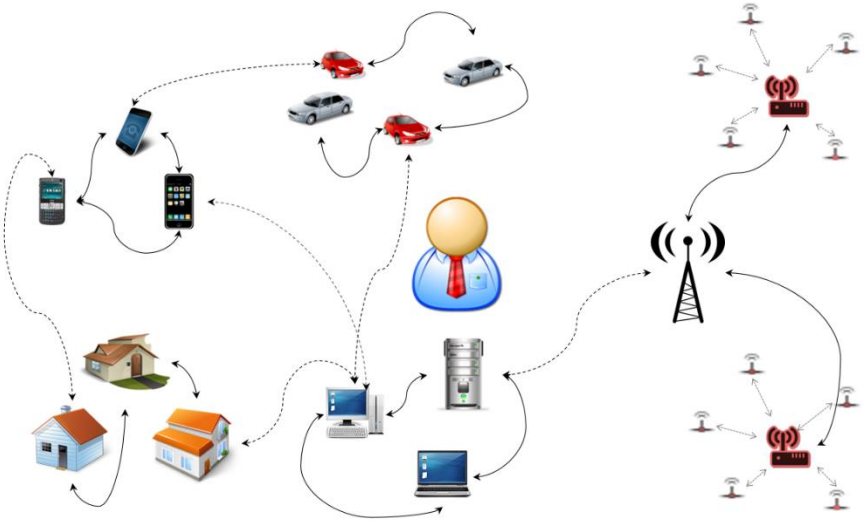
Čeprav bi se naj znani Moorov zakon iz leta 1965, ki trdi, da se bo število tranzistorjev na kvadratnem palcu vsako poldrugo leto podvojilo že ustavil ali se bo kmalu, se s tem tehnološka evolucija ni zaustavila [1]. Razvoj osredotočen na čisto zmogljivost se je prestavil na razvoj osredotočen na integracijo, povezljivost in multifunkcionalnost. Priča smo mobilnim napravam, ki so obogatene z različnimi senzorji (npr. kompas, mikrofon, žiroskop, GPS, itd.), hkrati pa imajo na voljo paleto tehnologij za povezovanje kot npr. WiFi, GPRS, Bluetooth, LTE, itd. Stroški takšnih tehnologij so hkrati padli na nivo, da dostopnost do le teh eksponentno raste. Mobilne naprave niso edine naprave, saj je vedno več raznolikih naprav, ki so med seboj povezane in vključene v internet, kot npr. pametne ure (npr. I'm Watch), pametna očala (npr. Google Glass), pametna kolesa (npr. FlyKly Smart Wheel), pametni senzorji ali števci (npr. oddaljeno odčitavanje porabe elektrike), RFID, itd. Ker so to vse naprave, katerim je skupna povezljivost, govorimo o konceptu internetu stvari. Kot končni uporabniki bomo prav tako del obogatenega internetnega prostora (tj. internet stvari), kjer bomo imeli možnost povezati se s slehernim udeležencem, tj. napravo in sodelovati na nivoju prejemanja ali oddajanja informacij.

Zaradi vseobsežne in vsesplošne medsebojne povezanosti različnih naprav ali »stvari« se poraja vprašanje varnosti in zasebnosti. V prispevku bomo obravnavali osnovne principe Interneta stvari in

se osredotočili na varnost znotraj le tega. Pogledali si bomo arhitekturo in infrastrukturo različnih skupin znotraj interneta stvari in specifičnosti le teh. Podrobneje bomo predstavili skupino brezžičnih senzorskih omrežij.

2. INTERNET STVARI

Koncept Interneta stvari je uporaba standardiziranih komunikacijskih protokolov in omrežne infrastrukture z namenom razširjanja navidezno prostorskih meja interneta na heterogene naprave, ki imajo sposobnost samostojne konfiguracije in medsebojnega sodelovanja (Slika 1) [2].



Slika 1: Predstavitev koncepta Interneta stvari.

Kevin Ashton, britanski inženir in oče besedne zveze internet stvari je s tem poimenovanjem želel opisati katero koli napravo ali bitje, ki je na neposreden ali posreden način povezana v Internet [3]. Podjetje Ericsson je leta 2010 napovedalo, da bo leta 2020 znotraj interneta stvari preko 50 milijard »stvari«. Priložnosti in potenciali znotraj Interneta stvari so zelo veliki in globalni trg se že nekaj let osredotoča nanje. Vse velike korporacije so svojo vizijo prihodnosti prilagodile konceptu Interneta stvari (tj. Intel, Ericsson, Google, Cisco, Microsoft, itd.) [3]. Prav tako se na nivoju držav in mednarodnih organizacij zavedajo teh priložnosti in tudi potreb po strukturiranju in standardizaciji (npr. Horizon 2020) [4].

3. ARHITEKTURA

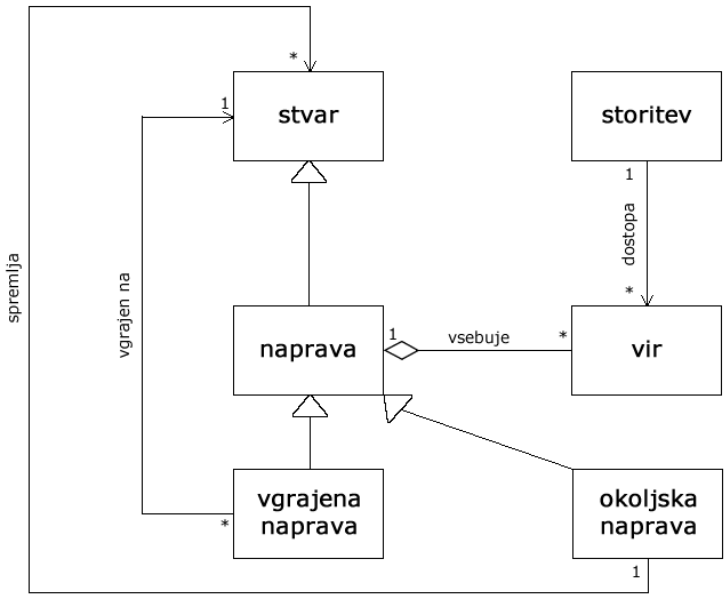
Vsem definicijam Interneta stvari je skupna integracija fizičnega sveta z virtualnim svetom interneta. Obstajajo subjekti znotraj fizičnega sveta, ki jih imenujemo subjekti interesa (angl. entities of interest) in le te želimo spremljati, zasledovati in z njimi stopiti v interakcijo (npr. hiša, avto, kolo, žival, paleta, embalaža, pašnik, gozd, itd.). Subjekti interesa dejansko predstavljajo »stvari« znotraj Interneta stvari.

Na osnovnem nivoju so za spremljanje in interakcijo med subjekti (tj. stvarmi) in med internetom, potrebne komunikacijske in senzorske naprave (npr. senzorji, aktuatorji, RFID, oddajniki, sprejemniki, itd.). Te naprave so lahko vgrajene v same subjekte (tj. telefone, hiše, itd.), ki skupaj

tvorijo pametne naprave ali pa so le nameščene v okolje, ki ga želimo slediti ali opazovati (npr. pašnik, gozd, žival, itd.) [5].

Subjekti gostijo *vire* (angl. resources), ki so atributi subjektov zaradi katerih jih sploh želimo spremljati ali biti z njimi v interakciji. Viri so računalniški elementi, ki zagotavljajo tehnično povezavo do samih subjektov oziroma, nudijo informacijo o samem subjektu ali stvari (npr. identifikator subjekta, zaznane podatke subjekta, itd.). Dostop do virov iz zunanjega sveta (tj. interneta) se izvrši s pomočjo *storitev* (angl. services), ki podpirajo storitveno orientirano arhitekturo (SOA). Subjekti lahko nudijo neposreden vmesnik za storitve (npr. pametni telefoni) ali posredno preko namestnika (angl. proxy) oziroma, prehodne točke (angl. gateway) omrežja (npr. brezžično senzorsko omrežje). Storitve lahko delujejo na principu REST, SOAP ali bolj specifičnih DPWS (Devices Profile for Web Services) [6, 7].

Razmerje med stvarmi, napravami, viri in storitvami je prikazano na sliki 2. Subjekt interesa ali v kontekstu Interneta stvari »stvar« se lahko spremlja s strani naprave v okolju. V tem primeru je subjekt embalaža, ki potuje skozi proizvodnjo, naprava iz okolja pa je senzor montiran na vhodu. Prav tako je lahko na sam subjekt interesa vgrajena ali pritrjena naprava. V tem primeru je na embalažo pritrjena RFID značka (angl. tag).



Slika 2: Razmerje med stvarmi, napravami, viri in storitvami [5].

3.1. Protokoli

Subjekti oziroma naprave morajo imeti možnost medsebojne komunikacije. Za ta namen se uporabljajo različni protokoli. Obstajajo tri relacije znotraj Interneta stvari, ki so ključnega pomena za delovanje komunikacije med »stvarmi«. Te relacije so naprava do naprave D2D (angl. device-to-device), naprava do strežnika D2S (angl. device-to-server) in strežnik do strežnika ali drugih končnih naprav S2S (angl. server-to-server) [8].

Protokoli, ki se uporabljajo pri relaciji D2D so DDS (angl. Data Distribution Service) protokoli, ki predstavljajo vodilo za integracijo inteligentnih strojev. Je podatkovno naravnan vmesnik, ki lahko učinkovito dostavi milijone sporočil na sekundo k več hkratnim sprejemnikom. Glavni namen DDS protokolov je povezovanje naprav z drugimi napravami. Protokoli, ki se uporabljajo pri relaciji D2S

so MQTT (angl. Message Queue Telemetry Transport) in XMPP (angl. Extensible Messaging and Presence Protocol). Cilj MQTT protokolov je zbrati podatke iz številnih naprav (npr. senzorji, RFID, pametni telefoni, itd.) in jih prenesti k IT infrastrukturi, tj. strežnikom, za analizo. XMPP protokol je najboljši za povezavo med napravami in ljudmi, kot v primeru D2S, saj so ljudje povezani s strežniki (npr. avtomatski sesalnik povežete z spletnim strežnikom do katerega lahko dostopate iz službe). Protokoli, ki se uporabljajo pri relaciji S2S so AMQP (angl. Advanced Message Queuing Protocol) protokoli, ki so sistemi čakanja (angl. queuing system) oblikovani za medsebojno povezovanje strežnikov [8].

Med drugim smo že omenili protokole za storitve, ki omogočajo dostop do podatkov na napravah kot npr. REST, SOAP, itd. Tukaj še lahko dodamo posebno obliko REST tehnologije namenjeno posebej za Internet stvari, Xively REST API, ki je kategorizirana kot platforma kot storitev PaaS (angl. Platform as a Service) [9]. Xively olajša medsebojno povezovanje naprav, podatkov, ljudi in krajev.

3.2. Tehnologije

Internet stvari sloni na raznoliki paleti različnih tehnologij, ki kot skupna celota predstavljajo hrbtenico interneta prihodnosti. Med drugim so del spodbujevalnih tehnologij Interneta stvari senzorji, aktuatorji, brezžična senzorska omrežja (angl. Wireless Sensor Network), I2Pack tj. pametno in interaktivno pakiranje (angl. inteligent and intearctive packaging), vgrajeni sistemi v realnem času (angl. real-time embeded systems), mobilne naprave, računalništvo v oblaku, RFID, QR, IPv6, NFC, WISP, M2M tj. komunikacija stroj do stroja (angl. Machine-to-Machine), interakcija človek-stroj (angl. human machine interaction), rudarjenje podatkov (angl. data mining), SOA tj. storitveno usmerjena arhitektura (angl. Service Oriented Architecture), EIS tj. podjetniški informacijski sistemi (angl. Enterprise Information System), itd. [10].

3.2.1. Brezžična senzorska omrežja

Brezžična Senzorska Omrežja (BSO) (angl. Wireless Sensor Networks, WSN) predstavljajo neprecenljiv vir za uresničevanje vizije Interneta stvari [11]. BSO so omrežja sestavljena iz številnih drobnih, brezžičnih, večinoma nepremičnih, ad hoc senzorskih vozlišč (angl. sensor nodes), ki imajo zaradi svoje specifične arhitekture, omejene vire (npr. nizka računska zmogljivost, omejen pomnilnik, majhen domet signala, baterijsko napajanje, itd.) [12]. Glavni namen BSO je zaznavanje območja zanimanja, kot so npr. gozd, nasad, žival, človek, itd. in sporočanje podatkov gozdarjem, kmetom, zdravnikom, itd. Odvisno od vrste senzorskega vozlišča lahko ti zaznavajo različne pojave kot so npr. tresljaji, zvok, svetloba, temperatura, ipd. Kadar so BSO integrirana v aplikacijski sistem Interneta stvari se le ta razširijo v ti. vseprisotna senzorska omrežja VSO (angl. Ubiquitous Sensor Networks, USN) [10]. Glavne komponente VSO so omrežje senzorjev (SAN) (angl. Sensor Area Network), omrežje dostopnosti (angl. access networking), infrastruktura omrežja, vmesnik (angl. Middleware) in aplikacijska platforma (angl. application platform) [10]. Veliko tehnologij je bilo namensko razvitih in standardiziranih za SAN, kot npr. ZigBee, IEEE802.15.6, WirelessHART, TinyOS, itd. Vsem so skupne značilnosti, ki so tudi del zahtev BSO, in sicer nizka poraba energije, kratek doseg komunikacije, prilagodljiva omrežna zmogljivost in lahki protokoli. Glavne značilnost omrežja dostopnosti (angl. access networking) so ti. prehodna vozlišča (angl. gateway nodes), ki so vmesna točka med samimi senzorji in kontrolnim centrom ali končnim uporabnikom, uporabljajo pa standardne komunikacijske protokole (IEEE 802.11, GPRS, itd.).

4. VARNOST

Koncept Interneta stvari, ki zajema komunikacijo med napravi sam po sebi ne predstavlja grožnjo za varnost in zasebnost. Težave nastanejo, ko se preko senzorjev na napravah ustvarjajo baze podatkov, ki lahko vodijo reference tudi na posameznega človeka oziroma, če je komunikacija med napravami nešifrirana vendar zajema podatke zasebne narave. Predstavljate si scenarij, kjer so vsi nakupovalni vozički v trgovini opremljeni s senzorji, ki stranki ob vsaki izbiri artikla, ki ga postavi v voziček, sproti na majhnem zaslonu prikazuje ceno artikla in skupno ceno nakupa še preden stranka pride do blagajne. Hkrati se voziček poveže s pametnim telefonom stranke in ji beleži nakup ter hkrati preverja seznam nakupa, ki si ga ja stranka sama ustvarila. Težave nastanejo takrat, ko vozički, ki so hkrati povezani s strežnikom trgovine shranjujejo vsak korak, ki ga stranka izvede v podatkovno bazo trgovine. Lastnik trgovine si lahko na koncu nakupa pogleda ne samo artikle, ki jih je stranka kupila, temveč tudi artikle, ki jih je stranka vrnila nazaj na polico hkrati pa tui točno pot, ki jo je stranka prehodila po trgovini. Korak naprej bi bil drug scenarij v katerem ima stranka pod kožo vsajen RFID mikročip kot jih že oglašujejo in uporabljajo v ZDA [13]. Le ta bi oddajal unikaten identifikator osebe, ki je hkrati povezan z določeno podatkovno bazo, ki hrani osebne podatke osebe v kateri je. V primeru, da kdo prestreže radijske signale med delovanjem mikročipa, lahko ugotovi kje in kdaj se je določena oseba nahajala.

V javnosti so že zabeleženi prvi resni kibernetski napadi na Internet stvari. Ko je ameriški State Department prvič začel opremljati ameriške potne liste z RFID oznakami se je kmalu ugotovilo, da bi lahko vsakdo, ki bi si lahko privoščil napravo vredno 250USD, prebiral podatke iz potnega lista kar iz razdalje desetih metrov [14]. Januarja 2014 so s podjetja Proofprint javnosti sporočili, da so zasledili še nikoli prej viden kibernetski napad Interneta stvari. Hekerji so uspeli v kratkem roku okužiti več kot tisoč naprav (npr. pametne hladilnike, usmerjevalnike, televizorjem, itd) in s njihovo pomočjo odposlati okrog tri četrt milijona nezaželene pošte [15].

Kako zelo pomembna je varnost znotraj razvoja Interneta stvari je pokazala tudi Evropska komisija (EK), ki izmed poglavitnih izzivov javnega upravljanja v zvezi z Internetom stvari vidi težavo: »Kako bo zagotovljena varnost informacij znotraj Interneta stvari?« [16]. Prav tako je v poročilu EK zapisano, da razvoj interneta ne sme potekati na škodo zasebnosti in varnosti osebnih podatkov.

Doseganje varnosti znotraj Interneta stvari je zelo velik izziv s katerim se še vedno ukvarjamo. Težave so v specifičnosti in raznolikosti naprav, ki so del Interneta stvari. Povrh vsega se omrežju Interneta stvari vsako toliko pridružijo novi subjekti in naprave, ki imajo nove specifične lastnosti. Največja težava je v omejeni arhitekturi določenih naprav (npr. senzorji, RFID, itd.). Senzorji in številne druge naprave znotraj Interneta stvari imajo nizko računsko zmogljivost, omejen pomnilnik, majhen domet signala, baterijsko napajanje, itd. Zaradi takšne arhitekture uporaba klasičnih varnostnih shem ne pride v poštev.

Varnosti pristopi znotraj Interneta stvari se lahko ločijo na dve različni skupini. Prvi pristop je splošen saj je povezan s tehnologijami in praksami, ki smo jih kot končni uporabniki že vajeni (npr. nastavitve varnosti WiFi omrežja). Drug pristop je specifičen varnostni pristop saj je osredotočen na tehnologije, ki so zelo specifične za Internet stvari in s katerimi se velika večina končnih uporabnikov nikoli ne sreča.

4.1. Splošni varnostni pristopi

Kot smo že omenili lahko ločimo med različnimi varnostnimi pristopi kadar govorimo o varnosti Interneta stvari. Ker je eden od trenutno najbolj uporabljenih medijev za povezovanje naprav WiFi, se lahko za izboljšanje varnosti znotraj Interneta stvari uporabljajo tudi klasični pristopi za zagotavljanje varnosti znotraj WiFi.

V primeru, da imamo zasebno zbirko senzorjev, ki nam npr. pomagajo pri proizvodnih procesih so le ti preko prehodnega vozlišča (angl. gateway) povezani s centralnim strežnikom. Prehodno vozlišče je s strežnikom povezano s pomočjo prenosnega medija WiFi. V takšnem primeru lahko za varnost na klasičen način poskrbimo tako, da WiFi omrežje šifriramo (npr. WEP, WPA, itd.), skrijemo SSID omrežja, filtriramo MAC naslove, itd. S tem onemogočimo potencialnim zlonamernim zunanjim opazovalcem ti. sniffing zasebnega omrežja.

4.2. Specifični varnostni pristopi

Kot smo že ugotovili lahko sami upravljamo z varnostjo omrežja in prometa na visoki ravni, težava se pojavi, ko želimo zaščititi ukoreninjene končne naprave (npr. RFID, senzorji, itd.). Kadar želimo uvesti varnost znotraj Interneta stvari kot npr. znotraj BSO, takrat govorimo o specifičnih varnostnih pristopih. Ker imajo naprave znotraj Interneta stvari omejeno arhitekturo, je potrebno uporabiti specifičen varnostni pristop, ki bo prilagojen omejeni arhitekturi le teh. Primer so lahko BSO, ki so sestavljena iz senzorskih vozlišč, ki so razporejena na območju zanimanja, so med seboj povezana in imajo še vedno stik s končnim uporabnikom, kateremu posredujejo zajete podatke. Iz tega razloga je potrebno poskrbeti za varnost pri prenosu podatkov med senzorskimi vozlišči ali od senzorskih vozlišč do končnega uporabnika, saj so podatki zaznavanja lahko zaupne naravne kot npr. pacientovi vitalni znaki, informacije o gibanju na bojišču, ipd.

Uporaba računsko zahtevnih varnostnih shem, ki se običajno uporabljajo, v tem primeru ne pridejo v poštev. Potreben je razvoj posebnih ti. »lahkih« (angl. lightweight) varnostnih shem in pristopov, ki omogočajo visok nivo varnosti, hkrati pa potrebujejo malo računske zmogljivosti za izpeljavo. *BSO in Internet stvari je področje kjer je kompromis med varnostjo in učinkovitostjo zelo pomemben*. Pri varnosti je potrebno upoštevati številne možne napade, med katerimi so določeni specifični samo za BSO, kot npr. kraja senzorskih vozlišč (angl. node capture attack) ali pa za kakšno drugo specifično tehnologijo znotraj Interneta stvari. Prav tako obstajajo splošno znani napadi, za katere so senzorska vozlišča ali druge majhne naprave znotraj Interneta stvari pogosto še bolj dovzetni. Primer takšnega napada je napad z zavrnitvijo storitve (angl. denial-of-service attack), ki ima lahko resne posledice zaradi omejene arhitekture (npr. majhne količina energije).

V znanstveni skupnosti je predlaganih veliko namenskih varnostnih shem, ki so prilagojene omejenim arhitekturam znotraj Internet stvari, posebej BSO. Večina shem temelji na uveljavljenih kriptografskih in varnostnih principih. Predlagane varnostne sheme lahko razdelimo na tri skupine glede uporabljeno kriptografsko tehniko in sicer na simetrične, asimetrične in hibridne. Med simetrične štejemo SPINS, LEAP in TinySec. Asimetrične varnostne sheme uporabljajo med drugim tudi RSA protokol ali ECC (angl. Elliptic Curve Cryptography) protokole. Med asimetrične varnostne sheme štejemo TinyPK, TinyECC, TinyPairing. Hibridni varnostni protokoli so SCUR, MASA in SecFleck [17].

Obstajajo tudi splošni standardi namenjeni za Internet stvari kot npr. ISO/IEC 14443, ISO/IEC 29192 in WirelessHAART. Prav tako se je razvoj zgoščevalnih funkcij (angl. hash function) usmeril v lahke oblike (npr. družine zgoščevalnih funkcije Quark, Photon, Gluon, itd.) [18].

5. ZAKLJUČEK

Internet stvari, ki se napoveduje za leto 2020 se nam počasi približuje. Že zdaj smo obdani z milijardami različnih elektronskih naprav, ki so med seboj povezane na načine za katere večine sploh še ne dojame. Čeprav se je pojem Internet stvari v javnosti že uveljavil, se razumevanje samega koncepta še ni. Veliko je še negotovosti in nestrinjanja v pogovorih vezanih na samo arhitekturo Interneta stvari. Svetovne korporacije in organizacije so se zaradi finančnega vpliva energično podale v boj zajemanja trga nove generacije interneta, bodisi z novimi produkti, standardi ali idejami. Na srečo pa se je tudi varnost uvrstila v dnevni red saj je na tem področju še veliko nerazumevanja in nepripravljenosti. V tem članku smo poskušali na kratko razložiti osnovno arhitekturo Interneta stvari in predstaviti tehnologije, ki so del le tega. Prikazali smo določene specifičnosti tehnologij Interneta stvari in s tem povezane varnostne težave in pristope.

LITERATURA

[1] B. Crothers, „End of Moore's Law: It's not just about physics,“ 28 08 2013. [Elektronski]. Available: http://www.cnet.com/news/end-of-moores-law-its-not-just-about-physics/.

[2] M. Mohorčič, „Internet stvari - izzivi in priložnosti.,“ v *Petindvajseta delavnica o telekomunikacijah.*, Brdo pri Kranju, 2011.

[3] T. Team, „Google's Strategy Behind The $3.2 Billion Acquisition Of Nest Labs,“ Forbes, 17 1 2014. [Elektronski]. Available: http://www.forbes.com/sites/greatspeculations/2014/01/17/googles-strategy-behind-the-3-2-billion-acquisition-of-nest-labs/. [Poskus dostopa 22 05 2014].

[4] W. Peter Friess, „ICT 30 2015: Internet of Things and Platforms for Connected Smart Objects,“ 2014. [Elektronski]. Available: https://www.google.si/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CC8QFjAB&url=http%3A%2F%2Fec.europa.eu%2Fdigital-agenda%2Fevents%2Fcf%2Fict2013%2Fdocument.cfm%3Fdoc_id%3D26272&ei=w9iBU-n6MKK27Qbl4IHgCQ&usg=AFQjCNGtEObyXUTmaNU42OJ3uk8zdaouVA&bvm=bv.677. [Poskus dostopa 22 05 2014].

[5] S. Haller, „The Things in the Internet of Things:Poster,“ v *Internet of Things Conference*, Tokyo, 2010.

[6] V. T. Dominique Guinard, „Towards physical mashups in the Web of Things,“ v *Sixth International Conference on Networked Sensing Systems (INSS)*, Pittsburgh, PA, 2009.

[7] A. B. ,. H. B. ,. S. P. ,. A. P. ,. H. K. ,. I. L. ,. F. G. ,. D. T. Elmar Zeeb, „WS4D: SOA-Toolkits making embedded systems ready for Web Services,“ v *Open Source Software and Product Lines Workshop (OSSPL07)*, 2007.

[8] S. Schneider, „Understanding The Protocols Behind The Internet Of Things,“ Electronic Design, 9 10 2013. [Elektronski]. Available: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things. [Poskus dostopa 22 05 2014].

[9] I. LogMeIn, „Xively REST API,“ LogMeIn, Inc., [Elektronski]. Available: https://xively.com/dev/docs/api/. [Poskus dostopa 25 05 2014].

[10] Z. Pang, Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being, Stockholm: KTH – Royal Institute of Technology , 2013.

[11] P. N. J. L. R. R. C. Alcaraz, „Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?,“ v *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, Tokyo, 2010.

[12] B. M. D. G. Jennifer Yick, „Wireless sensor network survey,“ *Computer Networks,* Izv. 52, pp. 2292-2330, 2008.

[13] T. Lewan, „Microchips in humans spark privacy debate,“ USA Today, 21 07 2007. [Elektronski]. Available: http://usatoday30.usatoday.com/tech/news/surveillance/2007-07-21-chips_N.htm. [Poskus dostopa 24 05 2014].

[14] A. Rose, „The internet of things is set to change security priorities,“ Computer Weekly, April 2013. [Elektronski]. Available: http://www.computerweekly.com/feature/The-internet-of-things-is-set-to-change-security-priorities. [Poskus dostopa 24 05 2014].

[15] Proofpoint, „Proofpoint Research: Internet of Things (IoT) Cyber Attack Security,“ Proofpoint, Inc. , UNNYVALE, California, 2014.

[16] E. Commission, „Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things : an action plan for Europe,“ European Commission, Brussels, 2009.

[17] S. B. A. K. V. Gaurav Sharmaa, „Security Frameworks for Wireless Sensor Networks-Review,“ v *2nd International Conference on Communication, Computing & Security [ICCCS-2012]*, 2012.

[18] P. N. J. L. Rodrigo Roman, „Securing the Internet of Things,“ *IEEE Computer,* Izv. 55, št. 9, pp. 51-58, 2011.

[19] C. F. Friedemann Mattern, „From the Internet of Computers to the Internet of Things,“ *From Active Data Management to Event-Based Systems and More,* Izv. 6462, pp. 242-259, 2010.