ISSN 0354-9852
DOI 10.7251/AKT3215001T

UDK 681.513.2
Pregledni rad/Overview paper

BEZBEDNOST IOT TEHNOLOGIJA I RAZVOJ BEZBEDNOSNIH MERA I TEHNOLOGIJA U OKVIRU INTERNETA STVARI

SECURITY OF IOT TECHNOLOGIES AND DEVELOPMENT OF SECURITY MEASURES AND TECHNOLOGIES WITHIN INTERNET OF THINGS

Branko Marković[1], Mihajlo Novaković[2]

Sažetak

Ovaj rad se bavi pregledom postojećih tehnologija, upoređuje stavove o pitanjima bezbednosti IoT tehnologija vodećih stručnjaka i kompanija iz ove oblasti i predlaže okvirna bezbednosna rešenja kako na nivou primene bezbednosnih rešenja tako i u pogledu uspostavljanja odgovarajuće bezbednosne klime i zakonske regulative koja bi trebala bliže i bolje da uredi ovu oblast.

Analizira se trenutna svest ponuđača rešenja i tržišta za uređaje IoT koncepta, te njihovi nasledni problemi vezani za potrebu za izuzetno brzim razvojem i stavljanjem u upotrebu, kao i problemi interoperabilnosti u uslovima stalno povećavajućeg broja uređaja i broja njihovih proizvođača.

Razmatraju se i aspekti bezbednosti IoT tehnologija kroz IoT koncept kao faktor promjene u načinu na koji poimamo našu svakodnevnicu, te posljedične uloge pojedinca u podsticanju bezbednosti IoT sistema.

U zaključku, pored potrebe za definisanjem bezbednosnih standarda i postojanjem ugrađene bezbednosti u svakom IoT uređaju, ističemo i potrebu za transparentnošću IoT bezbednosnih tehnologija.

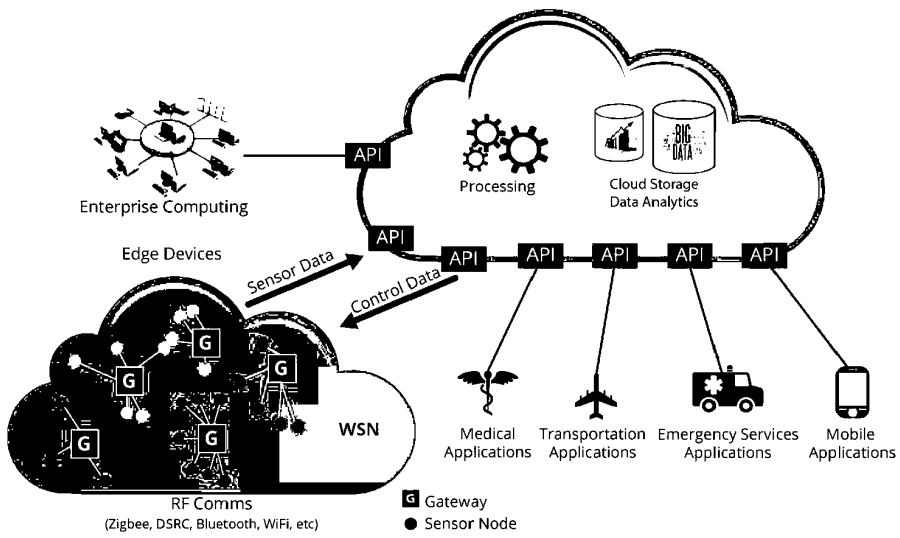
Ključne reči: *IoT, Internet stvari, tehnologija, trend, bezbednost, razvoj, industrija, društveni značaj*

JEL klasifikacija: C8

1 Branko Marković, Prointer ITSS Banja Luka
2 Mihajlo Novaković, ELNOSBL Banja Luka

UVOD

Problem bezbednosti u okviru IoT koncepta danas predstavlja dominantno pitanje primene IoT tehnologija u modernom poslovnom i privatnom okruženju. Razlozi zašto pitanje bezbednosti IoT tehnologija dolazi u prvi plan prilikom implementacije ovog modela u poslovno i privatno okruženje su višestruki, počev od posrednih koji proizilaze iz toga da IoT tehnologije vertikalno i horizontalno povezuju raznorodne, dosad nepovezane sisteme, te samim tim dozvoljavaju lak i nometan pristup svim vrstama informacija nakon inicijalne penetracije u IT sistem, do onih neposrednih i direktnih gde se pojedini nivoi tehnologije, a to je posebno izraženo kod krajnjih nodova - dakle senzora i aktuatora zbog njihovih ograničenih procesorskih kapaciteta te nedovoljne zaštićenosti bili na fizičkom ili nivou softvera, mogu upotrebiti za samu inicijalnu penetraciju u jedinstven ICT sistem kompanije.



Slika 1: Principijelna šema rada uređaja u okviru IoT tehnologije Izvor: Security Guidance for Early Adopters of the Internet of Things (IoT), April 2015

Poseban nivo bezbednosne pretnje koji do sada nije postojao u okviru ICT tehnologije predstavlja fizička pretnja proizišla iz prirode IoT tehnologija te činjenice da se one ne bave samo informacijama o realnom svetu već na njega mogu i da utiču. IoT tehnologije, pored elementa informacije, u sebi inherentno sadrže i element sile i kao takve predstavljaju bezbednosan problem kako sa stanovišta zaštite tako i sa stanovišta neovlaštene ili nedozvoljene primene. Kako IoT tehnologije postaju sve zastupljenije tako se

otvaraju i nova bezbednosna pitanja na koja treba dati odgovarajuće odgovore. Istovremeno vidan je i napor da se pitanje bezbednosti IoT tehnologija što jednoznačnije odredi te da se na njega daju valjani kvantitativni i kvalitativni odgovori. Neki od navoda vodećih IT i bezbednosnih stručnjaka koji okvirno govore o rasponu i dubini problema bezbedsnosnih tehnologija su:

- John Thompson, podpredsednik IoT divizije IBM napominje da je pitanje korporativne bezbednosti najvažniji kamen spoticanja za brzu primenu IoT tehnologije. Takođe, smatra da pritisak na postepenu primenu novih tehnologija dolazi u korporacijama od onih koji su zaduženi za korporativnu bezbednost: „Kada IoT uređaje „prikačite" na korporativni internet shvatite da oni ne govore standardnim (TCP/IP) protokolima već protokolima koje vi ne slušate i na koje je nemoguće primeniti standardne internet sisteme zaštite."[3]
- International Data Corporation (IDC) predviđa da će 90% organizacija koje rano implementiraju IoT tehnologije imati neki oblik bezbednosnog problema u svojoj IT infrastrukturi. Prema IDC IoT tehnologija će postati bezbednosno zrela tek 2017. godine.[4]
- Brian Witten, Direktor za IoT Security u Symantec korporaciji, smatra da je transparentnost neophodna kod IoT tehnologija kada je u pitanju njihova bezbednost. On ovo obrazlaže rečima: „Kada kupujete neki uređaj vaše je pravo da znate koliko bezbenosti je ugrađeno u taj proizvod, posebno ako vaš život i imovina direktno zavise od istog (medicinski uređaji, automobili,...)

RAZLOZI BEZBEDNOSNIH PROBLEMA U IOT TEHNOLOGIJI

Razlozi zašto ovo pitanje dolazi u fokus su mnogobrojni, ali možemo reći da osnovni razlog za naglo interesovanje stručne i šire javnosti za ovo pitanje poizilazi upravo usled porasta svesti o tome kakve sve bezbednosne rizike IoT tehnologije sa sobom nose. Rana primena IoT tehnolgije obavlja se danas kada postoji više od trideset godina razvoja svesti o IT tehnologijama i kada se generacije dece rađaju u vremenu zrelosti internet tehnolgija te svoju paradigmu formiraju zahvljujući okruženju koje zatiču. Znanje koje su predhodne generacije o primeni i eksplataciji IT stekle postoji i prilično je zrelo. Ono što je nezreli deo sadržaja kada su u pitanju nove IoT tehnolo-

3 John Thompson, Keynotes 2014 Chicago Internet of Things World Forum, Published on Oct 22, 2014, video, 30.12.2014, dostupno na mreži: https://www.youtube.com/watch?v=-lwl0GbZd_c

4 IDC Reveals Worldwide Internet of Things Predictions for 2015, Press Release, 03 Dec 2014, IDC Futurescape for Internet of Things, 13.01.2016, dostupno na mreži: https://www.idc.com/getdoc.jsp?containerId=prUS25291514

gije praktično potiče od potrebe da se povežu fizičke i hemijske veličine sa informacijama te da se sa njima direktno daljinski upravlja. Proizvođači senzora i aktuatora do sada nisu morali da vode brigu o bezbednosti svojih uređaja jer je ona bila obezbeđena na nivou fizičkog pristupa uređaju a samo u izuzetnim slučajevima na nivou pristupa nekog lokalnog SCADA sistema koji je bio toliko komplikovan i specifičan te lokalan da opasnost od internet upada čak i kada je postojala nije bila dovoljno verovatna pa se nije ni očekivala i zahtevala posebna zaštita. Širom upotrebom IoT tehnologija stvari su se naglo počele menjati. Sve više uređaja kroz razne vrste nadogradnji dobija spoljnju konekciju i to menja bezbednosne jednačine. U vreme svoje proizvodnje i instalacije „on site", ti uređaji su bili izolovani i niko sa njima nije komunicirao, pa je i bezbednost bila u skladu sa tim (bilo je dovoljno obezbediti da neautorizovan personal ne može da im priđe). Sada ceo svet komunicira sa njima, a inicijalni bezbednosni sistem se nije promenio. Taj disbalans zahteva da se istovremeno sa konekcijom ugradi i odgovarajući nivo bezbednosti. Ono što se pri ovome postavlja kao novi problem je činjenica da za većinu industrijske opreme važi pravilo da je na kupljenoj opremi zabranjeno bilo šta menjati (bilo tehnički bilo kroz ugovore o garanciji), čak i ukoliko to povećava bezbednost, te je od presudnog značaja da bezbednost bude ugrađena od samog početka.[5] Da će se postojeća brzina prevođenja industrijskih sistema na otvorene ili privatne IoT vertikale samo ubrzavati, a time i povećavati jaz između optimalne i na ovom nivou razvoja tehnologije nuđene bezbednosti vidljivo je i iz razloga zašto do ove pojave dolazi, a koji bi se mogli definisati na sledeći način[6]:

- Interoperabilnost danas predstavlja osnovni zahtev za šire industrijsko prihvatanje IoT tehnologije. Smatra se da 40% ukupne ekonomske vrednosti IoT tehnologija za sada ostaje neiskorišteno u industriji samo zato što uređaji nisu interoperabilni odnosno ne postoje jedinstveni standardi, inter-exchange formati fajlova, te jedinstveni protokoli. Moxa OPC server predstavljaju dobar način da se ovaj zahtev ispuni u industrijskim pogonima uz relativno niska ulaganja
- Uspeh IoT tehnologija zavisi od pouzdanosti i dostupnosti IP baziranih mreža i uređaja (u okviru industrijskih postrojenja još uvek preovlađuju ProfiBUS protokoli i mreže)
- Bezbednost, danas predstavlja vrlo veliki problem jer je sve više proizvođača opreme i/ili konsultanata koji, da bi nadgledali ili održavali

5 Brian Witten, IoT is Starving for Built-In Security, TIA NOW, Published on Sep 17, 2015, video, 10.01.2015, dostupno na mreži: *https://www.youtube.com/watch?v=v9vvNfe39is*

6 Tapping into the Potential of the Industrial IoT, Moxa, January 2016, newsletter, 13.01.2016, dostupno na: *http://www.moxa.com/newsletter/connection/2016/01/feat_01.htm?utm_source=2016_01_Connection&utm_medium=email&utm_campaign=Connection&mkt_tok=3RkMMJWWfF9wsRoiuq%2FAZKXonjHpfsX%2B4uQoXbHr08Yy0EZ5VunJEUWy3oEFSNQ%2FcOedCQkZHblFnV4JS62vS7cNoq0O*

opremu ili process, zahtevaju udaljeni pristup istoj, iako postoje bezbednosni standardi kakav je IEC-62443 oni još u potpunosti ne pokrivaju sve moguće scenarije korištenja IoT tehnologije u industriji

- Skalabilnost koja se zahteva kako na softverskom tako i na hardverskom nivou. Poseban nivo skalabilnosti zahteva se usled rasta broja uređaja, a kako bi se postigla redundantnost i izbegla jedinstvena kritična tačka infrastrukture čijim ispadom ispada i cela industrijska proizvodna ćelija. Navedeno, sa stanovišta IoT rešenja, povlači višestruke konekcije i redundantnost na nivou senzora i aktuatora
- Jedinstvena tačka upravljanja IoT uređajima i infrastrukturom danas skoro da i ne postoji jer se različiti softverski alati koriste za različite poslove upravljanja samim uređajima i/ili infrastrukturom

Pobrojani zahtevi se mogu ispoštovati isključivo podizanjem jedinstvenih vertikala koje su dovoljno robusne, skalabilne te zaštićene od gubljenja podataka i dostupne što sa sobom povlači i one bazirane na cloud platformama. Nerazmatrajući ni na koji način pravne i tehničke nivoe izolacije korisničkih okruženja unutar public cloud rešenja vidljivo je da je jedino tehnički ispravno rešenje private cloud sa kompletnom privatnom internet infrastrukturom. Ovakva rešenja su skupa, nepraktična te dostupna samo limitiranom broju velikih kompanija. Alternativno rešenje sa public i hybrid cloudom podrazumeva dodatne rizike koji ne potiču samo od mogućnosti penetracije te malicioznog delovanja unutar nekog okruženja već i od nivoa poverenja i garancija koje cloud provider može da ponudi krajnjem korisniku. Kako su ovo opšte poznati bezbednosni problemi fokusiraćemo se samo na probleme penetracije u sistem te zaštite tokom transporta podataka.

Treba naglasiti da IoT rešenja ne postaju predmet malicioznih napada sa interneta na isti način i sa istom svrhom kao kada su u pitanju klasične ICT tehnologije. IoT rešenja podložna su malicioznim napadima takođe i zbog toga što:

- Povezuju mnoge korisnike i širok spektar aplikacija
- Omogućavaju pristup kombinaciji informacija i kontrole veće vrednosti
- Obećavaju veću vrednost i uticaj korisnicima, operatorima ali i napadačima

Navešćemo samo neke od bezbednosnih problema koji dolaze u fokus nakon implementacije neke od IoT vertikala:

- Bezbednosni problem koji ozbiljno ugoržava bržu primenu koncepta pametne kuće otprilike bi se mogao svesti na to da se čitanjem obrazaca ponašanja vezanih za uključenje i isključenje prekidača za svetlo (eng. switching pattern) može, posle određenog vremena, sa sigurnošću odre-

diti ima li nekoga u kući ili ne i u zavisnosti od te informacije razne kriminalne grupe mogu maliciozno delovati (ući u posed, opljačkati posed...). Sličan bezbednosni propust odnosi se i na druge električne potrošače jer način na koji se upotrebljava energija i potrošnja iste jasno ukazuje na prisustvo ili odsustvo vlasnika

- IoT omogućava orkestrirane napade mnogo višeg opsega i dosega od onih na koje smo navikli. IoT tehnologije omogućavaju algoritamski terorizam ali i novu vrstu dominacije i kolonizacije sveta jer IoT uređaji rade u fizičkom a ne virtuelnom univerzumu.[7]
- Poznat je slučaj iz 2015 godine kada je grupa hakera uspela da preuzme komande i daljinski upravlja džipom Čiroki jer su zahvaljujući niskoj bezbednosti softvera za daljinsku dijagnostiku uspeli da pristupe sistemu za kočenje i njime manipulišu[8]
- Konstruktori neželjeno - usled toga što do sada o tome nisu morali da vode računa, povezujući raznorodne sisteme omogućuju curenje informacija kroz neki od portova ili komunikacionih protokola
- Tržište tera vendore da prave uređaje koji se mogu povezati iako još ne postoje standardi koji bi se bavili sigurnošću

Problem leži u osećaju lažne sigurnosti prema kojem se veruje da je sve ono što je nevidljivo ili strukturno udaljeno u dominantnom mentalnom modelu, nepostojeće, odnosno da ako nema opasnosti koja se zdravorazumski može detektovati i pojmiti onda nema nikakve opasnosti. Svima koji su se bavili bezbednosnim pitanjima ovaj model je poznat i predstavlja takozvani javni model ili „uverenje građana" i često je korišten za lažno predstavljanje stvarnosti tako da su određene informacije zataškavane i sprečavane da dođu u javnost. Ovaj model bezbednosti počiva na takozvanom javnom mnjenju odnosno na slobodnom uvjerenju – što znači da ako većina veruje da je nešto bezbedno a nema kontrainformacija ili iskustava koje bi tu realnost pobijala onda je realnost bezbedna. Iz iskustva znamo da je internet uspeo da promeni ovu vrstu bezbednosne paradigme. Današnje okruženje od nas zahteva da u naše bezbednosne proračune uzmemo u obzir i nevidljive pretnje jer su one nevidjive samo nama a ne mora da znači da su nevidljive i onima koji predstavljaju bezbednosnu pretnju pa je onda neophodno reagovati onemogućavanjem i tih nevidljivih - nepostojećih pretnji. Te pretnje postaju vidljive tek kada bude kasno. Prema tome, ubeđenje da je bezbedno koristiti neku novu tehnologiju ne sme biti presudno za njenu

7 Dr. Joseph Reger, Fujitsu Forum 2013 Keynote: Internet of Things, Fujitsu - Human Centric Innovation, Published on Nov 14, 2014, video, 08.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=dbPLQXABavw*

8 Andy Green, Hackers Remotely Kill a Jeep on the Highway—With Me in It, 07.21.2015, 08.01.2016, dostupno na mreži: *http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*

primenu. Načini i modeli njene primene moraju se pokoravati nekim osnovnim protokolima koji su predmet uopštene najbolje prakse iz srodnih oblasti. IoT tehnologije nisu bezbedne ali nisu ni nebezbedne a priori, ali ono što se nikako ne može i ne sme dozvoliti je njihova primena bez jasnog bezbednosnog protokola kod cloud provajdera te krajnjeg korisnika tehnologije dok se od proizvođača mora zahtevati odgovarajući nivo bezbednosti ugrađen u senzore i aktuatore te mogućnost prilagođavanja bezbednosnim standardima tokom vremena za svu isporučenu opremu za ceo životni vek uređaja. Ovako koncipirana bezbednosna platforma omogućava kasnije prilagođavanje kako potrebama korisnika tako i zahtevima eksploatacije.

Peter Warren Singer smatra da se pri analizi bezbednosnih rizika IoT tehnologije trebamo pridržavati proverljivih činjenica[9]:

1. Uređaji imaju komunikaciju bez nas (ovo je osnovni postulat M2M servisa). Uređaji su autonomni u svojoj operabilnosti sa hijerarhijski višim i horizontalno srodnim uređajima iste klase odnosno istog domena.
2. Postoji diskonekcija realnosti i javnog mišljenja po pitanju bezbednosti IoT vertikala
3. Kompleksnost tehnologije prevazilazi znanja i mogućnosti onih koji donose zakone
4. Bezbednosna paradigma mora biti u najširem fokusu određena sa sledeća dva pitanja:
   - Šta je moguće?
   - Šta je ispravno?
5. Tehnologija i politička dinamika određuju granice mogućeg i ispravnog (dozvoljenog)
6. Javnost, a i zakonodavci vezuju različite aktivnosti i tehnologije samo zato što koriste softver (IoT vertikala za telemedicinu nema nikakvih tehničkih sličnosti sa senzorskim sistemom za praćenje i predviđanje vremenskih prilika)
7. Strategija se svodi na mogućnosi i prioritete

Peter Warren Singer smatra da je stav mnogo veći problem od nivoa znanja, te smara da se bezbednosne strategije moraju svoditi na balansiranje između mogućnosti i prioriteta. Pri ovome se mora voditi računa o znanju, ljudima, motivaciji, relativnom i apsolutnom trošku izvođenja nekog IoT cyber napada, organizaciji, tenzijama između rivala.

Danas mnogi političari, javni govornici, pravnici, pa i pojedinci govore o bezbednosti pojedinih tehnologija. Barak Obama je izjavio da je Cyber bez-

9 Peter Warren Singer: "Cybersecurity and Cyberwar: What Everyone Needs to Know" | Talks at Google, Published on Feb 10, 2014, video, 17.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=h0SXO5KUZIo

bednost najvažnije bezbednosno pitanje 21-og veka.[10] Ali treba biti obazriv i priznati da je retko kad u ljudskoj istoriji „nešto tako značajno i tako kompleksno toliko javno raspravljano svaki put sa sve manje znanja i razumevanja"[11],7 koje ovo pitanje sa sobom nosi.

Peter Warren Singer takođe javno iznosi i podatak da su u EPM Kanade i SAD veverice više puta oborile mrežu od hakera, tako da se ideja širenja panike kako bi se prodalo što više „bezbednosnih rešenja" trebala što pre suzbiti jer „Al-Kaida bi htela al ne može, a Kina može ali neće- još da napravi ozbiljan Cyber napad na SAD"

Iako se stavovi Peter Warren Singer značajno razlikuju od ostalih pa im u mnogome i protivreče oni su bazirani na iskustvu i radu sa bezbednosnim tehnologijama najvišeg nivoa. Ono za šta se ovaj poznati autor zalaže može se sublimirati rečenicom: „Stuxnet[12] je pokazao da je efikasan sajber napad moguć ali i izuzetno težak." Te da je stoga industrijski napad malo verovatan ali to ne sme biti opravdanje za ne preduzimanje nikakvih mera bezbednosti.

Organski pristup bezbednosti je od presudnog značaja tokom celog životnog veka proizvoda odnosno usluge, ali on dosada nije bio podrazumevan u većini industrija koje su u IoT tehnologijama pronašle prostor dodatnog razvoja i rasta. Poseban problem predstavljaju različiti nivoi regulacije tržišta za različite industrijske grane ili nacionalne okvire a upravo nivo regulacije nekog tržišta regulisaće brzinu osvajanja tog tržišta IoT tehnologijama. Sa bezbednosnog stanovišta važno je napomenuti da IoT povezuje informacione i operacione tehnologije te da i pored svojih inherentnih bezbednosnih nedostataka podiže ukupan nivo bezbednosti, posebno u operacionom smislu, kao i u smislu kontrole i upravljanja vlasništvom.

10 Javno dostupni materijali sa govorima Baraka Obame, Bela kuća, Tehnology, Cybersecurity and Internet Policy, 17.01.2016, dostupno na mreži: https://www.whitehouse.gov/issues/technology

11 Remarks by Director David H. Petraeus at In-Q-Tel CEO Summit, Excerpts from Remarks Delivered by Director David H. Petraeus at the In-Q-Tel CEO Summit (March 1, 2012), 20.01.2016, dostupno na mreži: https://www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/in-q-tel-summit-remarks.html

12 Lawrence Conway, Obama ordered cyber-attacks on Iran's nuclear programme but created a super-virus that is now 'out of control', DailyMail, 1 June 2012, članak, 20.01.2016, dostupno na mreži: http://www.dailymail.co.uk/news/article-2153308/Cyberattacks-Iran-ordered-Obama-created-virus-creating-havoc-internet.html#ixzz3xmY9vj62

BLIŽI TEHNIČKI I ORGANIZACIONI OPIS BEZBEDNOSNIH PROBLEMA IOT TEHNOLOGIJA NA SADAŠNJEM NIVOU RAZVOJA TEHNOLOGIJE

Bezbednosni problemi koji se mogu pojaviti prilikom upotrebe privatnih i industrijskih IoT sistema mogli bi se sistematizovati na sledeći način[13]:

- Bezbednosni problemi u transportnom nivou rešenja koji se ogledaju u sledećem: enkriptovane konekcije su retke, API funkcije koje se koriste za očitavanje merenja sa senzora kao i upravljanje kućnim IoT uređajima nisu enkriptovane
- Arhiviranje i storniranje istorijskih podataka nije obezbeđeno mehanizmima enkripcije; u public cloud okruženjima pružaoci cloud usluge često nedovoljno obezbede podatke od drugih korisničkih naloga – izolacija je slaba ili nedovoljna
- Proizvođači „terenskih" – korisničkih uređaja ne teraju korisnike da pri prvom pokretanju sistema promene proizvođački sistemski password
- Višak mrežnih protokola i portova – uređaji često imaju više različitih portova i protokola koje koriste od kojih nisu svi zaštićeni na isti način od neovlaštenog korištenja – npr. LAN i Wi-Fi zaštićeni dok na istom uređaju istovremeno postoje i Bluetooth i ZigBee preko kojih je moguć pristup bez autentikacije
- Kriptografija nije adekvatna sa strane vendora – jedan ključ vendor koristi za sve svoje uređaje – proizvode, te je moguće lako pronalaženje liste passworda koji omogućavaju pristup velikom broju različitih uređaja
- Krajnji korisnik ne može da promeni password za backdoor
- Fizički pristup uređajima nije adekvatno obezbeđen, uređaji postavljeni van zaštitnih ormama (ovo predstavlja veliki sigurnosni problem u industriji – jer ako je moguć pristup preko USB portova ili konzola direktno na uređaj moguća je i manipulacija istim pa samim tim i njihovu rekonfiguraciju i direktno upravljanje industrijskim procesima što otvara mogućnost industrijskih diverzija i terorizma)
- Trust-chain između senzora i logike mora biti obezbeđen odgovarajućom vrstom sigurnosti inače je moguće upravljati „postupkom" manipulišući senzorima

13 Mark Stanislav, Top 3 Security Issues in Consumer Internet of Things (IoT) and Industrial IoT, The Internet of Things IoT Inc Business Channel, Published on Mar 4, 2015, video, 25.12.2015, dostupno na mreži: https://www.youtube.com/watch?v=QelfiNqvhPU

IoT vertikale izložene su i ranjive na različitim nivoima. Možemo razlikovati 4 nivoa na kojima postoje različite ranjivosti kojima je sistem izložen. Ove ranjivosti prema nivoima možemo podeliti na[14]:

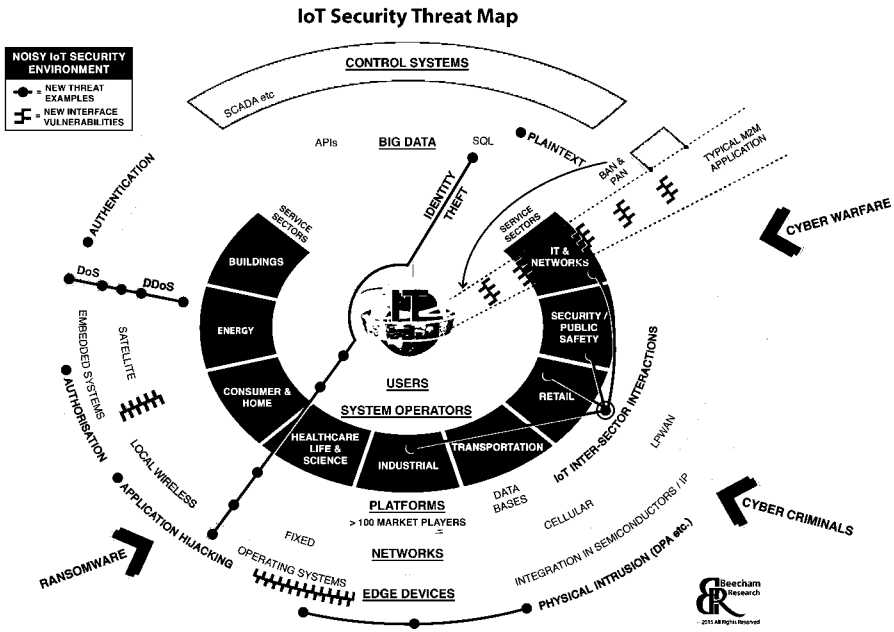
- Mrežni nivo obuhvata sve vrste LAN/WAN okruženja i saobraćaja i na njemu možemo da primetimo sledeće pretnje na koje je sistem ranjiv:
  - Nekonfigurisan ili pogrešno konfigurisan firewall
  - Skeniranje portova
  - Data injection
  - Denial of service
  - Man-in-the-middle
  - TCP napadi
  - Heartbeat
  - Nedostatak enkripcije nad podacima koji se transportuju
  - DDoS
  - BTF ranjivosti
  - Nezaštićeni web proxy-ji
- Infrastruktura je ranjiva na više načina pri čemu se kao osnovni bezbednosni nedostatak za krajnjeg korisnika postavlja pitanje bezbednosti cloud baziranih rešenja posebno na public cloud platformama jer krajnji korisnik niti ima uvid u preduzete bezbednosne mere niti na njih može izravno uticati. Takođe, zahvaljujući pomenutom, otežana je ili potpuno nemoguća adekvatna procena rizika i bezbednosni auditing. Sa druge strane u sistemima koji su izvedeni u potpunosti u privatnoj infrastrukturi postoji ozbiljna izloženost Brute Force napadima koji zahvaljujući dostupnim HPC računarima danas postaju sve češći oblik napada. U posebnu ranjivost na nivou infrastrukture svakako treba ubrojati (što je karakteristično za zdravstveni sektor i javnu upravu) da sve sve više zahteva da se korisnicima sistema (pacjentima) izdaje sve više dokumentacije u elektronskom obliku kako bi ih oni mogli koristiti i na drugim ICT sistemima pri čemu mnoge informacije ostaju nekriptovane (na nivou fajla) jer je prvobitni izveštaj bio samo za internu upotrebu. U nove pretnje na nivou infrastrukture možemo ubrojati:
  - Denial of services
  - DDoS napade
  - Nepoznate backdoor; Ovo je posebno karakteristično kod nadogradnje zastarele opreme kada se novi hardverski moduli (sa pripadajućim softverom) ugrađuju u već postojeća kućišta koja nisu bila ni namenjena za rad na mreži a kamoli da budu deo IoT vertikale

14 Joe Colantonio, Bob Crews, Shailesh Mangal, The Internet of Things - Risks Presented by Security, webinar part 2, test talks, www.getzephyr.com, **Published on Jul 31, 2015,** video, 10.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=ZodKWqiT5HE

  - Cyber ratovanje i Cyber terorizam; Zbog pogodnosti koje pružaju napadačima napadi na infrastrukturu, često se koriste da bi se napadom na pojedini njen deo došlo u poziciju preuzimanja kontrole nad istom i njenog obaranja.
- Interfejs se kod IoT tehnologija ne može koristiti za napade na M2M servise već samo u slučajevima kada postoji terenski / lokalni HMI na nekom IoT uređaju ili kontroleru (za veće industrijske sisteme kao što je SCADA). Tehnike koje se koriste za napad na interfejs su:
  - Cross site scripting (java, php, power shell)
  - Password cracking
  - SQL injection
  - URL manipulation (obično se koristi http get metod)
  - Bezbednosni auditing
  - Novi načini logovanja na sistem, novi interfesi kao što su skeneri za otisak prsta ili mrežnjače, prepoznavaje glasa i slično koriste se za brže i lakše logovanje na sistem i po pravilu nisu kombinovani sa password pravilima (smatra se da korisnik koji se logovao otiskom prsta ne mora da unese korisničko ime i lozinku)
  - Embeded hacker tools; Hakerski alati su napredovali i sada koriste i tehnologije kao što je anti-forensics, dynamic behavior, modularnost tako da je moguće da na nivou infrastrukture imate ugrađene hakerske alate za koje niste ni znali da postoje kada ste nabavljali opremu i gradili infrastrukturu.[15]
- Uređaji (terenski uređaji, odnosno krajnji nodovi); Prve tri nabrojane oblasti su standardne IT oblasti i u njima je rizik „razumljiv i vidljiv" IT i bezbednosnim stručnjacima. Na nivou uređaja zbog velikog broja tehnologija koje se ubrzano razvijaju, kao i zbog nepoznavanja matične tehnologije na kojoj uređaji rade može se reći da je rizik na nivou IoT uređaja još uvek „nepoznat i ne razumljiv" te vrlo težak za procenu, ali se može konstatovati da na ovom nivou postoje sledeće bezbednosne ranjivosti:
  - Fizička sigurnost uređaja nije uvek obezbeđena na adekvatan način. Ovo se posebno odnosi na nosive i prenosive uređaje
  - Privatnost podataka – ovi uređaji sadrže podatke u RAW obliku koji često nisu zaštićeni ni na koji način jer se smatra da korisnik vodi računa o uređaju. Ovo je posebno izraženo kad su u pitanju „nosiva zdrastvena pomagala" (hotleri, merači krvnog pritiska i otkucaja srca koji su integrisani u sat ili prsten kao krajnji čvor IoT vertikale)

15 Defcon 18 - SCADA and ICS for Security Experts: How to avoid Cyberdouchery, video, available online: http://www.youtube.com/watch?v=4gLAbIc2k9E

- Automatske nadogradnje (frimware ili softvera) o kojem krajnji korisnik ne zna ništa i na njega ne može da utiče
- Backdoor
- Mrežne mogućnosti na samom uređaju (uređaj ima više različitih oblika povezivanja sa internetom i koristi automatski algoritam da bira najpovoljniji oblik komunikacije)



Slika 2: Mapa bezbednosnih pretnji u IoT okruženju, Izvor: Beecham Research,03.05.2015, dostupno na mreži: http://www.beechamresearch.com/download.aspx?id=43

Poznati proizvođač antivirusa i ostalog bezbednosnog softvera Kaspersky Lab naglašava da se IoT vertikale značajno razlikuju po svojoj funkcionalnosti kao i po načinu transporta podataka od računarskih mreža jer su asimetrične po pitanju saobraćaja (saobraćaj ide od senzora ka Cloudu i od Clouda ka aktuatorima). Takođe upozorava na niz funkcionalnosti koji krajnji nodovi imaju nenamerno (eng. not-by-design).[16] Ove funkcionalnosti su posledica platforme koja se koristi i ne doprinose vrednosti vertikale ali su tu usled dizajna platforme koja se koristi i koja je robusnija i bogatija u odnosu na ogoljene zahteve vertikale. Upravo u tim dodatnim funkcionalnostima leži i ugrađena mogućnost zloupotrebe dizajna platforme za pene-

16 When IoT attacks, a case study, Kaspersky Lab, Billy Rios, Published on May 15, 2015, video, 17.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=j0QgDEB9yKo

traciju u IoT vertikalu. Posebnu mogućnost napadačima predstavlja činjenica da za sve standardne IoT platforme postoje detaljna upustva namenjena inžinjerima kako bi ih oni mogli prilagoditi svojim namenama. Dodatni bezbednosni problem, koji uočavaju stručnjaci iz Kaspersky laboratorija, leži u činjenici da su operativni sistemi za IoT platforme mali i nedovoljno robusni te podložni bafer overflow napadima, kao i da su dostupni kroz web servis pa je dovoljno da http post request pogodi odgovarajući DLL file kako bi napadač dobio informacije koje traži.

Gledano na nivou hardverskih platformi i novih IoT protokola postojeći nivo bezbednosti nije zadovoljavajući ali je očigledan napor proizvođača da se protokoli kao i bezbednosne mere za iste standardizuju. Jedan od boljih primera za to su svakako delovanja ZigBee Alliance ZARC Security Task Group i OIC – open interconnect consortium koji pokušavaju naći zajednički radni okvir koji treba da spoji različite tehnologije i uređaje odnosno da kroz standardizaciju omogući srvaranje vertikalnih tržišta sa industrijskim standardima kvaliteta.[17] Robert Cragie smatra da je sigurnost ZigBee uređaja u takozvanom centru poverenja. Za bezbedno funkcionisanje u mreži, ZigBee uređaj mora imati susedni uređaj sa kojim može razmeniti sigurnosne ključeve i koji kontroliše pristup. ZigBee zato uvodi concept centra poverenja koji: čuva sve ključeve za mrežu uređaja, koristi bezbednosne usluge da bi konfigurisao uređaj sa ključem, koristi bezbednosne usluge da autorizuje uređaj na mreži.ZigBee kordinator je obično posvećen kao usluga centara poverenja.[18]

Različite kompanije koje se bave IoT tehnologijama imaju potpuno različit pristup kada su u pitanju pojedini aspekti bezbednosti. Tako recimo Wind River smatra da metod stavljanja malicioznih korisnika interneta na crnu listu ne može biti primenjen na terenske uređaje jer zahtevaju previše prostora na disku. Takode, ne automatska autentikacija za terenske uređaje nema previše smisla jer kod senzora i aktuatora nema nekoga ko bi mogao da prosledi akreditive na server za autentikaciju.

Wind River, koji je vodeća kompanija na polju embedded softvera, predlaže da se za IoT vertikale bezbednost primenjuje tokom celokupnog životnog ciklusa i to na sledeći način[19]:

17 The Future of IoT: Why We Need the Open Interconnect Consortium, Samsung Developer Connection, Published on Nov 19, 2014, video, 20.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=D7zmqX5pmPc

18 Robert Cragie, ZigBee Security, ZigBee Alliance ZARC Security Task Group, ©2009 ZigBee Alliance, dostupno na mreži; https://docs.zigbee.org/zigbee-docs/dcn/09-5378.pdf

19 SECURITY IN THE INTERNET OF THINGS, Lessons from the Past for the Connected Future, White Paper, Wind River, 2015, dostupno na mreži: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

- Bezbedno podizanje operativnog sistema na uređajima (eng. Secure booting)
- Kontrola pristupa
- Autentikacija na nivou uređaja (svaki krajnji nod IoT vertikale bilo da je senzor ili aktuator mora se autentikovati svom mrežnom kontroleru, inteligentnom gateway ili na cloud pre nego što počne da prima ili šalje podatke)
- Krajnji nodovi moraju ispred sebe imati fajervol koji ih štiti od malicioznih napada sa interneta
- Pečevi i upgrade moraju se dostavljati tokom celog životnog veka ali moraju biti centralizovani za celu vertikalu, te zahtevati minimalni bandwith.

Osnovni organizacioni problem bezbednosne prirode mogao bi se opisati na sledeći način. IoT uređaji na mreži se ponašaju kao računari i imaju bezbednosne probleme „klasičnih" računara, ali se njima ne upravlja kao računarima. Najbolji primer ovoga su medicinski aparati koji su spojeni na LAN mrežu koje koristi medicinsko osoblje a setuje, održava, vrši daljinske dijagnostike i rešava probleme, vendor.[20]

Proizvođači IoT uređaja se bore s time kako da se uklope u postojeće bezbednosne strategije. Pritisak dovođenja proizvoda na tržište u što kraćem roku je takav da mnogi proizvođači preuranjeno iznose svoje uređaje na tržište u nadi da se bezbednosni problemi neće pojaviti u ranoj fazi razvoja IoT tržišta i da će im to obezbediti dovoljno vremena da uočene nedostatke isprave kroz upgrade i patch softvera. Ovakav pristup dovodi do toga da jedan bezbednosni propust u jednoj oblasti (sektoru) može lako da se prenese na drugu i to prestavlja osnovni bezbednosni nedostatak IoT vertikala.

MOGUĆA REŠENJA BEZBEDNOSNIH PROBLEMA U OKVIRU IOT TEHNOLOGIJA

Postojeća bezbednosna internet rešenja

Tokom istraživanja koje je SANS Institut uradio, bezbednost IoT tehnologija je ocenjena kroz sledeći niz karakteristika[21]:

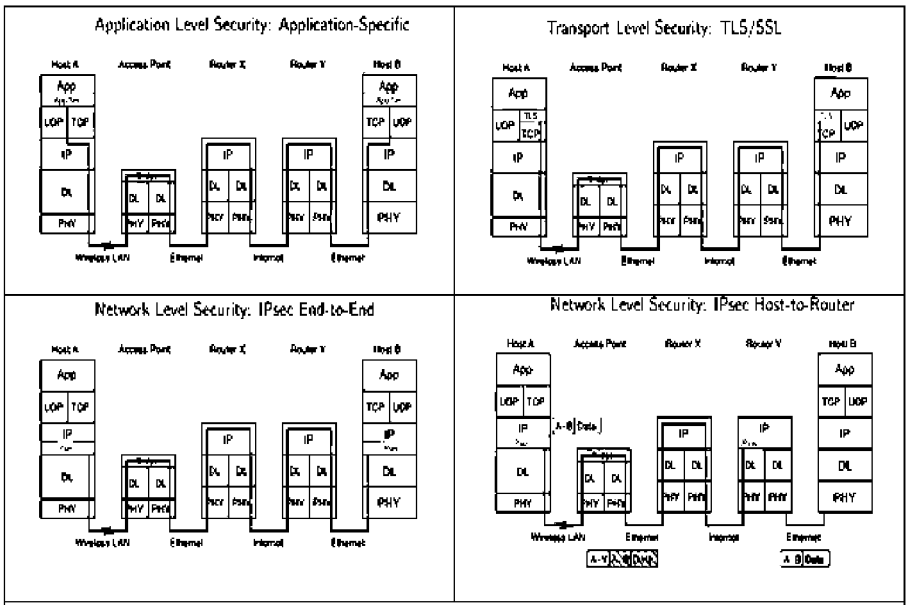
- 78% ispitanih smatra da mogućnosti za osnovnu vidljivost i upravljanje IoT uređajima treba obezbediti nekom od sigurnosnih mera i/ili porce-

20 James Kaplan, Cyber security and the Internet of things, Synergia Foundation, **Published on May 27, 2015, video, 09.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=h7Xk_KADKyo**

21 Security Realities of IoT (Internet of Things), CISCO Blog, 20.01.2016, dostupno na mreži: http://blogs.cisco.com/tag/siem

dura. Ovome treba dodati da čak 46% nema razvijene politike za pristup i upravljanje IoT uređajima.

- Najčešće korištene tehnologije za obezbeđenje IoT uređaja su:
  - 68% authentication/authorization,
  - 65% system monitoring,
  - 49% segmentation.
- Od ukupnog broja implementiranih IoT uređaja, do 74% njih može se doći isključivo ručnom pretragom odnosno skeniranjem mrežnog segmenta na kojem se nalaze.
- Oko 67% ranih korisnika IoT tehnologije koristi SIEM za prikupljanje i monitoring IoT uređaja.



Slika 3: Poređenje bezbednosnog modela na nivou aplikacije i u transportnom nivou; Izvor: Knowing Internet Security At Network Layer And Link Layer | IT Security Lecture, Tutorial Video, Published on May 28, 2014, video, 12.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=x2qbLCoM0BY

Razmatrajući pitanje bezbednosti IoT tehnologije u celini moramo primetiti da je često prisutan disbalans između primenjenih tehnologija i mesta njihove primene u IoT lancu informacija pri čemu je pitanjima bezbednosti na pojedinim mestima unutar lanca posvećena prevelika pažnja (čime se stvaraju bespotrebni troškovi) dok se drugi segmenti lanca ostavljaju neobezbeđeni i nebezbedni.

Mogućnost bezbednog korištenja uređaja nije pitanje budućnosti već način razmišljanja posebno u fazama projektovanja i održavanja uređaja kao

i načina na koji se oni koriste. Bezbednost mora biti ugrađena već na čipu – sigurnost mora biti uneta na najdubljem mogućem nivou.[22]

Kombinovanje bezbednosnih rešenja primenjenih u različitim oblastima ICT tehnologija je očigledno neophodno da bi se postigao odgovarajući nivo bezbednosti za pojedine IoT vertikale. Bezbednost zasnovana na principima klasičnih IT tehnologija primenjiva je na nivou Cloud-a kao i na nivou enkriptovanih end-to-end aplikacija što pojedine Cloud platforme već sada nude. Dobar primer ovakve implementacije bezbednosnih strategija nudi Microsoft Azure platforma koja tokom pisanja aplikacije za senzor zahteva da bilo koja API funkcija bude enkriptovana.[23]

Druga strategija primenjiva za industrijske IoT vertikale mogla bi da se zasiniva na zaštiti po dubini koja se već dugi niz godina koristi kao način zaštite za SCADA sisteme. U ovoj bezbednosnoj strategiji bezbednost se proverava na više hijerarhijskih i organizacionih nivoa, kao i u proaktivnom, aktivnom i retroaktivnom modu.[24] Praćenje bezbednosnih incidenata i istorijskih logova jedan je od široko rasprostranjenih načina da se uspostavi odgovarajući nivo ICT tehnologija. SIEM (eng. Security information and event management) tehnologije standardizovane su za većinu klasičnog ICT softvera i hardvera pa je uz odgovarajuće prepravke postojećih SIEM rešenja koje korporacije poseduju moguće integrisati i dobar deo IoT uređaja – posebno onih opšte upotrebe (ne važi za industrijske uređaje usled jednog inherentnog ograničenja SIEM rešenja – pravila i značenja variraju od slučaja do slučaja). Da bi se postojeća SIEM rešenja prilagodila primeni i nad IoT uređajima i tehnologijama potrebno je da se uvedu jedinstveni standardi za logove, takođe da se prognostika na industrijskom nivou ne radi samo na osnovu logova jer su oni uvek u prošlosti već uzimajući i ukupnu kolektivnu prognostiku za ponašanje pomenutih uređaja. Strategija zaštite po dubini zahteva integraciju IoT tehnologija sa firewall i antivirus rešenjima koja deluju po dubini dok se postojeća SIEM rešenja mogu primeniti u oba scenarija i kao dodatni sigurnosni layer nad sistemom i kao deo sistema, s tim da kad se koriste u prvom scenariju postoji realno kašnjenje nad događajima odnosno događaji se analiziraju sa istorijskog aspekta i sigurnost sistema prilagođava se novonastalim pretnjama.

Treća moguća strategija razvoja adekvatnih bezbednosnih rešenja za IoT tehnologije mogla bi da se ogleda u razvoju novih bezbednosnih paradigmi i

22 Alex Hawkinson, Digital Future: The Internet of Things, Milken Institute, Published on Apr 28, 2015, video, 30.12.2015, dostupno na mreži: https://www.youtube.com/watch?v=qWR32v5uaI8

23 Mobile Apps to IoT: Connected Devices with Windows Azure, Microsoft Virtual Academy, 05.12.2015, dostupno na mreži: https://mva.microsoft.com/en-US/training-courses/mobile-apps-to-iot-connected-devices-with-windows-azure-8588?l=BrvcQz20_504984382

24 Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, Homeland Security, October 2009, U.S. Government, 20.01.2016, dostupno na mreži: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

njihovom prevođenju na nivo funkcionalnosti sistema. Chris Rezendes, razvio je bezbednosnu paradigmu koja se zasniva na sledećih sedam pitanja[25]:

- Šta hoćemo da instrumentalizujemo?
- Koje podatke hoćemo da dobijemo - imamo dostupne?
- Ko ima pristup ovim podacima?
- Ko poseduje ove podatke - ima vlasništvo nad njima?
- Ko određuje prava pristupa?
- Koji je minimalni komunikacioni metod (VPN, SSL, SSH,...)?
- Šta se dešava kad neko prekrši pravila?

Takođe prilikom određivanja bezbednosnih pravila treba se pridržavati tri sledeće maksime:

- Ljudi su iznad mašina
- Lica su iznad ekrana
- Velike potrebe iznad malih pogodnosti

Cloud security alliance dala je u svom vodiču za bezbednost ranih korisnika IoT tehnologija sledeću matricu sastavljenu od pitanja i odgovora kao pomoć pri određivanju odgovarajućeg oblika autentikacije IoT uređaja[26]:

	Pitanje	Optimalni autentikacijski metod
1	Da li implementacija zahteva M2M komunikaciju?	Ako je odgovor da, ispitajte komunikacijske protokole na uređaju i odredite da li oni podržavaju native autentikaciju.
2	Da li vaš IoT uređaj podržava neki od komunikacionih protokola koji pružaju uslugu autentikacije?	Ukoliko ne, razmotrite layer security model višeg tipa kao što su TLS ili DTLS.
3	Da li vaš IoT uređaj ima ograničenja po pitanju memorije ili procesorske snage?	Ukoliko da, razmotrite rad sa vendorima koji podržavaju IEEE 1609.3 sertifikate.
4	Ko će upravljati vašim uređajem? Da li je udaljen nadzor zahtevan?	Planirajte svoju implementaciju u zavisnosti od matrice kontrole pristupa i odaberite najjači metod autentikacije podržan za svaki uređaj u vertikali.
5	Da li vaš IoT uređaj poseduje mrežne menadžment funkcije kao što su SNMP ili SSH?	Onemogućite višak funkcionalnosti i zaključajte terenske uređaje tako da podržavaju uslugu autorizacije. Napravite protokol i poceduru za mrežni menadžment vaših uređaja.

25 Chris Rezendes, Rethink money and meaning with the internet of things: Chris Rezendes at TEDxSanDiego 2013, TEDx Talks, Published on Feb 14, 2014, video, 06.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=Q40TyD6YxdI

26 Cloud Security Alliance, Security Guidance for Early Adopters of the Internet of Things (IoT), *April 2015,* Mobile Working Group, dostupno na mreži: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

6	Da li vaš uređaj poseduje RESTful interfejs?	Razmotrite autentikaciju krajnjih nodova pomoću token baziranih protokola kakav je OAUTH 2
7	Da li se uređaj konektuje na cloud direktno?	Osigurajte da API funkcije koriste odgovarajući ključ za autentikaciju na cloud uslugu.

Rešenja kroz nove tehnologije –nebezbednosne tehnologije

Zahtevi za bandwidth-om neophodnim da se prenese dovoljna količina podataka sa lokalnog IoT senzora, aktuatora ili drugog uređaja možda bi u budućnosti mogli da se ostvare primenom Li-Fi tehnologije.[27] Li-Fi tehnologija pored pitanja protoka i bandwith-a rešava još neke inherentne slabosti Wi-Fi tehnologije kada je u pitanju bezbednost podataka i energetska efikasnost transportnog modela, a kao posebnu pogodnost njenoj ubrzanoj primeni svakako pogoduje činjenica da infrastruktura za ovu tehnologiju već postoji na svakom našem plafonu – kao izvor /predajnik moguće je koristiti bilo koje sijalično mesto.[28] Ono što takođe pogoduje razvoju Li-Fi tehnologije je činjenica da je ona praktično imuna na ograničenja vezana za industrijske uslove i da se bez posebne već sa standardnom opremom može primenjivati i u industrijskim postrojenjima.

ZAKLJUČAK

Upravljanje bezbednošću IoT vertikala je stalan posao i nikada se ne završava, jer svakodnevno nastaju nove pretnje od kojih sistem treba odbraniti. To znači da sistem bezbednosti mora biti ne samo proaktivan već i sposoban da evoluira kroz vreme te obezbedi svu neohodnu zaštitu onda kada je potrebna a da istovremeno ne bude procesorski zahtevan zbog oskudne procesorske snage na krajnjim čvorovima IoT vertikale (senzorima i aktuatorima).

Bezbednost sa stanovišta IoT tehnologija treba posmatrati uvek u smislu konteksta na koje se pomenuta IoT vertikala i bezbednosno pitanje odnosi. Tako možemo razlikovati praktično dva potpuno suprostavljena tipa bezbednosti nad IoT vertikalama:

- Privatni, koji se zasniva na permisi da informacije i upravljanje nad industrijskim uređajima i tehnologijama te nad privatnim posedima mora biti zaštićeno od zloupotreba i obezbeđeno dovoljnim nivoom tehnološke, pravne i operacione bezbednosti, te da svaki vlasnik neke imovine o ko-

27 Li-Fi, 100X Faster Than Wi-Fi! | ColdFusion, ColdFusion, Published on Nov 27, 2015, video, 08.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=wqH9KX9o0vg

28 Harald Haas: Wireless data from every light bulb, TED, Uploaded on Aug 2, 2011, video, 08.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=NaoSp4NpkGg

joj se stara ili kojom upravlja neka IoT vertikala, ima pravo da zna na koji način je njegovo vlasništvo obezbeđeno i do kog nivoa. Takođe, ista bezbednosna paradigma mora da važi i u slučajevima kada se IoT koristi u medicinske, vojne ili svrhe upravljanja industrijskim kapacitetima, kod kojih bilo koji neovlašten ili maliciozni napad i proboj te neovlašteno pribavljanje i manipulacija sa informacijama koje potiču sa IoT sistema mogu da imaju štetne ili čak fatalne posledice. Postojeće tehnologije ne mogu u potpunosti da zaštite uređaje, vertikale i informacije ali proizvođači, vendori i zakonodavci traže adekvatna rešenja od kojih se najprihvatljivijim može oceniti strategija bezbednosti po dubini za koju zaključujemo da je osnovni pravac razvoja bezbednosnih tehnologija u okviru IoT tehnologija kada je u pitanju rad nad privatnim podacima i sistemima.

- Javni, koji se zasniva na permisi da su informacije, koje iz realnog sveta uzima, prenosi i transformiše odgovarajuća IoT vertikala, od opšteg javnog interesa i da ni na koji način ne smeju biti privatne već javno dostupne svima koji žele da ih koriste. Osnovni vid ovakvih informacija su informacije o vremenu, zagađenosti, vodi, elementarnim nepogodama ali i informacije od značaja za druga javna dobra i ustanove. U ovakvom okruženju, pitanje beznednosti se svodi na stalnu dostupnost i ispravnost informacija. Ipak, kako ovaj oblik informacija do sada nije bio u ovoj meri dostupan javnosti, postavlja se pitanje šta će se desiti ako sva javna vlasništva učinimo dostupnim (svim stejkholderima) u smislu informacije ili čak upravljanja? Ovo je važno pitanje jer značaj IoT tehnologija ide iznad tehnologije ili finansija, te ima opšti značaj.

Alicija Asin, CEO Libelium, smatra da zahvaljujući IoT tehnologijama u konceptu pametnih gradova javne informacije moraju biti dostupne u standardizovanim formatima i dostupne svima na način da im svako može pristupiti i tumačiti uz minimalni softver.[29] Takođe, smatra da bi u ovakvom scenariju razvoja pametnih gradova IoT tehnologija mogla da dovede do demokratizacije informacija od javnog značaja i time da veću mogućnost uvida, kontrole ali i odgovornosti svih građana za funkcionisanje istih. Slažući se sa mogućnostima demokratizacije informacija koje IoT tehnologije donose u ovom scenariju, zaključujemo da je implementacija istih u ovim scenarijama ne samo poželjna već neophodna, te da bi se radi realizacije opštih interesa morala što brže obaviti. U tom smislu preporučujemo svim javnim institucijama i dužnosnicima da razmotre ovu mogućnost za demokratizaciju javnih dobara kroz informacione tehnologije a posebno kroz IoT

29 Alicia Asin: "Big Data and the Hypocrisy of Privacy" - Strata Europe 2014, O'Reilly, Published on Nov 20, 2014, video, 08.01.2016, dostupno na mreži: https://www.youtube.com/watch?v=oWwQfgpvlzI

tehnologije koje bi bile javno dostupne. Takođe, na globalnom planu možemo zaključiti da bi zajednički cilj primene IoT tehnologija dugoročno mogao da se ogleda u maksimi prema kojoj svi živimo na istoj planeti, a IoT tehologije nam mogu pomoći da uvidimo načine na koje se naš zajednički životni prostor upotrebljava i kako da ga zaštitimo od zloupotreba.

Abstract

This paper deals with the review of the existing technologies, compares views on security issues of IoT technologies from leading experts and companies in the field and proposes a general security solution at the level of application and in terms of establishing appropriate safety conditions and legislation that would have to organize this field better and more thoroughly.

It analyzes current perception of solutions providers and the market about IoT devices and their hereditary problems related to the need for extremely rapid development and putting into use, as well as problems with interoperability that emerges from constant increase in number of IoT devices and the number of their manufacturers.

Considered are the safety aspects of IoT technologies through IoT concept as a factor of change in the way we think about our everyday lives and the consequential role of individuals in enforcing security of IoT systems.

In conclusion, adding to the needs to define security standards and the existence of built-in security in every IoT device, we emphasize the need for transparency of the IoT security technologies.

Keywords: *IoT, Internet of things, technology, trend, security, development, industry, social impact*

LITERATURA

1. John Thompson, Keynotes 2014 Chicago Internet of Things World Forum, Published on Oct 22, 2014, video, 30.12.2014, dostupno na mreži: *https://www.youtube.com/watch?v=--lwl0GbZd_c*
2. IDC Reveals Worldwide Internet of Things Predictions for 2015, Press Release, 03 Dec 2014, IDC Futurescape for Internet of Things, 13.01.2016, dostupno na mreži: *https://www.idc.com/getdoc.jsp?containerId=prUS25291514*
3. Brian Witten, IoT is Starving for Built-In Security, TIA NOW, Published on Sep 17, 2015, video, 10.01.2015, dostupno na mreži: *https://www.youtube.com/watch?v=v9vvNfe39is*
4. Tapping into the Potential of the Industrial IoT, Moxa, January 2016, newsletter, 13.01.2016, dostupno na: *http://www.moxa.com/newsletter/connection/2016/01/feat_01.htm?utm_source=2016_01_Connection&utm_medium=email&utm_campaign=Connection&mkt_tok=3RkMMJWWfF9wsRoiuq%2FAZKXonjHpfsX%2B4uQoXbHr08Yy0EZ5VunJEUWy3oEFSNQ%2FcOedCQkZHblFnV4JS62vS7cNoq0O*
5. Dr. Joseph Reger, Fujitsu Forum 2013 Keynote: Internet of Things, Fujitsu - Human Centric Innovation, Published on Nov 14, 2014, video, 08.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=dbPLQXABavw*

6. Andy Green, Hackers Remotely Kill a Jeep on the Highway—With Me in It, 07.21.2015, 08.01.2016, dostupno na mreži: *http://www.wired.com/2015/07/hackers-remotely-kill-jeep--highway/*
7. Peter Warren Singer: "Cybersecurity and Cyberwar: What Everyone Needs to Know" | Talks at Google, Published on Feb 10, 2014, video, 17.01.2016, dostupno na mreži: *https://www.youtube.com/watch? v=h0SXO5KUZIo*
8. Javno dostupni materijali sa govorima Baraka Obame, Bela kuća, Tehnology, Cybersecurity and Internet Policy, 17.01.2016, dostupno na mreži: *https://www.whitehouse.gov/issues/technology*
9. Remarks by Director David H. Petraeus at In-Q-Tel CEO Summit, Excerpts from Remarks Delivered by Director David H. Petraeus at the In-Q-Tel CEO Summit (March 1, 2012), 20.01.2016, dostupno na mreži: *https://www.cia.gov/news-information/speeches-testimony/2012--speeches-testimony/in-q-tel-summit-remarks.html*
10. Lawrence Conway, Obama ordered cyber-attacks on Iran's nuclear programme but created a super-virus that is now 'out of control', DailyMail, 1 June 2012, članak, 20.01.2016, dostupno na mreži: *http://www.dailymail.co.uk/news/article-2153308/Cyberattacks-Iran-ordered-Obama-created-virus-creating-havoc-internet.html#ixzz3xmY9vj62*
11. Mark Stanislav, Top 3 Security Issues in Consumer Internet of Things (IoT) and Industrial IoT, The Internet of Things IoT Inc Business Channel, Published on Mar 4, 2015, video, 25.12.2015, dostupno na mreži: *https://www.youtube.com/watch?v=QelfiNqvhPU*
12. Joe Colantonio, Bob Crews, Shailesh Mangal, The Internet of Things - Risks Presented by Security, webinar part 2, test talks, www.getzephyr.com, Published on Jul 31, 2015, video, 10.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=ZodKWqiT5HE*
13. Defcon 18 - SCADA and ICS for Security Experts: How to avoid Cyberdouchery, video, available online: *http://www.youtube.com/watch?v=4gLAbIc2k9E*
14. When IoT attacks, a case study, Kaspersky Lab, Billy Rios, Published on May 15, 2015, video, 17.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=j0QgDEB9yKo*
15. The Future of IoT: Why We Need the Open Interconnect Consortium, Samsung Developer Connection, Published on Nov 19, 2014, video, 20.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=D7zmqX5pmPc*
16. Robert Cragie, ZigBee Security, ZigBee Alliance ZARC Security Task Group, ©2009 ZigBee Alliance, dostupno na mreži; *https://docs.zigbee.org/zigbee-docs/dcn/09-5378.pdf*
17. SECURITY IN THE INTERNET OF THINGS, Lessons from the Past for the Connected Future, White Paper, Wind River, 2015, dostupno na mreži: *http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf*
18. James Kaplan, Cyber security and the Internet of things, Synergia Foundation, Published on May 27, 2015, video, 09.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=h7Xk_KADKyo*
19. Security Realities of IoT (Internet of Things), CISCO Blog, 20.01.2016, dostupno na mreži: *http://blogs.cisco.com/tag/siem*
20. Alex Hawkinson, Digital Future: The Internet of Things, Milken Institute, Published on Apr 28, 2015, video, 30.12.2015, dostupno na mreži: *https://www.youtube.com/watch?v=qWR32v5uaI8*
21. Mobile Apps to IoT: Connected Devices with Windows Azure, Microsoft Virtual Academy, 05.12.2015, dostupno na mreži: *https://mva.microsoft.com/en-US/training-courses/mobile--apps-to-iot-connected-devices-with-windows-azure-8588?l=BrvcQz20_504984382*
22. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense--In-Depth Strategies, Homeland Security, October 2009, U.S. Government, 20.01.2016, dostupno na mreži: *https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf*

23. Chris Rezendes, Rethink money and meaning with the internet of things: Chris Rezendes at TEDxSanDiego 2013, TEDx Talks, Published on Feb 14, 2014, video, 06.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=Q40TyD6YxdI*
24. Cloud Security Alliance, Security Guidance for Early Adopters of the Internet of Things (IoT), April 2015, Mobile Working Group, dostupno na mreži: *https://downloads.cloudsecurityalliance.org/whitepapers /Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf*
25. Li-Fi, 100X Faster Than Wi-Fi! | ColdFusion, ColdFusion, Published on Nov 27, 2015, video, 08.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=wqH9KX9o0vg*
26. Harald Haas: Wireless data from every light bulb, TED, Uploaded on Aug 2, 2011, video, 08.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=NaoSp4NpkGg*
27. Alicia Asin: "Big Data and the Hypocrisy of Privacy" - Strata Europe 2014, O'Reilly, Published on Nov 20, 2014, video, 08.01.2016, dostupno na mreži: *https://www.youtube.com/watch?v=oWwQfgpvlzI*

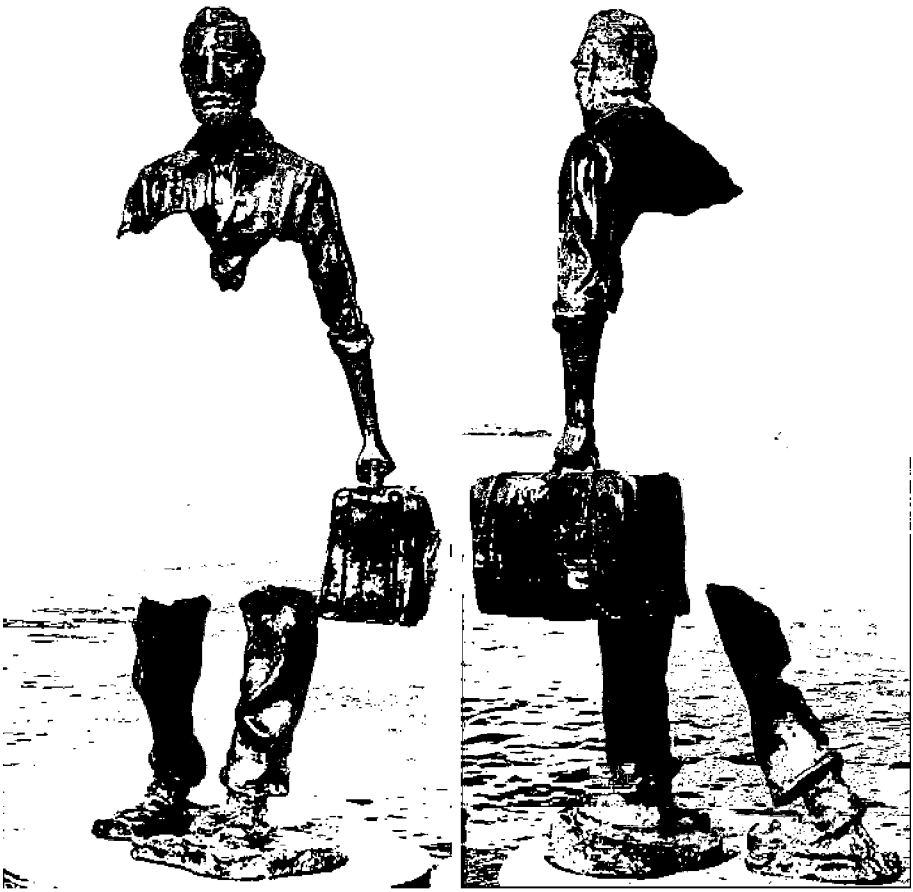


Image: „Refugee" by Frances Bruno Catalano