FBIM Transactions
DOI 10.12709/fbim.05.05.02.03

ČOVEK-U-SREDINI NAPADI I INTERNET STVARI

MAN-IN-THE-MIDDLE ATTACKS AND INTERNET OF THINGS

Zoran Čekerevac
Faculty of Business and Law, "Union - Nikola Tesla" University in Belgrade, Serbia

Zdenek Dvorak
Faculty of Security Engineering, University in Žilina, Slovakia

Ludmila Prigoda
Faculty of Economics and Service, Maykop State Technological University, Maykop, Russia

Petar Čekerevac
Hilltop Strategic Services, Belgrade, Serbia

JEL Category: **L86, O33**

Apstrakt

Izvanredno brz razvoj računara i računarskog softvera su neki od uzroka sigurnosnih propusta koji napadačima omogućavaju uspešno izvođenje napada na informacione sisteme njihovih korisnika. Masovno širenje Interneta stvari će napraviti veću razliku između trenutnog shvatanja Interneta, koje se ogleda u "dot-com", "društvenim mrežama" i veb "iskustvu", i novog Interneta koji će dobiti nove i revolucionarne aplikacije sa potencijalom da značajno poboljšaju kvalitet života. S obzirom na to da se različiti uređaji već isporučuju sa ugrađenim računarskim komponentama i sa mogućnošću povezivanja sa Internetom i mogućnostima međusobne komunikacije sasvim je realno da budu izloženi nekim varijantama napada koji su već viđeni u dosadašnjoj praksi. U ovom radu su analizirani neki aspekti "čovek u sredini" napada u vezi sa Internetom stvari. Posle kratkog uvodnog izlaganja o Internetu stvari i "čovek u sredini" napadu, u radu je prikazana tehnologija izvođenja ovog napada, kao i eventualne koristi koje napadač može imati od uspešno izvedenog napada. Takođe, prikazani su i neki poznatiji primeri uspešno izvedenih napada, kao i neki od načina zaštite od tih i sličnih napada. Razmotrene su i ekonomske posledice

Adresa autora zaduženog za korespodenciju:
Zoran Čekerevac
zoran@cekerevac.eu

ovakvih napada. U zaključku je prikazan rezime cele analize uz pretpostavke o budućem razvoju Interneta stvari i napadima na priključene uređaje.

Ključne reči: *Internet stvari, čovek u sredini, internet prisluškivanje, komunikacije*

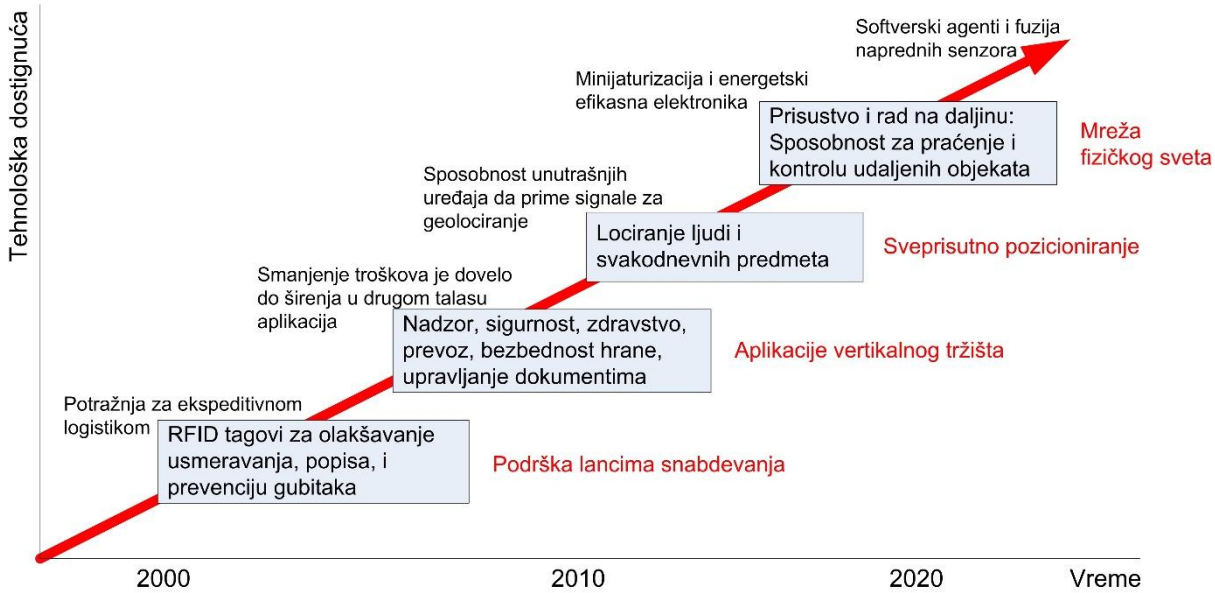
Abstract

A rapid development of computers and computer software are some of the causes of the security vulnerabilities that allow attackers to successfully carry out attacks on information systems of their users. The massive spread of the Internet of Things will make a greater difference between the current understanding of the Internet, which is reflected in the "dot-com", "social networks" and web of "experience", and the new Internet that will enable new and revolutionary applications with the potential to significantly improve the quality of life. Given that different devices have come with embedded computer components and connectivity to the Internet, and the possibilities of mutual communication, it is realistic they will be exposed to some variants of attacks that have been seen in practice so far. This paper analyzes some aspects of the "man in the middle" attacks related to the Internet of things. After a short introductory presentation on the Internet of things and "man-in-the-middle" attack, the paper presents the technology of this attack, as well as the benefits that an attacker could have from a successful attack. Also, here are shown some known examples of successful attacks, the economic consequences of such attacks, as well as some of the ways of protection against these and similar attacks. The conclusion shows the summary of the whole analysis together with the assumptions on the future development of the Internet of things and the possible attacks on the connected devices.

Keywords: *Internet of things, man-in-the-middle, IT, Internet, eavesdropping, ARP poisoning, DNS spoofing, SSL hijacking*

1 UVOD

„Internet Stvari“ (IoT), kao sistem međusobno povezanih računarskih uređaja, svojim ubrzanim razvojem i distribucijom u životu je interesovanja korisnika Interneta, posebno korisnika pametnih uređaja. Tome u prilog ide činjenica da IoT nije ograničen samo na mehaničke i digitalne mašine, već obuhvata i druge predmete, životinje, pa čak i ljude. Zajedničko im je da poseduju jedinstvene identifikatore koji imaju sposobnost da prenose podatke preko mreže. Zbog toga se danas često koristi, kao termin sa najširim značenjem, i termin „Internet svega“.



Slika 1 Razvoj Interneta Stvari

Izvor: Autori na osnovu (Mouser, 2015)

Internetom stvari omogućena je međusobna komunikacija priključenih uređaja putem Interneta. Priključeni uređaji poseduju ugrađenu inteligenciju koja im omogućuje da prate i analiziraju podatke i preduzimaju mere bez ljudske intervencije. Veštačka inteligencija čini ove sisteme mnogo efikasnijim za obavljanje mnogih poslova.

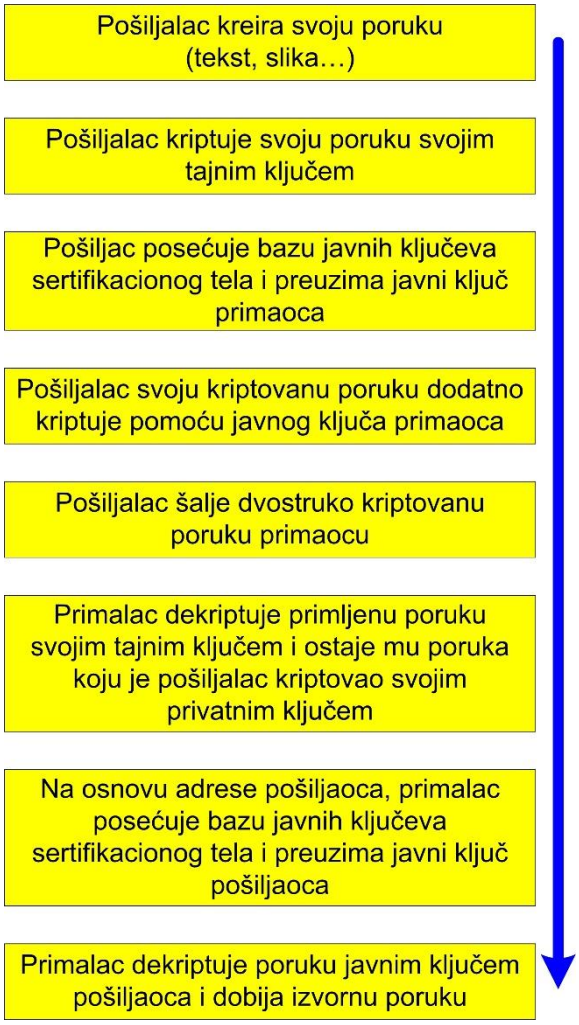
Vizualizacija razvoja Interneta stvari prikazana je na slici 1. Predviđa se da će u 2020-oj godini 50 milijardi uređaja biti priključeno na Internet. Takvo masovno širenje IoT će izazvati veću razliku između trenutnog shvatanja Interneta, koji se sveo na „dot-com“, „društvene mreže“ i veb „iskustva“, i novog Interneta koji će dobiti nove i revolucionarne aplikacije sa potencijalom da značajno poboljšaju kvalitet života. To će promeniti način na koji ljudi žive, uče, rade i zabavljaju se. (Evans, 2011). Pametni kućni uređaji u okviru pametne mreže mogu da reaguju na spoljašnje komande i da usklađuju svoj rad. Npr. u situacijama vršnog opterećenja električne mreže, da bi se izbeglo preopterećenje mreže, kućni aparati bi mogli da redukuju sopstvenu potrošnju, pa eventualno i da se privremeno isključe, ako to ne ugrožava izvršenje zadatka. Već danas postoje uređaji u teretanama koji snimaju parametre rada srca vežbača i druge parametre koje preuzimaju sa mašine na kojoj vežbač vežba. Oni zatim računarom obrađuju registrovane podatke i na displeju prikazuju rezultate treninga. Time se mogu optimizovati treninzi i postići bolji rezultati. Postoje i uređaji koji omogućavaju merenje nivoa šećera u krvi i koji mogu da aktiviraju insulinske pumpice kada je to potrebno. Mogućnosti su praktično neograničene.

Lepo je i korisno kada je pametni televizor, ili pametni sat, povezan sa Internetom i prima, ili šalje, podatke koje korisnik želi. Ali, pre nego što stignu do svoje konačne destinacije podaci prolaze kroz sva četiri sloja TCP/IP modela, a svi oni su izloženi brojnim rizicima. Sa intenzivnim korišćenjem skladišta podataka smeštenih u Oblaku, može se reći da se pojavio i peti sloj, sloj Oblak. Postoji niz načina da ovaj sloj bude napadnut, počevši od napada sa primenom brutalne sile pa do sofisticiranijih napada krađom lozinki. Korišćenjem MITM napade moguće je promeniti podatke u sloju sesije. Ne treba izgubiti iz vida ni snifer napade, DoS napade, kao i napade upotrebom kompromitovanog ključa.

Sa rastom umrežavanja, sa rastom računarstva u oblaku, sa pojavom Interneta stvari (IoT) i Bring-Your-Own-Technology (BYOT), napadači pronalaze nove načine kako da MITM napad ponovo postane atraktivan. Cilj ovog rada je da predstavi kratku analizu tehnologije MITM napada zajedno sa nekim primerima napada ove vrste i nekim ekonomskim faktorima s tim u vezi.

2 TEHNOLOGIJA MITM

Čovek u sredini napad je postojao i mnogo pre pojave kompjutera. Za prikaz osnova MITM napada može da se koristi primer zlonamernog poštara koji otvara pisma ljudima i čita ih ili menja njihov sadržaj pre nego što dostavi pismo primaocu.



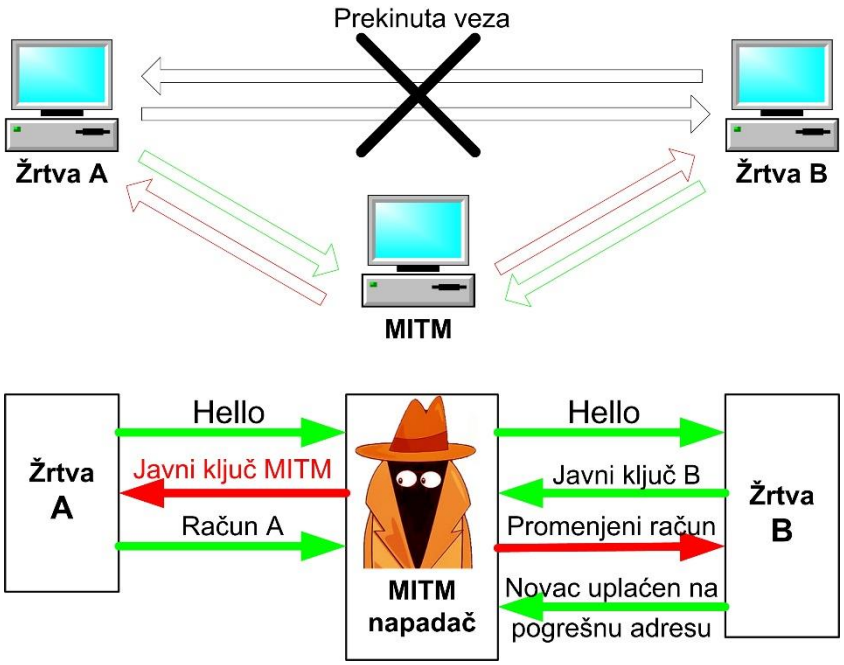
Slika 2. Algoritam slanja poruka na siguran način

Za pružanje usluga na bezbedan način većina internet aplikacija teži ka tome da koristi kriptovane veze koje nude TLS/SSL protokoli. Ovaj skup protokola obezbeđuje „point-to-point“

konekcije koje omogućavaju privatnu i bezbednu razmenu poruka između dve autentifikovane strane, kao što je prikazano na slici 2.

Međutim, zbog složenosti u administraciji, TLS/SSL se uglavnom koriste tako da samo jedan učesnik potvrđuje vezu. Pored toga, SSLv3 ne vrši validaciju određenih delova podataka koji prate svaku poruku (Jovanović, Maček, Franc, & Mitić, 2016). Ovaj način rada predstavlja slabost, koja se može iskoristiti za napad. Ta slabost je otkrivena septembra 2014. godine, pa je SSLv3 protokol zamenjen TLSv1.0 protokolom. Preporučeno je da se SSLv3 protokol potpuno isključi iz upotrebe zbog svojih slabosti, ali ga neki serveri i dalje koriste kako bi održali kompatibilnost sa IE6. Prema (Mutton, 2016), 95% HTTPS servera je podložno jednostavnim MITM napadima. Samo 1 od 20 HTTPS servera ispravno implementira HTTP Strict Transport Security mehanizam, široko podržane bezbednosne funkcije koja sprečavaju posetioce da ostvare nekriptovane HTTP veze sa serverom.

MITM napadač koristeći različite tehnike želi da presretne poruke između dva čvora. Kada uspe da prekine vezu svojih žrtava, on dolazi u situaciju da može da preuzme ulogu posrednika. Primer jednog MITM napada prikazan je na slici 3. Da bi korisnik A poslao (pred)račun korisniku B na "siguran" način, on želi da pošalje kriptovanu poruku. Komunikaciju počinje slanjem poruke "Hello" i od sertifikacionog tela traži javni ključ primaoca (pred)računa B. Pošto je veza prekinuta, umesto sertifikacionog tela poruku prima MITM napadač.



Slika 3 Jedan primer MITM napada
Izvor: Autori na bazi (DuPaul)

On prosleđuje poruku sertifikacionom telu sa svojim parametrima, primljeni (svoj) javni ključ šalje pošiljaocu A i prati njegovu reakciju. Pošiljalac A nesvesan da je poruku primio od napadača šalje dvostruko kriptovanu poruku koju napadač može da dekriptuje svojim privatnim ključem i javnim ključem pošiljaoca. Zatim napadač menja parametre u (pred)računu, preuzima javni ključ žrtve B i šalje joj svoju dvostruko kriptovanu poruku. Žrtva B dekriptuje primljenu dvostruko kriptovanu poruku svojim privatnim ključem i javnim ključem napadača. Ukoliko ne proverava sertifikate i ne primeti zamenu pošiljaoca, smatrajući da je primila traženi (pred)račun, žrtva B plaća novac na pogrešan račun u banci i počinje da čeka isporuku plaćene robe. Žrtva A nije svesna da je novac uplaćen, a žrtva B nije svesna da je novac uplaćen na pogrešan račun. Napadač uzima deponovana sredstva, nestaje, i ostavlja žrtve da se posle isteka roka isporuke sude. Ova vrsta napada se zove manipulacija. Napadi pri kojima se poruke

samo čitaju i prosleđuju nepromenjene pripadaju drugoj grupi MITM napada, prisluškivanju. Slaba karika u ovom napadu je komunikacija sa sertifikacionim telom, pošto napadač ostavlja svoj trag. Ukoliko napadač uspe da na neki od načina zaobiđe sertifikaciono telo, ima velike šanse na uspeh i kod iskusnijih korisnika.

MITM napadi mogu da se sprovode na nekoliko načina:

- Trovanje ARP keša;
- Trovanje DNS keša;
- Otmica sesije; ili
- SSL otmica.

Ove metode su u detalje objašnjene u brojnoj literaturi i ovde neće biti detaljnije razmatrane.

U okviru ovih metoda mogu se koristi dsniff aplikacije za prikupljanje tekstualnih podataka na nesigurnim vezama, što im je i osnovna funkcija. Dsniff, skup alata za analizu mrežnog saobraćaja, prikuplja korisnička imena i lozinke, adrese posećivanih veb stranica, sadržaj i-mejl poruka i sve ono što se po mreži kreće u obliku čistog teksta. Kada jednom uhvatiti korisničko ime i lozinku, napadač ima sve što mu je potrebno za napad. Napadač može imati i dodatne pogodnosti ako administrator koristi isto korisničko ime i lozinku za sve usluge i sisteme. U okviru dsniff paketa alata nalaze se i alati arpspoof, dnsspoof i macof koji mogu olakšati presretanje mrežnog saobraćaja normalno nedostupnog napadaču (na primer, zbog Layer 2 switching).

U prošlosti, MITM napadima su uglavnom pogađani laptop računari, ali, sada, zahvaljujući masovnoj primeni mobilnih telefona znatno veći broj korisnika može biti izložen napadima. Problem može postati još veći, jer je nedavna Simantekova studija pokazala da oko 50% ispitanika i ne razmišlja o zaštiti svojih podataka. (Covington, 2016). Povećavanje broja uređaja priključenih na Internet i širenje IoT predstavlja novu oblast koja će biti interesantna napadačima.

Jedan od prvih načina na koji se može izvesti napad je lokalni napad preko Eternet veze ili Wi-Fi. Napadač sa pristupom lokalnoj kućnoj mreži može izvršiti napade na pametne kućne uređaje na dva načina: Cloud polling i direktna veza.

U slučaju Cloud pollinga, pametni kućni uređaj je u stalnoj komunikaciji sa Oblakom. Pametan uređaj stalno proverava Cloud Server da li je dostupna novija verzija softvera. Ako jeste, tada on šalje svoj status. Ciljajući takvu aplikaciju, napadač može izvršiti MITM napad. On može da preusmeri mrežni saobraćaj korišćenjem npr. ARP trovanja. Za presretanje HTTPS saobraćaja napadač može da koristi samopotpisani sertifikat ili neke alate kao što su SSLstrip. Kada se veza vrši preko HTTPS, neki od pametnih uređaja ne proveravaju da li se može verovati sertifikatu. Prema (Barcena & Wueest, 2015), nijedan od uređaja koji su oni testirali ne vrši međusobnu obostranu SSL autentifikaciju. Uglavnom se vrši samo autentifikacija servera, a većina uređaja u potpunosti ignoriše sertifikat omogućavajući napadaču da koristi ukradene ključeve bez ikakvih problema.

U slučaju direktne veze, uređaji komuniciraju sa habom ili aplikacijom u istoj mreži. SSDP i UPnP (Simple Service Discovery Protocol i Universal Plug and Play) protokoli mogu da se koriste za otkrivanje uređaja. Svaki napadač može da uradi to isto. Na ovaj način, mobilna aplikacija može da pronađe nove uređaje skeniranjem i ispitivanjem, na određenom portu, svake IP adrese na lokalnoj mreži.

O traganju za žrtvama, auto detekciji lokalnih interfejsa i podrazumevanih mrežnih prolaza, kao i o podešavanjima MITM napada za žrtve, rutere, IP prosleđivanje, i vraćanje žrtve u prvobitno stanje nakon napada, može se naći u brojnim izvorima, npr. (Edwards, 2016), (How to conduct a simple man-in-the-middle attack, 2014) ili (Kapil, Manoj, & Borade, 2016), pa to ovde neće biti dublje analizirano.

Blutut sa niskom potrošnjom (BTLE, ili BLE), poznat i kao Bluetooth-Smart je novi način modulacije definisan u Bluetooth Core Spec 4.0. (Marquess & et al., 2010) Ova tehnologija je u velikom usponu, a može da se koristi za mnoge namene, uključujući i senzore, kućnu automatizaciju, kućne aparate, medicinska sredstva, brave, alarme, i druge „pametne“ stvari. Pametni uređaji, koji je koriste, a samim tim i IoT, mogu biti ugroženi blutut hakovanjem.

Neko može reći da je operativni domet blutut uređaja ograničen i da je MITM napad teško izvršiti zato što napadač mora da bude blizu napadnutih uređaja. Ali, BLE može imati domet i veći od 100 m. Osim toga, u nekim slučajevima, uređaji i ne moraju da budu blizu jedan drugom.

Napadač može da prenese pakete daljinski, preko Interneta.

Neke mobilne aplikacije poseduju mogućnost prenosa podataka direktnim kontaktom uređaja ili prinošenjem drugog uređaja u blizinu prvog uređaja. Te karakteristike se mogu zloupotrebiti približavanjem pametnog telefona, na kome se izvršava zaražena aplikacija, u opseg dometa telefona. Takvim malverom se upravlja daljinski, a teoretski je moguće izvršiti i masovni napad. (Jasek S. , 2016)

U svom radu, Slawomir Jasek (2016) je utvrdio da je sve veći broj blutut uređaja koji se koriste za ulaz bez ključa i mPOS sistema podložan MITM napadima. On je naveo da, iako BLE specifikacija obezbeđuje sigurne veze enkripcijom na sloju veze, putem bele liste uređaja, i povezivanja, „kompanije često nepravilno primenjuju ove mere zaštite i ovaj nedostatak može da dozvoli napadačima da kloniraju BLE uređaje.“ Nakon kloniranja, napadači „mogu da dobiju neovlašćeni pristup fizičkim uređajima kada se pametni telefon koristi kao kontrolor uređaja“, kao i hvatanje podataka i manipulaciju podacima prenetih između dva BLE uređaja." Jasek procenjuje da je 80 odsto BLE pametnih uređaja podložno MITM napadima. (Spring, 2016)” Po ovom istraživanju, IoT uređaji su pogrešno konfigurisani i omogućavaju hakerima da koristeći neke od hakerskih alata, kao npr. GATTacker, ostvare MITM napad. Jasek je objasnio da pomoću nekoliko jednostavnih trikova, napadač može da navede žrtvu da se umesto na pravi uređaj poveže na napadačev. Korišćenje uobičajenih mana, uključujući i nepravilnu autentifikaciju i statičke lozinke, može da omogući napadaču da preuzme kontrolu nad pametnim bravama i pametnim kućama (Spring, 2016)”.

3 KOLIKO SU ČESTI MITM NAPADI U IOT?

Postoje milijarde ugroženih IoT uređaja, i njihov broj rapidno raste. Većina njih je uvek uključena i boravi na nenadgledanim mrežama. Ako ove mreže omogućavaju veze velike brzine, kompromitovani uređaji mogu da budu učesnici masovnog DDoS napada. Takvi uređaji su već korišćeni za DDoS napade, slanje spam poruka, otmicu MITM akreditiva, pravljenje haosa na internetu, kao i za druge zlonamerne aktivnosti. Jedan od masovnih napada koji je uključio IoT uređaje protiv provajdera Dyn je analiziran u (Gallagher, 2016). Ovde neće biti detaljnije analizirani DDoS napadi, već će se uglavnom razmatrati rizici povezani sa uređajima kao što su automobili, veb kamere, digitalni video rekorderi, kablovska televizija, satelitski set-top boksovi, mobilni telefoni, itd. Svi ovi uređaji ne zahtevaju neko posebno održavanje i imaju nizak nivo interakcije. Korisnici su na to navikli i obično nisu ni svesni da mogu da budu žrtve potencijalnih napada.

Širenjem IoT, MITM napadi će postati sve veći izazov. Jedna vrsta MIT IoT napada cilja pametne telefone i koristi slabu validaciju sertifikata. Drugi primer, bliži kućnim uređajima, može biti ilustrovan IoT frižiderima koji prikazuju Google kalendar korisnika.

Barcena i Wueest, su u svom istraživanju (2015) analizirajući mrežni saobraćaj, primetili da "LightwaveRF smart hub generiše određeni mrežni saobraćaj pri svakom restartovanju i svakih 15 minuta da bi proverio da li treba ažurirati softver". Uređaj je ostvarivao komunikaciju sa udaljenim TFTP[1] serverom na Internetu. Kako je TFTP protokol vrlo bazičan fajl transfer protokol, ova veza nije kriptovana ni authentifikovana. Zbog toga može vrlo lako da postane predmet MITM napada.

Symantec je analizirao 50 pametnih kućnih uređaja uključujući Pametne termostate, pametne brave, pametne sijalice, pametne detektore dima, pametne sisteme za upravljanje energijom, itd., i ustanovio da nijedan od uređaja nije primenjivao jake lozinke, nije koristio međusobnu potvrdu identiteta, ili se štitio od napada grubom silom. Skoro 2 od 10 mobilnih aplikacija, koje su se koristile za kontrolu testiranih IoT, nisu koristile Secure Sockets Layer (SSL) za kriptovanje komunikacije u oblaku. Testirana IoT tehnologija je takođe sadržala mnoge uobičajene ranjivosti. (Barcena & Wueest, 2015)

U leto 2014. godine, Samsung je izneo na tržište svoj RF28HMELBSR pametni frižider. Frižider je

[1] TFTP – Trivial File Transfer Protocol

imao implementiran SSL, ali nije verifikovao SSL sertifikate. Ova slabost može dovesti do izvođenja uspešnog MITM napada i krađe korisnikovih Google akreditiva. (Gregg, 2015) Neverifikacija SSL sertifikata omogućuje MITM napade protiv drugih veza, uključujući i one koje se koriste za preuzimanje informacija iz Gmail kalendara za prikaz na ekranu frižidera. Korišćenjem MITM je moguće ukrasti žrtvine Google akreditive. Prema (Venda, 2015), potencijalni rizik nastaje kada se terminal povezuje sa serverom radi ažuriranja. Tokom testiranja bezbednosti, bilo je moguće izolovati URL https://www.samsungotn.net. Ovaj URL se takođe koristi kod Samsung televizora, itd., ali komunikacija između frižider-terminala i servera za ažuriranje tokom testiranja nije mogla da bude presretnuta..

I drugi uređaji povezani sa IoT takođe mogu biti žrtve MITM napada. Lako je zamisliti scenario u kome zlonamerni konkurent poželi da lažira podatke o temperaturi uređaja, promeni ih i dostavi ih nadzornom sistemu. Dobivši lažne podatke, regulator temperature može ostaviti mašine bez dovoljnog hlađenja što može da dovede do pregrevanja mašine i samim tim i prekida proizvodnje. Osim zaustavljanja proizvodnje, to može da izazove i fizičko oštećenje mašine i finansijsku štetu radnoj organizaciji. (Simko, 2016)

Jedan od razloga zašto su IoT uređaji atraktivni napadačima je da se mnogi od ovih uređaja isporučuju sa nesigurnim podrazumevanim vrednostima podešavanja. Ovo se pre svega odnosi na (Arbor, 2016):

- podrazumevane administrativne akreditive;
- otvoren pristup sistemima za upravljanje preko internet-orijentisanih interfejsa na ovim uređajima;
- ugrađene sisteme koji se retko, ako se uopšte, ažuriraju;
- nedostatak pružanja bezbednosnih popravki. Mnogi od proizvođača uopšte i ne vrše ažuriranje softvera, a pored toga,
- isporučuju se sa nesigurnim, daljinski iskoristivim kodom.

Jedno moderno motorno vozilo može biti povezano sa više mreža, uključujući mrežu mobilne telefonije, blutut, Wi-Fi i ožičeni mobilni Eternet. Ove prednosti se javljaju i kao dodatni rizik. Jedan od nedavnih MITM napada na pametna motorna vozila desio se u julu 2015, kada je hakovan Jeep Cherokee. Bez upotrebe važnih mera bezbednosti, hakeri mogu da dođu u poziciju da mogu da kontrolišu osnovne funkcije vozila, kao što su kočenje, upravljanje i/ili ubrzavanje, što bi moglo da bude veoma opasno. (Simko, 2016)

Prema SEC Consult i analizi u kojoj su posebnu pažnju posvetili kriptografskim ključevima, njihovi istraživači su pregledali firmver imidže više od 4000 uređaja proizvedenih od strane više od 70 proizvođača i otkrili više od 580 jedinstvenih privatnih. Upoređujući svoje rezultate sa podacima iz Internet-Wide Scan Data Repository (Scans.io i Censis.io) otkrila su da je njihov skup rezultata sadržao (SEC Consult, 2015):

- „privatne ključeve za više od 9% svih HTTPS hostova na Vebu (~ 150 serverskih sertifikata, koji se koriste na 3,2 miliona hostova) i
- privatne ključeve za više od 6% svih SSH hostova na Internetu (~ 80 SSH host ključeva koji se koriste na 900 hiljada hostova)“

Pored toga, oni su oporavili oko 150 HTTPS server sertifikata koji se koriste na 3,2 miliona uređaja, a zajedno sa 80 SSH host ključeva, koriste na najmanje 900 hiljada uređaja. U tu analizu su bili uključeni različiti uređaji: Internet mrežni prolazi, modemi, ruteri, IP kamere, VoIP telefoni, itd.

U narednom poglavlju će biti razmotreni još neki od MITM napada i ekonomske posledice tih napada.

4 EKONOMSKE POSLEDICE MITM NAPADA

Veoma je teško naći tačne podatke o gubicima usled MITM napada. MITM napadi obično ciljaju pojedince, a oni ne objavljuju svoje gubitke. Kompanije često i ne žele da kažu korisnicima da njihovi proizvodi mogu biti žrtva MITM napada. Stoga, lako je zaključiti da su objavljeni napadi samo vrh ledenog brega. Definisanje troškova povezanih sa posledicama MITM napada je još teže kada se MITM napadi posmatraju kao komponenta ostalih poznatih napada, uključujući i DDoS.

Ranije opisana situacija u kriptografiji može dovesti do velikih gubitaka uzrokovanih budućim MITM napadima. Situacija sa reciklažom

kriptografskih ključeva postaje još teža kada se uzme u obzir da se mnogim od uređaja može pristupiti iz javne mreže. Ovo omogućava MITM napadu lako otkrivanje akreditiva i/ili otmicu sesije.

Pomenuto hakovanje vozila Jeep dovelo je do toga da FIAT Chrysler opozove 1,4 miliona vozila, i automobila, i kamiona. (AP, 2015) Za proizvođača, FCA SAD, to je značilo veliku neprijatnost i velike potencijalne gubitke oko slanja više od milion USB memorija sa zakrpama za softver, ali ovi gubici mogu da budu i veći kada se uzmu u obzir gubici zbog gubljenja dobre reputacije i smanjenja blagonaklonosti klijenata. S druge strane, za korisnike, osim gubitka vremena, hakovanje vozila bi moglo da znači i gubitak njihovih (i ne samo njihovih) života.

Imajući u vidu mogućnost napada i sa njima povezanih gubitaka, korisnici Interneta imaju razloga da misle i o deljenju rizika sa osiguravajućim društvima. „Sajber osiguranje može da obezbedi dragocen i fleksibilan alat za pokrivanje mnogih vrsta sajber gubitaka.“ (Watson, 2016) Dobro je da se obezbedi pokrivenost štete od najčešćih mogućih napada, na najširim osnovama i to pre nastale štete. Ali, da bi se uspešno preneo rizik, zbog brzog razvoja u ovim oblastima, pokrivenost mora da bude fleksibilna i da nastupi pre nastanka štete, da bude proaktivna.

Na kraju, ali ne nevažne, su moguće štete koje bi mogle da budu uzrokovane MITM napadom u kombinaciji sa kripto analizom RSA algoritma. Takav napad, uz upotrebu skromnih računarskih resursa, može ugroziti bezbednost svakog od veb sajtova u slučajevima korišćenja 512 bitnih RSA ključeva. (Jovanović, Maček, Franc, & Mitić, 2016)

5 KAKO SE IOT MOŽE ZAŠTITI OD MITM NAPADA?

Potpuna eliminacija MITM napada je veoma težak zadatak, ali pažljivi korisnik može da značajno smanji rizik.

Zbog velikog broja funkcija koje svaki računar poseduje, postoje različite vrste MITM napada, ali i različite vrste odbrane koje se mogu primeniti. Iako ne postoji čarobni štapić koji može zaštititi IoT uređaj ili računar od svih napada, jedan od najboljih pristupa je da se o zaštiti razmišlja još u fazi kreiranja mreže, a zatim da se redovno ažurira operativni sistem. Mnogi uređaji su jedinstveni, napravljeni za posebne namene i stoga je i njihova zaštita specifična pa, u izvesnoj meri, može biti i lakša. Međutim, broj i raznovrsnost uređaja, i težnja da se primenjuju jeftinija rešenja su takođe i otežavajuća okolnost. Ovi uređaji se često puštaju u prodaju sa sigurnosnim propustima, pa mogu biti podložni MITM napadima.

U stabilnim uređajima, koji se nalaze u sigurnim privatnim mrežama, prva linija odbrane je na nivou rutera, a druga na nivou uređaja. S obzirom na činjenicu da su uređaji stalno povezani sa Internetom, da svaki uređaj ima svoj originalni softver i da se ga korisnici retko kontrolišu, moguće zaštita se svodi na odgovarajuću konfiguraciju fajervola i periodično (redovno) ažuriranje softvera iz proverenih izvora. Gde je to moguće, treba koristiti SSL sertifikate i jaku enkripciju između klijenta i servera. Ako se konfiguracija mreže retko menja, moguće je napraviti listu statičkih ARP ulaza i rasporediti ih na klijente automatskom skriptom. Ovo može osigurati da se uređaji oslanjaju na svoj lokalni ARP keš umesto da se oslanjaju na ARP zahteve i odgovore (Sanders, Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1), 2010).

U slučaju prenosnih uređaja, MITM napade je moguće sprečiti time da se uređaji nikada ne povezuju direktno na Wi-Fi rutere nesigurnih mreža. U takvim mrežama treba koristiti dodatnu zaštitu kad god je to moguće, na primer, HTTPS Everywhere ili ForceTLS.

DNS spufing je po svojoj prirodi uglavnom pasivan, tako da je teško odbraniti se. Kod vrlo ciljanih napada sasvim je moguće da žrtva nikada neće znati da je bila napadnuta. Ali, postoji nekoliko stvari koje se mogu uraditi (Sanders, 2010A):

- obezbediti unutrašnje mašine;
- nemati nikakve veze sa DNS serverima;
- koristiti sistem za detekciju napada (IDS); i
- koristiti DNSSEC.

Isto tako, nekoliko stvari može da se uradi u odbrani od krađe sesije (Sanders, 2010B):

- koristiti onlajn bankarstvo od kuće;
- biti svestan opasnosti i pratiti stvari koje izgledaju neobično; i
- obezbediti sopstvene mašine, jer se takvi napadi uglavnom izvršavaju unutar mreže.

SSL otmicu je praktično nemoguće otkriti sa strane servera, ali neke stvari mogu da se urade na strani klijenta (Sanders, 2010C):

- obezbeđivanje sigurne veze primenom HTTPS;
- korišćenje onlajn bankarstva od kuće; i
- obezbeđivanje sopstvenih mašina.

Da bi se obezbedila pouzdana identifikacija uređaja učesnika u IoT komunikaciji, IoT mora da obezbedi veću primenu kriptografije javnim ključem (PKC). Glavni izazov pri korišćenju PKC je utvrđivanje da li je javni ključ autentičan i da li pripada određenom licu, ili je zamenjen od strane napadača. Verifikacija zahteva da digitalni sertifikat bude izdat od strane sertifikacionog organa od poverenja. Kada jednom komunikacija počne bezbedno, rizici povezani sa MITM napadom su značajno smanjeni.

Međutim, ključevi iz infrastrukture javnog ključa (PKI) mogu biti ugroženi, a to može uticati na druge uređaje. Jedan od bitnih elemenata je par javnog ključa i privatnog ključa (tzv. „root key“, ili „rut ključ“) generisanih od strane sertifikacionog tela. Ključna komponenta rada sertifikacionog tela je prihvatanje sertifikata izdatih od tog sertifikacionog tela u okviru pretraživača, na primer Microsoft, Opera itd. Baš to je ostvareno rut ključevima koje brauzer provajderi uključuju u svoje operativne sisteme. Kada je jednom rut ključ postao rut ključ od poverenja - bilo koji digitalni sertifikat izdat od tog sertifikacionog tela će se smatrati legitimnim. Kada napadač ostvari pristup rut ključu, on je u poziciji da potpiše maliciozni softver i kreira lažne potvrde. Rešenje je da se uključi „root of trust“ (RoT), skup funkcija u posebnom računarskom modulu koji kontroliše kriptografski procesor na računarskoj platformi od poverenja. (Jamie, 2016)

Na kraju, neki od načina za smanjenje rizika od MITM napada na mobilne telefone, mogu da budu izbegavanje funkcija „Auto connect“ i „Reply“, izbegavanje upotrebe ugrađenih linkova na veb stranicama i mejlovima koji nisu od poverenja, kao i neotvaranje neočekivanih priloga. Treba ignorisati neočekivanu komunikaciju, ali i obratiti pažnju na eventualne nagle promene u poslovnoj praksi sa poznatim partnerima. Svaku takvu naglu promenu bi trebalo proveriti nekim drugim sredstvom komunikacije. Iako praktično ne postoji mogućnost potpune zaštite mobilnih telefona, rizik se može smanjiti nekorišćenjem softvera iz neproverenih izvora i neuklanjanje ograničenja u proverenom softveru.

6 ZAKLJUČAK

Zaštita IoT uređaja zavisi od niza faktora, počevši od proizvođača samog uređaja i njegove koncepcije zaštite uređaja, pa sve do krajnjeg korisnika i njegovog shvatanja rizika i potrebe za neprestanim ažuriranjem softvera. Između svih faktora najizraženiji su identifikacija uređaja i kripto zaštita veze uređaja i njegovog korisnika. Te komunikacije zahtevaju sertifikate za obostranu identifikaciju učesnika. S obzirom na to da već postoje milijarde uređaja i da njihov broj neprekidno raste, može se očekivati da će IoT uređaji vrlo često i dugo biti ugroženi, ako ništa drugo, a ono u periodu od momenta povezivanja uređaja na Internet do momenta otkrivanja ranjivosti uređaja. Ako se uzme u obzir i faktor „korisnik“ problem postaje izraženiji. Teško je verovati da će svaki korisnik redovno vršiti ažuriranje softvera svakog svog uređaja. Sa strane proizvođača, problem se pogoršava željom proizvođača da stalno snižava proizvodne troškove i koristi jeftinija rešenja. Jeftiniji proizvod vrlo često znači i od napada manje zaštićen proizvod. Posledica može da bude mnogo, ali jedna od njih je mogućnost da se napad sa jedne slabe tačke proširi na celu mrežu. Napadači su često u prednosti i u pogledu raspoloživog znanja i u pogledu opreme koja im stoji na raspolaganju.

MITM napadi svojim specifičnostima i raznovrsnošću opstaju kao efikasna tehnologija za vršenje napada i sticanje nelegalne koristi, posebno u kombinaciji sa drugim vrstama napada. Meta MITM napada su obično pojedinačni korisnici, a vrlo često takvi napadi ostaju neotkriveni i nezabeleženi u statistici. Kada se radi o kompanijama, one, i kada otkriju da su žrtve napada, vrlo često, iz marketinških razloga, nemaju interes da to i publikuju. Zbog toga se publikuju samo napadi širokih razmera koji se ne mogu prikriti ili bi njihovo prikrivanje moglo da dovede do enormnih gubitaka. Na osnovu analiziranih primera, analiza je pokazala moguće razmere posledica MITM napada na koje će uticati i rastući broj IoT uređaja. Istraživanje je pokazalo da pored izuzetnih potencijala IoT postoje i izuzetni rizici koji mogu nastati nedovoljnom zaštitom.

Iako ne postoji magični štapić koji će obezbediti potpunu zaštitu, postoje dve magične reči koje mogu smanjiti probleme: prevencija i proaktivnost!

CITIRANI RADOVI

AP. (2015, July 27). *Jeep Hacking Incident Leads to Fiat Chrysler Recall of 1.4M Vehicles*. Retrieved from Claims Journal: http://www.claimsjournal.com/news/national/2015/07/27/264766.htm

Barcena, M. B., & Wueest, C. (2015, Mar 12). *Insecurity in the Internet of Things.* Retrieved from Symantec: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf

Covington, M. (2016, Oct 8). *Free Wi-Fi and the dangers of mobile Man-in-the-Middle attacks.* Retrieved from betanews: http://betanews.com/2016/10/08/free-wi-fi-mobile-man-in-the-middle-attacks/

DuPaul, N. (n.d.). *Man in the Middle (MITM) Attack.* Retrieved Nov 28, 2016, from Veracode: http://www.veracode.com/security/man-middle-attack

Edwards, R. (2016, Aug 119). *Simple Man-in-the-Middle Script: For Script Kiddies.* Retrieved from Wonderhowto: http://null-byte.wonderhowto.com/news/simple-man-middle-script-for-script-kiddies-0168192/

Evans, D. (2011, Apr). *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything.* Retrieved from Cisco - White Paper: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Gregg, M. (2015, Dec). *How new technologies are reshaping MiTM attacks*. Retrieved from TechTarget: http://searchnetworking.techtarget.com/tip/How-new-technologies-are-reshaping-MiTM-attacks

How to conduct a simple man-in-the-middle attack. (2014). Retrieved from wonderhowto: http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/

Jamie. (2016, Feb 12). *Protecting IoT Against Man-in-the-Middle Attacks*. Retrieved from Bizety: https://www.bizety.com/2016/02/12/protecting-iot-against-man-in-the-middle-attacks/

Jasek, S. (2016). *Gattacking Bluetooth smart devices.* Retrieved from blackhat: https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf

Jasek, S. (2016, Jul-Aug). GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy. *Black hat USA 2016* (p. 49). Mandalaya Bay, Las Vegas: Black hat. Retrieved from Black hat: https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf

Jovanović, M., Maček, N., Franc, I., & Mitić, D. (2016). Modern cyber security threats: On software vulnerabilities and threats. *Zbornik radova ZITEH-16* (pp. 1-10). Belgrade: IT Veštak.

Kapil, J., Manoj, J., & Borade, J. (2016). A Survey on Man in the Middle Attack. *IJSTE, 2*(9), 277-280. Retrieved from http://www.academia.edu/24382368/A_Survey_on_Man_in_the_Middle_Attack

Marquess, K., & et al. (2010, Jun 30). *Bluetooth specification version 4.0.* Retrieved from Bluetooth.org: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737

Mouser. (2015, Jun 23). *The Internet of Things Hits Its Stride*. Retrieved from Mouser Elevtronics: https://www.eeweb.com/company-blog/mouser/the-internet-of-things-hits-its-stride

Mutton, P. (2016, Mar 17). *95% of HTTPS servers vulnerable to trivial MITM attacks*. Retrieved from Netcraft: https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html

Sanders, C. (2010, Mar 17). *Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1).* Retrieved from windowsecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

Sanders, C. (2010A, Apr 7). *Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing.* Retrieved from Windowsecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html

Sanders, C. (2010B, May 05). *Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking.* Retrieved from Windowsecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html

Sanders, C. (2010C, Jun 9). *Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking.* Retrieved from WindowSecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html

SEC Consult. (2015, Nov 25). *House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide.* Retrieved from Blog.sec-consult: http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html

Simko, C. (2016, Feb 26). *Man-in-the-Middle Attacks in the IoT*. Retrieved from GlobalSign Blog: https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

Spring, T. (2016, Aug 11). *Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable*. Retrieved from threatpost: https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

Watson, W. T. (2016, Oct 28). *The "Internet of Things" attacks.* Retrieved from Willis Towers Watson Wire: http://blog.willis.com/2016/10/the-internet-of-things-attacks/

Datum prve prijave: 05.02.2017.
Datum prihvatanja članka: 18.02.2017.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017, July 15). Čovek-u-sredini napadi i Internet stvari. (Z. Čekerevac, Ed.) *FBIM Transactions, 5*(2), 18-28. doi:10.12709/fbim.05.05.02.03

*Style – **Chicago** Sixteenth Edition:*

Čekerevac, Zoran, Zdenek Dvorak, Ludmila Prigoda, and Petar Čekerevac. "Čovek-u-sredini napadi i Internet stvari." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 5, no. 2 (July 2017): 18-28.

*Style – **GOST** Name Sort:*

Čekerevac Zoran [et al.] Čovek-u-sredini napadi i Internet stvari [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Belgrade - Toronto : MESTE, July 15, 2017. - 2 : Vol. 5. - pp. 18-28.

*Style – **Harvard** Anglia:*

Čekerevac, Z., Dvorak, Z., Prigoda, L. & Čekerevac, P., 2017. Čovek-u-sredini napadi i Internet stvari. *FBIM Transactions,* 15 July, 5(2), pp. 18-28.

Style – **ISO 690** Numerical Reference:

Čovek-u-sredini napadi i Internet stvari. **Čekerevac, Zoran, et al.** [ed.] Zoran Čekerevac. 2, Belgrade - Toronto : MESTE, July 15, 2017, FBIM Transactions, Vol. 5, pp. 18-28.