1 Uvod

Računari se sve više integrišu u naše živote. Od kada su nastali pa sve do danas, stepen primene računara i integracija u život pojedinca, preduzeća i država je rastao eksponencijalno. Iako nismo stigli do letećih automobila, izumi koji se razvijaju i otkrivaju u poslednjim godinama su izuzetno impresivni – autonomni kamioni, nanoroboti, ponovno-upotrebljive rakete i Nintendo svič. Prateći ovaj eksponencijalan razvoj tehnologija, moguće je zamisliti razne vizije budućnosti – apokaliptične, distopijske, ali i utopijske.

U ovom poglavlju će se razmotri digitalizacija sveta i uloga bezbednosti u ovakvom svetu. Analiziraće se spoj softverskog inženjerstva i informacione bezbednosti i izneće se motivacija za izradu bezbednog softvera. Na kraju će biti postavljena osnovna terminologija informacione bezbednosti, koja je neophodna za razumevanje svog daljeg gradiva iz ove oblasti.

1.1 Digitalna revolucija

Druga polovina dvadesetog veka je obeležena fenomenom koji se naziva digitalna revolucija. Od tada, pa sve do danas, računarski sistemi igraju sve veću ulogu u životu čoveka. Integracija informaciono komunikacionih tehnologija u ljudsku civilizaciju raste eksponencijalno i inovacije koje se danas uvode u razvoj i primenu softverskih sistema je mnogo teže ispratiti nego pre deceniju ili dve. Ispratiti samo najnovije radne okvire za razvoj *JavaScript* aplikacija je izazov, dok je održavanje koraka sa alatima i tehnologijama iz više domena gotovo nemoguće.

Danas je teško pronaći ozbiljno preduzeće koje nema svoj internet portal, ili makar *Facebook* stranicu. Mnoge korporacije idu korak dalje i unapređuju svoje poslovanja upotrebom računara i interneta. Glavni razlog iza ovoga je optimizacija poslovanja, odnosno smanjenje troškova i povećavanje profita preduzeća. Primenom novih tehnologija, firme uspevaju da:

- Ponude svoje proizvode i servise velikom broju ljudi, upotrebom interneta;
- Prikupljaju i analiziraju velike količine podataka koje je nemoguće ručno pregledati, kako bi stekli jasniji uvid u svoje poslovanje i prilagodili se potrebama tržišta;
- Uvedu automatizaciju u svoje operacije, bilo da je rad fabričkih postrojenja ili administrativnog posla, gde mašine efikasnije vrše posao od čoveka, sa manjim stepenom greške.

Upotrebom računarskih sistema, preduzeća unapređuju efikasnost svog poslovanja, ubrzavaju svoje poslovne procese i drastično smanjuju troškove. Jedan interesantan primer primene najnovijih tehnologija predstavlja metod *lights-out* izrade proizvoda. Ove autonomne fabrike zahtevaju od čoveka da donese sirovine potrebne za izradu proizvoda na jedan kraj fabrike i da pokupi gotov proizvod na drugom kraju. Ostatak posla, kao što je izrada samog proizvoda, je prepuštena orkestru robota.

Tesla, preduzeće koje proizvodi autonomna vozila, nastoji da načini svoje fabrike autonomnim [1]. Nije teško zamisliti scenario u bliskoj budućnosti gde autonomni kamion dostavlja sirovine za proizvodnju, spakovane u standardizovane kontejnere, do fabrike, koja ih potom preuzima i od njih pravi automobile. Čovek bi potom mogao, putem onlajn prodavnice i upotrebom kreditne kartice, da kupi autonomni automobil iz te fabrike, koji će se dovesti ispred kuće novog vlasnika. U čitavom scenariju jedino je kupac čovek, dok su svi ostali učesnici mašine.

Pravna lica nisu jedini subjekti koji su transformisani od strane digitalne revolucije. Računar je postao jednako zastupljen u domaćinstvu koliko i frižider, dok je pametan telefon nešto bez čega retko koji čovek prođe kroz dan. Vlasnici ovih uređaja pripadaju svim starosnim grupama, od dece do penzionera i procenat stanovništva koji koristi ove uređaja je prešao trećinu svetske populacije [2]. Dalje, većina ljudi će pogledati

u svoj telefon više puta na dan, i aktivno ga koristiti za komunikaciju, zabavu, posao, istraživanje i u druge svrhe i po više sati dnevno. Pametni telefon je u mnogim delovima sveta postao toliko sveprisutna tehnologija, da za mnoge ljude njihov telefon predstavlja produžetak njih samih, kolekcija digitalnih identiteta za razne servise i sajtove. Poredeći ovo sa stanjem kakvo je bilo pre samo deset godina, moguće je uočiti koliko je tehnološki skok transformisao svakodnevni život pojedinca.

Zahvaljujući tehnološkom razvoju i upotrebom računara u svim mogućim sferama života, ljudska civilizacija je krenula u eksponencijalan razvoj. Iako je teško odrediti precizno koliko podataka se danas skuplja i skladišti, mnogi izvori tvrde da je samo u sklopu 2017. godine sačuvano više podataka nego u prethodnih 5000 godina čovečanstva [3]. Veštačka inteligencija, autonomna vozila, fabrike, roboti, internet stvari (engl. *Internet of Things;* skraćeno *IoT*), 3d štampanje, kvantno računarstvo, nanotehnologije, sve su ovo tehnologije koje se danas razvijaju i koje obećavaju da će dovesti drastične promene kroz takozvanu četvrtu industrijsku revoluciju [4] (engl. *Industry 4.0*).

1.2 Kvalitet u softverskom inženjerstvu

U civilizaciji koja sve više zavisi od računara i softvera, softverski inženjeri su postala cenjena i tražena profesija. S' obzirom na trendove koji su prikazani u prethodnom poglavlju, jasno je da će posla za inženjere računarskih sistema biti još dugi niz godina, no svakako je pitanje šta će tačno biti problemi koje ćete baš vi rešavati, odnosno proizvodi koje ćete konstruisati.

To može biti nešto što vam je blisko, poput informacionog sistem za podršku rada preduzeća, veb-aplikacije koja pruža neki servis, a može biti i nešto potpuno drugačije, poput pametnog automobila, autonomne fabrike softvera ili video igre. Spektar mogućnosti je ogroman i raste iz dana u dan, te se ne treba ograničavati na već viđene probleme, pogotovo ne na samom početku karijere.

Nezavisno od toga kakav softver budete konstruisali, bilo da su to drajveri za 3d štampače ili inteligentni orkestratori IoT uređaja, ono što je zajedničko jeste da ćete imati zadatak da napravite **kvalitetno** rešenje koje ispunjava neke **funkcionalne zahteve**. Funkcionalni zahtevi diktiraju šta je ono što vaš softver treba da radi, odnosno koje su funkcije koje treba da ispunjava. Iako nije uvek lako definisati funkcionalne zahteve, pogotovo na početku razvoja projekta, vremenom se oni jasno definišu i moguće je relativno lako proveriti njihovu ispunjenost i ispravnost. Sa druge strane, izgradnja kvalitetnog rešenja i uopšte određivanje šta čini neko rešenje kvalitetnim je popriličan izazov.

Postoji više notacija i standarda koji govore šta predstavljaju aspekti kvaliteta softvera. Različiti izvori informacija navode različite aspekte, te skup najčešće navedenih aspekata kvaliteta podrazumeva:

- **Pouzdanost** (engl. *Reliability)*, što podrazumeva stabilan i ispravan rad softvera, tako da su greške sistema, njegov otkaz i period kada ne radi ispravno minimizovani;
- **Efikasnost** (engl. *Efficiency*), što podrazumeva visoke performanse sistema i neophodna skalabilnost, kako bi efikasno radio i u momentima kada je pod visokim opterećenjem;
- **Održivost** (engl. *Maintainability*), što podrazumeva pravljenje čistog rešenja koje se može ažurirati, ispravljati i održavati uz minimalno uloženog vremena. U sklopu ovog aspekta se često navode sledeća svojstva:
    - **Prilagodljivost** (engl. *Adaptability*) podrazumeva izradu softvera koji se brzo i jednostavno može izmeniti i nadograditi kako bi se lako moglo odgovoriti na dinamične promene potreba tržišta;
    - **Prenosivost** (engl. *Portability, Transferability*) sa jedne strane podrazumeva konstrukciju softvera koji se lako može preneti u drugo okruženje i postaviti da radi, dok sa druge strane podrazumeva izradu čistog i dobro dokumentovanog rešenja tako da se može preneti drugom timu inženjera za dalji razvoj.

- **Upotrebljivost** (engl. *Usability*), što podrazumeva sa jedne strane laku upotrebu softvera od strane njegovih ljudskih korisnika (ukoliko dati softver ima interfejs za čoveka), a sa druge strane jednostavnu konfiguraciju i održavanje sistema u produkciji, od strane administratora sistema;
- **Bezbednost** (engl. *Security*), što podrazumeva izgradnju rešenja koje adekvatno štiti sebe i osetljive podatke sa kojima radi od malicioznih napadača.

Primetićete da su u prethodnom nabrajanju korištene reči poput „lako“, „jednostavno“, „brzo“, „adekvatno“. Problem kod izgradnje kvalitetnog softvera je baš taj što su sami aspekti kvaliteta zasnovani na rečima koje imaju različito značenje za različite ljude, a čak i za istog čoveka u različitom vremenskom periodu. Kod koji vam danas deluje lak za održavanjem vam može za pola godine delovati nemoguć, kada se vratite da ga doradite. Isto tako, korisnički interfejs koji razvijate nedeljama može za vas biti potpuno intuitivan i jednostavan, a za korisnika koji ga vidi prvi put potpuno konfuzan i nejasan.

Treba istaći da različiti aspekti kvaliteta ne postoje u vakuumu. Ponekad će rad na jednom aspektu kvaliteta doprineti unapređenju drugog aspekta. Isto tako, unapređenje jednog aspekta može da degradira drugi. Na primer, pisanje čistog koda držeći se najboljih praksi definisanih od strane seniora u timu unapređuje održivost, ali takođe i bezbednost softvera. Sa druge strane, instalacija bezbednosne kontrole poput šifrovanja svog saobraćaja može da degradira performanse, dok zahtevanje od korisnika da poštuje strogu bezbednosnu polisu može da naruši upotrebljivost.

Razvoj kvalitetnog softverskog rešenja je veština koju ćete učiti tokom čitavog radnog veka. Kako da prepoznate kvalitet i integrišete ga u vašu izradu rešenja je nešto što ćete naučiti kroz rad na projektima, kroz diskusije sa kolegama ili na nekim okupljanjima poput *meet-up*-a. Knjige, članci, onlajn predavanja pa i fakultet i njegovo osoblje su dobar izvor saveta i caka kako možete dodatno da unapredite vaš proces razvoja softvera i učinite proizvode vašeg truda utoliko boljim. Fokus upravo ovog predmeta jeste da se analizira bezbednost kao jedan veoma relevantan i bitan aspekt kvaliteta u vremenu četvrte industrijske revolucije.

1.3 Bezbednost u softverskom inženjerstvu i šire

Sada kada je definisan položaj bezbednosti u softverskom razvoju, moguće je razmotriti svrhu ovog kursa. Ideja jeste da se kroz ovo potpoglavlje da odgovor na pitanje „Zašto da se cimam oko ovoga?“.

Za početak, formulisaćemo sledeću tvrdnju: *„Softverski inženjer, bilo da vrši funkciju arhitekte sistema, kodera, testera ili administratora, koji vrši svoje poslovanje tako da ima bezbednost na umu i trudi se da proizvede celokupno bezbednije rešenje je vredniji od onog inženjera koji vrši isti posao, samo bez obzira na bezbednost.“*

Ako je bezbednost definisana kao aspekt kvaliteta, onda je lako dokazati da je prethodna tvrdnja istinita, no to je ne čini previše mudrom. Zdravorazumski je da inženjer koji radi svoj posao kvalitetno je bolji od onog koji to ne čini. Postavlja se onda pitanje zašto je bezbednost posebno interesantna i da li je više ili manje bitna u odnosu na ostale aspekte kvaliteta. Odgovor je jednostavan – zavisi od zahteva biznisa. Da bi mogli da definišemo prioritet bezbednosnih zahteva, potrebno je da prođemo kroz niz događaja koji su se odvili na svetskoj sceni u proteklim godinama.

Poslednjih nekoliko godina su obeležene sa nekoliko značajnih napada i otkrića u domenu bezbednosti računarskih sistema koji su zabrinuli kako javnost tako i biznise. Navesti i adekvatno opisati svaki značajniji incident koji se odvio u protekloj deceniji bi zahtevalo nekoliko knjiga. Ono što sledi je samo mali podskup ovih incidenata, gde je svaki incident praćen kratkim opisom, bez nekog prioriteta ili pravila:

- U 2017. godini je grupa istraživača otkrila da većina procesora proizvedena u proteklih 20 godina ima ranjivost koja omogućuje programu da pročita kompletan sadržaj radne memorije, odnosno

RAM-a. Ovo nije ranjivost na nivou aplikacije, niti na nivou operativnog sistema, već na nivou dizajna samog procesora. Ranjivosti su nazvane Sepctre i Meltdown od kada su javno objavljene početkom 2018. i dobrog rešenja ne postoji. U međuvremenu su ažurirani operativni sistemi kako bi se izborili sa ovim ranjivostima, no pouzdanih rešenja i dalje ne postoji [5].

- 2016. i 2017. godina je obeležena kampanjama *ransomware* malicioznog softvera. Ransomware šifruje sadržaj hard diska računara, čime svi podaci skladišteni na disku bivaju zarobljeni. Inficirani računar ispisuje poruku sa instrukcijama za plaćanje otkupa i žrtvi je ostavljen izbor da plati određenu sumu novca (najčešće putem kriptovalute poput *bitcoin*-a), ili se oprosti od sadržaja svog hard diska, uključujući svih fotografija, poslovnih dokumenat i sličnih datoteka koje nisu podlegle *backup* proceduri. Bolnice su se pokazale kao posebno pogodne mete ovih napada, zbog vrednosti podataka sa kojim rade i slabe bezbednosti softvera koji koriste [6]. Ransomware se najčešće distribuira putem imejla, no moguće ga je preuzeti preko sajtova, USB-a, CD-a, itd.
- Krajem 2015. godine su ruski agenti sproveli hakerski napad nad Ukrajinom. Tokom operacije koja je trajala šest meseci, ovi sofisticirani napadači su uspeli putem interneta da dođu do sistema koji su upravljali sa električnom mrežom u jednoj od pokrajina Ukrajine. Na veče 23. decembra, četvrt miliona domaćinstva je ostalo bez struje na više sati, kada su napadači konačno pogasili sve sisteme i počistili većinu tragova da su ikada bili tu [7].
- 2013. godine je Edvard Snouden napustio svoje radno mesto u Državnoj bezbednosnoj agenciji (engl. *National security agency*; skraćeno *NSA*) Sjedinjenih Američkih Država, ponevši sa sobom mnoštvo dokumenata koji su opisivali razne programe o globalnoj špijunaži koju je američka vlada sprovodila kako nad svojim građanima, tako i nad tuđim [8].

Prethodno navedeni incidenti, napadi i ranjivosti spadaju u poznatije, no ovakvih događaja je bilo mnogo u proteklim godinama. Poenta priče jeste da je, zajedno sa poslovanjem preduzeća i svakodnevnog života pojedinca, rat, terorizam i kriminal takođe transformisan digitalnom revolucijom. Napadači kradu osetljive podatke, menjaju njihov sadržaj bez dozvole i sabotiraju računarska postrojenja.

Iz svega navedenog, moglo bi se argumentovati da je potreba za digitalnom bezbednošću samo moderna varijanta potrebe za fizičkom. Isto kao što preduzeća zaključavaju ulazna vrata od poslovnog prostora, angažuju obezbeđenje i postavljaju kamere, tako žele da imaju softverske sisteme koji su otporni na hakere koji iz svoje fotelje mogu da kradu poslovne tajne i remete poslovanje preduzeća.

Dakle, korporacije žele da zaštite sopstveno poslovanje. Firme angažuju mrežne administratore da obezbede njihovu internu mrežu i angažuju portire da čuvaju njihove zgrade. Informisana preduzeća, pogotovo ona koja operišu sa osetljivim podacima ili kritičnim sistemima (npr. banke, distribucije električne energije, nuklearne elektrane) prepoznaju da nije dovoljno obezbediti mrežu i operativne sisteme na svojim računarima, već da je neophodno osigurati da je sav softver koji se koristi u poslovanju bezbedan i bez kritičnih ranjivosti. Zbog ovoga, preduzeća koja kupuju softver sve više zahtevaju od preduzeća koja proizvode softver da im dostave rešenje koje je bezbedno.

Dakle, prvi izvor bezbednosnih zahteva dolazi direktno od klijenata koji žele da zaštite svoje poslovanje, no ovde se priča ne završava. Kako se svest o potrebi bezbednih sistema razvijala, tako su novi standardi i zakoni izlazili koji zahtevaju od preduzeća da brinu o bezbednosti. Primeri ovakvih dokumenata su:

- *General Data Protection Regulation* (GDPR), regulativa izdata od strane Evropske unije (EU), koja se odnosi na sve učesnike koji obrađuju podatke građana EU. Poenta regulative je da se štiti privatnost ličnih podataka građana EU, implementacijom organizacionih i tehničkih kontrola koje prate najbolje prakse. Ovo uključuje i zaštitu podataka na nivou softvera organizacija, što rezultuje da organizacije zahtevaju od proizvođača svog softvera da ispoštuju GDPR zahteve [9].

- *Health Insurance Portability and Accountability Act of 1996* (HIPAA), regulativa izdata od strane Sjedinjenih Američkih Država (SAD), koja između ostalog pokriva zaštitu elektronskih medicinskih podataka građana SAD-a. Bolnice i državni organi koji obrađuju ove podatke su primarna meta ove regulative, što utiče i na proizvođače njihovog softvera, od desktop aplikacija, preko mobilnih, pa sve do nosivih (engl. *Wearable*) aplikacija [10].
- *Payment Card Industry Data Security Standard* (PCI DSS), predstavlja tehnički standard čija svrha je zaštita podataka o platnim karticama. Preduzeća koja prihvataju plaćanje putem kartice ili ona koja obrađuju podatke sa platnih kartica su u obavezi da ispoštuju ovaj standard, što naravno uključuje i sav softver koji ima dodira sa platnim karticama. Konkretno, PCI DSS se sastoji od 12 grupa zahteva, gde se šesta grupa odnosi na obezbeđivanje softvera koje preduzeće koristi [11].

Kako bezbednosni incidenti postaju sve češći fenomen tako se sve više standarda i zakona formira i unapređuje, koji zahtevaju od preduzeća investiranje u bezbednost, gde se ti zahtevi onda propagiraju i na razvijače softvera koji opskrbljuju data preduzeća. Dakle, ovde identifikujemo još jedan skup bezbednosnih zahteva. Iako i ovi zahtevi dolaze od klijenta koji želi da ispoštuje određen zakon ili regulativu, ključna motivacija jeste izbegavanje sankcija od strane države.

Spram prethodne priče, moguće je istaći nekoliko razloga koje klijenti imaju da zaštite svoje sisteme:

- Zaštita poslovanja, što podrazumeva zaštitu delova sistema koji donose preduzeću profit, kao i zaštita delova sistema koji smanjuju troškove preduzeća;
- Zaštita brenda, što podrazumeva čuvanje poverenja klijenata preduzeća i izbegavanje javnih, skandaloznih, incidenata;
- Izbegavanje sankcija, usled nepoštovanja određenog zakona ili standarda.

Dok su prve dve teze relevantne za svako preduzeće, treća veoma zavisi od konteksta. Dok će neke firme biti pod strogom regulativnom kontrolom i preneti bezbednosne zahteve na proizvođače svog softvera, druge će zahtevati izradu softvera koji ne dotiče ni jedan zakon ili standard.

Ponovo se postavlja pitanje „Zašto da se cimam oko ovoga?“. Ignorisanjem sve veće potrebe za bezbednim softverom može rezultovati da propustite priliku da učestvujete u projektu koji zahteva inženjere koji umeju da razviju bezbedan softver. Još gore, može se desiti da budete uključeni, te da neadekvatno zaštite vaš dizajn i kod. U slučaju incidenta, vaša firma, a u zavisnosti od incidenta i vi lično možete biti krivično gonjeni.

Najzad, ne treba preuveličavati značaj razvoja bezbednog softvera za vašu karijeru. Iako jeste bitna crta kvaliteta u svakom softveru, a esencijalna za određeni podskup, dosta posla ima u razvoju softver gde bezbednost nije toliko bitna karakteristika.

1.4 Osnovna terminologija informacione bezbednosti

Ako smo prihvatili da vredi investirati u znanje potrebno za razvoj bezbednog softvera, potrebno je definisati osnovnu terminologiju informacione bezbednosti. Iako daleko od aksioma, definicije koje slede je neophodno dobro razumeti kako bi se jasno i efikasno moglo pričati o različitim mehanizama i aktivnostima koji doprinose razvoju bezbednog softvera.

Za početak se postavlja pitanje šta je informaciona bezbednost. Zvanično, informaciona bezbednost se definiše kao čin zaštite sistema, i podataka sa kojim sistem operiše, od nedozvoljenog pristupa, upotrebe, otkrivanja, ometanja, izmene ili uništenja [12].

1.4.1 CIA trijada

U oblasti informacione bezbednosti postoji takozvana CIA trijada koja navodi tri primarna koncepta, poverljivost, integritet i dostupnost. Ovo su bezbednosna svojstva koja postavljaju rečnik za svu drugu terminologiju u ovom domenu [13].

Poverljivost

Poverljivost (engl. *Confidentiality*) podrazumeva zaštitu podataka od agenata koji nemaju pravo da pristupe datim podacima.

U opštem slučaju poverljivost podataka se obezbeđuje upotrebom kriptografskih kontrola, poput algoritama za šifriranje ili heširanje podataka. U kombinaciji sa mehanizmima za kontrolu pristupa, moguće je ograničiti pristup podacima isključivo na subjekte koji imaju prava da pristupe datim podacima.

Na primer, kako bi upotrebio *GMail* servis, korisnik mora da se prijavi na sistem upotrebom postojećeg imejla i ispravne lozinke na neki od *Google* servisa. *Google* servis za prijavu na sistem prihvata korisničke kredencijale, obrađuje ih i poredi sa informacijama o korisnicima koje ima u bazi. Ukoliko su uneseni ispravni kredencijali korisnik je obavešten o uspešnoj prijavi i potom dobija prikaz sa svojom imejl listom. U ovoj interakciji, poverljivost korisničkih kredencijala, kao i njegovih ličnih imejlova je od kritične važnosti za reputaciju *Google* preduzeća. Napad na poverljivosti (engl. *Information leakage*; *Disclosure*) može nastati ukoliko mehanizmi za kontrolu pristupa imejlovima i korisničkim lozinkama nisu adekvatni da zaštite od malicioznog insajdera ili spoljnog napadača. Do gubitka poverljivosti može doći ukoliko je *keylogger* instaliran na mašini koju korisnik koristi ili ako je napadač fizički prisutan i posmatra unos kredencijala. U navedenim slučajevima *Google* nije u stanju da sprovede adekvatne mehanizme zaštite, niti je odgovoran za gubitak poverljivosti.

Integritet

Integritet (engl. *Integrity*) se odnosi na sposobnost sprečavanja nedozvoljene i nepredviđene promene podataka. Cilj je održati konzistentnost, preciznost i pouzdanost podataka tokom njihovog celog životnog ciklusa. Pored toga, integritet sistema podrazumeva neometano izvršavanje predviđenih funkcionalnosti, bez manipulacije od strane agenata koji za to nemaju pravo.

Ovo podrazumeva upotrebu ispravnih i dobro konfigurisanih mehanizama za kontrolu pristupa koji će garantovati da se podaci mogu menjati samo od strane agenata koji imaju dozvolu to da rade. Garancija integriteta takođe može da zahteva upotrebu *checksum* mehanizma, heš funkcije ili slične kontrole, koji nude garanciju da podaci nisu menjani u toku nekog intervala, na primer tokom transporta između klijenta i servera. Najzad, u zavisnosti od zahteva, može postojati potreba za redundantnim skladištima podataka, kako bi se moglo obnoviti ispravno stanje podataka ako dođe do eksploatacije, ili čak ako subjekt koji ima pravo da menja podatke greškom napravi pogrešne izmene.

Sistemi koji nude sve tri varijante zaštite integriteta su svi moderni distribuirani sistemi za kontrolu verzija. Putem mehanizama za kontrolu pristupa definisana su prava koji određeni nalozi imaju nad podacima koji se nalaze u repozitorijumu. Svaka izmena koja se desi je zabeležena, gde svaka datoteka, pa i *commit* sadrže heš koji se može smatrati kao *checksum*. Najzad, zbog prirode sistema za kontrolu verzija, moguće je, u opštem slučaju, vratiti se na ranije stanje repozitorijuma, čime se mogu opozvati izmene nastale usled greške.

Napad na integritet (engl. *Tampering*; *Alteration*), omogućava napadaču da korumpira datoteku, čime može biti onemogućen pristup podacima, ili izmenjen sadržaj podataka. Tako, na primer, u informacionom sistemu banke, napad na integritet može prouzrokovati da faktura korisnika banke bude izmenjena tako da se isplaćuje deset puta veća suma.

Dostupnost

Dostupnost (engl. *Availability*) podrazumeva sposobnost pristupa podacima, servisima, uređajima, hardveru ili bilo kom resursu u trenutku kada je to potrebno. Nedostatak dostupnosti ne mora nužno da znači potpunu nedostupnost nekog servisa, već podrazumeva i pad performansi ispod prihvatljivog nivoa.

Napad na dostupnost (engl. *Denial of Service; DoS*) predstavlja napad gde napadač pokušava da učini servis, računar, opremu, itd. nedostupnim korisnicima kojima je dati resurs namenjen. Ovo može da uradi na mrežnom nivou, tako što proizvodi veliku količinu mrežnog saobraćaja ka žrtvi ili na aplikativnom nivou, tako što učestalo poziva funkcije softvera žrtve. U slučaju DDoS napada (engl. *Distributed Denial of Service*), napadač upošljava grupu uređaja da vrše napad, gde se ova grupa može sastojati od desetine hiljada računara koje je napadač inficirao i preuzeo.

Očuvanje dostupnosti nekog resursa podrazumeva održavanje i ažuriranje infrastrukture koja nudi dati servis, poput hardvera, operativnog sistema, aplikativnog servera itd. U slučaju internet baziranih servisa neophodno je obezbediti prikladnu količinu protoka. Upošljavanje redundantnih servera, *load balancer*[1] rešenja i *high-availability*[2] klastera moguće je zaštiti se od otkaza infrastrukture usled kvara, prirodne nepogode ili napada. Najzad, ukoliko dođe do gubitka dostupnosti treba imati spreman plan za oporavak od katastrofe i odgovorne subjekte koji će minimizirati štetu nastalu usled gubitka dostupnosti.

Ako se uzme za primer DMS (engl. *Distribution Management* System) postrojenje zaduženo za upravljanje strujom nekog grada, može se smatrati da je dostupnost funkcionalnostima otvaranja i zatvaranja protoka struje od kritične važnosti. Kako bi se pojačala garancija dostupnosti sistema, ceo sistem bi mogao da ima duplikat (engl. *Hot-Standby Pair*) gde bi se prilikom otkaza neke mašine aktivirao njen *standby* par. Ukoliko bi se formirao klaster računara, umesto par, otpornost na DoS bi bila utoliko veća. Ako bi cilj bio zaštititi dostupnost i u slučaju kada je celo postrojenje ugroženo, na primer usled požara, moguće je napraviti rezervno postrojenje, takozvani *Hot site* ili *cold site*. *Hot site* predstavlja postrojenje koje ima svu opremu i podatke spremne, dok *cold site* uključuje praznu zgradu sa strujom i tekućom vodom.

Fokusiranjem na DoS koji cilja aplikativni nivo, odnosno naš softver, dobar način da se poveća otpornost na gubitak dostupnosti jeste da se analiziraju komponente softvera koje su dostupne napadaču, kao i one koje se najviše koriste i da se optimizuju njihove funkcije. Napadaču je u interesu da poziva funkcije koje više opterećuju sistem žrtve, s' obzirom da za manje svojih resursa pravi veće opterećenje. Primer kada ovo nije bilo ispoštovano se može pronaći u ranijim verzijama *Django* radnog okvira [14].

1.4.2 Terminologija pretnji

Dakle, informaciona bezbednost se bavi zaštitom resursa od zloupotrebe, odnosno analizira i definiše metode za očuvanje bezbednosnih svojstva datih resursa. Kako bi bilo moguće razgovarati o resursima, pretnjama na njihovu poverljivost, integritet i dostupnost, kao i napadima koji realizuju te pretnje, potrebno je uvesti nekoliko dodatnih termina.

Subjekt

Subjekt (engl. *Subject*; *Agent*; *Actor*), odnosno agent, je aktivan entitet na sistemu. Primeri subjekta uključuju:

- Čoveka, koji pristupa podacima i funkcionalnostima sistema;

[1] *Load balancer* je uređaj koji prihvata zahteve od udaljenih klijenata i distribuira zahteve na grupu servera, smanjujući opterećenje i povećavajući pouzdanost sistema.
[2] *High-availability* klaster predstavlja grupu računara koji pružaju određene servise tako da se minimizuje period kada sistem ne radi. Upotrebom redundantnih računara servisi se pružaju i u slučaju kada neka komponenta otkaže.

- Program, koji vrši procesiranje podataka sistema;
- DLL datoteka koja ažurira bazu podataka.

Resurs

Resurs (engl. *Asset*) je objekat koji sadrži određenu vrednost i koji treba da bude u nekoj meri zaštićen. Primeri resursa uključuju:

- Računi klijenata banke, gde su primarna svojstva koje treba očuvati poverljivost i integritet, ali je i sama dostupnost računa vlasniku bitna;
- Poslovne tajne preduzeća, poput algoritma, kalkulacija i podataka, gde je poverljivost tih tajni najznačajnije svojstvo;
- Javno dostupni servisi preduzeća kojem su to primaran izvor profita, gde je dostupnost datih servisa najbitnije svojstvo.

Napadač

Napadač (engl. *Threat Agent*), u našem kontekstu, predstavlja ljudskog subjekta koji žele da ugrozi neko preduzeće, odnosno resurs datog preduzeća. Napadači se mogu klasifikovati u nekoliko grupa, gde se za svaku grupu može definisati:

- Motivacija, odnosno šta je glavni razlog koji napadači imaju da ugrožavaju resurse nekog preduzeća;
- Sposobnost, što podrazumeva veštinu napadača, vreme i opremu sa kojom raspolažu;
- Prilika, što podrazumeva nivo pristupa koji napadači imaju ka sistemu koji žele da napadnu, kao i poznavanje sistema i konteksta u kom on postoji kako bi napadi mogli biti efikasniji.

Spram ovih svojstva, moguće je napadače podeliti u nekoliko grupa. Svaka od ovih grupa ima određenu motivaciju, sposobnost i priliku i spram ovih svojstava će ciljati mete koje su pogodne za ostvarivanje njihovih ciljeva. U nastavku sledi klasifikacija različitih grupa napadača:

- **Organizovan kriminal** uključuje pojedince ili grupe napadača koji kradu podatke koji se mogu prodati na crnom tržištu (npr. lični podaci, brojevi kreditnih kartica, zdravstveni podaci) ili sabotiraju preduzeća kako bi iznudili novac (npr. putem *ransomware* infekcija ili upotrebom DoS napada). Nivo sposobnosti i prilika sa kojim ove grupe raspolažu variraju od niskog (amateri koji koriste proste alate da ugroze stare sisteme putem interneta) do visokog (sofisticirana grupa koja ima čoveka unutar preduzeća da pomogne u ostvarivanju napada).
- **Preduzeća** umeju da angažuju napadače da oštete konkurenciju. Koliko je preduzeće koje je meta napada uspešno i kakvim poslovanjem se bavi su pitanja koja mogu da odrede nivo sposobnosti i prilika ove grupe napadača.
- Određene **države** angažuju veoma sofisticirane napadače sa ciljem da ugroze strane vlade. Mete ovakvih napadača variraju, no najčešće su to preduzeća koja rukuju sistemima koji su kritični za normalan rad države, odnosno predstavljaju njenu kritičnu infrastrukturu (engl. *Critical Infrastructure*). Ovo uključuje banke, sisteme za upravljanje električnom mrežom, branama, saobraćajem, itd.
- **Teroristi** se po mnogo čemu mogu posmatrati slično kao i državno-finansirani napadači, s' tim da po pravilu raspolažu sa manje resursa u vidu novca i opreme. Sve što bi teroristi ugrozili u fizičkom svetu može biti meta za napad u digitalnom.
- **Haktivisti** predstavljaju grupu napadača koja ugrožava neki sistem zbog neke ideje. Iz određene perspektive, ovi napadači se mogu posmatrati kao identični onim koji pripadaju terorističkim organizacijama.

- **Insajderi** mogu pripadati bilo kojoj od prethodno navedenih grupa. Osim dodatne motivacije koje ova grupa može da poseduje, a to je nezadovoljstvo svojim poslom, suštinski razlog zašto se insajder gleda kao posebna klasa napadač jeste zbog svog pristupa. Privilegovani administratori, poput sistem administratora, su najopasniji napadači zbog svog jedinstvenog položaja u sistemu.
- Najzad, **haotični napadači** podrazumevaju hakere čija motivacija je zabava i razvijanje veštine. Ova grupa nema ciljane mete, već napadaju nasumične mete. Iako nisu ljudski subjekti, u ovu grupu se mogu svrstati i razni virusi i drugi maliciozan softver (engl. *Malware*) koji se nalaze na internetu, a nisu konstruisani sa nekom posebno funkcijom (npr. kao što *ransomware* jeste).

Negativan uticaj

Prilikom obezbeđivanja resursa potrebno je uzeti u obzir vrednost koju konkretan resurs ima za preduzeće. Tačnije, treba razmotriti negativan uticaj (engl. *Impact*) koji bi uspešna eksploatacija sistema, odnosno kompromis bezbednosnog svojstva resursa, imao na preduzeće, u vidu finansijske štete, problemom sa zakonom ili štete na reputaciju.

Pretnja

Pretnja (engl. *Threat*) predstavlja okolnost ili događaj koji ima negativan uticaj na preduzeće, njene resurse, pojedince, druge organizacije, državu ili ljudski život. Jedna pretnja se potencijalno može realizovati na više načina. U kontekstu informacionih sistema, pretnja se može realizovati neautorizovanim pristupom, modifikacijom ili uništenjem podataka ili servisa. Primeri pretnji uključuju:

- Krađa sadržaja baze podataka, odnosno gubitak poverljivosti tih podataka;
- Krađa korisničke sesije na sajtu banke, odnosno gubitak poverljivosti sesije;
- Neautorizovana izmena konfiguracionih datoteka aplikativnog servera, odnosno gubitak integriteta konfiguracione datoteke;
- Gubitak dostupnosti neophodnih servisa za rad socijalne mreže.

U literaturi se pod pojmom pretnje ponekad smatra napadač. Dakle, ono što je definisano kao *threat agent* se u određenim dokumentima naziva *threat*, usled čega može nastati dosta konfuzije.

Najzad, iako pretnja podrazumeva bilo kakav događaj koji ima negativan uticaj na preduzeće, u našem kontekstu pretnju definišemo kao podskup ovih događaja, te je fokus stavljen na događaje koji podrazumevaju gubitak bezbednosnog svojstva nekog resursa. Dakle, gubitak poverljivost, gubitak integriteta ili gubitak dostupnosti nekog resursa predstavlja pretnju.

Ranjivost

Ranjivost (engl. *Vulnerability*) je svojstvo koje komponenta ili sistem ima, putem koje je omogućena eksploatacija. Ranjivost može da se nalazi u bilo kom delu sistema, od koda aplikacije, do biblioteke koja je u upotrebi, pa i do verzije operativnog sistema na kom je aplikacija postavljena. Ranjivost može da bude na nivou dizajna sistema, njegovoj implementaciji, ili čak na nivou dizajna poslovnog procesa u kom računarski sistem ima neku ulogu. Primeri ranjivosti uključuju:

- Upotrebu zastarelih i slabih kriptografskih algoritama za šifrovanje poruka koje se razmenjuju između dva servisa;
- Neadekvatno konfigurisan aplikativni server koji i dalje dozvoljava prijavu putem podrazumevanog privilegovanog naloga (npr. admin, admin);
- Konfiguracioni fajlovi koji nisu zaštićeni na nivou operativnog sistema, te svako ko ima pristup računaru može da ih menja;
- Nedostatak validacije korisničkog unosa na serveru, usled čega je širok spektar napada omogućen;

- Nedostatak antivirus aplikacije na produkcionom serveru.

Napad

Napad (engl. *Attack*; *Exploit*) predstavlja akciju koja eksploatiše jednu ili više ranjivosti kako bi realizovao pretnju. Svaka eksploatacija ranjivosti se realizuje putem vektora napada (engl. *Attack Vector*). Vektor napada predstavlja putanju ili način na koji napadač ostvaruje maliciozni cilj. Primeri vektora napada uključuju:

- Imejl sa *ransomware* virusom;
- Pažljivo kreiran korisnički unos koji će naterati parser SQL instrukcija da obriše bazu podataka;
- Skripta postavljena na maliciozni sajt koja izaziva uplatu novca sa naloga žrtve na nalog napada;
- USB sa *keylogger* virusom.

Jedna pretnja može da se potencijalno realizuje na više načina, sprovođenjem različitih napada koji eksploatišu različite ranjivosti. Na primer, za **pretnju krađe korisničkih kredencijala iz baze podataka** možemo identifikovati sledeće napade i ranjivosti koje oni eksploatišu:

- Krađa sadržaja baze podataka od strane malicioznog administratora baze, gde korisnički kredencijali nisu adekvatno zaštićeni;
- Osluškivanje saobraćaja (engl. *Packet Sniffing*) između korisničkog veb-čitača (engl. *Browser*) i serverske aplikacije i krađa paketa koji nisu šifrovani tokom tranzita;
- Mehanizam za izmenu zaboravljene lozinke se zasniva na pitanjima čiji se odgovori lako mogu pronaći, na primer analizom žrtvinog naloga na socijalnoj mreži;
- Korisnik se nije odjavio sa deljenog računara i maliciozni kolega pristupa sajtu gde je nalog prethodnog korisnika i dalje aktivan.

Rizik

Usled HIPAA zakona, gubitak poverljivosti podataka o pacijentima američke bolnice je pretnja koja bi imala izuzetno visok negativan uticaj na preduzeće koje je proizvelo dati informacioni sistem. Ukoliko se ispostavi da je dato preduzeće krivo što nije opskrbilo odgovarajuće bezbednosne mere, pored štete na reputaciju, preduzeće može da podlegne novčanim kaznama i krivičnom gonjenju. U najjednostavnijem obliku, rizik (engl. *Risk*) se može računati kao proizvod verovatnoće da će se neka pretnja realizovati i veličine negativnog uticaja koji data pretnja ima na preduzeće.

Grubo gledano, verovatnoću da će se pretnja realizovati se računa tako što se razmatraju relevantne ranjivosti koje trenutni sistem ili dizajn sistema ima, zatim koji nivo resursa, veštine i vremena je potreban da se formira uspešan napad da eksploatiše identifikovane ranjivosti. Sa druge strane, intenzitet negativnog uticaja najčešće određuju procenitelji rizika i to u zavisnosti od resursa koji se razmatra, vezanih pretnji, konteksta čitavog sistema, zahteva klijenta i zakonskih regulativa, itd.

Za prethodni primer krađe korisničkih kredencijala postoji niz ranjivosti koje nisu regulisane. Napadi koje eksploatišu neke od ovih ranjivosti zahtevaju minimalno uloženih resursa (npr. sedanje za tuđi računar). Verovatnoća za izvršavanje ovog napada je visoka, dok je negativan uticaj relativno nizak (kompromitovan je jedan nalog). Sa druge strane, krađa svih korisničkih kredencijala od strane malicioznog administratora nosi visok negativan uticaj. Ukoliko ne postoji neki mehanizam praćenja akcija administratora (npr. log) ili taj mehanizam nije adekvatno zaštićen (npr. administrator može da menja logove) onda je verovatnoća da se ova pretnja uspešno realizuje visoka, te je rizik ove pretnje visok.

Kontrole

Kada se ispostavi da je određen rizik visok, odnosno da je značajan negativan uticaj eksploatacije, i da je ujedno lako eksploatisati određenu ranjivost, potrebno je definisati bezbednosne kontrole (engl. *Security controls*; *Countermeasures*), ili protivmere, kako bi se regulisale ranjivosti i smanjila verovatnoća eksploatacije. Iako će se detaljno učiti i razrađivati kontrole za zaštitu softverskih sistema, radi kompletnosti se navode kontrole koje bi regulisale ranjivosti vezane za pretnju krađe korisničkih kredencijala, iz prethodnog primera:

- Upotreba *hash & salt* mehanizma za skladištenje korisničkih lozinka, oslanjajući se na savremen, proveren algoritam za heširanje;
- Upotreba HTTPS protokola za svu komunikaciju između veb-čitača i servera, što uključuje sigurnu konfiguraciju TLS protokola prateći aktuelne najbolje prakse;
- Onemogućiti mehanizam za izmenu lozinke putem sigurnosnih pitanja, ili koncipirati adekvatna pitanja do čijih odgovara se ne može jednostavno doći;
- Ukoliko je u pitanju nalog sajta sa osetljivim funkcionalnostima, poput servisa za upravljanje bankovnim računom, zahtevati ponovnu prijavu na sistem prilikom svih osetljivih operaciji, i dodatno odjaviti korisnika sa sistema posle kraćeg perioda neaktivnosti.

1.4.3 Osnovne bezbednosne kontrole

Iako će se u svakom poglavlju ovog udžbenika razmatrati razne bezbednosne kontrole u različitim kontekstima, ovde će se istaći tri osnovna bezbednosna mehanizma kako bi se kompletirala osnovna terminologija koja je neophodna za razgovor o informacionoj bezbednosti. To su mehanizmi za autentifikaciju (engl. *Authentication*), autorizaciju (engl. *Authorization*), i neporecivost (engl. *Non-repudiation*).

Autentifikacija

Autentifikacija je proces utvrđivanje ispravnosti tvrdnje da je neki subjekat to za šta se predstavlja. Sam čin predstavljanja se naziva identifikacija, gde je najprostiji primer identifikacije tvrdnja „Moje ime je Pera Perić“. Zbog nedostatka dokaza da je tvrdnja ispravna uvodi se autentifikacija.

U domenu veb-aplikacija, autentifikacija se najčešće vezuje za prijavu na sistem, gde korisnik aplikacija dokazuje da je to za šta se predstavlja tako što unosi korisničko ime i lozinku. Složeniji proces autentifikacije se može videti kod bankomata, gde korisnik dokazuje da je vlasnik svog računa tako što ubacuje karticu u mašinu i unosi PIN kod. Autentifikacija nije samo prijava na sistem od strane čoveka, već uključuje proveru identiteta bilo kog subjekta, poput spoljnog ili internog servisa, datoteke ili programa.

Autorizacija

Autorizacija, ili kontrola pristupa, predstavlja proces utvrđivanja i provere prava koje neki subjekat ima nad resursima sistema. Da bi se autorizacija mogla vršiti, neophodno je pre toga utvrditi identitet subjekta, odnosno proći kroz proces autentifikacije. Kada subjekat pokušava da izvrši neku akciju, poput pristupa podacima ili poziva određene funkcije, kontrola pristupa proverava prava autentifikovanog subjekta, i u zavisnosti od definisanih pravila akcija biva odobrena ili odbijena.

Ako se uzme kao primer informacioni sistem jedne bolnice, pravila kontrole pristupa nad podacima o pacijentima bi trebala da garantuju da lekar može da pristupi samo podacima od svojih pacijenata, kada nije hitan slučaj. Kontrola pristupa može biti fizička, gde su u nuklearnoj laboratoriji postavljeni čitači mrežnjače oka kod bitnih prolaza. Naučnik se autentifikuje na sistem tako što približi oko čitaču, i u zavisnosti od pravila kontrole pristupa vrata se otvaraju ili ostaju zatvorena.

Neporecivost

Kada neki subjekat izvrši akciju, pogotovo ako je ona osetljive prirode, potrebno je na bezbedan način zabeležiti informaciju da je ta akcija izvršena, u kom trenutku se to desilo, i koji subjekat je bio izvršitelj. Na ovaj način se sprečava poricanje. Neporecivost zahteva autentifikaciju, kako bi se znalo ko izvršava akcije, i integritet, kako bi se moglo verovati zapisima. Dodatan zahtev može uključiti beleženje vremenske komponente, što podrazumeva trajanje upotrebe datog servisa.

Primer za osnovni mehanizam koji garantuje neporecivost je log veb-aplikacije, koji beleži svaki zahtev koji pristigne, što uključuje vreme kada je zahtev pristigao, IP adresu sa kog je zahtev napravljen, i sadržaj samog zahteva. U nedostatku ovakvih mehanizama u bankarskim sistemima, klijent bi mogao da podigne pare sa svog računa putem bankomata, i zatim prijavi da su pare nestale sa njegovog računa bez njegove intervencije. U normalnom sistemu zaposleni banke bi mogao da prođe kroz elektronske logove, uoči transakciju preuzimanja novca sa određenog bankomata, upali kameru koja posmatra dati bankomat i dokaže da je klijent stvarno bio tamo u dato vreme i podigao novac sa svog računa. Video snimak bi autentifikovao klijenta, ali da bi se neporecivost mogla ostvariti potrebno je dokazati i integritet video snimka, odnosno da snimak nije bio menjan na nepredviđen način.

1.5 Rezime

U ovom poglavlju je definisan položaj informacione bezbednosti u kontekstu softverskog inženjerstva. Dat je uvid u trendove digitalizacije civilizovanog sveta i istaknuta je glavna motivacija iza izrade bezbednih softverskih rešenja. Najzad, predstavljena je osnovna terminologija koja je neophodna za razumevanje složenijih pojmova, metoda i mehanizama iz domena razvoja bezbednog softvera.

1.6 Zadaci

1. Analizirati trendove integracije računara i pratećih tehnologija u svakodnevni život pojedinca kroz proteklih par decenija i koncipirati rešenja koja će se koristiti kroz narednih dvadeset godina.
2. Razmotriti značaj bezbednosti u računarskim sistemima, na nivou pojedinca, preduzeća i država.
3. Definisati šta je sistem i zbog kojih faktora je danas teže obezbediti sistem nego pre par decenija.
4. Identifikovati položaj bezbednosti u softverskom inženjerstvu i razmotriti poslovne mogućnosti za one koje domen informacione bezbednosti zainteresuje.
5. Navesti tri primera koji nisu ranije navedeni, koji predstavljaju potrebu za svojstvom poverljivosti, način na koji to svojstvo može biti ugroženo, i kontrole koje bi postavili da zaštitite ovo svojstvo.
6. Navesti tri primera koji nisu ranije navedeni, koji predstavljaju potrebu za svojstvom integriteta, način na koji to svojstvo može biti ugroženo, i kontrole koje bi postavili da zaštitite ovo svojstvo.
7. Navesti tri primera koji nisu ranije navedeni, koji predstavljaju potrebu za svojstvom dostupnosti, način na koji to svojstvo može biti ugroženo, i kontrole koje bi postavili da zaštitite ovo svojstvo.
8. Analizirati poznate incidente koji su opisani u potpoglavlju 1.3 i identifikovati ko je bio žrtva, ko je bio napadač, i šta je bila njihova motivacija.
9. Posmatrajući sef, identifikovati glavnu pretnju nad ovim objektom, potencijalne ranjivosti koje sef, prostor oko sefa, ili ljudi koji upravljaju sa sefom imaju, osmisliti napade koji eksploatišu date ranjivosti i formirati kontrole za regulisanje slabosti.
10. Razmatrajući fakultetsku studentsku službu (što uključuje informacioni sistem, ali i fizički prostor), identifikovati osetljive resurse i pretnje nad tim resursima, ranjivosti koje bi sistem studentske službe mogao da poseduje i kontrole koje bi se mogle postaviti da se regulišu date ranjivosti.
11. Razmatrajući kompletan sistem fakulteta, identifikovati celine i resurse čija eksploatacija bi mogla da ima visok negativan uticaj na fakultet. Identifikovati grupe napadača koji bi želeli da ugroze ovaj sistem, ranjivosti koje bi napadači mogli da eksploatišu i kontrole da regulišu date ranjivosti.

Reference

[1] DeBord, M., *Tesla's future is completely inhuman*, http://www.businessinsider.com/tesla-completely-inhuman-automated-factory-2017-5, pristupljeno: 27.1.2018.

[2] Statista, *Number of smartphone users worldwide from 2014 to 2020*, https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, pristupljeno: 27.1.2018.

[3] Harris, R., *More data will be created in 2017 than the previous 5,000 years of humanity*, https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/, pristupljeno: 27.1.2018.

[4] Rahman, A., Hamid, U., Chin, T., *Emerging Technologies with Disruptive Effects: A Review*, https://www.researchgate.net/publication/321906585_Emerging_Technologies_with_Disruptive_Effects_A_Review, pristupljeno: 27.1.2018.

[5] Graz University of Technology, *Sepctre and Meltdown*, https://meltdownattack.com/, pristupljeno: 27.1.2018.

[6] Hern, A., *WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017*, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware, pristupljeno: 27.1.2018.

[7] E-ISAC, 2016. *Analysis of Cyber Attack on Ukrainian Power Grid*, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, pristupljeno: 27.1.2018.

[8] The Guardian, *NSA whisteblower Edward Snowden*, https://www.youtube.com/watch?v=0hLjuVyIlrs, pristupljeno: 27.1.2018.

[9] Santala, A., *What Should Software Engineers Know About GDPR?*, https://www.infoq.com/articles/gdpr-for-software-devs, pristupljeno: 1.2.2018.

[10] TrueVault, *Developers Guide to HIPAA Compliance*, https://github.com/truevault/hipaa-compliance-developers-guide, pristupljeno: 1.2.2018.

[11] Whitelegg, D., *A developer's guide to complying with PCI DSS 3.2 Requirement 6*, https://www.ibm.com/developerworks/library/se-pcireq6/index.html, pristupljeno: 1.2.2018.

[12] US Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, y 3542, Cornell University Law School, www.law.cornell.edu/uscode/44/3542.html, pristupljeno 27.1.2018.

[13] CIA triad, What Is, http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA, pristupljeno: 27.1.2018.

[14] Bennett, J., *Security releases issued*, https://www.djangoproject.com/weblog/2013/sep/15/security/, pristupljeno: 1.2.2018.