Centar Informacijske Sigurnosti

Modeliranje sigurnosnih prijetnji (Threat modeling)

svibanj 2012.

CIS-DOC-2012-05-049

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Modeliranje prijetnji (eng. *threat modeling*) je inženjerska tehnika koja se može koristiti za identificiranje prijetnji, napada, ranjivosti te odgovarajućih protumjera u kontekstu promatrane aplikacije. Modeliranje prijetnji pomaže kod definiranja sigurnosnih ciljeva, pronalaženja relevantnih prijetnji, ranjivosti te protumjera. To je strukturirani pristup koji je znatno učinkovitiji i jeftiniji od nasumičnog primjenjivanja sigurnosnih svojstava, bez pravog poznavanja koje prijetnje pojedino svojstvo opisuje. Uz primjenu takvog lošeg slučajnog pristupa javlja se problem kako odrediti da je sustav ili aplikacija dovoljno sigurna. Zbog svega toga, za odgovarajuću zaštitu sustava potrebno je prije svega dobro poznavati i ocijeniti prijetnje. Modeliranje prijetnji nije jednokratan proces, on je usko povezan i isprepleten s fazama dizajniranja i razvoja aplikacije ili sustava.

Uz identificiranje i procjenu prijetnji usredotočenu na razumijevanju arhitekture i izvedbe aplikacije, moguće je identificirati i prijetnje te odgovarajuće protumjere počevši od prijetnji koje predstavljaju najveći rizik. Kada se koristi u ranim fazama razvoja programskog rješenja, modeliranje prijetnji je od višestruke koristi programerima.

U ovom dokumentu opisano je modeliranje sigurnosnih prijetnji. Pristupi modeliranja prijetnji navedeni su u drugom poglavlju. U trećem poglavlju raščlanjena su i detaljnije opisana dva procesa modeliranja prijetnji sa svim svojim koracima. Četvrto poglavlje opisuje primjenu modeliranja prijetnji na analizu rizika. U petom poglavlju navedeni su neki od popularnijih alata za modeliranje prijetnji i rizika te su ukratko opisani najvažniji alati.

2. Modeliranje prijetnji

Modeliranje sigurnosnih prijetnji u računalnoj sigurnosti ima dva različita, ali povezana značenja. Prvo se značenje odnosi na opis sigurnosnih problema kojima dizajneri trebaju posvetiti pažnju. Drugo značenje definira modeliranje prijetnji kao skup mogućih napada koje treba uzeti u obzir za pojedini dio programa ili računalnog sustava. Često se za jedan sustav definira više različitih modela prijetnji. Pritom svaki model opisuje uzak skup mogućih napada na koje je potrebno usmjeriti pažnju. Model prijetnji može pomoći u procjeni vjerojatnosti pojavljivanja i potencijalne štete napada kao i njihovog prioriteta te se na taj način može koristiti u smanjivanju ili iskorjenjivanju prijetnji. Odnedavno je modeliranje prijetnji postalo sastavni dio SDL (eng. *Security Development Lifecycle, SDL*) procesa tvrtke Microsoft.

Modeliranje prijetnji zasnovano je na ideji da svaki sustav ili organizacija ima vrijedne resurse koje je potrebno zaštititi. Ti resursi imaju određene slabe točke koje određene vanjske i unutarnje prijetnje mogu iskoristiti kako bi naštetile tim resursima, no istovremeno postoje i odgovarajuće sigurnosne protumjere koje ublažavaju prijetnje, [4].

Modeliranje prijetnji omogućuje primjenu strukturiranog pristupa sigurnosti u pronalaženju i procjeni glavnih prijetnji koje potencijalno imaju najveći utjecaj na računalni sustav ili aplikaciju. Uz identificiranje i procjenu prijetnji temeljenu na razumijevanju arhitekture i metoda razvoja aplikacije, moguće je identificirati i prijetnje te odgovarajuće protumjere u logičkom poretku, počevši od prijetnji koje predstavljaju najveći rizik. Modeliranje prijetnji osigurava dobre temelje za specifikaciju sigurnosnih zahtjeva tijekom razvoja aplikacije. Kada se koristi u ranim fazama razvoja programskog rješenja, modeliranje prijetnji na više načina koristi programerima; od ovjeravanja arhitekture aplikacije, identifikacije i procjene prijetnji, pronalaženja protumjera do penetracijskog ispitivanja temeljenog na modelu prijetnji, [6].

Modeliranje prijetnji koristi se prilikom oblikovanja aplikacije kako bi se ostvarili sigurnosni ciljevi, zatim kao pomoć u donošenju ključnih inženjerskih odluka te kako bi se smanjio rizik sigurnosnih problema koji se javljaju s razvojem sustava.

2.1. Pristupi modeliranju prijetnji

Postoji više pristupa modeliranju prijetnji:

- **pristup usredotočen na napadača** (eng. *attacker-centric*) započinje s napadačem te procjenjuje njegove ciljeve i načine na koje ih može ostvariti. Često se razmatra i

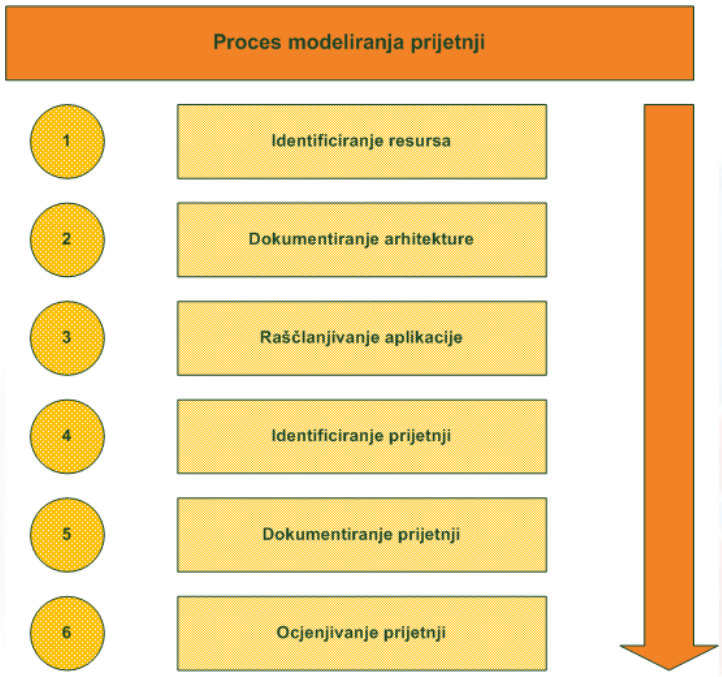
napadačeva motivacija. Ovaj pristup započinje od napadačevih ulaznih točaka u sustav ili resursa.

- **pristup usredotočen na programsko rješenje** (eng. *software-centric*) naziva se još i pristup usredotočen na sustav (eng. *system-centric*), dizajn (eng. *design-centric*) ili arhitekturu (eng. *architecture-centric*). Ovaj pristup započinje od dizajna sustava i pokušava proći kroz model sustava u potrazi za napadima na svaki element modela. Upravo se ovaj pristup koristi u modeliranju prijetnji u Microsoftovom SDL-u.
- **pristup usredotočen na resurs** (eng. *asset-centric*) započinje od resursa povjerenih sustavu, poput skupa osjetljivih osobnih podataka.
- **pristup usredotočen na obranu** (eng. *defense-centric*) procjenjuje slabosti u sigurnosnom nadzoru, [4], [8].

3. Principi modeliranja prijetnji

Modeliranje prijetnji ne bi trebao biti samo jednokratan, već iterativan proces koji započinje u ranim fazama razvoja aplikacije i nastavlja se kroz čitav životni ciklus aplikacije. Dva su glavna razloga za ovakav pristup. Za početak, nemoguće je identificirati sve postojeće prijetnje u jednom prolazu. S druge strane, proces modeliranja prijetnji potrebno je ponavljati zajedno s razvojem aplikacije zbog toga što su aplikacije rijetko statične te ih je potrebno poboljšavati i prilagođavati kako bi se prilagodile poslovnim zahtjevima.

Proces modeliranja prijetnji koji se sastoji od šest faza shematski je prikazan na Slika 1 i opisan u nastavku, [1].



Slika 1. *Proces modeliranja prijetnji u šest faza*
Izvor: *CIS*

3.1. Identificiranje resursa

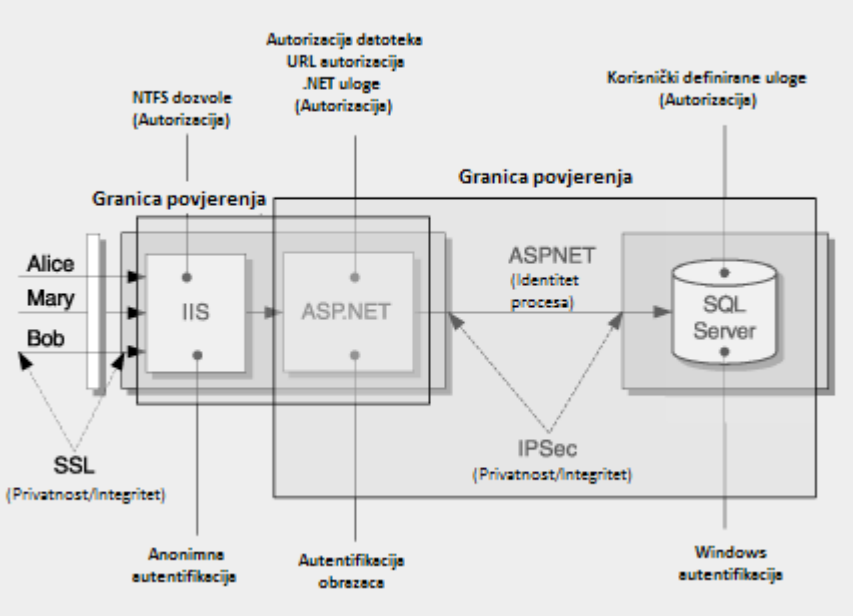
U ovom koraku obavlja se identificiranje resursa koje je potrebno zaštititi. Resursi pokrivaju širok raspon, od povjerljivih podataka do dostupnosti internetskih stranica. Među povjerljive podatke spadaju osobni podaci, podaci o intelektualnom vlasništvu, podaci o brojevima kreditnih kartica te podaci o zaporkama, [1].

3.2. Dokumentiranje arhitekture

Glavni cilj ovog koraka je dokumentiranje funkcije aplikacije, njezine arhitekture i fizičkog razmještaja te tehnologija kojima je aplikacija ostvarena. Potrebno je pronaći moguće ranjivosti dizajna ili izvedbe promatrane aplikacije. U ovoj fazi potrebno je obaviti sljedeće zadatke:

- **identificirati funkciju aplikacije** - identificirati što aplikacija radi te kako koristi ulazne resurse, što kasnije može koristiti za otkrivanje mogućih zloupotrebljavanja,
- **stvoriti dijagram arhitekture** - stvoriti dijagram arhitekture visoke razine (Slika 2) koji opisuje kompoziciju i strukturu aplikacije te njezinih podsustava, kao i osobine fizičkog razmještaja. Za složenije sustave možda će biti potrebno stvaranje dodatnih dijagrama za pojedine dijelove.

- **identificiranje tehnologija** - identificiranje različitih tehnologija koje su korištene u ostvarenju rješenja. Kasnije može biti od koristi kako bi se moglo usredotočiti na prijetnje svojstvene za pojedinu tehnologiju, [1].



Slika 2. *Dijagram arhitekture sustava*
Izvor: *msdn.microsoft.com*

3.3. Raščlanjivanje aplikacije

Raščlanjivanje aplikacije podrazumijeva razbijanje aplikacije i stvaranja sigurnosnog profila za aplikaciju temeljenog na ranjivosti. Poželjno je što veće znanje o funkcioniranju aplikacije kako bi se što lakše otkrile prijetnje. Zadaci koje je potrebno obaviti u ovoj fazi su:

- **identificiranje granica povjerenja** (eng. *trust boundaries*) koje okružuju svaki resurs aplikacije. Za svaki podsustav potrebno je razmotriti je li pouzdan ulazni tok podataka ili korisnički unos. U slučaju kada nije, treba razmotriti kako bi se tokovi podataka i unosi mogli autentificirati i autorizirati. Na jednak način potrebno je razmotriti pozivajući kod. Potrebno je osigurati odgovarajuću zaštitu svih ulaznih točaka u određenu granicu povjerenja kako bi se na ulaznim točkama primatelja mogla potvrditi valjanost svih podataka koji su prešli granicu.
- **identificiranje protoka podataka** (eng. *data flow*) - jednostavan pristup je započeti s najvišom razinom te zatim iterativno dekomponirati aplikaciju analizirajući protok podataka između pojedinih podsustava. Posebno je važan protok podataka preko granica povjerenja. U tom slučaju programski kod koji prenosi podatke izvan granice povjerenja treba pretpostaviti da su podaci zlonamjerni te treba provesti temeljitu provjeru njihove valjanosti.
- **identificiranje ulaznih točaka** (eng. *entry points*) - ulazne točke u aplikaciju mogu poslužiti kao ulazne točke za napade. Dodatno, potrebno je poznavati smještaj unutarnjih ulaznih točaka te tipove ulaza koje one primaju u slučaju da napadač uspije premostiti 'prednja vrata' (eng. *front door*) aplikacije i napasti izravno na unutarnje ulazne točke. Za svaku ulaznu točku potrebno je odrediti 'čuvare' (eng. *gatekeepers*) koji osiguravaju autorizaciju i određeni stupanj provjere valjanosti.
- **identificiranje privilegiranog koda** (eng. *privileged code*) - privilegirani kod pristupa specifičnim vrstama sigurnih resursa i izvodi ostale privilegirane operacije. Privilegiranom kodu moraju biti dodijeljena odgovarajuća sigurnosna odobrenja za pristup kodu.

Također, privilegirani kod mora osigurati da resursi i operacije koje on enkapsulira[1] ne budu izloženi neprovjerenom i potencijalno zlonamjernom kodu.

- **dokumentiranje sigurnosnog profila** (eng. *security profile*) - potrebno je identificirati pristupe u dizajnu i ostvarenju aplikacije koji su korišteni za:
  - ulaznu provjeru (eng. *input validation*) - način na koji aplikacija filtrira, pročišćava i odbacuje ulazne podatke prije njihove daljnje obrade,
  - autentikaciju (eng. *authentication*) - proces u kojem korisnik dokazuje svoj identitet,
  - autorizaciju (eng. *authorization*) - način na koji aplikacija osigurava pristup resursima i operacijama,
  - upravljanje konfiguracijom (eng. *configuration management*) - načini na koje aplikacija rukuje konfiguracijom,
  - osjetljive podatke (eng. *sensitive data*) - način na koji se obrađuju svi podaci koji moraju biti zaštićeni,
  - upravljanje sjednicama (eng. *session management*) - rukovanje i zaštita međudjelovanja korisnika i web aplikacije,
  - kriptografiju (eng. *cryptography*) - način na koji aplikacija štiti i osigurava tajnost podataka,
  - upravljanje parametrima (eng. *parameter manipulation*) - način na koji aplikacija obrađuje ulazne parametre te ih štiti od mijenjanja,
  - upravljanje iznimkama (eng. *exception management*) - što se događa prilikom neuspjelog poziva metoda u aplikaciji,
  - reviziju i prijavljivanje (eng. *auditing and logging*) - način na koji aplikacija pohranjuje podatke o događajima vezanim uz sigurnost.

Provedbom navedene identifikacije stvara se sigurnosni profil aplikacije [1].

3.4. Identificiranje prijetnji

Ovaj korak sastoji se od identificiranja prijetnji koje mogu utjecati na sustav i ugroziti resurse. Za klasificiranje prijetnji mogu se koristiti dva temelja pristupa:

- **STRIDE** - pristup temeljen na cilju kod kojega se razmatraju ciljevi napadača,
- **kategorizirani popisi prijetnji** - kod ovog pristupa započinje se od popisa učestalih prijetnji svrstanih u mrežnu, domaćinsku i aplikacijsku kategoriju, [1]. Navedene kategorije detaljnije su opisane u poglavlju 3.4.2. Kategorizirani popisi prijetnji.

3.4.1. STRIDE

STRIDE je klasifikacijska shema za karakteriziranje poznatih prijetnji prema vrsti iskorištavanja za koju se koriste ili prema motivaciji napadača. STRIDE je akronim sastavljen od prvih slova svake od šest kategorija prijetnji:

- **pretvaranje identiteta** (eng. ***S****poofing identity*) - pokušaj pristupa sustavu pomoću lažnog identiteta. To je ključan rizik za aplikacije koje imaju mnogo korisnika, a osiguravaju jedan kontekst izvođenja na aplikacijskoj razini i razini baze podataka.
- **uplitanje** (eng. ***T****ampering*) - neovlaštena promjena podataka. Postoji mogućnost da korisnici promijene primljene podatke te ih tako izmijenjene vrate natrag. Aplikacija ne bi smjela korisniku slati podatke koji se mogu dobiti samo unutar nje same. Isto tako, aplikacija bi trebala pažljivo provjeriti podatke primljene od korisnika te provjeriti njihovu valjanost i primjenjivost prije njihovog korištenja ili pohranjivanja.
- **odbijanje** (eng. ***R****epudiation*) - korisnik može osporiti transakcije s nedovoljnim revizijama i pohranama aktivnosti. Stoga je potrebno razmotriti zahtijeva li aplikacija

[1] Enkapsulacija u objektno orijentiranom programiranju je mehanizam kojim se ograničava pristup nekim komponentama objekta

neodbijajuće nadzore poput zapisa o web pristupu ili zapisa o pristupu i korištenju sustava (eng. *audit trail*).

- **povreda informacija** (eng. ***I****nformation disclosure*) - neželjeno čitanje privatnih podataka. Aplikacija mora uključivati strogi nadzor kako bi spriječila mijenjanje i zlouporabu korisničkog ID-a (eng. *identifier*), posebice ako koristi jedan kontekst za izvođenje cijele aplikacije. Jednako tako, valja imati na umu da internetski preglednici mogu biti izvori 'curenja' informacija, stoga je potrebno količinu informacija pohranjenu web preglednikom svesti na najmanju moguću.
- **uskraćivanje usluge** (eng. ***D****enial of Service*) - djelovanje onemogućavanjem usluge. Kako bi se pokušalo izbjeći ovu vrstu napada potrebno je korištenje skupih resursa omogućiti isključivo autentificiranim i autoriziranim korisnicima, a onemogućiti anonimnim korisnicima. Za aplikacije za koje ovo nije moguće postići, potrebno je svaki njezin aspekt najviše pojednostaviti kako bi se spriječili jednostavniji DoS napadi.
- **podizanje prava** (eng. ***E****levation of privilege*) - korisnik s manjim pravima preuzima identitet privilegiranijeg korisnika. Potrebno je sve akcije ograditi pomoću autorizacijske matrice, kako bi se osiguralo da samo korisnik s dopuštenim pravima može pristupiti privilegiranoj funkcionalnosti, [1].

3.4.2. Kategorizirani popisi prijetnji

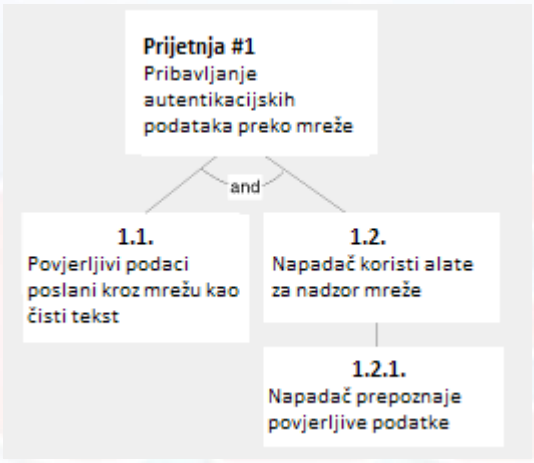
Kod ovog pristupa potrebno je obaviti sljedeća tri zadatka:

- **identificirati mrežne prijetnje** (eng. *network threats*) - zadatak za mrežne dizajnere i administratore. Najznačajnije mrežne prijetnje koje treba razmotriti u fazi dizajna uključuju:
  - korištenje sigurnosnih mehanizama koji se oslanjaju na IP (eng. *Internet Protocol*) adresu pošiljatelja (relativno je jednostavno poslati IP pakete s lažnom IP adresom izvora),
  - prosljeđivanje identifikatora sjednice ili kolačića (eng. *cookies*) preko nešifriranih mrežnih kanala (što može dovesti do krađe IP sjednice),
  - prosljeđivanje tekstualnih akreditacijskih uvjerenja ili ostalih osjetljivih podataka preko nešifriranog komunikacijskog kanala (što može omogućiti napadaču da nadzire mrežu, dobije podatke o logiranju i ostale osjetljive podatke).
- **identificirati domaćinske prijetnje** (eng. *host threats*) - koristi se pristup podjele konfiguracije u odvojene kategorije. Glavne ranjivosti koje ovdje treba uzeti u obzir su:
  - održavanje 'nezakrpanih' (eng. *unpatched*) poslužitelja koji mogu biti izloženi zlonamjernim programima,
  - korištenje vrata (eng. *ports*), protokola i usluga koje nisu nužne,
  - dozvoljavanje anonimnog neovlaštenog pristupa,
  - korištenje slabe politike zaporki i računa.
- **identificirati aplikacijske prijetnje** (eng. *application threats*) - razmatraju se svi aspekti sigurnosnog profila aplikacije. Naglasak je na aplikacijskim prijetnjama, prijetnjama svojstvenim za pojedine tehnologije i prijetnjama koda. Neke od glavnih ranjivosti koje ovdje treba razmotriti su:
  - korištenje slabe provjere valjanosti ulaznih podataka, koja vodi do više vrsta napada (XSS napad, napad umetanjem SQL koda, napad prepunjenjem spremnika),
  - prijenos autentikacijskih uvjerenja ili kolačića preko nekriptiranih mrežnih poveznica, što može dovesti do hvatanja podataka ili krađe sjednice,
  - korištenje slabe politike zaporki i računa što može dovesti do neovlaštenih pristupa,
  - pohranjivanje konfiguracijskih tajni u otvorenom, nešifriranom tekstu,

- korištenje nesigurnog rukovanja iznimkama, koje može dovesti DoS napada te otkrivanja detalja o sustavu koji mogu biti korisni napadaču,
- korištenje slabe i nedovoljnog šifriranja te nedovoljna zaštita kriptirajućih ključeva, [1].

3.4.3. Korištenje stabla napada i uzoraka napada

Stabla napada (eng. *attack trees*) i uzorci napada (eng. *attack patterns*) nisu nužni dijelovi faze identificiranja prijetnji, no mnogi ih smatraju korisnima. Omogućuju dubinsko analiziranje prijetnji u kojem se otkrivaju nove mogućnosti koje se nalaze u slojevima aplikacije koji su ispod dotad promatranie. Stablo napada je način prikupljanja i dokumentiranja mogućih napada na sustav na strukturiran i hijerarhijski način. Stvaranjem stabla napada stvara se reprezentacija sigurnosnih poglavlja koja se može ponovno upotrijebiti. Gradnja stabla napada započinje stvaranjem korijenskih čvorova koji predstavljaju ciljeve napadača. Zatim se dodaju čvorovi listovi koji predstavljaju pojedinačni napad. Primjer jednostavnog stabla napada dan je u nastavku (Slika 3).



Slika 3. *Primjer stabla napada*
Izvor: *msdn.microsoft.com*

Uzorci napada su formalizirani pristup prikupljanju informacija o napadu. Oni predstavljaju generičke reprezentacije napada koji se često javljaju i koji se mogu pojaviti u različitim kontekstima. Definiraju se pomoću:

1. cilja napada kao i uvjeta koji moraju biti zadovoljeni da bi došlo do napada,
2. koraka napada koje je potrebno provesti,
3. rezultata napada.

Usmjereni su na napadačke tehnike, [1].

3.5. Dokumentiranje prijetnji

Za dokumentiranje prijetnji koristi se predložak koji sadrži nekoliko atributa prijetnji kao što je to prikazano u Tablica 1. Najbitniji atributi su opis prijetnje te meta prijetnje. Atribut napadačke tehnike može naglasiti iskorištene ranjivosti, dok je atribut protumjere nužan za adresiranje prijetnji. Atribut rizik se u ovoj fazi ostavlja prazan te se popunjava u završnoj fazi procesa modeliranja prijetnji, [1].

Tablica 1. *Primjer dokumentiranja prijetnje*

Opis prijetnje	**Napadač dobiva autentikacijske podatke nadzirući mrežu**
Meta prijetnje	Proces korisničke autentikacije kod web aplikacije
Rizik	Visok
Napadačke tehnike	Korištenje programa za nadzor mreže
Protumjere	Korištenje SSL-a kako bi se osigurao kriptirani kanal

3.6. Ocjenjivanje prijetnji

Do ovog koraka procesa sastavljena je lista prijetnji za promatranu aplikaciju. U završnom koraku ovog procesa prijetnje se ocjenjuju na temelju rizika kojeg uzrokuju. Na ovaj način dobivena je lista prijetnji u kojoj se na vrhu nalaze prijetnje koje sa sobom donose najviše rizika. S druge strane su prijetnje čija je vjerojatnost pojavljivanja vrlo mala i koje ne mogu prouzročiti veliku štetu, mogu zanemariti.

Osnovna formula prema kojoj je moguće izračunati rizik kojeg uzrokuje pojedina prijetnja je:

Rizik = **Vjerojatnost pojavljivanja** * **Potencijalna šteta**,

što dobro oslikava posljedice na sustav u slučaju pojave napada. Jedna od skala koje se mogu koristiti za vjerojatnost pojavljivanja i potencijalnu štetu je takozvana skala 110. Pri čemu za vjerojatnost pojavljivanja 1 označava prijetnju koja je najmanje vjerojatna, dok 10 označava gotovo izvjesno pojavljivanje. Analogno tome, potencijalna šteta 1 označava najmanju štetu, dok 10 označava katastrofu. Korištenjem ovog pristupa rizik uzrokovan prijetnjom s malom vjerojatnošću pojavljivanja, ali s velikom potencijalnom štetom jednak je riziku kojeg uzrokuje prijetnja ograničenog potencijala, ali uz veliku vjerojatnost pojavljivanja. Ovaj pristup rezultira skalom 1100, odnosno, skalom s rasponom od 1 do 100 koji se može podijeliti u tri područja: visok, srednji i nizak rizik. Na temelju dobivene podjele jasno je koje prijetnje je potrebno najprije riješiti, dok se prijetnje s niskim rizikom mogu i zanemariti, [1].

3.6.1. DREAD

DREAD je klasifikacijska shema za kvantificiranje, usporedbu i određivanje prioriteta rizika prisutnog u svakoj promatranoj prijetnji. Razvijen je i široko korišten u tvrtki Microsoft. DREAD je akronim dobiven od prvih slova svake od kategorija:

- **potencijalna šteta** (eng. ***D****amage potential*) - kolika je šteta ako su iskorištene ranjivosti,
- **reproduktivnost** (eng. ***R****eproducibility*) - koliko je jednostavno proizvesti napad,
- **iskoristivost** (eng. ***E****xploitability*) - koliko je jednostavno iskoristiti pojedinu prijetnju,
- **zahvaćeni korisnici** (eng. ***A****ffected users*) - gruba procjena koliki postotak korisnika je zahvaćen pojedinom prijetnjom,
- **mogućnost otkrivanja** (eng. ***D****iscoverability*) - koliko je jednostavno otkriti ranjivosti.

Svaka od navedenih kategorija ocjenjuje se skalom od 1 do 3 te se u konačnici dobiva skala s rasponom od 5 do 15. Dobivenu skalu moguće je podijeliti na visoke (od 12 do 15), srednje (od 8 do 11) i niske rizike (od 5 do 7). Primjer ocjenjivanja prijetnji pomoću DREAD metode prikazan je u tablici (Tablica 2), [1].

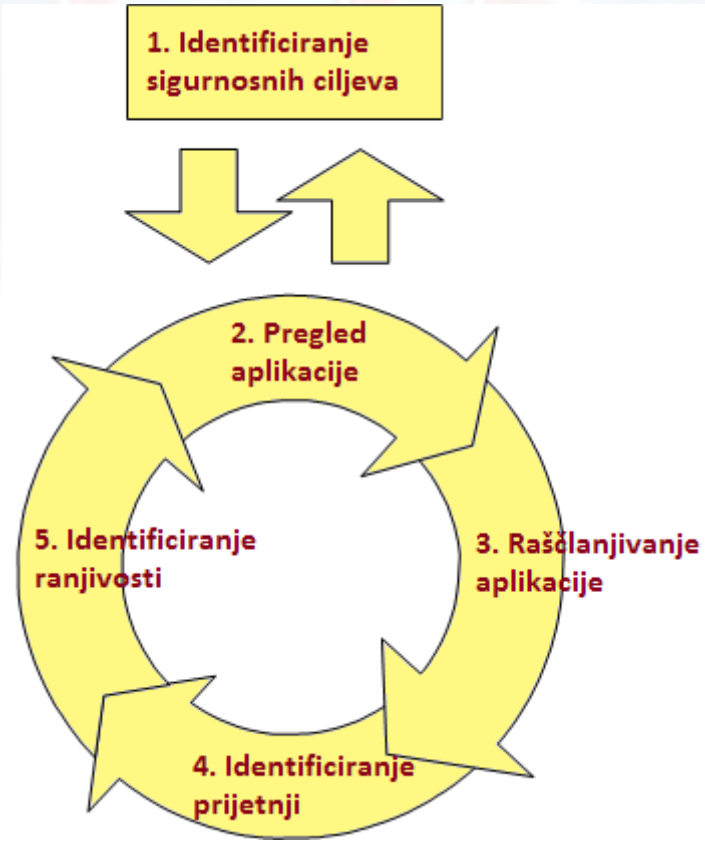
Tablica 2. *DREAD ocjenjivanje prijetnji*

Prijetnja	D	R	E	A	D	Ukupno	Ocjena
Napadač dobiva autentikacijske podatke nadzirući mrežu	3	3	2	2	2	12	Visok
SQL naredbe ubačene u aplikaciju	3	3	3	3	2	14	Visok

3.7. Modeliranje prijetnji web aplikacija

Kod početka dizajniranja web aplikacije ključno je primijeniti modeliranje prijetnji kako bi se uštedjeli resursi, vrijeme i novac koji bi se utrošili na nepotrebni nadzor koji ne zahvaća stvarne rizike. Modeliranje prijetnji web aplikacija provodi se procesom modeliranja prijetnji koji se sastoji od pet koraka, a prikazan je (Slika 4) i opisan u nastavku. Model prijetnji moguće je postupno rafinirati ponavljanjem koraka 2 do 5. Koraci u ovom procesu su sljedeći:

1. **identificiranje sigurnosnih ciljeva** - jasni ciljevi pomažu kod aktivnosti modeliranja prijetnji te kod određivanja vremena koje će se utrošiti na podkorake,
2. **stvaranje pregleda aplikacije** - popisivanje važnih značajki aplikacije pomaže kod identificiranja prijetnji u koraku 4,
3. **raščlanjivanje aplikacije** - detaljno razumijevanje strukture aplikacije olakšava otkrivanje važnijih i detaljnijih prijetnji,
4. **identificiranje prijetnji** - korištenje detalja dobivenih u prethodna dva koraka za identificiranje prijetnji koje odgovaraju promatranoj aplikaciji,
5. **identificiranje ranjivosti** - pregled slojeva aplikacije kako bi se identificirale slabosti povezane s identificiranim prijetnjama, [2].



Slika 4. *Proces modeliranja prijetnji u pet koraka*
Izvor: *CIS*

3.7.1. Identificiranje sigurnosnih ciljeva

Za olakšano razumijevanje i identificiranje sigurnosnih ciljeva najbolje ih je podijeliti u sljedeće kategorije:

- **identitet** - štiti li aplikacija korisnikov identitet od zlouporabe,
- **financije** - procjena razine rizika u vidu financijskog gubitka koje je organizacija spremna utrošiti u sanaciju eventualne štete,
- **ugled** - mjerenje ili procjena gubitka ugleda uzrokovanog pogrešnom uporabom aplikacije ili provedenim napadom,
- **privatnost i regulacija** - do koje mjere bi aplikacija trebala štititi korisničke podatke,
- **dostupnost jamstva** - zahtijeva li aplikacija neki oblik jamstva.

Ovime je dobiven iscrpan popis koji može biti od velike koristi u daljnjim koracima, [2], [3].

3.7.2. Pregled aplikacije

Nakon što su definirani sigurnosni ciljevi, dizajn aplikacije se analizira kako bi se identificirale komponente, tokovi podataka i granice povjerenja. Ovaj korak provodi se pregledavanjem arhitekture aplikacije i dokumentacije. Posebice, potrebno je stvoriti UML (eng. *Unified Modeling Language*) komponentne dijagrame. Takvi komponentni dijagrami visoke razine uglavnom su dovoljni za razumijevanje toka podataka između pojedinih dijelova aplikacije. Primjerice, kretanje podataka preko granice povjerenja treba biti pažljivo analizirano, dok podaci koji se kreću unutar iste razine povjerenja (eng. *trust level*) ne trebaju tolika ispitivanja, [3].

3.7.3. Raščlanjivanje aplikacije

Nakon razumijevanja arhitekture aplikacije, slijedi njezino daljnje raščlanjivanje kako bi se otkrila svojstva i moduli čiji sigurnosni utjecaj treba provjeriti. Primjerice, prilikom istraživanja modula za autentikaciju potrebno je razumjeti kako podaci ulaze u modul. Osim toga, potrebno je poznavati kako modul provjerava i obrađuje podatke, gdje se nalaze tokovi podataka, na koji način se pohranjuju podaci te koje temeljne odluke i pretpostavke su donijete prilikom izrade modula, [3].

3.7.4. Identificiranje prijetnji

Nemoguće je zapisati nepoznate prijetnje, no isto tako je vjerojatno da će biti stvoreni novi zlonamjerni programi koji će iskorištavati nove ranjivosti nekog sustava. Stoga je potrebno usredotočiti se samo na poznate rizike. Dva najčešća pristupa prilikom zapisivanja potencijalnih prijetnji su graf prijetnji (eng. *threat graph*) i strukturirane liste. Graf prijetnji predstavlja proširenje modela stabla prijetnji (eng. *threat tree*) i prikazuje područja utjecaja pojedine prijetnje. Strukturirane liste ne sadrže tako jasan prikaz prijetnji i njihovih međuovisnosti kao graf prijetnji te imaju jednostavnu strukturu. Tipično, graf prijetnji pruža više informacija, no potrebno je više vremena za njegovu izradu. S druge pak strane, strukturirane liste je lakše stvoriti, no potrebno je više vremena kako bi se shvatili utjecaji prijetnji. Za bolje razumijevanje relevantnih prijetnji korisno je razmotriti tko bi mogao napasti aplikaciju. Potencijalne napadače moguće je podijeliti u sljedeće kategorije:

- **slučajna otkrića** - običan korisnik naleti na funkcijsku pogrešku u aplikaciji koristeći samo internetski preglednik i pritom dobije pristup privilegiranim informacijama ili funkcionalnosti,
- **automatski zlonamjerni programi** - programi ili skripte koji traže poznate ranjivosti te zatim vraćaju informacije na središnju stranicu koja ih sakuplja,
- **radoznali napadač** - istraživač sigurnosti ili običan korisnik koji primjećuje kako nešto nije u redu s aplikacijom te odlučuje nastaviti istraživati,

- ***script kiddies*** - često su to odmetnici koji traže kako kompromitirati ili naštetiti aplikaciji zbog kolateralnog probitka, vlastite ozloglašenosti ili političkog programa,
- **motivirani napadač** - nezadovoljan zaposlenik sa znanjem iznutra ili plaćeni profesionalni napadač,
- **organizirani kriminal** - kriminalci koji se bave probijanjem bankovnih aplikacija kako bi ostvarili financijsku korist, [3].

3.7.5. Identificiranje ranjivosti

Sigurnosni okvir web aplikacije (eng. *Web Application Security Frame*) definira skup kategorija ranjivosti za web aplikacije. Ove kategorije predstavljaju područja u kojima najčešće dolazi do pogrešaka te stoga na njih treba obratiti posebnu pažnju. Do tih kategorija došli su sigurnosni stručnjaci ispitivanjem i analiziranjem glavnih sigurnosnih poglavlja u mnogim web aplikacijama. Kategorije su sljedeće:

- **provjera valjanosti ulaza i podataka** - odnosi se na način na koji aplikacija filtrira, pročišćava i odbacuje ulazne podatke prije njihove daljnje obrade,
- **autentikacija** - proces u kojem osoba dokazuje svoj identitet, najčešće pomoću korisničkog imena i zaporke,
- **autorizacija** - način na koji aplikacija osigurava pristup resursima i operacijama,
- **upravljanje konfiguracijom** - odnosi se na načine na koje aplikacija rukuje konfiguracijom,
- **osjetljivi podaci** - način na koji se obrađuju svi podaci koji moraju biti zaštićeni, bilo da su oni u memoriji, prolaze mrežom ili su trajno pohranjeni,
- **upravljanje sjednicom** - rukovanje i zaštita niza povezanih međudjelovanja korisnika i web aplikacije,
- **kriptografija** - odnosi se na zaštitu i tajnost važnih podataka te način na koji aplikacija osigurava povjerljivost i cjelovitost,
- **upravljanje parametrima** - odnosi se na način na koji aplikacija štiti parametre od mijenjanja te na koji način aplikacija obrađuje ulazne parametre,
- **upravljanje iznimkama** - što se događa prilikom neuspjelog poziva metoda u aplikaciji,
- **revizija i prijavljivanje** - način na koji aplikacija pohranjuje podatke o događajima vezanim uz sigurnost.

Kod identificiranja ranjivosti aplikacija se proučava sloj po sloj te se razmatra svaka od navedenih kategorija ranjivosti u svakom sloju, [2].

4. Primjena u analizi rizika

Sigurnost u bilo kojem sustavu proporcionalna je rizicima koji se javljaju u njemu. No, proces određivanja koje sigurnosne provjere su prikladne i učinkovite je često složen i subjektivan. Jedna od glavnih zadaća sigurnosne analize rizika (eng. *risk analysis*) jest postavljanje ovog procesa na objektivnije temelje. Postoji mnogo različitih pristupa u analizi rizika, no oni se temeljno mogu podijeliti u dvije skupine: kvantitativni i kvalitativni, [5].

4.1. Kvantitativna analiza rizika

Ovaj pristup koristi dva temeljna elementa:

1. vjerojatnost pojavljivanja događaja,
2. vjerojatni gubitak koji se javlja s njim.

Kvantitativna analiza rizika koristi svaki podatak koji proizvedu ova dva elementa. Problemi kod ove vrste analize rizika najčešće su povezani s nepouzdanošću i netočnošću podataka.

Vjerojatnost je u rijetkim slučajevima potpuno točna. Dodatno, upravljanje i protumjere često se bave većim brojem mogućih događaja koji su često međusobno povezani. Unatoč navedenim nedostacima, brojne organizacije su uspješno prihvatile kvantitativnu analizu rizika, [5].

4.2. Kvalitativna analiza rizika

Kvalitativna analiza rizika je daleko najraširenija pristup u analizi rizika. Ne zahtjeva vjerojatnosne podatke, već koristi samo procjenu potencijalnog gubitka. Većina metodologija kvalitativne analize rizika koriste brojne međusobno povezane elemente:

- **prijetnje** - stvari koje mogu poći po zlu ili koje mogu 'napasti' sustav. Prijetnje su prisutne uvijek i u svakom sustavu,
- **ranjivosti** - čine sustav podložniji napadima ili povećavaju vjerojatnost uspjeha napada odnosno njegov utjecaj na sustav,
- **provjere** - protumjere za ranjivosti. Postoje četiri tipa provjera:
  - **provjere odvraćanja** (eng. *deterrent controls*) - smanjuju izglednost pojave namjernih napada,
  - **preventivne provjere** (eng. *preventative controls*) - štite ranjivosti te onemogućuju napad ili umanjuju njegov utjecaj,
  - **popravne provjere** (eng. *corrective controls*) - umanjuju utjecaj napada,
  - **detektivske provjere** (eng. *detective controls*) - otkrivaju napade i pokreću preventivne ili ispravljačke provjere, [5].

4.3. Norma AS/NZS 4360

Australska i Novozelandska norma za upravljanje rizicima 'AS/NZS 4360:2004' predstavlja prvu formalnu normu za dokumentiranje i upravljanje rizikom. Prvi puta je objavljena 1999. godine, a 2004. godine obavljena je posljednja revizija. Pristup ove norme je jednostavan, prilagodljiv i iterativan. Sam proces podijeljen je u pet koraka:

- **uspostavljanje konteksta** (eng. *establish context*) - uspostavljanje domene rizika,
- **identifikacija rizika** - koji specifični rizici su prisutni unutar domene rizika,
- **analiza rizika** - određivanje postoje li odgovarajući nadzor nad rizicima,
- **ocjenjivanje rizika** - određivanje preostalog rizika,
- **postupanje s rizicima** - opisivanje metode za postupanje s rizikom kako bi se ublažio odabrani rizik.

Ova norma usmjerena je prvenstveno na poslovne primjene, a zbog nedostatka strukturnih metoda njezina primjena kud računalnih sustava je znatno manja, [3].

5. Alati za modeliranje

U novije vrijeme sve je više različitih alata za modeliranje prijetnji i upravljanje rizikom. Mnogi od njih otvorenog su koda te su stoga lako dostupni. Ne postoji sveobuhvatni alat koji bi bio optimalan za svaku namjenu. Stoga je potrebno proučiti prednosti i nedostatke postojećih alata kako bi se odabrao onaj alat koji najbolje odgovara postojećim zahtjevima. Neki od popularnijih alata za modeliranje prijetnji i rizika su:

- **Microsoft Threat Analysis and Modeling Tool** - moćan i opsežan Microsoftov alat za analizu i modeliranje prijetnji,
- **Trike** - jedinstveni konceptualni okvir za modeliranje prijetnji koji ima određene sličnosti s Microsoftovim procesom modeliranja prijetnji,
- **OSMR** (eng. *Open Source Management of Risk*) - otvoreni program za upravljanje rizikom,
- **MARCO** (eng. *MAximized Risk COntrol*) - alat za prikupljanje i analizu rizika u složenim kompanijama,

- **CORAS platforma za procjenu rizika** (eng. *CORAS Risk Assessment Platform*) - platforma za analizu rizika kritičnih IT sustava korištenjem UML-a,
- **OCTAVE** (eng. *Operationally Critical Threat, Asset and Vulnerability Evaluation*) - skup alata tehnika i metoda za procjenu i planiranje informacijske sigurnosti, [3].

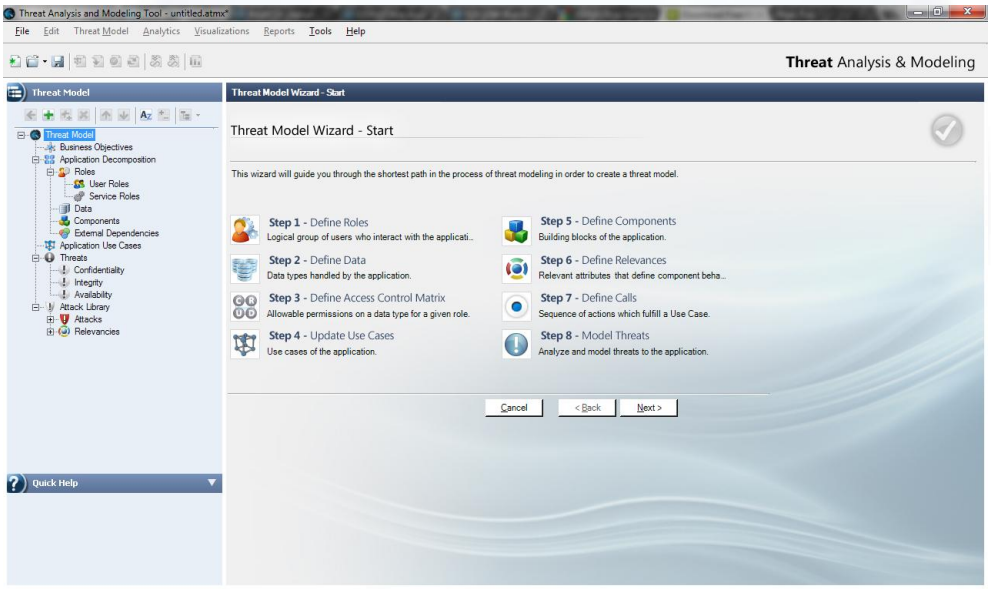
U nastavku će biti opisani neki od najkorištenijih alata: Microsoft Threat Analysis and Modeling tool, OCTAVE i Trike.

5.1. Microsoft Threat Analysis and Modeling Tool

Alat Microsoft Threat Analysis and Modeling vjerojatno je najpoznatiji besplatan alat za analiziranje i modeliranje sigurnosnih prijetnji. On omogućuje ekspertima koji se ne bave sigurnošću pristup poznatim informacijama kao što su poslovni zahtjevi i arhitektura aplikacije. Oni se zatim koriste za stvaranje modela prijetnji bogatog značajkama. Pored automatskog identificiranja prijetnji, alat daje i vrijedne sigurnosne artefakte. Alat je moguće preuzeti sa sljedeće poveznice, [7]:

http://www.microsoft.com/en-us/download/details.aspx?id=14719

Izgled glavnog prozora alata prikazan je u nastavku (Slika 5).



Slika 5. *Glavni prozor alata Microsoft Threat Analysis & Modeling*
Izvor: *CIS*

5.2. OCTAVE

OCTAVE je skup alata tehnika i metoda za procjenu i planiranje informacijske sigurnosti nastalih na Carnegie Mellon Universitiy. OCTAVE metoda je samousmjerena (eng. *self-directed*). Manji timovi zaposlenika iz različitih sektora tvrtke zajedno identificiraju sigurnosne potrebe tvrtke. Jedna od prednosti OCTAVE metoda je i fleksibilnost, odnosno mogućnost prilagođavanja potrebama i zahtjevima pojedine organizacije. Ograničenje OCTAVE metoda jest njihova nekompatibilnost s normom AS/NZS 4360, odnosno pretpostavka da je vjerojatnost pojavljivanja prijetnje jednaka 1. Još jedan nedostatak ovog alata jest i njegova složenost.

5.3. TrikeTrike je okvir za modeliranje prijetnji koji je sličan Microsoftovom procesu modeliranja prijetnji. Razlikuje se po tome što koristi pristup temeljen na riziku s različitom izvedbom, te modelima prijetnji i rizika od modela koji koriste STRIDE i DREAD sheme. Trike omogućuje visoku razinu automatizacije te daje pogled na sustav s obrambene perspektive.

6. Zaključak

Modeliranje prijetnji postaje neophodan dio dizajniranja i razvoja računalnog sustava ili aplikacije. Uz učestale napade te opasnosti koje prijete iz raznih smjerova modeliranje sigurnosnih prijetnji postaje iznimno važno i s financijskog pogleda. U tom vidu, iznimno je značajna ocjena prijetnji koja se koristi za brže i učinkovitije uklanjanje ili ublažavanje najopasnijih prijetnji. Jasno identificiranje prijetnji i ranjivosti sustava početna su točka u pronalaženju zaštitnih protumjera. Pritom je od velike koristi poznavanje arhitekture i funkcionalnosti promatranog sustava. To znanje olakšava pronalaženje prijetnji koji su na prvi pogled skrivene ili teško raspoznatljive, a predstavljaju potencijalno veliku opasnost sustavu.

Novije metode modeliranja prijetnji i analize rizika postaju sve pristupačnije za korištenje korisnicima koji nisu sigurnosni stručnjaci. U tome im mnogo pomažu i dostupni programski alati. Iz do sada navedenog može se zaključiti da je pred metodama modeliranja sigurnosnih prijetnji svijetla budućnost. Sasvim je izvjesno kako će modeliranje prijetnji u budućnosti postati iznimno rasprostranjeno.

Leksikon pojmova

Autentikacija - Proces potvrđivanja identiteta podatka ili osobe

Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Najčešći primjeri su: uz korištenje kartice na bankomatu i upisivanje PIN-a, ili upisivanje (korisničkog) imena i zaporke.

http://searchsecurity.techtarget.com/definition/authentication

Cyber kriminalac - Osoba koja se bavi cyber kriminalom

Cyber kriminalac je osoba koja koristi računala i Internet za počinjenje kaznenih dijela.

http://www.webopedia.com/TERM/C/cyber_crime.html

DOS napad - Napad uskraćivanjem usluge

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

http://searchsoftwarequality.techtarget.com/definition/denial-of-service

IP - IP protokol

Internet Protocol - IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

IP zavaravanje

Pojam se odnosi na pokušaj neautoriziranog entiteta da dobije autoriziran pristup sustavu pretvarajuci se da je autoriziran korisnik.Sastoji se od slanja IP paketa s lažiranom izvorišnom IP adresom - Pojam se odnosi na pokušaj neovlaštenog entiteta da dobije autoriziran pristup sustavu pretvarajući se da je autoriziran korisnik.Sastoji se od slanja IP paketa s lažiranom izvorišnom IP adresom.

http://www.symantec.com/connect/articles/ip-spoofing-introduction

Kolačić - Kolačić datoteka

Datoteka koja sadrži podatke o posjeti web stranici. Na taj način vlasnici web stranice rade statistiku posjeta. Cookie također pamti neke postavke koje ste namjestili i podatke koje ste upisali na posjećenoj stranici (npr. lozinku). Cookie datoteka.

http://www.httpwatch.com/httpgallery/cookies/

Kriptografija - Kriptografija u računarstvu

Kriptografija je područje kriptologije koje se bavi stvaranjem kriptografskih algoritama za zaštitu podataka. Točnije, podrazumijeva stvaranje i analizu protokola i algoritama koji osiguravaju siguran prijenos i pohranu informacija, bilo u računalnoj mreži ili mediju za pohranu podataka.

http://searchsoftwarequality.techtarget.com/definition/cryptography

SQL - Structured Query Language

SQL je programski jezik za pohranu, upravljanje i dohvat podataka pohranjenih u relacijskoj bazi podataka. SQL je najrašireniji programskih jezik za upravljanje bazama podataka.

http://www.1keydata.com/sql/sql.html

SQL injection napad - Napad injekcijom SQL naredbe

Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika. - Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web programa bazi podataka. Na taj način moguće je ugroziti sigurnost web programa koji konstruira SQL upite iz podataka koje su unijeli korisnici.

https://www.owasp.org/index.php/SQL_Injection

UML - Unified Modeling Language

Unified Modeling Language (UML) ili jezik za unificirano modeliranje grafički je jezik za vizualiziranje, specificiranje, konstruiranje i dokumentiranje artefakata softverski intenzivnog sustava.

http://spvp.zesoi.fer.hr/seminari/2003/duvnjak/UML3.htm

XSS napad - Cross-site scripting napad

Napadačka tehnika koja prisiljava web aplikaciju da korisniku proslijedi zlonamjerni izvršni kod, koji se zatim učitava i izvršava u korisnikovom web pregledniku.

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

Zlonamjerni program - Programi namijenjeni ugrožavanju računalnog sustava

Zlonamjerni programi (eng. malware) su programi (mogu biti i skripte i kodovi) namijenjeni ometanju operacija u računalu, prikupljanju osjetljivih informacija ili dobivanju neovlaštenog pristupa računalnim sustavima. To je općenit naziv koji se koristi za sve vrste programa ili koda koji su namijenjeni zlonamjernom iskorištavanju računala i podataka u njemu bez korisnikova znanja.

www.wisegeek.com/what-is-a-malware-virus.htm

Reference

[1] J.D. Meier i ostali: Threat modeling, lipanj 2003.
http://msdn.microsoft.com/en-us/library/ff648644.aspx, svibanj 2012.

[2] A. Mackman i ostali: Threat Modeling Web Appliccations, svibanj 2005.
http://msdn.microsoft.com/en-us/library/ms978516.aspx, svibanj 2012.

[3] OWASP, Threat Risk Modeling, rujan 2010.
https://www.owasp.org/index.php/Threat_Risk_Modeling, svibanj 2012.

[4] Wikipedia, Threat model, siječanj 2011.
http://en.wikipedia.org/wiki/Threat_model, svibanj 2012.

[5] Introduction to Risk Analysis,
http://www.security-risk-analysis.com/introduction.htm, svibanj 2012.

[6] E.A. Oladimeji i drugi: Security threat modeling and analysis: A goal-oriented approach
http://www.utd.edu/~eao015100/documents/SecurityThreatModeling.pdf, svibanj 2012

[7] Microsoft Threat Analysis & Modeling v2.1.2, ožujak 2007.
http://www.microsoft.com/en-us/download/details.aspx?id=14719, svibanj 2012.

[8] N.Sportsman: Threat modeling, 2011.
http://www.praetorian.com/downloads/presentations/Praetorian_Threat_Modeling_Presentation.pdf, svibanj 2012.