Centar Informacijske Sigurnosti

Common Weakness Risk Analysis Framework

veljača 2012.

CIS-DOC-2012-02-039

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 4
2. POVIJEST CWE PROJEKTA 5
3. VEZA IZMEĐU CWE, CWSS I CWRAF 6
4. SUSTAV CWSS 7
4.1. UTJECAJ KORISNIKA 7
4.2. METODE VREDNOVANJA PROPUSTA 7
5. OKRUŽENJE CWRAF 8
5.1. MODELIRANJE OKRUŽENJA 8
5.1.1. Poslovna domena 8
5.1.2. Tehnološke skupine i arhetipovi 9
5.1.3. Vinjete 10
6. KORIŠTENJE OKRUŽENJA CWRAF I VINJETA U SUSTAVU CWSS 13
7. BUDUĆNOST PROJEKTA CWE I OKRUŽENJA CWRAF 15
8. ZAKLJUČAK 16
9. LEKSIKON POJMOVA 17
10. REFERENCE 18

1. Uvod

Sigurnosna analiza programa provedena nekim alatom za provjeru koda nerijetko rezultira velikim brojem pronađenih slabosti. Programer se mora snaći među upozorenjima, pronaći one koji predstavljaju sigurnosnu prijetnju i njih prve ispraviti. Ponekad se to pokazuje kao vrlo težak zadatak upravo zbog prevelikog broja upozorenja te je teško odlučiti se kojim redoslijedom obavljati popravke u programima. Dodatni otežavajući čimbenik je i činjenica da važnost propusta u programu ovisi o okruženju u kojem se koristi.

Iako postoje različite metode vrednovanja važnosti propusta u programima (npr. NIH sustav vrednovanja te Microsoft STRIDE), nijedna ne nudi općenito rješenje koje će se moći primjenjivati neovisno o korištenoj tehnologiji, programskom okruženju ili potrebama organizacije koja koristi program.

Iz tog je razloga pokrenut projekt CWE (eng. *Common Weakness Enumeration*), čiji je cilj kategorizirati propuste i prijetnje u programima, stvoriti alat koji će automatizirati traženje takvih propusta te odrediti prioritet njihovog rješavanja uzimajući u obzir kako i gdje se program koristi. Dio tog projekta su i sustav CWSS (eng. *Common Weakness Scoring System*) i okruženje CWRAF (eng. *Common Weakness Risk Analysis Framework*). CWSS je zadužen za procjenu i rangiranje propusta, dok CWRAF omogućuje korisnicima da koriste CWSS na način optimalan za njihovo poslovno okruženje.

U poglavljima 2 i 3 ukratko je opisana povijest CWE projekta te veza između sustava CWSS i okruženja CWRAF. Poglavlje 4 ukratko opisuje sustav CWSS. Nužno je razumjeti osnove sustava CWSS prije nego se prijeđe na samo okruženje CWRAF u poglavlju 5. Primjer korištenja okruženja CWRAF u sustavu CWSS dan je u poglavlju 6.

2. Povijest CWE projekta

Krajem devedesetih godina prošlog stoljeća organizacija MITRE je započela s kategorizacijom propusta u programima i izdala popis CVE (eng. *Common Vulnerabilities and Exposures*) oznaka. Iako je takav popis davao dobru informaciju o čestim propustima, nije bio dovoljno detaljan da bi se iskoristio za procjenu sigurnosti koda u programima. Stoga je 2005. godine MITRE u suradnji s Američkim odjelom za državnu sigurnost (eng. *United States Department of Homeland Security*) započeo s prilagodbom CVE liste za primjenu u području procjene sigurnosti koda. Rezultat ove suradnje je dokument PLOVER (eng. *Preliminary List of Vulnerability Examples for Researchers*) kojim se pokušalo pobrojati i grupirati propuste u kodu te odrediti njihovu iskoristivost za napade. U njemu je opisano 290 tipova programskih propusta te velik broj primjera iskoristivosti za svaki od propusta (ukupno preko 1500 primjera kako se u stvarnim napadima mogu iskoristiti ti propusti).

CVE lista i PLOVER bili su prethodnici današnjeg projekta CWE. Motivacija za projekt CWE bio je nedostatak nomenklature, taksonomija i standarda koji bi se koristili u svim alatima za provjeru sigurnosti programa i na taj način omogućili objektivnu usporedbu mogućnosti takvih alata. CWE se stoga razvija s idejom da služi kao referentni popis programskih pogrešaka koje bi alati za provjeru sigurnosti trebali prepoznati.

Godine 2010. u sklopu CWE projekta razvijen je i sustav CWSS čiji je cilj usporediti različite propuste kako bi im se mogli dodijeliti različiti prioriteti. Godinu dana kasnije započet je razvoj okruženja CWRAF koje omogućuje korisnicima da koriste CWSS kako bi otkrili propuste koji su najvažniji u okruženju u kojem koriste ispitivani program.

3. Veza između CWE, CWSS i CWRAF

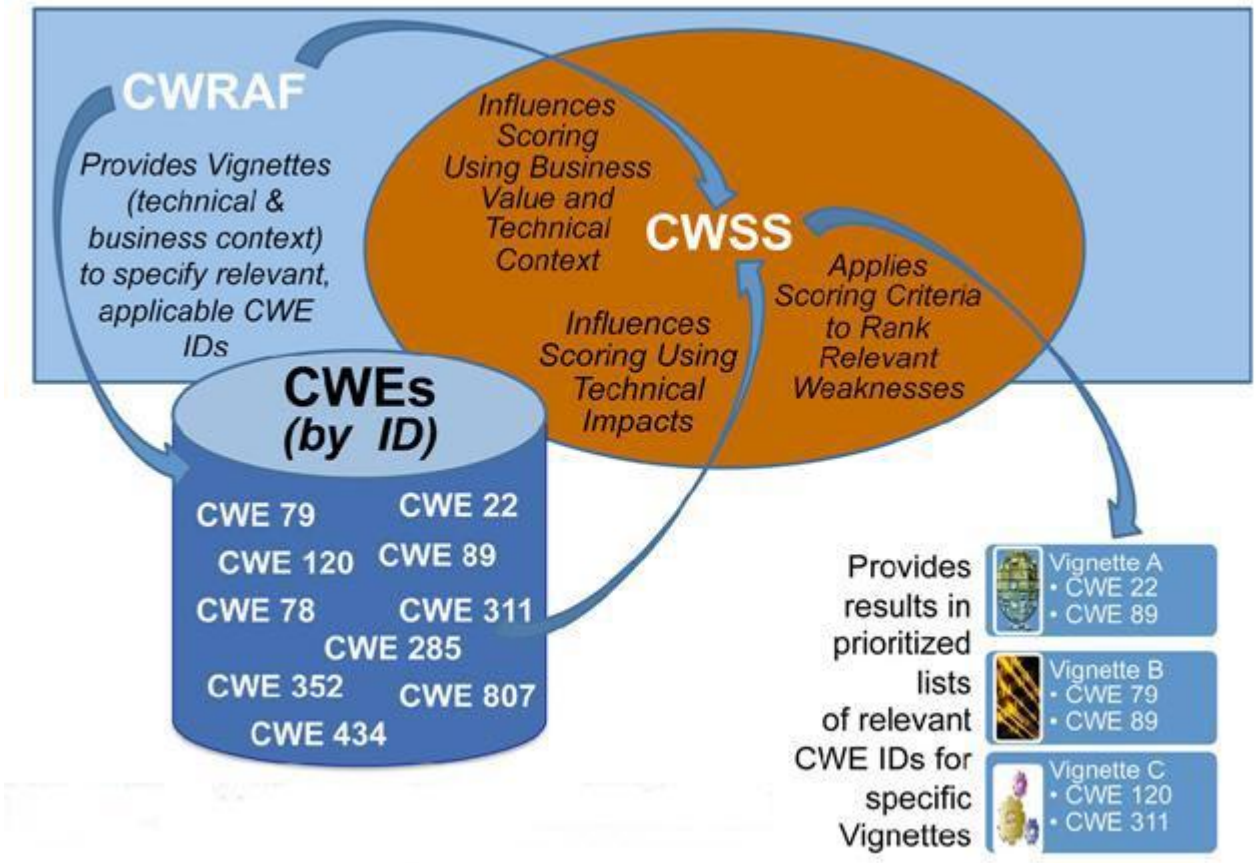
Projekt CWE sastoji se od tri glavna dijela. Prvi dio je osnova projekta u kojem se radi o kategorizaciji propusta. Svakoj od klasa propusta dodjeljuje se CWE oznaka po kojoj se prepoznaju. Tako npr. SQL injekcije imaju oznaku CWE-89, a prepisivanje memorije (eng. *buffer overflow*) CWE-120.

Drugi dio pokrenut u sklopu CWE projekta je sustav CWSS. CWSS koristi CWE identifikacije propusta, na njih primjenjuje razne kriterije za rangiranje te određuje prioritet i važnost prepoznatih propusta.

Treći dio je okruženje CWRAF. CWRAF utječe na rezultat sustava CWSS na način da prilagođava rezultat korisniku koji koristi CWSS. Komunikacija između sustava CWSS i okruženja CWRAF odvija se preko vinjeta (eng. *Vignettes*). Vinjetama korisnik opisuje okolinu u kojoj koristi neki program. Koncept vinjeta detaljnije je opisan u poglavlju 5.1.3.

Važno je napomenuti da sustav CWSS može funkcionirati i samostalno, bez okruženja CWRAF, ali obrat naravno ne vrijedi.

Slika 1 prikazuje odnos projekta CWE, sustava CWSS i okruženja CWRAF. Nakon što neki alat za automatsko traženje propusta pronađe propuste u programu, sustav CWSS traži CWE oznaku za svaki od pronađenih propusta i korištenjem raznih formula određuje rezultat za svaki od njih. Ako se u proces uključi i okruženje CWRAF, rezultat sustava CWSS se mjenja kako bi se što bolje prilagodio korisniku i okolini u kojoj on koristi testirani program.



Slika 1. - *Odnos CWE, CWSS-a i CWRAF-a*
Izvor: *mitre.org*

4. Sustav CWSS

Sustav CWSS je dio projekta CWE koji se bavi u problemom usporedbe i vrednovanja različitih propusta u programima.

4.1. Utjecaj korisnika

Različiti korisnici sustava CWSS (npr. programeri, razvojni menadžeri) imaju različite zahtjeve kod određivanja prioriteta rješavanja programskih propusta. CWSS omogućuje postavljanje različitih scenarija koji odgovaraju pojedinim klasama korisnika kako bi se rezultati što bolje prilagodili korisniku. U nastavku su opisane neke od tipičnih klasa korisnika te njihovi mogući zahtjevi.

- **Programer** je često vremenski ograničen i mora dovršiti program do određenog datuma. Ponekad ne stigne popraviti sve propuste i slabosti, već se mora odlučiti na one koji imaju velik omjer potencijalne opasnosti i vremena potrebnog za popravak. Kod korištenja automatskog traženja propusta logično je kod popravaka zanemariti one rezultate kod kojih je velika vjerojatnost da su lažno pozitivni (alat prepoznaje neki bezopasni propust kao potencijalno opasan).
- **Razvojni menadžeri** stvaraju strategije za uklanjanje čitavih klasa propusta i slabosti iz programa definiranjem tzv. "Top-N" lista u kojima rangiraju najopasnije propuste.
- **Preuzimatelji programa** (krajnji korisnici, sistemski administratori, ali i programeri koji koriste program koji su razvili drugi programeri) traže određenu razinu sigurnosti da su u programu uklonjeni kritični propusti.
- **Procjenitelji alata za analizu propusta u programskom kodu** žele mehanizam koji će im omogućiti konzistentno i nepristrano vrednovanje rezultata raznih alata.

4.2. Metode vrednovanja propusta

Postoje različite metode vrednovanja propusta, a u nastavku su ukratko opisane tri koje se koriste u sustavu CWSS i okruženju CWRAF.

- **Ciljana** (eng. Targeted) metoda vrednuje propuste koji su otkriveni u nekom specifičnom, ciljanom dijelu programa, npr. prepisivanje memorije u korisničkom imenu u određenoj liniji koda nekog programa za autentifikaciju korisnika. Alati za automatsku provjeru programa koriste ovu metodu, a ona je i osnovna metoda u sustavu CWSS.
- **Generalizirana** metoda međusobno uspoređuje različite tipove propusta te ih zatim rangira, npr. prepisivanje memorije je većeg prioriteta od curenja memorije (eng. *memory leak*). Ova se metoda koristi kod izrade "Top-N" lista na kojima se rangiraju trenutno najopasniji (najčešće i najlakše iskoristivi) propusti. Primjer takve liste može se pogledati na MITRE web stranici na.

http://cwe.mitre.org/top25

- **Metoda prilagođena kontekstu** (eng. *Context-adjusted*) kombinira se s ciljanom ili generaliziranom metodom i prilagođava njihove rezultate ovisno o nekim zadanim čimbenicima (tolerancija rizika, okruženje u kojem se program koristi i sl.).

5. Okruženje CWRAF

Okruženje CWRAF omogućuje ljudima koji sudjeluju u razvoju programa, ali i krajnjim korisnicima programa, primjenu sustava CWSS na individualan, specifičan način. Umjesto rangiranja klasičnim korištenjem sustava CWSS, okruženje CWRAF nudi korisniku da u obzir uzme i npr. područje primjene programa, tehnologije koje se koriste i slične čimbenike. Na taj se način određuju kritični propusti u programu za ciljanu primjenu, što omogućuje programerima da se usredotoče na popravljanje tih, važnijih propusta, kao i korisnicima programa da provjere njegovu sigurnost u okruženju u kojem ga namjeravaju koristiti.

5.1. Modeliranje okruženja

Svaka organizacija koja koristi neki program radi u drugačijem okruženju. Drugačije su prijetnje koje utječu na sigurnost programa, a razlikuju se i tolerancije rizika te mnogi drugi čimbenici. Zbog toga je teško napraviti mehanizam koji će provesti dobro rangiranje propusta u svim situacijama i za sve korisnike. Okruženje CWRAF tom problemu pristupa na način da korisniku omogućuje modeliranje nekih čimbenika koji su specifični za okruženje u kojem se program koristi i te informacije uključuje u sustav CWSS kod rangiranja propusta.

U nastavku su opisani čimbenici koji modeliraju okruženje CWRAF.

5.1.1. Poslovna domena

Poslovna domena opisuje općenito područje djelatnosti kojim se organizacija bavi. U nastavku su nabrojane poslovne domene ponuđene u okruženju CWRAF te primjeri institucija i organizacija iz svake od njih:

- **e-trgovina** – uključuje organizacije koje koriste Internet za obavljanje trgovine,
- **banke i financije** – institucije povezane s financijskim sektorom (banke, štedionice, osiguravateljske kuće, investicijske kuće i sl.),
- **energetika** – u ovu poslovnu domenu spadaju sve organizacije povezane sa proizvodnjom i distribucijom energije, npr. sustavi za proizvodnju i distribuciju nafte i plina, elektrane i pametne mreže [1](eng. *Smart grid*),
- **kemija** – uključuje organizacije koje se bave proizvodnjom i distribucijom kemijskih proizvoda,
- **proizvodnja** – organizacije koje se bave proizvodnjom i distribucijom proizvoda koji nisu obuhvaćeni u nekoj od prethodne dvije poslovne domene,
- **prijevoz** – organizacije koje su vezane za promet, npr.brodske luke, zračne luke, autoceste,
- **državna sigurnost** – organizacije koje su uključene u zaštitu državne sigurnosti, npr. tajne službe, obalna straža,
- **obrana** – organizacije zadužene za obranu, npr. vojska, oružje, vojne baze,
- **državna uprava** – poslovna domena koja uključuje sve što ne spada u državnu sigurnost ili obranu,
- **hitne službe** – službe za hitne intervencije – vatrogasci, policija, hitna pomoć, službe za krizna razdoblja,
- **javno zdravstvo** – organizacije i sustavi iz sektora javnog zdravstva, npr. bolnice, baze podataka s informacijama o pacijentima, proizvodnja i distribucije lijekova,
- **hrana i voda** – organizacije koje se bace proizvodnjom i distribucijom hrane i vode,

[1] Pametna mreža je električna mreža koja sakuplja informacije o potrošnji korisnika i koristi ih na način da poveća učinkovitost mreže.

- **telekomunikacije** – organizacije iz sektora telekomunikacije koje nude mobilne i fiksne mreže, VoIP[2] (eng. *Voice over Internet Protocol*) i sl.,
- **rad na daljinu** (eng. *Teleworking*) – zaposlenici koji izvana imaju pristup računalnoj mreži neke organizacije,
- **e-glasanje** – sustavi za elektroničko glasanje,
- **društveni mediji** – organizacije koje koriste Internet za komunikaciju, suradnju, zabavu ili djeljenje medijskog sadržaja, npr. blogovi, društvene mreže,
- **ljudski resursi** – poslovna domena koja opisuje korištenje programa u svrhu upravljanja zaposlenicima unutar organizacije, vrbovanja novih zaposlenika, procjenom učinkovitost zaposlenika i sl.

5.1.2. Tehnološke skupine i arhetipovi

Sustavi, arhitekture i tehnologija općenito koja se koristi u radu organizacije u okruženju CWRAF se opisuju tehnološkim skupinama. Jedna tehnološka skupina koristi se u različitim poslovnim domenama, tako da je već samo s ove dvije kategorije moguće opisati velik broj različitih okruženja.

Tehnološke skupine sadrže arhetipove (eng. *Archetype*), konkretne arhitekture koje se koriste u radu. Primjerice, sustav SCADA (eng. *Supervisory Control and Data Acquisition*) je arhetip tehnološke skupine kontrolnih sustava. Tehnološke skupine i neki od pripadnih arhetipova u CWRAF-u su dani u nastavku, a potpun popis moguće je pronaći na

http://cwe.mitre.org/cwraf/vignettes.html#techgroups.

- **web aplikacije** – ova kategorija uključuje aplikacije kojima se pristupa preko mreže, web klijente i web poslužitelje,
- **ugradbeni računalni sustavi za rad u stvarnom vremenu** – računalni sustavi koji su dio nekog većeg sustava, najčešće se radi o PLC[3]-ovima (eng. *Programmable Logic Controler*) i mikrokontrolerima,
- **kontrolni sustavi** – sustavi ili uređaji koji služe za upravljanje drugim sustavima ili uređajima, primjerice SCADA i distribuirani kontrolni sustavi,
- **mobilni uređaji** – danas su sve više rasprostranjeni pametni telefoni, prijenosna računala i tablet uređaji,
- **baze podataka i sustavi za pohranu podataka** – baze podataka,
- **operacijski sustavi** – virtualni operacijski sustavi, operacijski sustavi opće namjene,
- **računarstvo u oblaku** – IaaS[4] (eng. *Infrastructure as a Service*), PaaS [5](eng. *Platform as a Service*), SaaS [6](eng. *Software as a Service*),
- **mrežne komunikacije** – VPN (eng. *Virtual Private Network*), vatrozid,
- **sustavi za autorizacije** – digitalni certifikati, infrastruktura javni ključeva (eng. *Public Key Infrastructure, PKI*),
- **poslovni sustavi i aplikacije** – u ovu kategoriju spadaju antivirusni programi, vatrozidi, VPN i sl.

[2] VoIP je skup internetskih tehnologija, komunikacijskih protokola i tehnologija prijenosa kako bi se ostvario prijenos govora preko IP mreže. VoIP koristi protokole za podršku sjednice popus SIP-a i SAP-a za uspostavljanje i raskid sjednica, tj. poziva.

[3] PLC je digitalno računalo koje se koristi u industriji za automatizaciju u elektromehaničkim procesima.

[4] IaaS je arhitektura u računarstvu u oblaku kod koje pružatelj usluge korisniku nudi računalo (fizičko ili virtualnu mašinu), mrežnu opremu i opremu za pohranu podataka.

[5] PaaS je arhitektura u računarstvu u oblaku kod koje pružatelj usluge korisniku nudi računalnu platformu, operacijski sustav, okruženje za izvođenje nekog programskog jezika, bazu podataka i web poslužitelj.

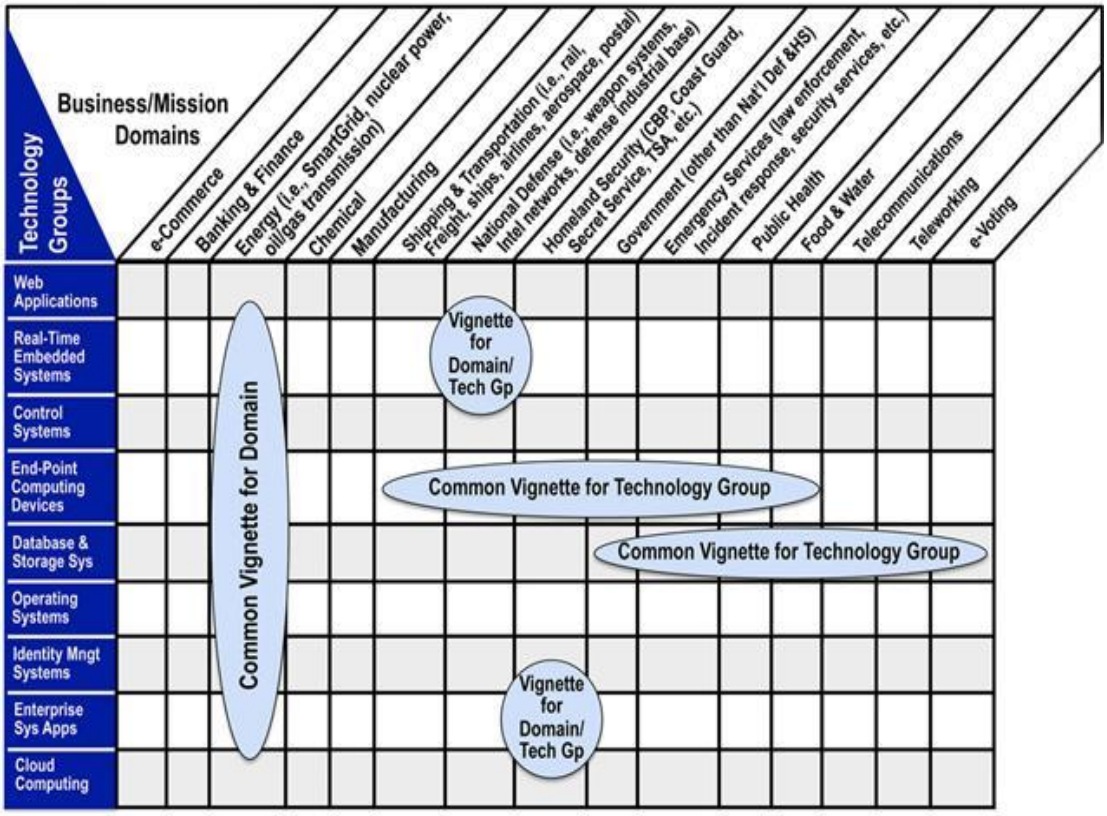
[6] SaaS je arhitektura u računarstvu u oblaku kod koje pružatelj usluge korisniku nudi da instalira programe u oblaku kojima zatim korisnik može pristupiti sa svojih računala.

5.1.3. Vinjete

Vinjete su element okruženja CWRAF koji je zapravo odgovoran za vezu sa sustavom CWSS. One predstavljaju formalni opis tehnoloških skupina, arhetipova i poslovnih domena koje je korisnik odabrao.

Vinjete su još u razvoju i trenutno ne postoje vinjete za sve kombinacije tehnoloških skupina i poslovnih domena. Slika 2 prikazuje koje su kombinacije tehnoloških skupina i poslovnih domena trenutno pokrivene. Najnoviju inačicu s trenutnim popisom vinjeta moguće je vidjeti na web stranici

http://cwe.mitre.org/cwraf/vignettes.html#matrix.



Slika 2. *- Matrica s postojećim vinjetama za određene kombinacije poslovnih domena i tehnološih skupina*
Izvor: *mitre.org*

Tablica 1**Error! Reference source not found.** prikazuje primjer dijela definicije vinjete za kućni "Smart meter". Radi se o uređaju koji se koristi u pametnim mrežama, a koji služi za praćenje potrošnje električne energije korisnika i komunikaciju s proizvođačem i distributerom električne energije. Prvi dio vinjete sastoji se od sedam polja. Prvo je samo ime vinjete, a zatim oznaka vinjete. Treće polje označava u kojoj je fazi razvoja ta vinjeta. U slučaju "Smart meter-a", vinjeta je još uvijek u fazi razvoja. Iduće polje označava poslovnu domenu, koja je u ovom slučaju energetika. U polju s opisom ukratko je opisan sustav (u ovom slučaju "Smart meter") kako bi svaki korisnik mogao pronaći onu vinjetu koja mu najbolje odgovara. U šestom su polju pobrojani arhetipovi u koje spada "Smart meter" – zbog njegove kominikacije s električnom mrežom dodjeljen mu je arhetip "web klijent", a budući da se radi o uređaju u kojem se tipično nalazi ugradbeno računalo dodjeljen mu je i arhetip "ugradbeni sustav". Arhetip "sustav za kontrolu procesa" dodjeljen mu je zbog same svrhe "Smart metera".

BVC (eng. *Business Value Context*) je dio vinjete koji opisuje arhetipove važne za sigurnost sustava.

Ime	Kućni *Smart meter*
ID	smart-meter
Zrelost	u razvoju
Domena	energetika
Opis	Mjerač u pametnoj mreži koji prati potrošnju električne energije i komunicira s mrežom.
Arhetipovi	Web klijent, sustavi za kontrolu procesa, ugradbeni sustavi
Kontekst poslovne vrijednosti (BVC)	Važna je povjerljivost korisnikove statistike potrošnje energije – mogla bi se iskoristiti za marketing ili u ilegalne svrhe. Primjerice, statistike potrošnje po satima mogu biti korisne za praćenje korisnika. Za pružatelja usluge je važna sigurnost izmjerenih podataka kako potrošač ne bi manipulirao cijenama električne energije.

Tablica 1. *- Primjer definicije vinjete za kućni Smart meter*
Izvor: *mitre.org*

Drugi dio vinjete čini tzv. rezultat tehnološkog utjecaja, TIS (eng. *Technical Impact Scorecard*). U njemu su opisane i vrednovane posljedice u slučaju iskorištenja pojedinih propusta i ovaj dio izravo utječe na izračun CWSS rezultata. Iskorištavanje propusta može imati jednu od sljedećih posljedica:

- promjena podataka - napadač može promijeniti podatke u memoriji i na taj način ozbiljno ugroziti rad napadnutog sustava te izazvati veliku štetu,
- čitanje podataka – napadač može pročitati podatke iz memorije, ali ih ne može promijeniti,
- Denial of Service: nepouzdano izvođenje – napadač može izazvati probleme (ili čak prekid) u radu napadnutog sustava,
- Denial of Service: trošenje resursa – napad utječe na učinkovitost u radu napadnutog sustava,
- izvođenje nedozvoljenog koda ili naredbi – napadač dobiva mogućnost izvođenja vlastitih naredbi u napadnutom sustavu,
- dobivanje privilegija ili preuzimanje identiteta – napadač dobiva pristup sustavu kao neki od korisnika (ili čak administrator) stvaranjem novog korisničkog računa ili korištenjem nekog od postojećih korisničkih računa,
- zaobilaženje mehanizama zaštite – napadač može neometano pristupati sustavu bez da ga detektira neki od mehanizama zaštite (npr. vatrozid),
- sakrivanje aktivnosti – napadač iskorištava propust u programu na način da se njegovo djelovanje ne dokumentira i samim time gotovo ne može otkriti.

Svaka od tih posljedica događa se na jednom od četiri sloja:

- sustav – čitav sustav u kojem je pokrenuta napadnuta aplikacija je ugrožen napadom,
- aplikacija – propust utječe na sam rad aplikacije,
- mreža – propust ili omogućuje napadaču da napad vrši preko mreže, ili da dobije pristup mreži napadnute organizacije,
- infrastruktura – propust utječe na kritičnu točku poslovne infrastrukture organizacije (npr. ruter, DNS i sl.).

Za svaku posljedicu postoji i ocjena važnosti (eng. *Subscore*) te objašnjenje. Ocjena važnosti se dodjeljuje između 0 (najmanje važna posljedica) i 10 (najviše važna posljedica).

Tablica 2 prikazuje dio rezultata TIS za vinjetu kućnog "Smart metera". Budući da je vinjeta još uvijek u razvoju, izdvojene su samo one komponente kojima je dodjeljena ocjena važnosti. Vidljivo je da je najkritičnija posljedica izvođenje nedozvoljenog koda ili naredbi s ocjenom 10. Zbog toga će u sustavu CWSS oni propusti koji potencijalno omogućuju napadaču da na uređaju izvede nedozvoljene naredbe imati veće težine od, primjerice, propusta koji potencijalno omogućuju samo nedozvoljeno čitanje podataka na uređaju.

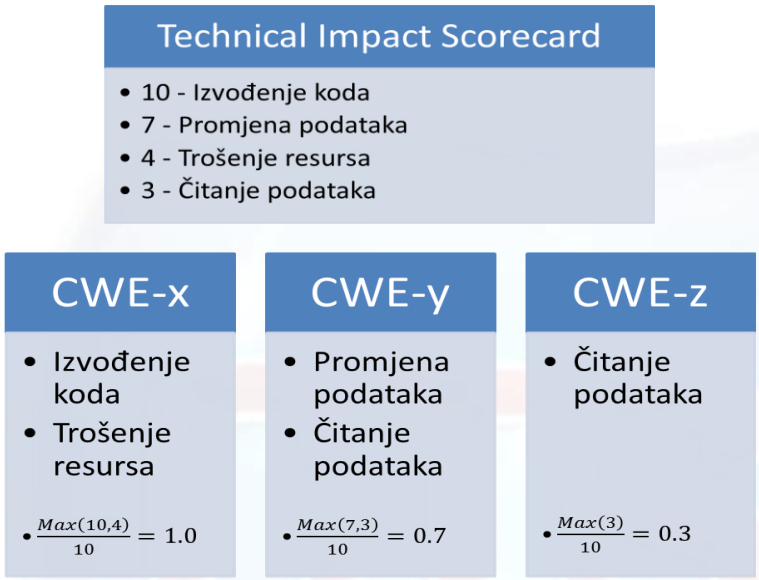
	Sloj	Važnost	Objašnjenje
Promjena podataka	Aplikacija	8	Napadač bi mogao promijeniti podatke o potrošnji i na taj način uzrokovati financijske gubitke (za potrošača ili proizvođača). Mogućnost smanjenja učinkovitosti u radu mreže zbog pogrešnih podataka. Napadač može paliti i gasiti sustave u kući.
Čitanje podataka	Aplikacija	4	Napadač može pročitati statistike potrošačeve potrošnje i iskoristiti tu informaciju u svrhu marketinga ili nadzora potrošača.
Denial of Service: nepouzdano izvođenje	Aplikacija	4	Kašnjenja u komunikaciji. Mogući financijski gubitci.
Denial of Service: trošenje resursa	Aplikacija	4	Kašnjenja u komunikaciji. Mogući financijski gubitci.
Izvođenje nedozvoljenog koda ili naredbi	Aplikacija	10	Napadač može dobiti pristup statistikama korisnika, isključiti "Smart meter", promijeniti informacije o potrošnji i tako uzrokovati financijske gubitke. Mogućnost smanjenja učinkovitosti u radu mreže zbog pogrešnih podataka.
Dobivanje privilegija, preuzimanje identiteta	Aplikacija	7	
Zaobilaženje mehanizma zaštite	Aplikacija	7	
Sakrivanje aktivnosti	Sustav	5	Nemoguće sakupiti dovoljno dokaza za optužbu za prijevaru.
Skrivanje aktivnosti	Aplikacija	5	Nemoguće sakupiti dovoljno dokaza za optužbu za prijevaru.

Tablica 2. *- Technical Impact Scorecard za kućni Smart meter*
Izvor: *mitre.org*

6. Korištenje okruženja CWRAF i vinjeta u sustavu CWSS

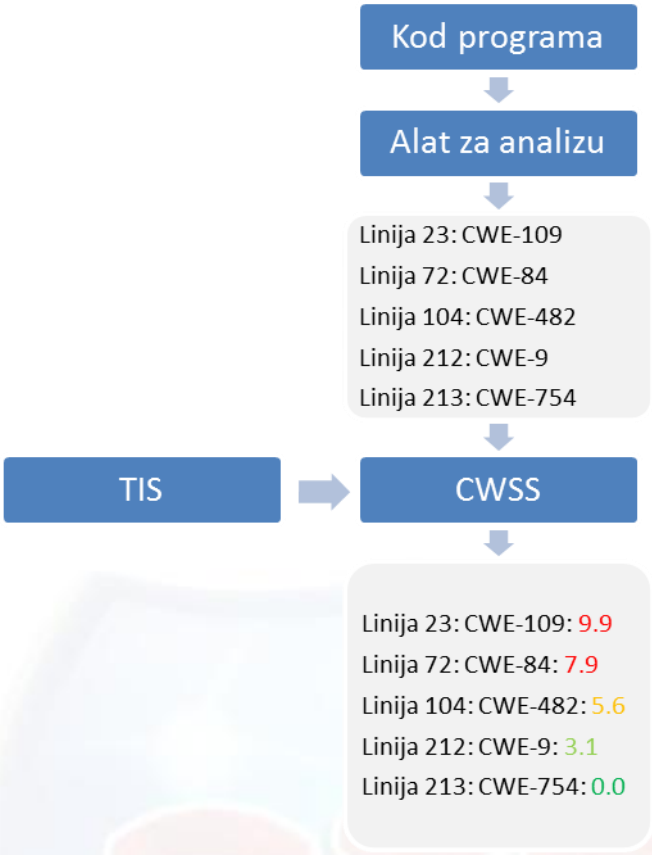
U poglavlju o vinjetama spomenuto je da ocjene u TIS-u izravno utječu na CWSS rezultat s nekim težinskim faktorima. Postupak kojim se određenom propustu (tj. njegovoj CWE oznaci) dodjeljuje određena težina je opisan u nastavku.

U prvom se koraku za svaki pronađeni CWE određuju posljedice koje taj propust može izazvati. Svaki CWE može imati jednu ili više posljedica navedenih u TIS-u. Težinski faktor kojim će se taj CWE vrednovati izračunava se kao najveća ocjena koju ima neka posljedica u TIS-u podjeljena s najvišom ocjenom (10). Jednostavni primjer ovog postupka prikazuje Slika 3. Za tri CWE-a, s oznakama x, y i z, određuju se težinski faktori. CWE-x kao moguću posljedicu ima nedozvoljeno izvođenje koda, koje u TIS-u ima ocjenu 10 te trošenje resursa sustava, koje ima ocjenu 4. Težinski faktor za CWE-x stoga iznosi 1.0. Na isti se način računaju težinski faktori i za CWE-y i CWE-z.



Slika 3. *- Računanje težinskih faktora za tri različita CWE*
Izvor: *CIS*

Slika 4 prikazuje blok dijagram korištenja sustava CWSS i okruženja CWRAF u analizi propusta. Nakon što alat za automatsku analizu propusta prepozna propuste u kodu, linije na kojima se pojavljuju te njihovu CWE oznaku, težinski faktori u vinjetama (odnosno u TIS-u) se kombiniraju sa sustavom CWSS za rangiranje propusta. Formule po kojima se računa CWSS rezultat mogu se pronaći na web stranicama organizacije MITRE. Rezultat je lista propusta rangirana ocjenama 0.0-10.0.



Slika 4. *- Korištenje CWRAF-a i vinjeta za izračun CWSS-a*
Izvor: *mitre.org*

7. Budućnost projekta CWE i okruženja CWRAF

Budući da se projekt CWE u smislu kategorizacije propusta u programima nastavio na projekt CVE započet krajem devedesetih godina prošlog stoljeća, već je razvijena prilično velika baza i opisi čestih propusta. Međutim, rangiranje propusta, CWSS i CWRAF su krenuli s razvojem tek u protekle dvije godine i još uvijek je potrebno puno posla da bi se omogućila njihova primjena na način na koji su zamišljeni.

Prva stvar koju je potrebno napraviti za daljnji razvoj projekta je definiranje većeg broja vinjeta. Trenutno postoje vinjete za samo neke kombinacije poslovnih domena i tehnoloških skupina. Budući da je cilj projekta omogućiti korištenje sustava CWSS u što većem broju različitih situacija, očito je da je nužno definirati i što više vinjeta koje će omogućiti korisnicima to precizniju definiciju okruženja u kojima oni koriste neki program. Organizacija MITRE trenutno traži zainteresirane organizacije koje bi se uključile u postupak definiranja vinjeta i izrade TIS-a.

Što se tiče samog sustava CWSS i načina ocjenjivanja, organizacija MITRE stalno radi na manjim promjenama u metodama ocjenjivanja i formulama koje se koriste kod izračuna CWSS rezultata kako bi dale što točnije rezultate. U kontaktu s velikim organizacijama koje se bave razvojem programa te drugim organizacijama radi se na poboljšanju ovog sustava.

8. Zaključak

Ideja automatske analize propusta u potrazi za propustima te automatskog ocjenjivanja prioriteta pronađenih propusta mogli bi dovesti do značajnog olakšanja posla programerima. Umjesto da troše vrijeme na neki manje značajan propust koji ne predstavlja prijetnju u okruženju u kojem korisnik namjerava koristiti program, programer bi dobio listu po kojoj bi obavljao popravke i tako prvo riješio one propuste koji predstavljaju veći sigurnosni rizik. Samim time vjerojatno bi došlo do povećanja sigurnosti. S druge strane, korisnici bi dobili mogućnost da na jednostavan način provedu analizu i odluče koji program najbolje zadovoljava njihove potrebe.

Moguća negativna strana postojanja ovako moćnog alata je zanemarivanje onih manje značajnih propusta. To bi bilo posebno opasno u slučaju da je, kod ocjenjivanja, takav propust zapravo pogrešno protumačen kao bezopasan.

Projekt CWE, kao i njegove komponente CWSS i CWRAF, predstavljaju odličnu ideju, ali su još uvijek dosta daleko od konačnog cilja. Ako se nastavi s ozbiljnim razvojem, te ako se uključe i zainteresirane organizacije koje bi pripomogle u definiranju vinjeta i integraciji CWSS i CWRAF sustava u postojeće alate za automatsku analizu koda, sigurno je da ovaj projekt ima dobru budućnost.

9. Leksikon pojmova

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

DNS – Domain Name System

Domain Name System (DNS) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.

http://www.kb.iu.edu/data/adns.html

CVE – Common Vulnerabilities and Exposures

CVE je rječnik javno poznatih sigurnosnih ranjivosti. Sadrži dodatne usluge koji imaju cilj korisnike informirati o sigurnosnim rizicima i prijetnjama.

http://searchfinancialsecurity.techtarget.com/definition/Common-Vulnerabilities-and-Exposures

10. Reference

[1] Steve Christey: Common Weakness Risk Analysis Framework, http://cwe.mitre.org/cwraf/index.html, veljača 2012.

[2] Steve Christey: Common Weakness Scoring System, http://cwe.mitre.org/cwss/index.html, veljača 2012.

[3] Common Weakness Enumeration, http://cwe.mitre.org/, veljača 2012.

[4] Common Weakness Enumeration Documents, http://cwe.mitre.org/about/documents.html, veljača 2012.

[5] CWE – Common Weakness Enumeration, http://nvd.nist.gov/cwe.cfm, veljača 2012.

[6] Common Weakness Enumeration Documents, http://cwe.mitre.org/about/documents.html, veljača 2012.