Posvet
AVTOMATIZACIJA STREGE IN MONTAŽE 2019 – ASM '19

Ljubljana, 04. december 2019

Izzivi kibernetska obrambe proti hekerskim napadom

Robert Bergles,
Pro Astec d.o.o.

Povzetek

Že na začetku zapišimo, da absolutno varnega sistema ni, zato lahko govorimo samo o bolj ali manj zavarovanih sistemih. Zaščita in varovanje zajema široko področje, od varne prijave uporabnikov v omrežje, zaščiten prenosa informacij, kriptiranje podatkov, varno komunikacijo med oblakom in nadzornimi sistemi..

V večini primerov se klasični načini varovanja kot so požarni zidovi, kriptografija, osnovna autentikacija in avtorizacija ne zadostujejo več. Varnostne prijeme in sisteme moramo razširiti na način tako da samodejno zaznajo anomalije, škodljivo programsko opremo in se sproti prilagajajo in učijo iz baze znanj "BIG data". Komunikacijski protokol TCP/IP sestavljajo štirje sloji, katere je pri zaščiti potrebno obravnavati ločeno. Vsak sloj zahteva svoje metode in tehnike varovanja. Zaščita in varovanje informacij zajema sledeče dejavnike:

- *Kriptiranje*
- *Avtentikacija*
- *Avtorizacija*
- *Zagotavljanje redundantne povezljivosti*

Vrste napadov in grožnje

Najpogostejše napade na stabilnost in integriteto sistemov bomo razdelili v skupine glede na to, kako heker vstopi v računalnik oz. omrežje, ter glede na to, kaj počne (ko si je zagotovil vstop). Preden se posvetimo posameznim vrstam napadov, si oglejmo tri kriterije, ki morajo biti izpolnjeni, da nastane vdor:

- **Motiv**: heker mora imeti motiv za to, da se loti določenega sistema. Ne pozabimo: tudi "za zabavo" je motiv.
- **Sredstvo**: heker mora imeti orodje, s katerim si zagotovi nepooblaščen dostop.
- **Priložnost**: nepooblaščen dostop je tesno povezan z varnostnimi pomanjkljivostmi v sistemu. Le-te so lahko posledica slabega varnostnega načrta in politike, lahko pa nastanejo kot posledica čisto specifične pomanjkljivosti servisa.

Prevare IP

Prevare (IP Spoofing) delujejo na protokolni sklad IP tako, da v čelu paketa spremenijo izvorni IP naslov naprave. Običajno je novi IP naslov takšen, da ga usmerjevalnik uvrsti med naslove lokalnega omrežja. Prevare se uporabljajo tudi v kombinaciji z drugimi napadi (predvsem DoS), ko je potrebno skriti izvorni naslov napadalnih naprav.

Napadi SYN in LAND

Napadi Synchronization request (SYN) vplivajo na tri nivojsko rokovanje pri vzpostavitvi povezave v TCP sloju. Tisti, ki podrobneje poznate dogajanje v transportnem sloju, veste, da se pri uporabi TCP (za razliko od UDP) pred

prenosom podatkov med napravama vzpostavi seja.

Prisluškovanje

Odvisno od transportnega medija brezžično, žično, optika je prisluškovanje, zajem in prestrezanje podatkov možno na vseh komunikacijskih poteh in vozliščih.

Prevzem povezave (hijacking)

Iz komunikacijskega protokola napadalec odstrani pravega pošiljatelja ali prejemnika iz komunikacije ter ga zamenja s svojo identiteto.

Denial of service (DOS)

Pogosto delujejo tako, da računalniško omrežje zasujejo z več podatki, kot ga omrežje lahko procesira. Na tak način onemogočijo dostop do omrežnih servisov. Napad DoS je lahko osredotočen samo na specifično (znano) pomanjkljivost, ki povzroči zaustavitev servisa in posledično izpad storitve. Med posebne vrste DOS napadov sodita tudi

- **DDoS** je izpeljanka osnovnega napada, kjer za napad uporabimo več računalnikov (agentov) na katere smo predhodno namestili programe za sočasno napadanje (zombije).
- **DNS DoS** je izpeljanka osnovnega napada, ki uporablja DNS strežnike za "ojačevalce" DNS prometa. Napadalec pošlje kratko DNS povpraševanje veliko DNS strežnikom, s tem da se jim predstavi z IP naslovom naprave, ki naj bo napadena.Zagotavljanje varne komunikacije

Pri varni komunikaciji moramo upoštevati več varnih mehanizmov s katerimi zagotovimo uspešno in zanesljivo komunikacijo znotraj omrežja. Upoštevati moramo sledeče elemente varne komunikacije:

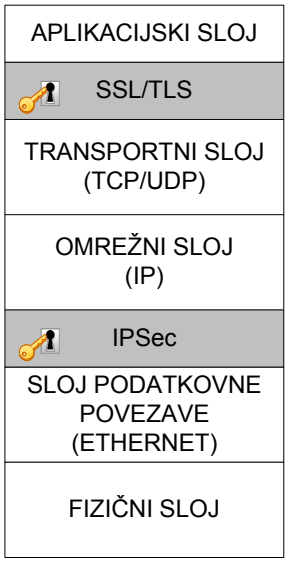
- **Zaupnost** (Kriptiranje vseh komunikacijskih poti in informacij)
- **Avtentikacija** (Zagotavljanje identitete, po možnosti dvo faktorska)
- **Avtorizacija** (Dovoljenja za dostop do virov in informacij)
- **Integriteta** (nadzor sprememb poslane informacije)
- **Preprečevanje zanikanja** (enolično določanje pošiljatelja)
- **Revizijske sledi** (redno beleženje dogodkov)
- **Nadzor prometa v vozliščih**
- **Zagotavljanje visoke razpoložljivosti komunikacijskih poti**

Izbor ustreznih metod in algoritmov je odvisna od vrste storitve, ki bodo implementirane na komunikacijskih poteh. Vsekakor je izbor algoritmov odvisen od kritičnosti informacij ter posledično od finančnih sredstev, ki smo jih pripravljeni vložiti v varovanje prenosnih poti.

Načrtovanje zaščite po slojih

Za varen prenos podatkov med napravami moramo v referenčnem modelu predvideti zaščite. Naslednja slika prikazuje popravljen referenčni

model, v katerega smo dodali možnosti zaščite po slojih.



Na zgornji sliki vidimo, da lahko zaščito podatkov preko varnostno vprašljivih omrežij izvedemo v **aplikacijskem** sloju ali pa v **omrežnem** sloju. Lahko pa uporabimo oboje. Naštejmo nekaj dejavnikov, ki jih velja upoštevati pri izbiri zaščite:

- hitrost delovanja oz. odzivnost: z uporabo kriptografskih tehnologij se (pri isti strojni opremi) zmanjša hitrost delovanja aplikacij,
- administracija: z uvedbo dodatne zaščite je potrebno upoštevati stroške, ki nastanejo zaradi dodatnih nastavitev aplikacijske in/ali sistemske programske opreme,
- načrtovanje, testiranje, implementacija: za realizacijo dodatne zaščite pri prenosu podatkov je potrebno predvideti vse tri razvojne faze.

Zaščita v aplikacijskem sloju

Na razpolago imam kopico protokolov, ki zagotavljajo varen prenos podatkov v aplikacijskem sloju. Izbor protokola je odvisen od želenih rezultatov. Naslednji protokoli omogočajo zaščito v aplikacijskem sloju:

- Secure Socket Layer,
- Secure Multipurpose Internet Mail Extensions,
- Pretty Good Privacy,
- Server Message Block Signing,
- Transport Layer Security.

Secure Socket Layer (SSL)

Uporaba SSL (in PKI) zagotavlja zasebnost, avtentifikacijo in integriteto sporočil.

Secure Multipurpose Internet Mail Extensions (S/MIME)

Protokol omogoča kriptiranje in digitalni podpis sporočil med poštnima strežnikoma, ne glede na uporabljeno platformo. Zasnovan je tako, da se proces šifriranja izvaja na odjemalni napravi in zato ne zahteva S/MIME podpore na poštnem strežniku.

Server Message Block Signing

Server Message Protokol opravlja prenos datotek med odjemalci in SMB strežnikom. Privzeto deluje SMB tako, da odjemalna naprava pošlje strežniku uporabniško ime, geslo in ime skupne

rabe. SMB Signing (imenovan tudi Common Internet File System: CIFS) omogoča dvosmerno avtentifikacijo odjemalne naprave in strežnika. Sistem deluje tako, da odjemalna naprava in strežnik vsak blok označita z digitalnim podpisom. Z uporabo SMB Signinga pridobimo predvsem dvoje:

- dvosmerna avtentifikacija (mutual autentication), ki preprečuje t.i napad *man-in-the-middle*, kjer tretje oseba na prenosni poti prestreza in spreminja podatke. SMB Signing zagotavlja, da strežnik in odjemalna naprava nedvoumno ugotovita pristnost,
- avtentifikacija sporočilnih blokov (message authentication): vsak sporočilni blok se pred pošiljanjem opremi z digitalnim podpisom.

Transport Layer Security (TLS)

Je zelo podoben SSL in z uporabo PKI omogoča zasebnost, avtentifikacijo in integriteto sporočil. Najpomembnejša razlika je, da TLS podpira različne kriptirne algoritme in je (za razliko od SSL) javno veljavni IETF standard.

Zaključek

V praksi praviloma ni zaščite pred prisluškovanjem, lažnim predstavljanjem, motenjem in drugim. Varnost temelji predvsem na zaščiti infrastrukture omrežja, prenosnih poti in terminalov. Vsebino podatkov varujemo z uporabo zanesljivih in varnih kriptografskih algoritmov v kombinaciji s primernimi elektronskimi ključi.

Osnova za varno komunikacijo je kriptiranje (zakrivanje) vsebine is sporočil. Na ta način se obranimo med pasivnimi prisluškovalci in aktivnimi vdiralci. Priporočljiva je uporaba javne asimetrične enkripcije s katero zagotovimo tri osnovne prvine varne komunikacije (zaupnost, integriteto in preprečevanje zanikanja).

Avtentikacijski in avtorizacijski algoritmi morajo imeti možnost sekundarnega preverjanja identitete v primeru suma zlorabe identitete. Komunikacijski kanal in algoritem mora zagotavljati preprečevanje zanikanja pošiljatelja sporočila na način, da se da ga ne more ponarediti.

Glede na komunikacijske poti je potrebno zagotoviti nadzor prometa in ugotavljanje ustreznost paketov na omrežju, da lahko preprečimo zlorabe. V primeru ugotovljene zlorabe moramo imeti pripravljene metode in postopke (varnostno politiko) kako reagirati v takšnih primerih.