PREPORUKE ZA POVEĆANJE SIGURNOSTI INFORMACIJA U MENADŽMENTU RAČUNARSKIH MREŽA

RECOMMENDATION FOR IMPROVEMENT OF NETWORK MANAGEMENT SECURITY

Esad Saitović[1], Ivan Ivanović[1]

[1]Računarski Centar Univerziteta u Beogradu

Sadržaj – U ovom radu su opisani osnovni koraci koji su potrebni za implementaciju i unapređenje sistema za nadgledanje svih hardverskih resursa u računarskim mrežama. Opisane su prednosti korišćenja SNMP verzije 3 protokola, razmotreni potencijalni problemi koji se mogu javiti prilikom implementacije samog protokola, kao i preporuke za impelementaciju u sistemima za menadžment u kampus mrežama.

Ovaj rad je nastao kao deo internacionalnog GEANT3 projekta, *Network Activity 3 - Task 4 (NA3-T4),* u kome AMRES učestvuje. Cilj NA3-T4 aktivnosti je kreiranje BPD dokumenata koji bi pomogli administratorima prilikom projektovanja mreže i implementacije servisa u kampus okruženju.

Abstract – *This document presents basic steps that are required for implementation and improvement of network management systems. Document also provides information about benefits of using SNMP V3 protocol, and problems that could occur during the implementation and usage of SNMP v3 protocol in the campus networks NMS systems.*

This work represents part of a international GEANT3 project, Network Activity 3 - Task 4 (NA3-T4) in which AMRES participate. The purpose of NA3-T4 activity is to create BPD documents in order to ease building of network topology and services to administrators of network campuses.

1. UVOD

Razvoj mrežnih uređaja i novih kompleksnih protokola doveo je do toga da se današnji mrežni sistemi ne mogu održavati bez dobrog sistema za nadzor, kontrolu i konfigurisanje mreže. Takođe, rapidno širenje korišćenja mrežnih resursa, kao i povezanosti sa Internetom, sa sobom nose i potrebu za zaštitom komunikacije kao i informacija koje se prenose putem sistema za menadžent mreže. Za pouzdan i siguran sistem za menadžment mreže je pored arhitekture same mreže, potrebno koristiti i skup protokola kojima se povećava sigurnost prenosa kritičnih informacija koje su sastavni deo menadžment poruka.

2. UVOĐENJE SIGURNOSTI PRILIKOM PRENOSA OSETLJIVH INFORMACIJA

Jedan od osnovnih zahteva koji se javlja prilikom implementacije softvera za nadzor i kontrolu mreže jeste obezbeđivanje sigurnosti prilikom prenosa podataka. Postoje dva različita pristupa koja doprinose sigurnom prenosu menadžment saobraćaja.

Prvi pristup je razdvajanje menadžment saobraćaja od produkcionog saobrćaja, što se postiže implementacijom *Out-Of-Band-Managament* (OOBM) dela mreže. OOBM zahteva dodatnu fizičku infrastrukturu (zasebne mrežne uređaje, mrežne interfejse na svim uređajima nad kojima se vrši funkcija menadžmenta) koja će se koristiti isključivo za menadžment saobraćaj. OOBM deo mreže nema vezu sa ostalim delovima mreže, kao ni sa Internetom, čime se postiže visok stepen sigurnosti informacija koje se prenose kroz ovaj deo mreže. Sa druge strane, troškovi implementacije ovakvog rešenja koji uključuju dodatnu fizičku infrastrukturu, kao i vreme koje administratori treba da utroše na implemenatciju, predstavljaju ograničavajući faktor u primeni ovog pristupa.

Drugi pristup je korišćenje protokola koji imaju mogućnost autentifikacije i enkripcije menadžment saobraćaja, kao što je SNMP v3. Implementacija SNMP v3 protokola na mrežnim uređajima zavsi od verzije operativnog sistema koji postoji na uređajima i eventualno može zahtevati nadogradnju podrške za ovaj protokol. U praksi se pokazalo da je kombinacija prethodno opisana dva pristupa, model koji je u

najvećem broju slučajeva primenljiv. Ovakav kombinovani model podrazumeva implementaciju OOBM rešenja u delovima mreže u kojima uređaji imaju OOBM portove ili gde je moguće da se na uređajima izdvoji jedan mrežni interfejs samo za svrhu menadžmenta. Za uređaje ili delove mreže kod kojih nije moguće obezbediti OOBM preporučuje se korišćenje SNMP v3 protokola.

3. SNMP PROTOKOL

SNMP predstavlja najčešće korišćeni protokol za nadgledanje i kontrolu mreže. Sastoji se od skupa standarda kojima se definišu: način upravljanja mrežom, baze podataka za čuvanje informacija i strukture korišćenih podataka. Razvoj SNMP protokola se ogleda kroz tri verzije. Verzija SNMP v1 se smatra zastarelom i više se ne koristi. Verzija 2c se danas najčešće koristi i smatra se nepouzdanim sa aspekta sigurnosti. Autentifikacija se obavlja jedino na osnovu *community-based* sigurnosnog modela, dok se podaci kroz mrežu šalju u neenkriptovanom obliku. *Community-based* sigurnosni model koristi string za autentifikaciju i prilikom slanja SNMP poruka string se takođe šalje neenkriptovan. U praksi se najčešće sreće implementacija jednog istog *community* stringa u celoj mreži. To predstavlja veliki sigurnosni rizik.

U slučaju nekog malicioznog napada u kojem bi se prisluškivanjem (*sniffing*) prikupio menadžment saobraćaj, iz istog se lako može otrkiti *community* string koji se koristi za autentifikaciju i na taj način se može doći do osetljivih informacija o mreži i uređajima. Takođe se može izazvati neka vrsta DoS napada na NMS server koji prikuplja SNMP podatke.

Razvojem verzije 3 SNMP protokola unose se tri važna servisa u menadžment sisteme.

Ti servisi su:

- Autentifikacija
- Privatnost
- Kontrola pristupa

Bezbednosni aspekti koji se uvode na ovaj način su:

- Integritet poruke (*Message integrity*) - sprečava mogućnost izmene paketa prilikom prenosa
- Autentifikacija - potvrda da je poruka stigla sa pravog izvorišta
- Kriptovanje paketa - sprečavanje čitanja poruka od strane neautorizovanog izvora

Pored bezbednosnih aspekta koje nudi SNMP v3 ostavljena je mogućnost izabora tipa sigurnosti na osnovu tri sigurnosna modela koja su uvedena u verziji 3. Za razliku od verzije 2c koja koristi *community-based* sigurnosni model, verzija 3 koristi *user-based* sigurnosni model.

Sigurnosni modeli SNMP v3 protokola:

- NoAuthNoPriv – Koristi se korisničko ime za autentifikaciju, slično kao *community* string kod verzije 2c. U ovom modelu se saobraćaj šalje u neenkriptovanom obliku.
- AuthNoPriv – Za autentifikaciju se koriste korisničko ime i lozinka a prilikom autentifikacije se šalje MD5 ili SHA1 heš. Ostali saobraćaj se u ovom modelu šalje u neenkriptovanom obliku.
- AuthPriv – Za autentifikaciju se koriste korisničko ime i lozinka i prilikom autentifikacije se šalje MD5 ili SHA1 heš, dok se ostali saobraćaj enkriptuje pomoću DES56 ili AES128 algoritma.

SNMP v3 koristi *user-based* sigurnosni model odnosno autentifikacija se bazira na korisničkim nalozima. Takođe je moguće uvesti ograničenja prilikom očitavanja MIB (*Management Information Base*) baze za svakog korisnika pojedinačno. Na taj način se vrši kontrola pristupa pojedinim varijablama u MIB bazi.

Za svakog korisnika je moguće definisati sigurnosni model, izvršiti ograničenja u MIB bazi i omogućiti mu *read-only* ili *read-write* privilegije.

Korisnicima je ostavljena mogućnost da uvedu željeni nivo sigurnosti izborom jednog od tri sigurnosna modela.

4. PROBLEMI

Uobičajeno je da Administratori implementiraju SNMP v2c zato što je dosta jednostavnija za konfigurisanje i upotrebu. Može se reći i da su delom i sami proizvođači mrežnih uređaja odgovorni za ovakav pristup, obzirom da se prilikom inicijalnog pokretanja SNMP protokola na uređaju aktivira verzija 2c u *read-only* modu sa predefinisanim *community* stringom koji obično ima vrednost "*public*". Takođe, dozvoljava se očitavanje cele MIB baze što predstavlja sigurnosni rizik, obzirom da se poznavanjem samo *community* stringa može sakupiti dosta informacija o stanju sistema.

Problem se takođe može javiti i na samim uređajima. Naime, u slučaju da želimo da koristimo SNMP v3 sa AuthPriv sigurnosnim modelom, potrebno je da na uređajima postoji podrška za enkripciju. Ukoliko uređaji ne podržavaju enkripciju, ili su već opterećeni drugim procesima ili servisima koji koriste enkripciju, pokretanje ovakvog sigurnosnog modela može doprineti dodatnom opterećenju uređaja (ruteri i svičevi su podložni ovom problemu) što može uticati i na performanse istog u produkcionom radu. Ukoliko je to slučaj, preporuka je pokretanje nižeg sigurnosnog modela AuthNoPriv koji ne koristi enkripciju, ali koristi autentifikaciju.

Obzirom na performanse današnjih računara, kod servera se ne očekije problem sa resursima usled korišćenja AuthPriv sigurnosnog modela SNMP v3 protokola.

Problem koji se kod servera javlja je izbor operativnog sistema. Pojedini operativni sistemi u svojoj standardnoj instalaciji ne podržavaju SNMP v3 i u tom slučaju je potrebno pronaći softver nekog drugog proizvođača, koji podržava v3, i instalirati ga na operativni sistem servera.

SNMP *trap* mod rada se često implementira u monitoring mreže. Ispravno podešen *trap* mod omogućuje pravovremeno otkrivanje problema u mreži a samim tim se smanjuje vreme potrebno za otklanjanje problema. Prilikom pojave problema na uređaju SNMP agent generiše trap poruku i šalje je NMS serveru čija je odgovornost da ispravno primi poruku i obavesti administratora o problemu. Prilikom podešavanja SNMP *trap* moda rada u v3 potrebno je, u zavisnost od sigurnosnog modela, na strani koja prima *trap* poruke konfigurisat informacije o korisniku (uređaju) koji je generisao *trap*. Sam sistem slanja *trap* poruka ne zahteva odgovor o tome da li je poslati *trap* ispravno primljen ili ne. Stoga udaljeni uređaj ne zna da li je NMS server primio poruku. Da bi NMS dekriptovao trap poruku mora imati informacije o sigurnosnom modelu i podatke o korisniku koji šalje *trap*.

U slučaju slanja *trap* poruke putem AuthPriv sigurnosnog modela na strani koja prima *trap* poruku potrebno je imati podešenog korisnika sa lozinkom koji je genersiao taj *trap* kao i ostale parametre koji se koriste za autentifikaciju i enkripciju. Ovo predstavlja jedini način na koji se može ispravno dekriptovati *trap* poruka i obavestiti korisnik o problemu koji se javio.

Sama kompleksnost implementacije se dodatno usložnjava ako je potrebno konfigurisati SNMP v3 *trap* mod rada na većem broju uređaja. Jedno od rešenja jeste kreiranje jednog *trap* korisnika koji će se konfigurisati na svim uređajima. Taj korisnik će na svim uređajima imati isto korisničko ime i lozinku, isti sigurnosni model i isti tip autentifikacije i enkripcije. Na strani NMS servera potrebno je konfigurisati samo tog jednog *trap* korisnika sa istim parametrima kao na ostalim mrežnim uređajima.

Iz prethodnog se vidi da je kompleksnost prilikom implementacije SNMP v3 daleko veća u odnosu verziju 2c kod koje je samo potrebno konfigurisati *comunity* string i pokrenuti SNMP servis. Upravo ovo predstavlja još jedan od razloga zašto se danas i dalje više koristi verzija 2c.

5. ZAKLJUČAK

Sve veći razvoj mrežnih servisa i potreba za korišćenjem centralizovanog sistema za nadgledanje mreže sa sobom nose i potrebu da se informacije koje se prenose putem menadžmenta zaštite od neovlašćenog pristupa i zloupotrebe. Upravo je sigurnost ključni aspekt o kome treba voditi računa pri implementaciji menadžment sistema. Iako je trenutno najviše korišćena verzija 2c SNMP protokola, preporučuje se praćenje razvoja sigurnosti u menadžment protokolima i implementacija svih raspoloživih rešenja, kao što je to slučaj sa verzijom 3 SNMP protokola.

6. LITERATURA

[1] Esad Saitović i Ivan Ivanović - Recommended network management architecture, Beograd 2009.

[2] Douglas Mauro, Kevin Schmidt - Essential SNMP, O'Reilly Media, July 2001

[3] www.net-snmp.org