MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA

ISSN 2029-2341 print / ISSN 2029-2252 online
2011 3(1): 20–24 doi: 10.3846/mla.2011.004

Sistemų inžinerija, kompiuterių technologija T 120
Systems Engineering, Computer Technology T 120

Elektronika ir elektrotechnika
Electronics and Electrical Engineering

STOCHASTINIS TCP SYN ATAKŲ MODELIS

Simona Ramanauskaitė[1], **Antanas Čenys**[2]

[1]*Šiaulių universitetas*
[2]*Vilniaus Gedimino technikos universitetas*
El. paštas: [1]*simram@it.su.lt;* [2]*antanas.cenys@vgtu.*lt

Santrauka. Vis didesnė dalis svarbių paslaugų persikelia į internetinę erdvę, todėl didėja ir DoS atakų potenciali grėsmė. Šio tipo atakų grėsmės vertinimui realiai sudėtinga išbandyti galimai įvyksiančias atakas, bet paprasčiau tai įvertinti gali padėti DoS atakų matematiniai / programiniai modeliai. Šiame darbe apžvelgiami egzistuojantys TCP SYN tipo atakų modeliai bei siūlomas stochastinis modelis TCP SYN atakoms modeliuoti. Jis leidžia atsižvelgi į teisėtą sistemos srautą, galimą atakos galingumą, aukos naudojamų apsaugų savybes ir gali būti naudojamas ne tik TCP SYN, bet ir kitoms atminties išnaudojimo DoS atakoms modeliuoti.

Reikšminiai žodžiai: TCP SYN, SYN užtvindymas, DoS, DDoS, modeliavimas.

Įvadas

Interneto teikiamos galimybės suteikia vis daugiau papildomų funkcijų jo vartotojams. Tačiau kartu su naujomis galimybėmis kyla ir vis daugiau rūpesčių tas paslaugas teikiančių sistemų administratoriams, besirūpinantiems ne tik pačios sistemos tinkamu funkcionavimu, bet ir jos saugumu.

Viena iš aktualiausių atakų prieš sistemas, teikiančias paslaugas internetu, yra atsisakymo aptarnauti (angl. *Denial of Service* ar tiesiog DoS) ataka. Ja siekiama tam tikrą sistemą ar jos paslaugą padaryti neprieinamą teisėtiems jos vartotojams. Jei atsisakymo aptarnauti atakoje dalyvauja keli kompiuteriai (dar vadinami agentais ar zombiais), ataka tampa paskirstyta (ang. *Distributed Denial of Service* arba sutrumpintai DDoS) ir gali būti daug kartų galingesnė nei DoS ataka.

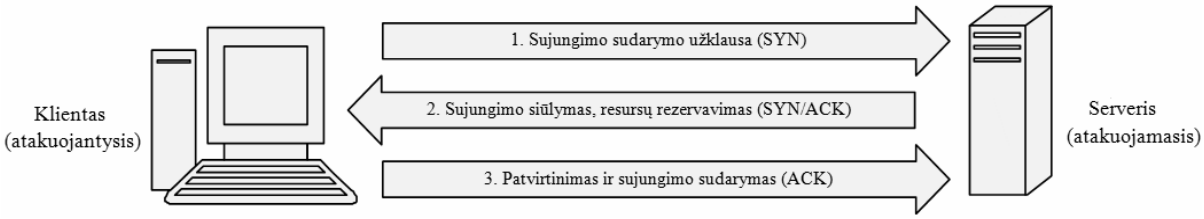
Atsisakymo aptarnauti atakų yra įvairių tipų, bet viena žinomiausių yra TCP SYN arba SYN užtvindymo ataka. TCP SYN atakai įvykti leidžia trišalis TCP sujungimo sudarymo protokolas, nes vartotojui, norint sudaryti sujungimą, yra skiriama atminties vieta reikiamos informacijos saugojimui. Sujungimui reikiama informacija laikoma atmintyje tol, kol sujungimas užbaigiamas, arba kol praeina sistemoje numatytas sujungimui sudaryti laikas (žr. 1 pav.). SYN užtvindymo atakos išnaudoja šią protokolo savybę siųsdamos didelį kiekį parodijuotų (su netikru ar neegzistuojančiu siuntėjo adresu) TCP sujungimų sudarymo užklausų. Jos užima vietą serverio buferyje, taip jį išnaudoja parodijuotų užklausų informacijai saugoti ir nepalieka laisvos vietos teisėtiems sujungimams (jei nebėra vietos buferyje, visos kitos užklausos tiesiog blokuojamos ir neaptarnaujamos).

Norint apsisaugoti nuo TCP SYN atakos ar tinkamai jai pasiruošti, galimos kelios pagrindinės kontrpriemonės, kurios reikalauja serverio (aukos), bet ne vartotojų papildomų veiksmų ar nustatymų (Burdach 2003):

- parodijuotų užklausų filtravimas;
- sujungimams skirto buferio talpos didinimas;
- neužbaigtų sujungimų laikymo sistemoje laiko mažinimas.

Derinant visas šias apsaugos priemones, galimas optimalus serverio nustatymas, kai esant tam tikrai SYN užtvindymo atakai, DoS efektas pakankamai mažas ir nejuntamas teisėtiems sistemos vartotojams. Tačiau praktiškai įvertinti kiekvienos kontrpriemonės įtaką bendram serverio nustatymų efektyvumui skirtingų TCP SYN atakų metu yra gan sudėtinga (realių atakų bandymai įtakoja kitas sistemas, todėl yra sunkiai stebimi ir gali sukelti pernelyg didelę nepageidautiną įtaką su tuo nesusijusioms sistemoms). Tai gali reikalauti itin daug įvairių bandymų ir užtrukti gan ilgai.

Šio darbo tikslas – aprašyti ir realizuoti TCP SYN DDoS atakos matematinį modelį, kuris leistų vertinti pagrindinių serveryje taikomų kontrpriemonių efektyvumą skirtingo pajėgumo SYN užtvindymo atakose.



1 pav. TCP trišalio sujungimo schema
Fig. 1. The scheme of triple TCP connection

Egzistuojančių TCP SYN atakų modelių apžvalga

Egzistuoja keletas DoS atakų modelių ir įrankių, kuriais galima nustatyti norimo galingumo atakos sėkmės tikimybę:

1. Huang *et al.* (2003a) taiko supaprastintą Engest praradimo modelį G(N)/G/m(0) SYN užtvindymo atakose.
2. Huang *et al.* (2003b) aprašo anksčiau minėtą modelį, pritaikydami jį bevieliams tinklams.
3. Chang (2002) taiko G/D/∞/N modelį nustatyti minimaliam atakos srautui, kuris įvykdytų DoS ataką.
4. Wang *et al.* (2007) taiko dvimates Markovo grandines DoS atakų modeliavimui.
5. Xiang *et al.* (2006) apibendrina atakos ir apsaugos priemonių efektyvumo nustatymą lygtimi.
6. Chen *et al.* (2002) analizuoja DoS atakas tinklo (maršrutizatorių) lygyje.
7. Blackert *et al.* (2003) analizuoja OPNET įrankio naudojimą DoS atakoms modeliuoti.
8. Kotenko *et al.* (2006) išplečia OMNeT+ įrankį, jam suteikiant papildomų galimybių.

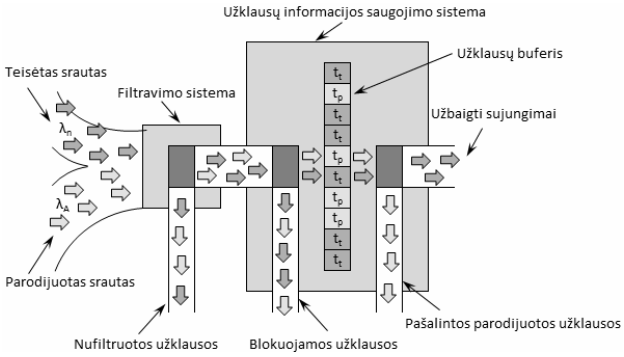
Visi šie modeliai turi savų privalumų ir trūkumų bei yra skirtingo detalumo ar orientuoti į skirtingas sritis. Susistemintai šiuos modelius galima aprašyti suvestinėje, kurioje nurodomas jų pilnumas ir tipas (žr. 1 lentelę).

Apibendrinant apžvelgtus modelius galima teigti, kad:

- egzistuojantys stochastiniai ir deterministiniai modeliai neatsižvelgia į atakos tinklo tipologiją ir naudojamas filtravimo priemones;
- agentų modeliai reikalauja labai detalaus atakos detalių išmanymo (orientuoti į atakos rengimą, o ne į pasiruošimą jai);
- didžioji dalis egzistuojančių modeliavimo įrankių naudoja agentų modelius;
- agentų modeliai leidžia detaliau stebėti atskirus atakos taškus, bet kartu reikalauja daugiau modeliavimui skirtų laiko ir atminties resursų.

Siūlomas SYN užtvindymo modelis

TCP SYN ataką galima įsivaizduoti kaip sistemą, kurioje užklausos aptarnaujamos tam tikru laiku, o į ją netelpančios užklausos yra tiesiog prarandamos. Atsižvelgiant į naudojamus filtrus, turėtų būti nusakoma filtravimo sistema, kuri prieš į sistemą patenkant visoms užklausoms, dalį jų iš anksto blokuoja (žr. 2 pav.).



2 pav. TCP SYN atakos konceptualusis modelis
Fig. 2. A conceptual model of a TCP SYN attack

1 lentelė. Egzistuojančių DoS atakų modelių pilnumo ir naudojamų modelių tipų palyginimas

Modelis	Savybės, į kurias atsižvelgiama modelyje					Modelio tipas
	Buferio talpa	Skirtingi užklausų aptarnavimo laikai	Atskirti parodijuotas ir teisėtas srautas	Užklausų filtravimas	Tinklo topologija	
Nr. 1	Atsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Stochastinis
Nr. 2	Atsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Stochastinis
Nr. 3	Atsižvelgta	Atsižvelgta	Atsižvelgta	Neatsižvelgta	Neatsižvelgta	Stochastinis
Nr. 4	Atsižvelgta	Atsižvelgta	Atsižvelgta	Neatsižvelgta	Neatsižvelgta	Stochastinis
Nr. 5	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Neatsižvelgta	Deterministinis
Nr. 6	Neatsižvelgta	Neatsižvelgta	Atsižvelgta	Atsižvelgta	Atsižvelgta	Agentų
Nr. 7	Atsižvelgta	Neatsižvelgta	Atsižvelgta	Neatsižvelgta	Neatsižvelgta	Agentų
Nr. 8	Atsižvelgta	Atsižvelgta	Atsižvelgta	Atsižvelgta	Atsižvelgta	Agentų

Norėdami detaliau aprašydami SYN užtvindymo sistemą, darome žemiau išvardintas prielaidas.

P1. Atakuojamoje sistemoje vienu metu gali būti saugoma K sujungimų informacija. Jei šis atminties buferis yra užpildytas, t. y. jame jau yra visos K vietos užimtos, naujų sujungimų sudaryti nebegalima ir nesvarbu, ar sistemą pasiekia teisėtos ar parodijuotos užklausos, jos yra tiesiog blokuojamos ir prarandamos, neaptarnaujamos.

P2. Teisėtų vartotojų vieno sujungimo informacija šiame buferyje vidutiniškai užtrunka t_t laiko, t. y. vidutiniškai per tiek laiko visiškai sudaromas trišalis rankų paspaudimas, o parodijuotos užklausos informacija šioje atmintyje laikoma t_p laiko tarpą ir nesulaukus jokio atsako yra pašalinama, kad nesikauptų nereikalinga informacija.

P3. Normalaus sistemos darbo metu trišalio rankos paspaudimo sudarymo užklausų būna λ_n per sekundę. Tačiau atakuojantysis gali dar papildomai generuoti λ_a sujungimų per sekundę srautą. Jei atakai naudojamas ne vienas, o n agentų (DDoS atakos atveju), tada bendras atakos srautas yra λ_A sujungimų per sekundę, kur $\lambda_A = \lambda_a \cdot n$. Tokiu atveju visas auką pasiekiantis trišalių rankos paspaudimo užklausų srautas tampa lygus $\lambda = \lambda_a \cdot n + \lambda_n$, čia λ_a ir λ_n yra tarpusavyje nepriklausomi.

P4. Jei atsižvelgtumėme, kad vartotojas imasi tam tikrų parodijuotų užklausų filtravimo priemonių, kurios atpažįsta ir sėkmingai blokuoja X procentų parodijuotų užklausų, bet tuo pačiu atmeta ir Y procentų teisėtų vartotojų užklausų, tai TCP trišalio sujungimo procese dalyvaujančių užklausų srautas būtų lygus:

$$\lambda = \lambda_a n\left(1 - X/100\right) + \lambda_n \left(1 - Y/100\right), \qquad (1)$$

t. y. priimame, kad nufiltruojamos ir tinkamos užklausos yra pasiskirsčiusios tolygiai.

P5. Atakos sėkmės tikimybę galima apspręsti teisėtų vartotojų užklausų blokavimo tikimybe, bet kadangi mes priimame, kad atakos ir teisėtas srautas yra vienodai pasiskirstę ir nėra imamasi jokių kontrpriemonių, galinčių reitinguoti į sistemą patenkančias užklausas, tai teisėtų užklausų blokavimo tikimybė yra tokia pati, kaip ir visų, bendro srauto blokavimo tikimybė.

P6. Pasak Zukerman (2008), internetinio srauto pasiskirstymą geriausiai atitinka eksponentinis pasiskirstymas (angl. *Poisson Pareto Burst Process*), tad TCP SYN atakos modeliavimui galima taikyti M/M/K/K sistemą, kuri įvertina sistemą pasiekiančio srauto intensyvumą, paraiškų aptarnavimo greitį ir buferio dydį, bei priima, kad vienu laiko momentu yra aptarnaujama tiek paraiškų, kiek jų telpa sistemoje.

P7. Remiantis S. K. Bose, paraiškų praradimo tikimybę galima apskaičiuoti taip:

$$p_p = \left(\frac{\rho^K}{K!}\right) \Big/ \sum_{i=0}^{K} \frac{\rho^i}{i!}, \qquad (2)$$

čia ρ yra atvykstančio srauto ir jo aptarnavimo greičių santykis $\rho = \lambda/\mu$ arba atvykstančio srauto ir vienos paraiškos aptarnavimo greičio sandauga $\rho = \lambda \cdot t$.

P8. Bendrą atvykimo srautą λ žinome, o vidutinį aptarnavimo greitį galime rasti žinodami, kiek vidutiniškai skiriama laiko aptarnauti paraiškai, t. y., kiek vidutiniškai buferyje išlieka vieno trišalio rankos paspaudimo informacija (neišskiriant tai teisėta ar parodijuota užklausa), kol ji yra galutinai baigiama aptarnauti ar tiesiog pašalinama iš buferio. Tam vidutiniam užklausos sistemoje buvimo laikui t rasti negali būti vedamas vidurkis, o reikia atsižvelgti į teisėtų ir parodijuotų užklausų santykį bendro srauto atžvilgiu:

$$\begin{aligned} t &= \frac{\lambda_n \cdot \left(1 - X/100\right)}{\lambda} \cdot t_t + \frac{\lambda_A \cdot \left(1 - Y/100\right)}{\lambda} \cdot t_p \\ &= \frac{\left(100 - X\right) \cdot \lambda_n \cdot t_t + \left(100 - Y\right) \cdot \lambda_A \cdot t_p}{100 \cdot \lambda}. \end{aligned} \qquad (3)$$

P9. Žinant vidutinį vienos užklausos buvimo buferyje laiką ir vidutinį bendro srauto pasirodymo sistemoje greitį, išreiškiama ρ išraiška formule:

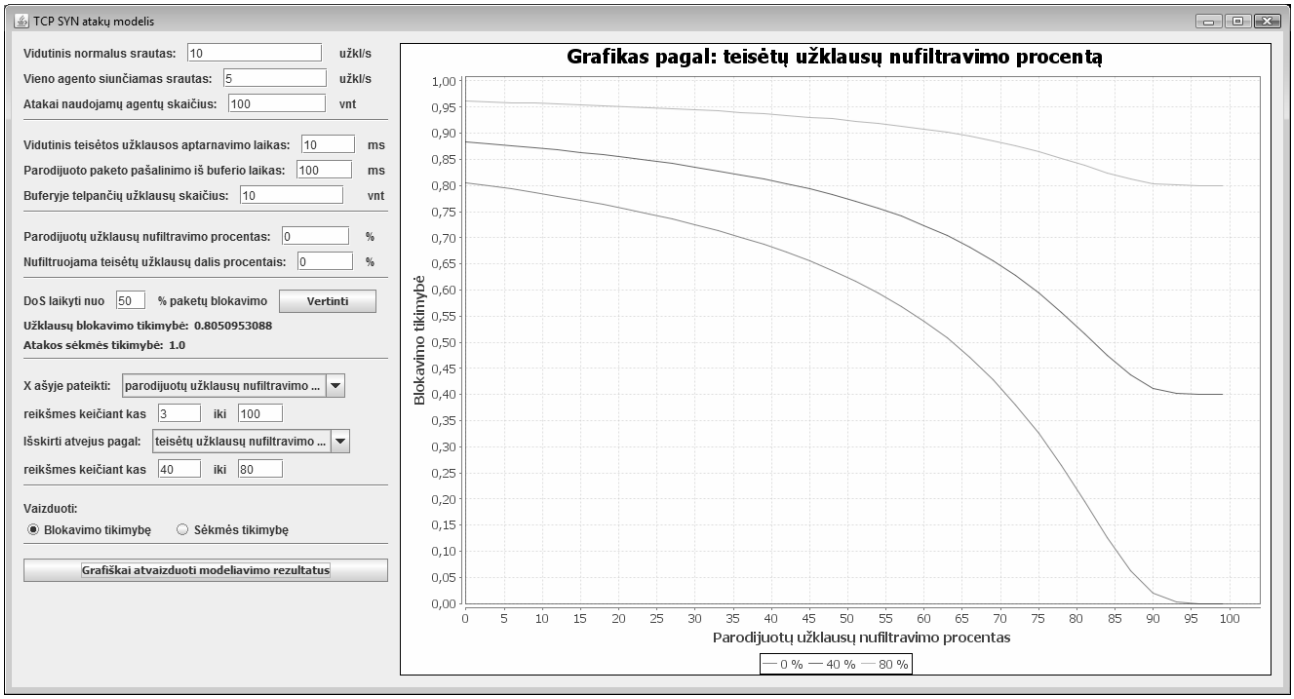
$$\begin{aligned} \rho &= \lambda \cdot t \\ &= \lambda \cdot \frac{\left(100 - X\right) \cdot \lambda_n \cdot t_t + \left(100 - Y\right) \cdot \lambda_A \cdot t_p}{100 \cdot \lambda} \\ &= \frac{\left(100 - X\right) \cdot \lambda_n \cdot t_t + \left(100 - Y\right) \cdot \lambda_A \cdot t_p}{100}. \end{aligned} \qquad (4)$$

P10. Atsižvelgiant į tai, kad dalį teisėto srauto galėjo blokuoti ir pačios sistemos filtrai nuo parodijuotų užklausų, tai bendra teisėtų vartotojų sujungimų blokavimo tikimybė būtų lygi:

$$\begin{aligned} P_b &= Y + (100 - Y) \cdot p_p \\ &= Y + (100 - Y) \cdot \left(\frac{\rho^K}{K!}\right) \Big/ \sum_{i=0}^{K} \frac{\rho^i}{i!}. \end{aligned} \qquad (5)$$

Modeliavimo rezultatai

Pagal aprašytą TCP SYN atakų modelį sukurta programa, leidžianti stebėti, kaip keičiasi atakos sėkmės ar užklausų blokavimo tikimybė, priklausomai nuo norimų dviejų atakos ar aukos savybių (vidutinio normalaus srauto, atakai naudojamų agentų skaičiaus, vieno agento generuojamo atakos srauto, vidutinio vienos užklausos aptarnavimo laiko, maksimalaus parodijuotos užklausos laikymo buferyje laiko, buferio talpos, parodijuotų užklausų

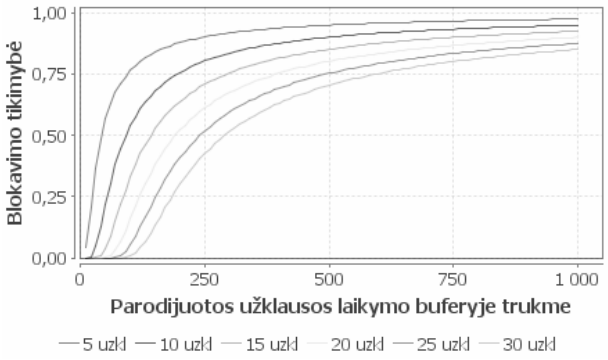


3 pav. Modeliavimo programos grafinis vaizdas
Fig. 3. A screen of modelling software

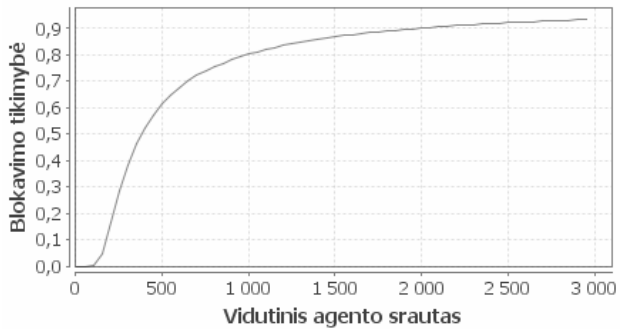
filtro efektyvumo, teisėtų paketų praradimo tikimybės, dėl netinkamai sukonfigūruoto užklausų filtravimo).

Modeliavimo rezultatas pateikiamas grafiškai. Tai leidžia aiškiau suvokti tų savybių įtaką atakai. Naudojantis šiuo modeliu, pastebėtos šios SYN užtvindymo DDoS atakų ir jų aukų savybės:

- pernelyg griežtas parodijuotų užklausų filtravimas gali padaryti daugiau žalos nei naudos, nes neteisingai parinkti filtrai gali sudaryti DoS atakų efektą, nes jei pati ataka ir nevyksta (3 pav.);
- didinant parodijuotų paketų filtravimo efektyvumą, TCP SYN atakos sėkmės tikimybė eksponentiškai mažėja: esant galingoms atakoms ir palyginti mažam filtravimo efektyvumui filtravimo įtaką juntama ryškiau, o sumažėjus atakai ar esant labai efektyviam filtravimui, skirtumai tarp filtrų efektyvumo atakos sėkmės tikimybei yra ne be tokie žymūs (3 pav.);
- buferio talpa ir parodijuotų užklausų laikymo buferyje laikas atakos sėkmei nėra tiesiškai proporcingi, t. y. norint pasiekti tokią pačią atakos sėkmės tikimybę, vienos papildomos vietos buferyje suteikimas gali prilygti nuo kelių iki keliolikos ar net keliasdešimties parodijuotų užklausų laikymo buferyje milisekundžių sumažinimui (tai priklauso nuo pačios atakos galingumo ir esamų reikšmių) (4 pav.);
- atakos sėkmės tikimybė nėra lygiagrečiai proporcinga atakos galiai, nes pradžioje didėjant atakos srautui, atakos sėkmės tikimybė beveik nedidėja (kol tai leidžia buferio talpa), tada eksponentiškai auga didele sparta, o atakai itin išaugus vėl kinta ne taip žymiai (5 pav.);



4 pav. Buferio talpos ir maksimalaus laikymo jame laiko priklausomybės užklausų blokavimo tikimybei, kai teisėtas srautas – 10 užkl./s, parodijuotas – 200 užkl./s, teisėtos užklausos aptarnaujamos per 10 ms, filtravimo nesiimama
Fig. 4. The dependence of buffer capacity and maximum time of storage on the probability of blocking requests, when legitimate traffic – 10 requests/s, feigned ones – 200 request/s, legitimate requests are served within 10 ms, no filtering is used



5 pav. Atakos srauto įtaka parodijuotų užklausų blokavimo tikimybei, kai buferyje telpa 20 užklausų, normalus srautas – 10 užkl./s, teisėti sujungimai užbaigiami per ~ 10 ms, o parodijuoti buferyje laikomi 100 ms, filtravimo nesiimama

Fig. 5. The effect of attack traffic on the probability of blocking feigned requests, when the buffer can store 20 requests, the normal traffic is 10 requests/s; legitimate connections completed within ~ 10 ms, feigned ones are kept in buffer for 100 ms, no filtering is used

Išvados

1. Egzistuojančiuose DoS atakų modeliuose plačiau ataką aprašyti galima naudojant agentų modelius, o stochastiniai modeliai dar ne taip dažnai naudojami, todėl nėra tokie išsamūs, bet lengviau taikomi praktikoje.
2. Sukurtas stochastinis SYN užtvindymo modelis leidžia išsamiau modeliuoti šio tipo atakas, nei kitais anksčiau aprašytais stochastiniais modeliais, nes atsižvelgia ne tik į pagrindines atakos ir aukos savybes, bet ir į naudojamų filtrų efektyvumą.
3. Modeliavimo rezultatai parodo, kad TCP SYN atakos negalima aprašyti tiesinės priklausomybės formulėmis, nes keičiant daugelį atakos savybių, atakos sėkmės tikimybė keičiasi ne tiesiškai, o eksponentiškai.
4. Aprašytas TCP SYN atakų modelis gali būti taikomas TCP SYN ir kitų atminties išnaudojimo DoS atakų modeliavimui, nes aprašo pagrindines savybes, jų sąveiką bei yra pagrįstas skirtingo tipo užklausų aptarnavimo skirtumais ir su tuo sekančiomis pasekmėmis.

Literatūra

Blackert, W. J.; Gregg, D. M.; Castner, A. K.; Kyle, E. M.; Hom, R. L.; Jokerst, R. M. 2003. *Analyzing Interaction Between Distributed Denial of Service Attacks And Mitigation Technologies* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.lasr.cs.ucla.edu/classes/239_1.spring03/papers/DDOS_interactions.pdf>.

Bose, S. K. 2001. *M/G/m/m Loss System* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.iitg.ac.in/skbose/qbook/MGmm_Queue.PDF>.

Burdach, M. 2003. *Hardening the TCP/IP stack to SYN attacks* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.securityfocus.com/infocus/1729>.

Chang, R. K. C. 2002. *Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www .docstoc.com/docs/12333600/Defending-against-Flooding-Based-DDOS>.

Chen, L.-C.; Carley, K. M. 2002. *Modeling Distributed Denial of Service Attacks and Defenses* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.casos.cs.cmu.edu /publications/papers/chen_ddos.pdf>.

Huang, Q.; Kobayashi, H.; Liu, B. 2003b. *Modeling of Distributed Denial of Service Attacks in Wireless Networks* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.hisashikobayashi.com/papers/Network%20Security%20Protocols/Modeling%20of%20distributed%20denial%20of%20service%20attacks%20in%20wireless%20networks.pdf>.

Huang, Q.; Kobayashi, H.; Liu, B. 2003a. *Analysis of a New Form of Distributed Denial of Service Attack* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.hisashikobayashi.com/papers/Network%20Security%20Protocols/Analysis%20of%20a%20New%20Form%20of%20Distributed%20Denial%20of%20Service%20Attack.pdf>.

Kotenko, I.; Stepashkin, M.; Ulanov, A. 2006. *Agent-based modeling and simulation of malefactors' attacks against computer networks* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://stepashkin.com/pubs/2005/nato-asi-06-paper.pdf>.

Wang, Y.; Lin, C.; Li Q.-L.; Fang, Y. 2007. *A queueing analysis for the denial of service (DoS) attacks in computer networks* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.fang.ece.ufl.edu/mypaper/comnet07wang.pdf>

Xiang, Y.; Zhou, W. 2006. *An Analytical Model for DDoS Attacks and Defense* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <https://agora.cs.illinois.edu/download/attachments/7344168/An+Analytical+Model+for+DDos+Attacks+and+Defense.pdf>.

Zukerman, M. 2008. *Introduction to Queueing Theory and Stochastic Teletraffic Models* [interaktyvus], [žiūrėta 2010-03-14]. Prieiga per internetą: <http://www.ee.cityu.edu.hk/~zukerman/classnotes.pdf>.

STOCHASTIC MODEL OF TCP SYN ATTACKS

S. Ramanauskaitė, A. Čenys

Abstract

A great proportion of essential services are moving into internet space making the threat of DoS attacks even more actual. To estimate the real risk of some kind of denial of service (DoS) attack in real world is difficult, but mathematical and software models make this task easier. In this paper we overview the ways of implementing DoS attack models and offer a stochastic model of SYN flooding attack. It allows evaluating the potential threat of SYN flooding attacks, taking into account both the legitimate system flow as well as the possible attack power. At the same time we can assess the effect of such parameters as buffer capacity, open connection storage in the buffer or filtering efficiency on the success of different SYN flooding attacks. This model can be used for other type of memory depletion denial of service attacks.

Keywords: TCP SYN, SYN Flooding, DoS, DDoS, Modelling.