BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 31, 2011

Cyber Defence – rozproszona obrona przed atakami DDoS

Adam E. PATKOWSKI

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Przedstawiono propozycję federacyjnej obrony przez rozproszonymi atakami prowadzącymi do odmowy usługi (DDoS). Zaproponowano najprostsze, minimalne rozwiązanie takiej obrony. Cechy charakterystyczne to całkowicie rozproszona realizacja oraz zdolność do adaptowania się do zmiennego ruchu sieciowego. Osiągalny jest też efekt stopniowego upadku. Rozwiązanie może stanowić podstawę do budowania systemu obrony cyberprzestrzeni kraju.

SŁOWA KLUCZOWE: sieci komputerowe, rozproszone ataki sieciowe, obrona, cyberprzestrzeń.

1. Wstęp

Zasoby informacyjne instytucji państwowych oraz ważnych dla życia publicznego organizacji prywatnych narażone są na ataki. Napastnicy działają z pobudek politycznych, terrorystycznych, a także czysto komercyjnych. Może nie czas jeszcze na trawestację powiedzenia von Clausevitza[1] do postaci „Internet jest kontynuacją polityki innymi środkami" ale najwyraźniej ku temu zmierza. Atrybuty bezpieczeństwa zasobów informacyjnych – tajność, integralność i dostępność – mogą być naruszane (ze szkodą dla właścicieli zasobów) zdalnie, przez wykorzystanie oddziaływania za pomocą ruchu sieciowego. Takie oddziaływanie nazywa się obecnie „cyberatakami", zaś obrona przed nim, polegająca na wpływaniu na medium ataku – ruch sieciowy – nazywana jest Cyber Defence.

Warto zauważyć, że naruszenie tajności zasobów informacyjnych jest umiarkowanie atrakcyjne dla napastników, zaś naruszanie integralności (rozumiane jako skryte zmiany ważnych danych) zwykle znajduje się poza

[1] *Wojna jest kontynuacją polityki innymi środkami* – Carl von Clausevitz, „O naturze wojny".

technicznymi możliwościami zdalnego oddziaływania. Natomiast atrybut dostępności jest szczególnie trudny do ochrony, ze względu na szerokie możliwości wykonywania ataków przeciążeniowych, należących do klasy tak zwanych ataków *Denial of Service* (DoS). Najbardziej rozpowszechnionymi sposobami realizacji ataków DoS są ataki rozproszone *Distributed Denial of Service* (DDoS: [1], [2], [3]).

Należy się spodziewać, że podstawową techniką cyberataków terrorystycznych lub ataków destabilizujących politycznie będą właśnie ataki sieciowe powodujące wyłączenie usług, które są ważne dla ludności w skali całego kraju. Przykładem może być sparaliżowanie systemu bankowości detalicznej lub ataki wyłączające niektóre usługi lub systemy w momentach, gdy stają się one szczególnie ważne. Spowodowanie niedostępności rejestracji zgłoszeń do systemu pomocy lub rekompensat unijnych w końcówce okresu rejestracji może spowodować niezadowolenie potencjalnych beneficjentów, ewentualnie niewywiązanie się w terminie ze zobowiązań. W kolejnych wyborach parlamentarnych i samorządowych można spodziewać się wykorzystania systemu głosowania przez Internet. Sparaliżowanie takiego systemu również może być atrakcyjnym celem. Przykłady można mnożyć, tym bardziej że zależność systemów społecznych i politycznych od sieci teleinformatycznych może tylko rosnąć z upływem czasu.

Dalej przedstawiono mechanizm Cyber Defence skierowany przeciw atakom DDoS, proponując jego minimalne rozwiązanie do wdrożenia w środowisku spełniającym warunki federacji (ang. *Federation of Systems*, FoS). Wskazano też, że związki federacyjne między zarządcami poszczególnych systemów nie są konieczne dla realizacji tej propozycji – skuteczne mogą okazać się dostatecznie liczne umowy o świadczenie usługi zdalnej ochrony między wybranymi zarządcami systemów lub obszarów sieci.

Obecnie obrona przed atakami przeciążeniowymi DDoS polega przede wszystkim na zwiększaniu zdolności działania pod obciążeniem (np. [3], [4], [5] i [9]), chociaż już na początku wieku rozważano ideę tzw. *geoblockingu* [6], polegającą na blokowaniu agresywnego ruchu „gdzie się da" na świecie. Szczególny wariant obrony na potrzeby federacji systemów autor niniejszego artykułu zaproponował w [7].

W niniejszym artykule zaproponowano adaptacyjną metodę obrony: elastyczne dopasowywanie miejsc blokowania ruchu sieciowego, odcinające od agresywnego ruchu pewien obszar sieci, zawierający serwer atakowanych usług (zasobów) tak, aby wewnątrz chronionej strefy znajdowało się możliwie wielu klientów atakowanych usług oraz możliwie mało atakujących komputerów. To pozwoli na zachowanie dostępności serwera dla klientów zlokalizowanych wewnątrz strefy.

2. Ataki DDoS

Wspomniane na wstępie rozproszone ataki sieciowe prowadzące do odmowy świadczenia usług (cyberataki DDoS) w swoich podstawowych postaciach są dobrze znane. Ich celem jest obniżenie miary atrybutu dostępności pewnych zasobów informacyjnych, w szczególności usług. Miarą tego atrybutu dla pewnej usługi może być liczba klientów, dla których w jednostce czasu dostępny jest zasób/usługa, może nią być też odwrotność czasu odpowiedzi lub czasu realizacji transakcji. Obecnie najczęściej używanym narzędziem do ataków DDoS jest botnet – zbiór komputerów, na których, najczęściej ukrywając to przed jego właścicielem/administratorem, osadzono niepożądany program sterowany zdalnie przez napastnika. Komputery składające się na botnet wykonują działania obciążające cel. Najbardziej znane techniki rozproszonych ataków przeciążeniowych to różne sposoby zalewania (ang. *flooding*).

Najprostszym sposobem prowadzenia ataku DDoS przez botnet jest po prostu wielokrotne nawiązywanie połączenia (sesji) z atakowanym serwerem, co powoduje przeciążenie łącza lub przekroczenie zdolności obsługi serwera i znaczny wzrost czasu odpowiedzi. Im bardziej skomplikowane jest nawiązanie połączenia z serwerem (obejmujące np. wykorzystanie SSL lub próby uwierzytelnienia), tym efektywniejszy jest atak. Na trasie od atakującego komputera może zostać użyta dowolna technika ukrywania jego adresu, celowo (np. użycie anonimizującego proxy lub wykorzystanie sieci Tor) bądź może ona wynikać z topologii sieci – np. komputer źródłowy może być w sieci stosującej mechanizm NAT (ang. *Network Address Translation*) na brzegu. W każdym jednak przypadku adres źródłowy IP ruchu sieciowego docierającego do celu ataku może być powiązany z konkretnym atakującym komputerem.

Alternatywnym sposobem ataku – niepozwalającym na wykrycie adresu IP napastnika – może być wykorzystanie techniki nazywanej *SYNflooding*, polegającej na wysyłaniu przez napastnika pakietów z ustawioną flagą SYN i ignorowaniu odpowiedzi serwera (SYN/ACK). Ten sposób działania prowadzi do przepełnienia tablicy półotwartych połączeń serwera, która jest zwykle dużo mniejsza od tablicy otwartych połączeń. Z punktu widzenia napastnika zaletą tej techniki jest możliwość wysyłania pakietów z fałszywym adresem nadawcy (ang. *spoofing*). Ogólnie trzeba przyjąć, że ten sposób ataku nie dostarcza wiarygodnych danych o źródle ataku (miejscu generowania agresywnego ruchu sieciowego).

Najogólniej rzecz biorąc ataki DDoS wykrywalne są tylko w pobliżu celu ataku, czyli tam, gdzie strumienie agresywnego ruchu sieciowego łączą się, pozwalając na rozpoznanie działań „jałowych" z punktu widzenia klienta. Tylko w pobliżu celu możliwe jest rozpoznanie adresów atakujących komputerów, gdyż tylko tam można dostrzec różnicę zachowania się napastników i klientów.

W przypadku bardziej wyrafinowanych ataków, mechanizm wykrywania ataków DDoS musi być wręcz wbudowany w atakowaną aplikację webową. Jako przykład można wskazać hipotetyczny atak na systemy bankowości detalicznej, zmierzający do zablokowania kont klientów bankowych. Atak taki, przeprowadzony i utrzymywany przez dłuższy czas, może jeszcze nie mógłby doprowadzić do krachu systemu finansowego, ale z pewnością mógłby w czasie kryzysu przeważyć szalę na stronę katastrofy lub znacznego wzburzenia społecznego. W bankach internetowych zwykle działa zabezpieczenie przed zgadywaniem haseł *on-line* polegające na blokowaniu konta (stałym lub czasowym) po kilkukrotnych nieudanych próbach zalogowania klienta. Ten mechanizm, zmierzający do podniesienia poziomu bezpieczeństwa dzięki uniemożliwieniu ataku zgadywania haseł, może zostać wykorzystany na szkodę chronionych obiektów. Atak rozproszony polegający na kilkakrotnych próbach zalogowania się na konto każdego klienta banku (powtarzany według potrzeb) spowoduje stałe utrzymywanie niedostępności kont klientów. Wielki botnet, lub wyspecjalizowane komputery obcych państw, mogłyby zablokować większość polskich banków internetowych. Szczególnie efektywne mogą okazać się ataki na serwery webowe udostępniające połączenia szyfrowane https (SSL). Dzięki temu, że dla pojedynczego połączenia serwer SSL jest obciążany piętnastokrotnie bardziej od klienta, nawet niewielka liczba atakujących komputerów wystarczy do wyczerpania możliwości serwera [8].

Mechanizmy wykrywania ataków wbudowane w aplikację mogą oczywiście wykrywać tylko ataki, które docierają do celu. Jednak z chwilą zidentyfikowania ataku, łącza do atakowanego komputera mogą już być przeciążone!

3. Idea rozwiązania

Proponowane rozwiązanie wykorzystuje oczywiste założenia:

- Wykrywanie ataków musi się odbywać w pobliżu celu ataku, najlepiej dzięki wbudowanym weń mechanizmom;
- Ataki przeciążeniowe powinny być blokowane jak najdalej od celu, najlepiej przed połączeniem się strumieni agresywnego ruchu w jeden, przed osiągnięciem celu;
- Idea odpierania powinna się opierać na modelu twierdzy: **blokowanie ruchu sieciowego zmierzającego do serwera atakowanej usługi powinno być prowadzone w takich miejscach (zapewne na granicach obszaru administracji FoS), by wewnątrz obszaru chronionego znajdowała się absolutna większość klientów tej usługi, zaś by większość napastników znajdowała poza pierścieniem zapór blokujących**. Dalej zakłada się

racjonalnie, że obszar federacji jest podobszarem sieci, w której zlokalizowana jest większość klientów chronionych usług. W przypadku cyberprzestrzeni kraju rozsądne jest też założenie, że większość atakujących komputerów leży poza obszarem federacji;

- Dla odparcia ataku przeciążeniowego DDoS nie trzeba blokować całego ruchu – wystarczy blokować tylko tyle, by zniknęło zjawisko przeciążania, tzn. by miara dostępności osiągnęła minimalną akceptowalną wartość.

Dla osiągnięcia skuteczności działania w warunkach przeciążania łączy najlepsza byłaby realizacja mechanizmów ochronnych niewymagająca żadnego sterowania centralnego: w pełni rozproszona. Mechanizmy ochronne same mogą stać się celem ataku zmierzającego do ich wyłączenia lub wręcz wykorzystania przeciw chronionym zasobom. Rozproszenie i brak centralnego zarządzania może zwiększyć odporność systemu ochrony.

Idea rozwiązania polega na wykryciu ataku tam, gdzie to jest najłatwiejsze, a czasami jedynie możliwe, czyli w pobliżu celu ataku. Wykrywanie powinno zapewne odbywać się w warstwie aplikacji. Natomiast odpierać ataki powinno się jak najdalej od celu. Dobrym miejscem może być połączenie z inną dużą siecią, wejście do sieci szkieletowej lub łącze do punktu wymiany ruchu międzyoperatorskiego (ang. *Internet eXchange Point*, IXP). W takich miejscach możliwe jest stosowanie zapór sieciowych co najwyżej wprowadzających minimalne opóźnienia, a zatem filtrujących w warstwie trzeciej i to za pomocą prostych reguł (standardowe reguły według zawartości nagłówka IP, ewentualnie z wykorzystaniem tzw. „dzikich masek"). To oznacza, że mechanizm wykrywający atak powinien wygenerować proste reguły dotyczące ruchu w warstwie trzeciej i przekazać je do zapór sieciowych.

Należy zwrócić uwagę na to, że reguły służące do odpierania ataku DDoS mają zastosowanie tylko w trakcie trwania tego ataku – po jego zakończeniu przestają być potrzebne. Powinny to być zatem reguły dynamiczne, szybko aplikowalne i szybko usuwalne.

4. Jak zbudować system

Minimalny system ochrony przed atakami DDoS powinien składać się ze zlokalizowanych w newralgicznych punktach sieci szybkich zapór sieciowych działających w warstwie trzeciej, zdolnych do przyjmowania dynamicznych reguł filtrowania bez opóźnień. Dla niewielkiej liczby reguł realizacja techniczna takich zapór nie stanowi problemu.

W systemach federacyjnych sieć podzielona jest na spójne podobszary zarządzane przez pojedynczych zarządców, nazwane domenami. Problemy związane z zabezpieczeniem interesów tych zarządców, w szczególności nadzór

nad informacją opuszczającą domenę i regułami zlecanymi z zewnątrz, nie będą szczegółowo rozważane w niniejszym opracowaniu.

W pełni rozproszony mechanizm odpierania ataków można wprowadzić, dodając do każdej z zapór lokalny mechanizm przesyłania reguł. Na jego potrzeby należy zdefiniować abstrakcyjny opis topologii sieci, obejmujący komputery zawierające chronione zasoby (i zdolne do wykrywania ataków) oraz urządzenia filtrujące ruch (zapory). Dla każdego z takich węzłów sieci można opisać relację sąsiedztwa, gdy ruch sieciowy pomiędzy tymi węzłami jest przekazywany bezpośrednio – nie przechodzi przez inny węzeł. Jeśli ruch sieciowy dociera do węzła z innych domen bez pośrednictwa innych węzłów, to przyjmuje się, że węzeł sąsiaduje także z „otoczeniem".

Algorytm przesyłania reguł jest stosunkowo prosty: po wykryciu ataku i określeniu reguły jest ona przekazywana do wszystkich węzłów sąsiadujących (poza tym, z którego przybyła). Reguła jest wprowadzana do lokalnej zapory tylko w przypadku, gdy węzeł sąsiaduje z otoczeniem. Ten sposób postępowania zapewnia „wędrowanie" reguł do najdalszych zapór federacji.

Aby zrealizować taki system, należy określić następujące elementarne bloki funkcjonalne:

1. IDS: wykrywanie ataku i generowanie reguł niskopoziomowych;
2. Zapora: filtrowanie ruchu sieciowego według dynamicznych reguł;
3. Sterowanie (integrowane z IDS lub zaporą, tworząc węzeł): zarządzanie regułami realizujące algorytm przesyłania i utrzymywania reguł na zaporach.

Algorytm przesyłania i utrzymywania reguł może wystąpić w różnych wariantach – dla minimalnej realizacji można zaproponować rozwiązanie pozwalające osiągnąć m.in. efekt samoadaptowalności elementów systemu, a polegające na wyłączaniu tych reguł, których częstość stosowania spadnie poniżej pewnej zadanej wartości progowej. Przez stosowanie reguły rozumie się wykrycie w ruchu sieciowym informacji spełniającej warunek reguły. Częstość stosowania każdej reguły może być zliczana i stanowić podstawę do automatycznego usuwania reguły z zapory. Ograniczy to komunikację między tymi węzłami, co w warunkach przeciążania łączy może okazać się szczególnie korzystną cechą. Przez wyłączenie rozumie się usunięcie reguły z zapory.

5. Wykrywanie ataku

Blok funkcjonalny wykrywania ataku powinien wykryć atak DDoS i wypracować niskopoziomowe reguły pozwalające odfiltrować szkodliwy ruch sieciowy (generowany przez licznych napastników), w miarę możliwości pozostawiając klientom możliwość komunikacji z chronionymi zasobami.

Chociaż największe możliwości, w szczególności w wykrywaniu ataków specjalnie projektowanych (ang. *targeted attacks*), dają mechanizmy wykrywania wbudowane w aplikacje, to można też wskazać samodzielne urządzenia wykrywające podstawowe ataki przeciążeniowe DDoS. Takie IDS (*Intrusion Detection Systems*) federacyjne, dopasowywane do miejsca obserwacji ruchu sieciowego, mogą wykrywać ataki:

1. SYNflood: gdy w pewnym przedziale czasowym liczba przychodzących pakietów TCP z ustawioną flagą SYN znacząco przekracza liczbę pakietów z flagą ACK. W atakowanym serwerze można również wykrywać wysokie wykorzystanie (zajętość pozycji) tablicy półotwartych połączeń. Ponieważ dla ataków SYNflood adres IP napastnika nie jest wiarygodny, można tylko wygenerować generalną regułę blokowania ruchu DO atakowanego zasobu. Bardziej szczegółowe reguły można wygenerować, znajdując wspólne cechy wszystkich pakietów SYN, dla których nie nadszedł pakiet ACK, unikalne dla tej grupy;
2. Zalewanie otwieranymi połączeniami TCP. Ten rodzaj ataku można wykrywać przez zliczanie pakietów TCP z flagą SYN (lub ACK) z poszczególnych adresów IP (można wyłączyć niektóre adresy znanych użytkowników). Jeśli dla jakiegoś adresu IP ta wartość w pewnym przedziale czasowym przekroczy zadany próg, można wygenerować regułę blokującą ruch z tego adresu;
3. Zgadywanie haseł lub blokowanie kont może zostać wykryte przez rozpoznanie w ruchu wychodzącym do klienta wybranych kodów odpowiedzi serwera WWW. Można wykorzystać stałe położenie kodów odpowiedzi w pakietach i zliczać, ile razy w pewnym przedziale czasowym każdemu z adresów IP serwer odpowiedział wartością 401 (*unauthorized*). Po przekroczeniu zadanej wartości progowej odpowiedni IP można uznać za wrogi i wygenerować odpowiednią regułę blokującą ruch z tego adresu.

Pominięto rozważania pewnych szczególnych właściwości – na przykład konsekwencji ataku na serwer wirtualny dzielący adres IP z innymi serwerami, czy działania klientów zza NAT z wielkich organizacji. W takich przypadkach pewne możliwości dają elementy samouczące: progi reakcji na DDoS mogą być zależne od dotychczasowego zachowania się, można też wykorzystać listy adresów IP dotychczasowych, godnych zaufania klientów.

Bloki funkcjonalne IDS powinny być wbudowane w chronione zasoby (najlepiej tak, by działały w warstwie aplikacji) lub być zlokalizowane na trasie ruchu do tych zasobów w ich bezpośredniej bliskości. Należy zwrócić uwagę, że w przypadku przeciążania łączy, komunikacja tych bloków z pozostałymi częściami systemu może być utrudniona.

6. Zapory sieciowe i komunikacja

Bloki funkcjonalne realizujące filtrowanie ruchu sieciowego to zapory sieciowe działające w warstwie trzeciej, według reguł dotyczących nagłówka pakietu IP i wybranych obszarów pakietu. W praktyce rolę zapory może pełnić każde sterowane zewnętrznie urządzenie dysponujące listami kontroli dostępu (ACL – ang. *Access Control Lists*), przyjmującymi dynamiczne reguły filtrowania. Zapora musi posiadać zdolność sygnalizowania do sterowania każdej sytuacji, gdy została zastosowana dowolna reguła (gdy zablokowano pakiet spełniający warunek reguły). Jeśli liczba zastosowań reguły w ustanowionym przedziale czasowym spadnie poniżej zadanej wartości – reguła zostanie usunięta z zapory („wyłączona").

Komunikacja między elementami systemu musi zapewnić niezaprzeczalność i integralność przesyłanych komunikatów. Dowolny wariant szyfrowania asymetrycznego zapewne okaże się wystarczający. Dzięki temu, że poszczególne reguły będą stosunkowo krótkie, każda z nich może zostać przesłana nawet w pojedynczym pakiecie wybranego protokołu bezpołączeniowego.

7. Zarządzanie regułami, algorytm

Blok funkcjonalny zarządzania regułami (sterowanie) realizuje algorytm przesyłania reguł i ich używania w zaporach. Ta funkcja powinna być wbudowana w urządzenia realizujące funkcje zapór i wykrywania ataków. Istotną cechą zarządzania regułami jest to, że nie powinno ono wymagać oddzielnego sterowania i że powinno zapewniać właściwe działanie całego systemu bez wyróżniania któregokolwiek z węzłów.

Dla przekazywania reguł między blokami zarządzania regułami, każdy z tych bloków musi znać adresy bloków sąsiadujących oraz mieć informację, czy do lokalnej zapory dociera ruch trasami, na których nie ma żadnej zapory – bezpośrednio z otoczenia federacji. To wystarczy do pożądanego przekazywania informacji w systemie zapór po rozpoczęciu ataku. Jeśli węzeł, czyli blok zarządzania regułami i lokalna zapora, sąsiadują z otoczeniem, to reguła powinna być umieszczona w konfiguracji lokalnej zapory. W przeciwnym wypadku wystarczy przekazanie reguły do sąsiadów.

Jeśli atak zostanie odparty, to dalsze utrzymywanie reguł jest niepożądane. Zakończenie ataku nie może być jednak rozpoznawane przez elementy centralne – tylko odległe od celu zapory odnotują zakończenie ataku jako spadek częstości stosowania reguł. Zatem wystarczy z każdą regułą związać pewną wartość częstotliwości zastosowań, poniżej której reguła zostanie usunięta z zapory. W tym celu sterowanie (we współpracy z zaporą) powinno

zliczać liczbę wystąpień zastosowania reguły w zadanych kwantach czasu. Jak wspomniano wcześniej, przez zastosowanie reguły rozumie się wykrycie, że dla pewnej jednostki ruchu sieciowego (pakietu) warunek reguły jest spełniony i, zwykle, zablokowanie przekazania tego pakietu między interfejsami zapory.

Na marginesie można wskazać alternatywny, jeszcze prostszy wariant realizacji algorytmu utrzymywania reguł, w ogóle nie rozważając sąsiedztwa z otoczeniem. Po prostu blok zarządzania regułami zawsze może umieszczać regułę w lokalnej zaporze i przekazywać regułę do sąsiadujących zapór. Jeśli lokalna zapora nie sąsiaduje z otoczeniem, to agresywny ruch do niej nie dotrze, bo sąsiednie zapory go odfiltrują. W rezultacie reguła nie będzie stosowana i zostanie usunięta. W przypadku, gdy do lokalnej zapory dociera ruch bezpośrednio z otoczenia, reguła ta będzie stosowana i nie ulegnie usunięciu, dopóki będzie trwał atak.

8. Rola IDS, stopniowa degradacja

Chociaż blok funkcjonalny wykrywania ataków pełni rolę inicjującą reguły, to mogą być one przyjmowane także z innych źródeł i mimo że w prezentowanym wariancie nie przewiduje się centralnego odwoływania rozesłanych reguł, to w trakcie trwania ataku DDoS ten blok funkcjonalny ma ważną rolę do odegrania w miarę rozwijania się ataku.

W trakcie ataku DDoS dołączają do niego kolejni napastnicy, np. gdy botnet się włącza lub rozwija, infekując kolejne komputery, lub gdy przeciwnik uruchamia kolejne komputery do ataku. W rezultacie pomimo trwającego już blokowania według pewnych reguł generowane są kolejne reguły i wysyłane do zapór. Jeśli liczba reguł wskazujących na adresy napastników przekracza wartość dopuszczalną i grozi opóźnieniami na zaporach, wówczas można dokonywać sumowania logicznego warunków reguł. Jeśli nowa reguła jest wstawiana na początek listy[2] reguł zapory, stare reguły o podobnym warunku nie mają okazji być stosowane i w rezultacie zostaną usunięte z listy, z powodu małej częstości stosowania. Dzięki temu użycie/wygenerowanie nowych reguł, o szerszych warunkach niż stare reguły, nie wymaga odwoływania żadnych reguł. W ten też sposób, pomimo dołączania kolejnych napastników, lista reguł może zachowywać rozsądną długość, nie powodując zatorów czy opóźnień na zaporach. Niestety sumowanie warunków zwykle spowoduje też, że warunek wynikowy będzie się stosował do ciągów binarnych, do których nie stosuje się żaden z warunków sumowanych. W przypadku reguł dotyczących adresów IP oznacza to blokowanie nie tylko IP wskazywanych przez sumowane reguły. To

[2] Reguły są sprawdzane zgodnie z porządkiem ich umieszczenia na liście.

nieunikniony koszt ograniczania długości listy reguł: pewien spadek dostępności.

Blok funkcjonalny IDS w trakcie ataku DDoS może reagować, uwzględniając historię i/lub natężenie ataku. Jeżeli wybrany sposób reagowania okazuje się nieskuteczny i agresywny ruch nadal dociera do IDS, może on zmienić generowane reguły na bardziej restrykcyjne. IDS może generować zbiory reguł powodujące:

- blokowanie ruchu z pojedynczych adresów IP;
- blokowanie ruchu z podzbiorów adresów IP (w wyniku sumowania reguł);
- blokowanie ruchu do atakowanej usługi (adres IP i port);
- blokowanie ruchu do atakowanego serwera;
- blokowanie wszelkiego ruchu do wnętrza federacji.

Jeśli polityka generowania pewnego zbioru reguł okazuje się nieskuteczna lub liczba reguł przekracza wartość akceptowaną przez zapory, IDS powinien przejść do generowania bardziej restrykcyjnego zbioru reguł. Ostatni z nich powoduje odcięcie sfederowanych domen od świata zewnętrznego, co w przypadku gwałtownego ataku na wielkie federacje (np. na polską cyberprzestrzeń) wydaje się całkiem uzasadnione. Opisany sposób postępowania tworzy z federacji obszar sieci reagujący na atak DDoS stopniową degradacją funkcji wymiany ruchu z otoczeniem.

W przypadku ataków SYNflood, gdy nie ma możliwości wiarygodnej identyfikacji źródła ataku, jedynym sposobem jest blokowanie ruchu według adresu (i portu) docelowego. W tym przypadku zasoby atakowanego komputera staną się niedostępne dla klientów spoza chronionego obszaru federacji, za to dla wewnętrznych komputerów dostępność zostanie zachowana.

Należy zwrócić uwagę, że IDS działający w warstwie aplikacji zwykle ma możliwość odróżnienia ruchu generowanego przez botnet od „normalnego" ruchu. W konsekwencji możliwe jest rozpoznanie pewnych unikalnych właściwości niepożądanych pakietów i uzyskanie sygnatury ataku nadającej się do wykorzystania w regułach warstwy trzeciej. IDS wykrywający atak w niskiej warstwie tylko na podstawie badania cech statystycznych ruchu sieciowego nie daje takiej możliwości.

9. Ochrona interesów lokalnego zarządcy domeny

Ważnym elementem systemu federacyjnego jest zapewnienie ochrony interesów właściciela/zarządcy domeny, w której instalowane są bloki funkcjonalne proponowanego systemu obrony przed atakami DDoS. Taka ochrona musi odbywać się automatycznie i musi zapewnić, że poza domenę nie

wydostaną się informacje (w tym przypadku reguły), które mogą zostać wykorzystane na szkodę właściciela domeny, ani że nie zostaną zaakceptowane reguły mogące przynieść mu szkodę.

Najprostszym sposobem na zapewnienie ochrony właścicielowi domeny jest założenie, że domena przyjmie reguły dotyczące blokowania wyłącznie ruchu adresowanego do domeny oferującej regułę. Każda reguła musi zatem uwzględniać w warunku adres IP celu. Takie podejście zapewnia, że żadne reguły, które mają innego adresata niż „regułodawca", nie będą przeszkadzać w przesyłaniu informacji do pozostałych domen. To pewna i prosta metoda zwalniająca administratorów od ręcznego akceptowania reguł i pozwalająca na natychmiastowe oddziaływanie na wzrost agresywnego ruchu. Niestety jest to jednocześnie ograniczenie, które powoduje, że inne domeny nie mogą automatycznie korzystać z doświadczeń sąsiada, na przykład blokując ruch do swoich serwerów od rozpoznanego wroga, zapewne wspólnego dla wszystkich członków federacji. Zarządca domeny może jednak obdarzyć sąsiednią domenę zaufaniem, pozwalając akceptować z niej dowolne reguły, i następnie wprowadzać te reguły na wszystkie własne zapory.

Nic nie stoi na przeszkodzie w sformułowaniu pewnego zbioru zasad służących do automatycznego sprawdzania i akceptacji reguł przesyłanych z zewnątrz.

10. Wnioski: FoS a usługa ochrony

Warto zauważyć, że wizja obrony federacyjnej z regułami przekazywanymi pomiędzy sąsiadami tak, że w końcu docierają one do granic federacji, może zostać zastąpiona modelem, w którym każdy IDS rozsyła reguły do wszystkich zapór, pozwalając, by wygasły one w tych miejscach, w których są niepotrzebne. Co więcej, można w ogóle nie używać modelu federacji i domen, zastępując go modelem, w którym występują tylko usługodawcy wynajmujący swoje zapory. Każdy IDS wybiera sam odległe zapory, na których powinny zostać zaaplikowane reguły, i tam je wysyła. Ten model wymaga jednak znajomości topologii sieci przez IDS, a ponadto środków zapewniających, że żaden właściciel IDS nie wykorzysta możliwości oddziaływania za pomocą reguł na „cudzy" ruch, na szkodę innych podmiotów. Tych postulatów nie można osiągnąć bez skomplikowanego i centralnie sterowanego mechanizmu badania przesyłanych reguł. Zatem rozproszona realizacja zaprezentowanego tu modelu, alternatywnego dla modelu federacyjnego, wydaje się niemożliwa.

Należy zwrócić uwagę na to, że model federacyjny nie jest przeszkodą w umieszczaniu w domenach zapór, do których prawa własności ma jakiś obcy w domenie podmiot. Jeśli sterowanie tych zapór będzie kontrolowane

i akceptowane przez zarządcę domeny, to można abstrahować od formalnego prawa własności.

Zaprezentowany minimalny model obrony federacyjnej może zostać rozbudowany na przykład o wprowadzenie:

- zwrotnej komunikacji, dzięki której można np. w odpowiedzi na żądanie zastosowania reguły przekazać informację, czy nie została ona odrzucona;
- mechanizmów odwoływania reguł;
- parametru „czasu życia" reguł, po którym zostaną one usunięte z zapory;
- mechanizmów tworzenia przez IDS list znanych klientów serwisów (ang. *whitelists*) i oceny typowego obciążenia przez nich generowanego;
- wykorzystywania przez domeny przysyłanych z zewnątrz reguł do własnych celów: zidentyfikowania potencjalnych zewnętrznych napastników na własne serwery oraz zlokalizowania wrogich komputerów (elementów botnetu) we własnej domenie.

Na potrzeby ochrony polskiej cyberprzestrzeni najlepszym rozwiązaniem byłoby sformowanie federacji ze wszystkich operatorów sieci, w których znajdują się serwery należące do infrastruktury krytycznej lub liczne komputery potencjalnych klientów tych serwerów. Na granicach między domenami oraz na wyjściach do sieci szkieletowej (czy do punktów wymiany ruchu) należy zapewnić odpowiednie zapory filtrujące w warstwie trzeciej za pomocą list (ACL) prostych reguł. Zarządzanie listami powinno realizować odpowiedni, prosty algorytm, jak opisano w rozdziale 7. Takie rozwiązanie zapewnić może efekt łagodnego upadku, a w skrajnym przypadku odcięcie polskiej cyberprzestrzeni od zewnętrznego Internetu. Całość może być realizowana w pełni automatycznie, bez angażowania powolnego w reakcjach człowieka-operatora.

W systemie mogą być wykorzystywane różne dostępne zapory sieciowe dające m.in. możliwość blokowania ruchu z małych wewnętrznych poddomen. W sieciach dostawców publicznego Internetu pozwoli to na działanie reguł blokujących ruch od pojedynczych klientów. To nowa jakość: zablokowanie ataków, a nawet wyeliminowanie botnetów, znajdujących się w obszarze federacji.

W niniejszym opracowaniu nie rozważano szczegółowo możliwych rozwiązań mechanizmów wykrywania ataków na potrzeby generowania reguł. Autor jest zdania, że największe możliwości da wbudowywanie odpowiednich funkcji w aplikacje i wykrywanie ataków w warstwie aplikacji tak, aby w wyniku wykrycia ataków generować reguły blokowania ruchu sieciowego działające w warstwie trzeciej.

Literatura

[1] PATRIKAKIS C., MASIKOS M., ZOURARAKI O., *Distributed Denial of Service Attacks*, "The Internet Protocol Journal" – Vol. 7, No. 4, CISCO, December 2004.

[2] *Denial of Service Attack*, Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack, stan na dzień 16.11.2011.

[3] *Four Steps to Defeat a DDoS Attack*, Imperva White Paper, Imperva 2011.

[4] KARGL F., MAIER J., SCHLOTT S., WEBER M., *Protecting Web Servers from Distributed Denial of Service Attacks*, WWW10, Hong Kong , 1–5 May, 2001.

[5] FROUTAN P., *How to defend against DDoS attacks*, http://www.computerworld.com /s/article/94014/How_to_defend_against_DDoS_attacks, COMPUTERWORLD, 24 June, 2004.

[6] NOURELDIEN A., *Protecting Web Servers from DoS/DDoS Flooding Attacks. A Technical Overview*, International Conference on Web-Management for International Organizations, Geneva, 30–31 October 2002.

[7] PATKOWSKI A.E., *Specyfikacja mechanizmów wykrywania działań nieuprawnionych typu DDoS oraz sposobów reagowania na nie w środowisku federacyjnym*, Sprawozdanie z realizacji zadania projektu rozwojowego Nr 0 R00 0125 11: *System ochrony sieci teleinformatycznych przed działaniami nieuprawnionymi*, WIŁ 2011.

[8] MUSIL S., *New attack tool targets Web servers using secure connections*, http://news.cnet.com/8301-1009_3-20125058-83/new-attack-tool-targets-web-servers-using-secure-connections/, CNET News, 24 October, 2011.

[9] *Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks*, CISCO, Document ID: 13634, 22 April, 2008.

Cyber Defense – Distributed defense against DDoS attacks

ABSTRACT: A proposal of a federal defense against distributed attacks causing denial of service (DDoS) is presented. This is a very simple, minimal solution of such a defense. Characteristic features are: a fully distributed implementation and the ability to adapt to the behavior of a network traffic. A gradually degradation during the attack is also allowed. The solution can provide a basis for building a national cyber-defense system.

KEYWORDS: computer networks, DDoS, cyber-defense, cyberspace.

Praca wpłynęła do redakcji: 19.11.2011