

Vladimir "vovcia" Mitiouchev <vovcia@irc.pl>

icmp blind attacks

Oparto o draft-gont-tcpm-icmp-attacks-04 (Fernando Gont)

Spis treści:

1. Wprowadzenie
2. Działanie ICMP
3. Ataki blind icmp
4. Przeciwdziałanie

1. Wprowadzenie

ICMP czyli Internet Control Message Protocol jest jednym z podstawowych protokołów stosu TCP/IP. Jest on używany głównie do raportowania problemów sieciowych, takich jak brak trasy do hosta czy brak obsługi danego protokołu.

Od początku istnienia ICMP znane były problemy z nim związane, brak autoryzacji komunikatów czynił i czyni go nadal niebezpiecznym narzędziem w rękach hakera. Oryginalna specyfikacja nie zaleca żadnych procedur sprawdzania wiarygodności otrzymanych pakietów, a konkretne rozwiązania implementujące takie procedury nigdy nie przyjęły wymiaru standardu.

Brak takich procedur stwarza możliwości resetowania połączeń TCP oraz zmniejszania MTU (maksymalnego rozmiaru pakiety) do drastycznie małych wartości. Ataki te mogą być przeprowadzone bez potrzeby sniffowania sesji TCP, nawet bez potrzeby zmiany adresu źródłowego, parametry wystarczające do przeprowadzenia ataku to adresy IP hostów i numery portów danej sesji TCP, które najczęściej są standardowe (zgodne z RFC 1700).

Niedawno brytyjska organizacja NISCC (National Infrastructure Security Co-ordination Centre) współpracując z innymi organizacjami zajmującymi się bezpieczeństwem zajęła się problemem ICMP blind attacks. W trakcie badań znaleziono wiele implementacji TCP podatnych na ataki opisane w tym dokumencie, od typowo desktopowych OS'ów do ważnych routerów na których działaniu opiera się INTERNET.

W 2 części tej opowieści będzie mowa o technicznych aspektach protokołu ICMP i reakcjach TCP na błędy ICMP. W części 3 opiszę znane ataki blind icmp. W części 4 jest opis mechanizmów przeciwdziałania tym atakom i zalecane zabezpieczenia.

2. Działanie ICMP

ICMP jest powszechnie używanym protokołem internetowym służącym do raportowania problemów z siecią oraz niektórych prostych czynności (np. icmp echo request popularnie zwany pingiem). Tutaj będzie mowa tylko o aspekcie raportowania problemów z siecią. Komunikaty ICMP mogą być generowane zarówno przez routery pośredniczące jak i hosty. Kiedy router wykrywa problem wysyła do nadawcy pakietu komunikat ICMP, który zostaje obsłużony przez odpowiedzialny za pakiet protokół, który może: spróbować naprawić problem, zignorować go lub zerwać połączenie.

Komunikaty ICMP mogą wysyłać zarówno routery pośredniczące jak i hosty, więc adres nadawcy komunikatu tak naprawdę nie mówi nic o jego autorze i wiarygodności.

W każdym komunikacie oprócz numeru błędu znajduje się początek pakietu który spowodował błąd, jest to konkretnie nagłówek IP i 8 oktetów (czasem więcej ale minimalny rozmiar to właśnie 8 oktetów) nagłówka warstwy wyższej (w naszym przypadku TCP). W załączonym nagłówku IP znajduje się m.in. źródłowy i docelowy adres IP, a w 8 oktetach nagłówka TCP zawierają się porty źródłowy i docelowy oraz TCP Sequence Number (unikalny numer nadawany każdemu pakietowi służący do ustalania ich kolejności i wysyłania potwierdzeń przez odbiorcę).

Typ: 3	Kod: 4	Suma kontrolna		
nieużywane				
Nagłówek IP		Źr. port	Doc. port	TCP Seq Num

Budowa przykładowego pakietu ICMP Destination Unreachable: Fragmentation needed and DF set (bez nagłówka IP).

Komunikaty ICMP dzielą się na tzw. soft errors i hard errors. Po otrzymaniu hard error TCP musi zerwać połączenie, natomiast po soft error komunikacja może być kontynuowana.

Zgodnie z RFC 1222 każda implementacja TCP/IP musi reagować na komunikaty o błędach ICMP w powyższy sposób. Rodzaj błędu jest zapisany w nagłówku ICMP i opcjonalnym kodzie który określa w czym dokładnie tkwi problem. Oto kategorie błędów i reakcje TCP na nie (RFC 792 1122):

- Destination Unreachable (cel nieosiągalny) [patrz niżej]
- Source Quench: (brak buforów do obsługi transmisji) TCP musi zmniejszyć prędkość wysyłania danych. Jednak w obecnych implementacjach TCP zwykle ignoruje ten komunikat, ma bowiem wbudowane własne mechanizmy wykrywania prędkości połączenia.
- Time Exceeded: (pakiet został odrzucony z powodu osiągnięcia przez jego TTL wartości 0) soft error
- Parameter Problem: (niepoprawna wartość parametru w nagłówku IP) soft error

Kody błędów dla Destination Unreachable to:

- 0 net unreachable: (brak trasy do sieci) soft error
- 1 host unreachable: (brak trasy do hosta) soft error
- 2 protocol unreachable: (nieobsługiwany protokół) hard error
- 3 port unreachable: (nieobsługiwany port) hard error
- 4 fragmentation needed and DF bit set: (pakiet jest zbyt duży żeby go przetworzyć i ma ustawioną flagę zabraniającą fragmentacji) hard error
- 5 source route failed: (nie udało się ustawić ręcznej trasy do hosta) soft error

Skąd TCP wie której sesji dotyczy dany komunikat? Jak już wiemy, ICMP w każdym błędzie przekazuje nagłówek IP i pierwsze 8 oktetów danych IP pakietu który spowodował błąd. Z nagłówka IP odczytywany jest adres hosta docelowego, a z danych pakietu które w tym przypadku są początkiem nagłówka TCP porty źródłowe

i docelowe co wystarcza do jednoznacznego zidentyfikowania sesji TCP. Nie wystarcza natomiast do zabezpieczenia się przed fałszywymi komunikatami ICMP.

PMTU Discovery (PMTUD)

RFC 1191 określa mechanizm wykrywania MTU (Maximal Transfer Unit) na trasie do hosta. Polega on na wysyłaniu pakietów z ustawionym bitem DF (Don't Fragment) i nasłuchiwanie komunikatów ICMP sygnalizujących zbyt duży pakiet i brak możliwości jego fragmentacji. Jeżeli taki komunikat się pojawi, PMTUD zmniejsza rozmiar pakietu i ponawia próbę jego wysłania. Dzięki temu TCP jest w stanie znaleźć optymalny MSS (Maximal Segment Size, maksymalny rozmiar segmentu danych).

3. Ataki blind icmp

Ataki blind icmp nazywają się 'ślepe' dlatego że do ich przeprowadzenia nie jest potrzebne sniffowanie połączenia. Do przeprowadzenia każdego z nich wystarczy znać cztery parametry:

- adres IP źródła
- adres IP przeznaczenia
- port źródłowy
- port docelowy

Jak wiemy numery portów mieszczą się w zakresie 0-65535, jednak zwykle jesteśmy w stanie przewidzieć jakie wartości będą one przyjmować. Np. sesje BGP zwykle używają portu nr 194. Windows dla połączeń wychodzących używa portów 1025-4999. Połączenia wychodzące zza maskarady mają zwykle numery portów większe od 60000. Jasne jest że nawet nie znając konkretnych wartości jesteśmy w stanie zawęzić nasze poszukiwania do akceptowalnych zakresów. Dla przykładu zerwanie połączenia TCP za pomocą komunikatu ICMP Destination Host Unreachable znając docelowe i źródłowe IP i port jednego z hostów, zawężając zakres nieznanego portu do 1025-4999 na łączy o przepustowości 128kbps trwa... 12 sekund.

Aby zerwać połączenie atakujący musi wysłać do którejkolwiek ze stron pasujący do numerów portów komunikat ICMP rodzaju hard error. Jak napisałem powyżej

nieznajomość jednego z portów *nie jest problemem*. Zgodnie ze specyfikacją TCP musi natychmiast zerwać połączenie. Na szczęście większość poważnych systemów operacyjnych (*BSD, Linux, Windows, IOS) jest już przed nim zabezpieczona.

Drugi atak polega na ciągłym wysyłaniu komunikatów "fragmentation needed and DF bit set" co zmusza PMTUD do zmniejszanie MSS dla połączenia, które przy drastycznie małych wartościach MSS praktycznie uniemożliwia komunikację (Patrz opis PMTU Discovery). Jest to atak najniebezpieczniejszy ponieważ większość systemów nie jest na niego odporna. Sesje BGP (Border Gateway Protocol) okrojone w ten sposób z przepustowości do nieprzyjemnie małych wartości przestają spełniać swoją funkcję co skutkuje poważnymi problemami z komunikacją w sieci opartej o BGP.

Trzeci atak bazuje na komunikatach ICMP Source Quench. Zgodnie z RFC mają one zmuszać host do zmniejszenia prędkości na ok. 10 minut. Stopień zagrożenia tym atakiem jest znikomy ponieważ większość systemów ignoruje komunikaty Source Quench.

4. Przeciwdziałanie

Zostały opracowane różne strategie przeciwdziałania atakom blind icmp, m.in zmiana reakcji TCP na hard errors, sprawdzanie TCP Sequence Number oraz zabezpieczona wersja mechanizmu PMTUD.

Zmiana reakcji polega na traktowaniu hard errors jako soft errors dla nawiązanego połączenia i poleganie na mechanizmach warstwy wyższej do wykrywania problemów z połączeniem, co od ponad 10 lat robią systemy z rodziny BSD oraz Linux.

Sprawdzanie numerów sekwencyjnych polega na ustaleniu czy numer ten mieści się w zakresie numerów sekwencyjnych pakietów już wysłanych na które jeszcze nie otrzymaliśmy potwierdzenia.

Metodą zaproponowaną przez Fernando Gonta jest opóźnianie reakcji na icmp hard error do czasu osiągnięcia określonej liczby nieudanych prób retransmisji odpowiadającego komunikatowi pakietu.

Przeciwdziałanie atakom bazującym na ICMP Source Quench polega na ich kompletnym ignorowaniu, ponieważ badania wykazały że jest on nieprzydatny i nie spełnia swojego zadania w sieci. Linux i BSD od wielu lat ignorują ICMP Source Quench.

Zabezpieczenie mechanizmu PMTUD najprościej realizować poprzez opóźnianie reakcji na błędy w celu upewnienia się że pakiet nie został doręczony. Bardziej skomplikowane mechanizmy zaproponowane przez Fernando wykraczają poza zakres tego dokumentu, warto jednak wiedzieć że zostały one w roku 2005 zaimplementowane w systemy NetBSD i OpenBSD.

Obecnie podatne na te (wszystkie lub niektóre, głównie atak na PMTUD) ataki są m.in. wszystkie urządzenia Cisco działające pod kontrolą systemu IOS i systemy Microsoftu, co umożliwia bardzo poważne ataki DoS (Denial of Service - odmowa usługi) na sieci kontrolowane przez te systemy.

Na dzień dzisiejszy (13 września 2005) najbardziej niebezpieczny jest atak na PMTUD, ponieważ wciąż można za jego pomocą przeprowadzać DoS na połączenia TCP. Zaleca się wszystkim administratorom systemów podatnych na ten atak wyłączenie mechanizmu PMTUD lub/i ignorowanie komunikatów fragmentation needed and DF flag set, do czasu wydania stosownych patchy przez producentów oprogramowania.

Literatura:

- draft Fernando Gonta
<http://ietfreport.isoc.org/idref/draft-gont-tcpm-icmp-attacks/>
- dokumenty RFC nr 1222, 792, 1192

Podziękowania: Fernando Gont, Tomasz Huć, Olgierd Pieczul