Protokół DHCP

Patryk Czarnik

Bezpieczeństwo sieci komputerowych – MSUI 2009/10

DHCP – *Dynamic Host Configuration Protocol*

Zastosowanie

- Pobranie przez stację w sieci lokalnej danych konfiguracyjnych z serwera
- Dotyczy zwykle konfiguracji sieci IP:
  - adres IP, maska podsieci
  - adres routera
  - adres serwera DNS
- Inne możliwości:
  - lokalizacja obrazu systemu (zwykle adres dla protokołu TFTP)

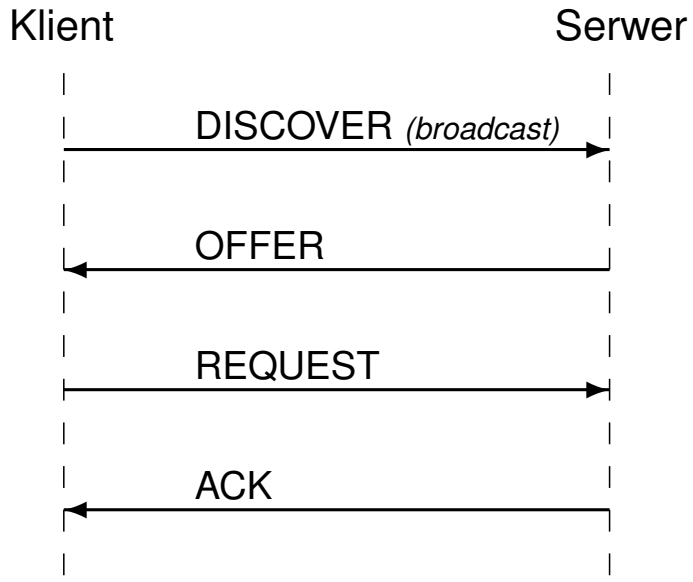
Polityki przypisania adresu IP

- ręczne (stała tabelka)
- automatycznie (na stałe)
- dynamiczne (na określony okres czasu)

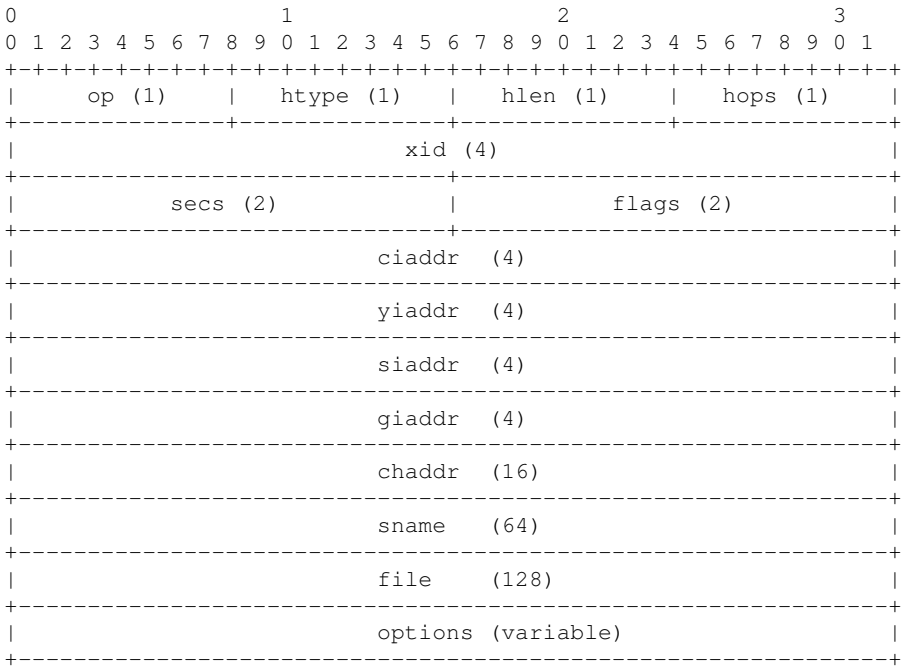
Historia i standaryzacja

- 1985 – BOOTP (*Bootstrap Protocol*)
  - dla bezdyskowych stacji roboczych,
  - poznanie własnego adresu IP oraz położenia obrazu rozruchowego do załadowania systemu operacyjnego.
- 1993 – RFC 1531
  - pierwsza wersja DHCP.
- 1997 (RFC 2131, 2132)
  - obecnie stosowana wersja.
- DHCPv6 (RFC 3315)
  - DHCP dla IPv6.
- Authentication for DHCP Messages (RFC 3118)
  - rozszerzenia dla bezpieczeństwa.

Schemat komunikacji



DHCP – komunikaty



DHCP – problemy z bezpieczeństwem

DHCP zbudowane na niezabezpieczonym IP (UDP).
Zagrożenia:

Złośliwy serwer

- przypisywanie nieprawidłowych lub fałszywych adresów
- przypisywanie duplikatów adresów
- podawanie nieprawidłowych lub fałszywych adresów bramy, serwera DNS itp.

Złośliwy klient

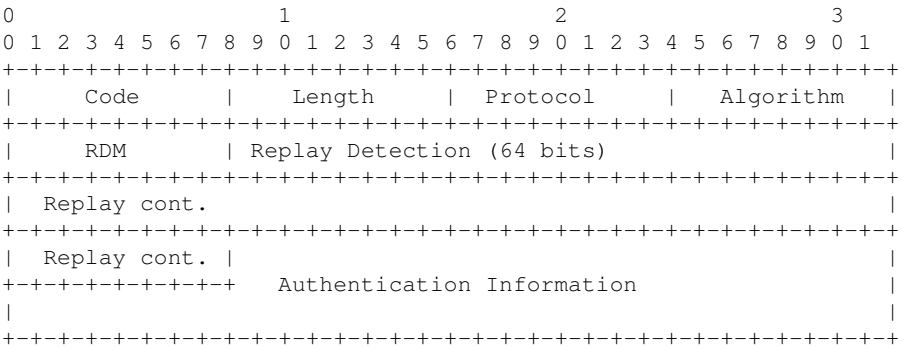
- zdobywanie informacji przeznaczonych dla innego klienta
- kradzież adresu IP (i często dostępu do sieci)
- przy dynamicznym przyznawaniu adresów możliwe wyczerpanie puli adresów serwera
- DoS na serwerze

DHCP – opcja uwierzytelnienia

- RFC 3118: wprowadzenie możliwości uwierzytelniania komunikatów DHCP
- Technicznie: opcja w komunikatach DHCP
- Dwa sposoby uwierzytelniania:
  - uwierzytelnienie przez znacznik
  - uwierzytelnienie opóźnione

Format opcja uwierzytelnienia

Format opcji w komunikacie

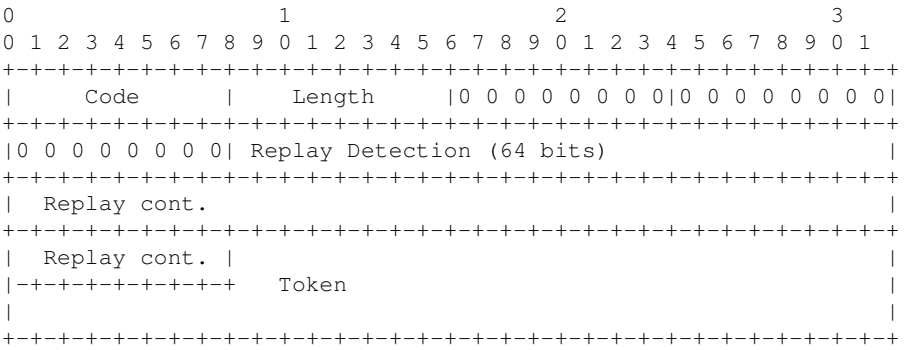


Uwagi

- Kod tej opcji – **90**
- Długość liczona od pola `Protocol`

Uwierzytelnienie przez znacznik

Format opcji w komunikacie



Idea

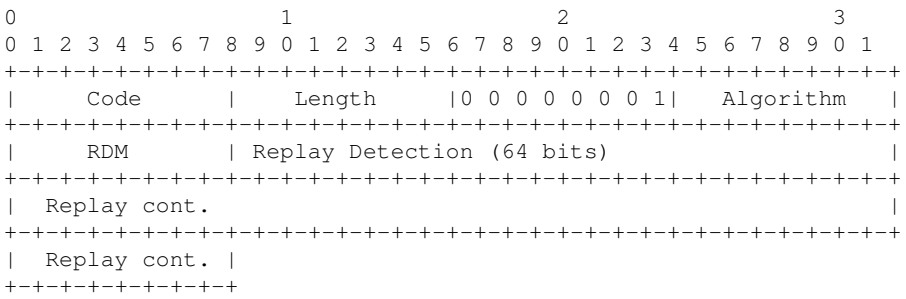
- Obie strony mają wspólny znacznik
- Znacznik jest przesyłany w opcji jawnym tekstem
- Jeśli znacznik w komunikacie nie zgadza się z lokalną kopią,
  to komunikat porzucany

Uwierzytelnienie opóźnione

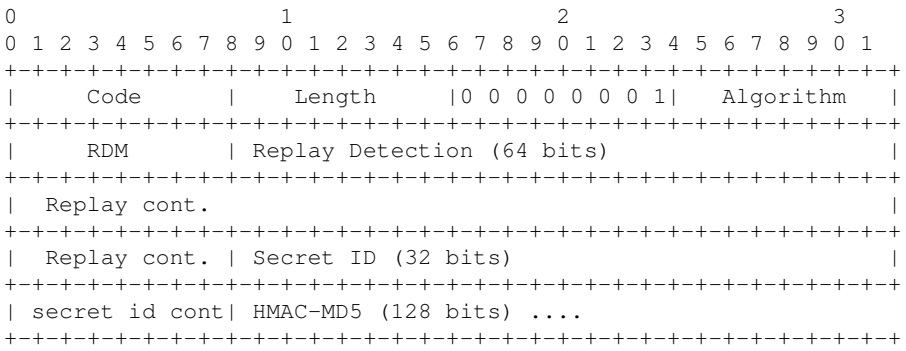
- Klient żąda uwierzytelnienia od serwera, komunikat zawiera m.in.:
  - identyfikator klienta (opcja 61),
  - unikalną wartość.
- Serwer podaje w odpowiedzi:
  - unikalną wartość od klienta,
  - identyfikator sekretu,
  - HMAC-MD5 z zawartości komunikatu DHCP (z wyjątkami) oraz wskazanego sekretu.
- Klient w kolejnych komunikatach także się uwierzytelnia dodając HMAC.

Uwierzytelnienie opóźnione – komunikaty

DISCOVER lub INFORM



OFFER, REQUEST lub ACK



Opcja uwierzytelniania – zagrożenia

- Znacznik łatwo przechwycić.
- Przy uwierzytelnianiu z opóźnieniem można zablokować dostęp do DHCP przez zalanie komunikatami początkowymi:
  - nasycenie sieci,
  - wyczerpanie adresów.
- Zalanie komunikatami uwierzytelnionymi – wykonywanie obliczeń kryptograficznych może zająć cały czas procesora.
- Podszycie się pod pośrednika DHCP (relay agent).

Opcja uwierzytelniania a pośrednicy DHCP

Problemy

Przy przekazywaniu komunikatów zmiana niektórych pól:

- pola ’giaddr’ i ’hops’
- opcja 81 (pośrednik)

Rozwiązanie

Do liczenia skrótu:

- pola ’giaddr’ i ’hops’ – wyzerowane
- opcja 81 – usunięta

- Zostało zaproponowane wprowadzenie podopcji – działanie jak w opcji DHCP.
- Podopcja zawiera identyfikator pośrednika.
- Podpis generowany jest z całego komunikatu DHCP w tym z
  - nagłówka DHCP,
  - opcji DHCP,
  - podopcji pośrednika.

Opcja uwierzytelniania a pośrednicy DHCP

Rozwiązanie bardziej ogólne

- Zostało zaproponowane („internet-draft”) wprowadzenie podopcji – działanie jak w opcji DHCP.
- Podopcja zawiera identyfikator pośrednika.
- Uwierzytelnianie pomiędzy każdymi pośrednimi węzłami na drodze komunikatu.
- Podpis generowany jest z całego komunikatu DHCP w tym z
  - nagłówka DHCP,
  - opcji DHCP,
  - podopcji pośrednika.

Opcja uwierzytelniania — implementacje

- Wzorcowa implementacja Internet Software Consortium
  `http://www.isc.org/products/DHCP/`
  dostępny dla większości systemów uniksowych i dla Windows.
- Program *ethereal* rozpoznaje pakiety RFC 3118.

Egzamin

- Prawie na pewno w piątek, 25 czerwca, o 18:00
- Czas trwania: 60 minut
- Test, 20 pytań po 3 odpowiedzi (8 możliwości)

Przykładowe pytania

- Protokół SSL:
  - ☐ A służy wyłącznie do zabezpieczania połączeń HTTP
  - ☐ B umożliwia ustalenie klucza sesji gdy żadna ze stron nie posiada certyfikatu
  - ☐ C umożliwia ustalenie klucza sesji w oparciu o certyfikat serwera i kryptografię klucza publicznego
- Pakiety między nadawcą a odbiorcą przechodzą przez NAT i podlegają translacji adresów. W takiej sytuacji w IPsec można skutecznie stosować:
  - ☐ A tryb tunelowy ESP
  - ☐ B uwierzytelnianie wraz z trybem transportowym ESP
  - ☐ C uwierzytelnianie przed szyfrowaniem

Przykładowe pytania

- Zmodyfikowany schemat Needhama-Schrödera:
  - ☐ A wymaga od serwera uwierzytelnienia (*authentication server*) znajomości hasła-klucza zleceniodawcy
  - ☐ B wymaga od serwera przepustek (*tickets server*) znajomości hasła-klucza zleceniodawcy
  - ☐ C wymaga od zleceniodawcy znajomości hasła-klucza serwera usługi
- Zabezpieczenie „przez znacznik” w DHCP:
  - ☐ A chroni przed wyczerpaniem całej puli adresów IP przez złośliwego klienta
  - ☐ B używa technik kryptograficznych do ochrony przed podsłuchaniem hasła-znacznika
  - ☐ C w pewnym stopniu chroni przed atakami intruzów nie mających wcześniejszego dostępu do danej sieci