Spis treści

1. Tytuł pracy

Studium możliwości zastosowania technik hashcash dla ograniczenia transmisji nielegalnych komunikatów w sieciach bezprzewodowych

Study of possibilities of thwarting transmission of illegal messages in wireless networks using the hashcash approach

2. Cel pracy

Niektóre rozproszone protokoły dla sieci bezprzewodowych są bardzo wrażliwe na rozpowszechnianie nielegalnych komunikatów przez niewłaściwie zachowujące się terminale lub sensory. Przykładem są fałszywe rekomendacje w systemach reputacyjnych lub lawiny uaktualnień tablic rutingowych. W pracy dokonana zostanie próba zastosowania technik sztucznego zwiększania kosztu transmisji przy pomocy funkcji umiarkowanie złożonych obliczeniowo.

3. Zadania do wykonania

1. Analiza kosztów transmisji, przetwarzania i odbioru w istniejących kartach bezprzewodowych.
2. Zapoznanie się z zasadami wykorzystania funkcji umiarkowanie złożonych.
3. Opracowanie przykładowego protokołu wykorzystującego schemat challenge-response.

4. Literatura

1. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," LNCS 740, Springer 1992, pp. 139–147

2. A. Back, "Hashcash - a denial-of-service countermeasure," 2002, referenced 2004 at http://www.hashcash.org/hashcash.pdf

5. Plan pracy

Po rozbiorze tytułu dokładne zapoznanie sie z ogólna wiedzą na temat techniki hashcash bezpośrednio związanej z tematem pracy.

Źródło:

1. Materiały internetowe (nie Wikipedia) z fachowych stron związanych z tematem pracy
2. Znalezienie literatury związanej z tematem
3. Literatura podana w tabeli pracy magisterskiej

Znalezienie wiarygodnych źródeł wiedzy na temat elementów zawartych w celu pracy (tabela):

1. Rozproszone protokoły sieci bezprzewodowych.
2. Rozpowszechnianie nielegalnych komunikatów przez terminale i sensory.
3. Rekomendacje w systemach rozproszonych.
4. Uaktualnienie tablic routingowych.
5. Techniki sztucznego zwiększania kosztów transmisji.
6. Funkcje umiarkowanie złożone obliczeniowo.

Wstępna analiza zadań do wykonania w pracy (analiza przykładów dla zrozumienia istoty zagadnienia):

1.Analiza kosztów (transmisji, przetwarzania, odbioru) w kartach bezprzewodowych.
2. Zasady wykorzystania funkcji umiarkowanie złożonych.
3. Przykładowy protokół wykorzystujący schemat challenge-response.

ad.1 (Koszty)

Zwiększenie kosztów operacji na procesorze komputera wysyłającego niepożądane, niechciane przez innych wiadomości.

Gdy koszt już nie w milisekundach lecz minutach to dobrze, bo już jakiś dodatkowy niemały koszt.

Przy sztucznej reputacji wzrost kosztów (reputacja wirtualna - wizerunek poprzez swoje informacje umieszczane w sieci).

ad.2 (Funkcje umiarkowanie złożone)

Funkcja umiarkowanie złożona: policzenie trudne, ale możliwe przy sporym koszcie (nie milisekundy lecz minuty).

Np. logarytm z wielu bitów ze wzrostem liczby bitów jest coraz trudniejszy do obliczenia; coraz szybciej narasta ilość operacji obliczeniowych; logarytm liczby całkowitej 200-bitowej praktycznie niewykonalny i robiony metodą prób i błędów nie jest już funkcją umiarkowanie złożoną; przy mniejszej ilości bitów (100?) trudne, sporym kosztem ale wykonalne

Mechanizm proof-of-work (nie co chwilę robione lecz trzeba się zastanowić).

Chodzi o to, by przy każdej próbie połączenia klient musiał wykonać pewną pracę (kosztowną obliczeniowo), serwer natomiast powinien być w stanie zweryfikować wykonanie tej pracy bez angażowania w to większych zasobów. „Uczciwy" klient takiego dodatkowego nakładu pracy w trakcie nawiązywania połączenia

prawdopodobnie nawet nie zauważy. Dla atakującego może to już być istotnym problemem, ponieważ nie będzie w stanie alokować zasobów na tyle szybko, by serwer nie nadążył ich zwalniać.

Atakujący może rozwiązać ten "problem" przez wykorzystanie większej ilości zasobów. Koszt takiego ataku wówczas jednak rośnie i przestanie on być atrakcyjny dla atakujących.

ad.3 (protokół wykorzystujący schemat challenge-response)

Schemat challenge-response:

Jest metodą oparta na zasadzie wyzwanie-odzew (zagadka-odpowiedź).

Ciężko funkcję policzyć, ale potem już bardzo łatwo zobaczyć, że dobrze policzona. Ktoś się dużo napracował, ale dla mnie bez dodatkowych kosztów sprawdzenie.

Protokół:

- wymyślić zasady zadania
- jak działa
- zasady wymiany informacji
- pokazanie, że faktycznie wykonuje zadanie
- w jaki sposób zniechęcić węzły by nie wykonywały

Protokół challenge-response oparty jest na uwierzytelnianiu.

Uwierzytelnianie (challenge-response) przebiega w jednym kierunku.

Sprawdzający wysyła wyzwanie i sprawdza otrzymaną odpowiedź, która powinna być zaszyfrowana kluczem połączeniowym. W przypadku wzajemnego uwierzytelniania proces musi być powtórzony z zamianą ról.

W celu ochrony przed atakami typu DoS (oznacza zwykle zalewanie sieci nadmiarową ilością danych mających na celu wysycenie dostępnego pasma, którym dysponuje atakowany host), czas odstępu pomiędzy kolejnymi próbami uwierzytelniania narasta wykładniczo do pewnej wartości maksymalnej. Nowy klucz szyfrujący jest wytwarzany na podstawie klucza połączenia, dla każdej sesji inny.