POLITECHNIKA BIAŁOSTOCKA

WYDZIAŁ INFORMATYKI

KATEDRA

PRACA DYPLOMOWA

TEMAT: BRAK TYTUŁU

WYKONAWCA: BRAK AUTORA

.....

podpis

PROMOTOR:

BIAŁYSTOK 2019 r.

Karta dyplomowa

Politechnika Białostocka Wydział Informatyki	Studia	Numer albumu studenta:
		Rok akademicki
Katedra		Kierunek studiów: Specjalność:

Brak autora

TEMAT PRACY DYPLOMOWEJ: Brak Tytułu

Zakres pracy:

.....	.....
Imię i nazwisko promotora podpis	Imię i nazwisko kierownika katedry - podpis

.....	.....	.....
Data wydania tematu pracy dyplomowej - podpis promotora	Regulaminowy termin złożenia pracy dyplomowej	Data złożenia pracy dyplomowej - potwierdzenie dziekanatu

.....	.....
Ocena promotora	Podpis promotora

.....	.....	.....
Imię i nazwisko recenzenta	Ocena recenzenta	Podpis recenzenta

Spis treści

1. Wstęp

Anomalią ruchu sieciowego nazywamy każde odstępstwo od wcześniej obserwowanego wzorca przepływu danych w sieci komputerowej. Wykrywanie takich zjawisk może być wykorzystane m.in. w procesie zabezpieczania sieci (systemy wykrywania intruzów) lub w systemach wykrywania/zapobiegania awariom network failure. Niezależnie od tego, czy ruch sieciowy rozpatrujemy jako pewną ilość przepływów flows czy też analizujemy przesyłanie poszczególnych jednostek transmisyjnych, rozmiar danych analizowanych jest zawsze olbrzymi. Dodatkowo wykrywanie anomalii jest z samego założenia procesem, który powinien być realizowany w czasie pracy sieci, co z kolei stawia określone wymagania dotyczące szybkości przetwarzania. Uzasadnione zatem wydaje się podejście oparte na analizie danych agregowanych. Stosowanie metod statystycznych w procesie analizy utrudnia ich interpretację w odniesieniu do realnych zdarzeń w sieci komputerowej. Wykrywanie anomalii ruchu sieciowego jest jednym ze sposobów identyfikacji naruszeń bezpieczeństwa sieci komputerowej oraz wykrywania uszkodzeń sieci.

Celem pracy jest analiza dynamiki protokołu komunikacyjnego ARP w lokalnej sieci Ethernet...

Praca podzielona jest na pięć rozdziałów. W rozdziale drugim przedstawiono przegląd literatury dotyczący metod badań sieci komputerowych. W rozdziale 3 ..... W rozdziale czwartym przedstawiono wyniki analizy zmian w czasie ilości ramek ARP rejestrowanych w jednominutowych przedziałach czasu. Badania przeprowadzono w małej akademickiej sieci komputerowej składającej się z 42 komputerów.

Listing 1.1: Zwycieżca 14th International Obfuscated C Code Contest w kategorii Best Self-Documenting - Tom Torfs

```
#include <stdio.h>
#include <stdlib.h>

int main(int a,char **A){FILE*B;typedef unsigned long C;C b
[8]; if(!(a==7&&(B=fopen(1[A],"rb")))) return 1;for(7[b]=0
;7[b]<5;7[b]++)b[7[b]]=strtoul(A[2+7[b]],0,16-!7[b]*6);5[
b]=3[b]; while((6[b]=getc(B)
)!=(C)-1){if(2[b])for(7[b]=0
```

```
;7[b]<4          ;7[b]++      )if(((6      [b]>>7[
b])^(6[          b]>>(7-7[b])))&1)6[      b] ^=(1
<<7[b])          ^(1<<(7-7[b]));5[b]      ^= 6[b]
<<(0[b]          -8);for(7[b]=0;7[b]      <8;7[b]
++)if((          5[b]>>(0[b]-             1))&1)5
[b]=(5[          b]<<1)^ 1[b];            else 5[
b]<<=1;          }5[b]&=((((C)1           <<(0[b]
-1))-1)          <<1)|1; if(2[b]          )for(7[
b]=0;7[          b]<(0[b ]>>1);7          [b] ++)
if(((5[b]>>7[b])^(5      [b]>>(0  [b]-1-7      [b])))&1)5[b]^=((C)
1<<7[b])^((C)1<<(0[      b]-1-7[   b]));5[     b]^=4[b];fclose(B);
printf("%0*lX\n", (      int)(0[     b]+3)>>   2,5[b]); return 0;}
```

2. Metody badania sieci komputerowych

Analiza ruchu sieciowego to proces pozwalający na pozyskiwanie wiedzy dotyczącej pracy sieci komputerowej. Wiedza ta może zostać wykorzystana do usprawnienia zarządzania siecią (wykrywania uszkodzeń, błędnej konfiguracji itp.) [**?**] lub do wykrywania naruszeń bezpieczeństwa sieciowego [**?**] . Zakłócenia normalnego funkcjonowania sieci nazywa się anomaliami sieciowymi. Wykrywanie takich anomalii jest jednocześnie kluczem do wykrywania uszkodzeń lub ataków sieciowych [**?**]. Badanie ruchu sieciowego wymaga skonstruowania modeli takiej aktywności [10,11] oraz opracowania metod analizy zebranych danych. Można wyróżnić przynajmniej dwie grupy technik analizy ruchu sieciowego. Jedną z nich jest wnikliwa analiza pakietów (deep packet inspection) [21] wykorzystywana np. w przełącznikach aplikacyjnych (tzw. content switch). Drugą grupą technik są analizy ruchu zagregowanego [**?**, **?**].

3. ARP

Badania dynamiki zmian w czasie ilości ramek ARP przeprowadzono w małej lokalnej sieci komputerowej składającej się z 42 urządzeń. W sieci znajdowały się:

- przełącznik (Allied Telesyn) pracujący jako brama internetowa,
- router (Cisco),
- trzy serwery (dwa Windows i GNU/Linux),
- komputery pracowników naukowych głównie z systemem Windows.

Analizowano szeregi minutowych ilości ramek ARP. Analizowano szeregi zawierające ramki odnoszące się do pięciu najbardziej aktywnych urządzeń. Wykaz badanych urządzeń pokazano w Tabeli 3.1.

3.1 Metody analizy

Wykresy rekurencyjne wykorzystywane są do oceny stopnia aperiodyczności układów nieliniowych. Pomocne są również w analizie wielowymiarowej przestrzeni fazowej w której zrekonstruowany jest atraktor. Wykres rekurencyjny jest zawsze dwuwymiarowy mimo, że może reprezentować zachowanie układu wielowymiarowego. Wykres rekurencyjny opisany jest zależnością:

$$R_{i,j} = H(\varepsilon_i - \|x_i - x_j) \tag{3.1}$$

$P \xrightarrow{\tau} P'$ definicja ...:

a) a.

b) i b.

Nazwa urządzenia	Typ
dev0	przełącznik (Allied Telesyn)
dev1	router (Cisco)
dev2	serwer Windows
dev3	serwer GNU/Linux
dev4	komputer pracownika naukowego

Tabela 3.1: Wykaz badanych urządzeń

Spis listingów

Spis rysunków

Spis tabel

OŚWIADCZENIE

Ja, niżej podpisany, wyrażam / nie wyrażam zgody na udostępnienie mojej pracy dyplomowej, pt: „Tytuł pracy” w Bibliotece Politechniki Białostockiej

.....

data, podpis czytelny