Atacuri distribuite în Internet

Mihai Budiu — mailto:mihaib+@cs.cmu.edu
http://www.cs.cmu.edu/~mihaib/

iunie 2001

Subiect: o evaluare a numărului de atacuri distribuite de sabotaj al serviciilor în Internet

Cunoştinţe necesare: cunoştinţe elementare despre funcţionarea Internetului

Cuvinte cheie: atac distribuit (DDoS: distributed denial of service), rutare, pachet, împrăştiere (back-scatter)

Cuprins

1 Internetul: capcane la fiecare pas

Într-un articol anterior din PC Report arătam că Internetul a fost construit ca reţea militară, pentru a rezista chiar şi unor atacuri nucleare. Deşi nu a fost testat în condiţii atît de dramatice, putem însă afirma că arhitectura sa se ridică la înălţimea aşteptărilor.

Proiectanţii însă nu au conceput reţeaua pentru a rezista unui alt tip de atac: din interior. Acum, cînd reţeaua s-a întins la dimensiuni neimaginate, această lipsă se dovedeşte foarte gravă.

Dimensiunea uriaşă a reţelei, numărul enorm de calculatoare cuplate, existenţa a zeci de bug-uri în implementărilor programelor care se execută pe aceste calculatoare, şi intenţiile duşmănoase a cîtorva inşi formează un cocteil exploziv. Situaţia se înrăutăţeşte pe zi ce trece, şi cracker-ii sunt într-o cursă continua cu proiectanţii reţelei şi cu administratorii de sistem, care încearcă să remedieze defecţiunile acesteia. Din păcate, aceasta este un război la al cărui început abia asistăm, şi care nu are un sfîrşit previzibil în viitorul apropiat.

În acest articol voi discuta doar despre un anume tip de atac electronic, în care victima primeşte o cantitate enormă de pachete care îi consumă toate resursele, împiedicînd-o să funcţioneze normal. Deşi acest gen de atac nu extrage nici un fel informaţii de la victimă, el poate fi foarte costisitor; acest gen de atac a fost observat pentru prima oară cu aproximativ un an şi jumătate în urmă şi a ajuns pe prima pagină a multor ziare datorită numelor importante ale victimelor: Yahoo, CNN, ebay, etc.

În textul de faţă vom vedea cum, la ora actuală, orice ins mînat de intenţii rele poate pune în genunchi practic orice site din Internet, oricît de sofisticat, împiedicîndu-l să funcţioneze. Vom vedea de asemenea că acest lucru se întîmplă foarte frecvent, şi că în fiecare zi se desfăşoară sute de astfel de atacuri. În fine, vom vedea că, în mod extrem de surprinzător, România se clasează pe locul întîi în lume într-un trist clasament, al ţărilor după numărul de victime ale unor astfel de atacuri.

2 Funcţionarea Internetului

Pentru a putea înţelege cum funcţionează un atac distribuit de genul menţionat, şi mai ales pentru a înţelege cum a putut fi măsurat numărul de atacuri din întreaga reţea fără participarea voită a vreunui atacator sau victime, va trebui sa facem o scurtă incursiune în tehnologiile care fac Internetul sa funcţioneze. Vom recapitula pe scurt, şi uşor simplificat, funcţionarea rutării în Internet; am tratat acest subiect pe larg în numere anterioare din PC Report.

Calculatoarele din Internet pot fi clasificate în două mari categorii: noduri terminale şi rutere. Nodurile terminale sunt majoritare, şi sunt punctele care oferă sau accesează informaţia. Ruterele sunt calculatoare specializate, al căror scop este doar să transporte informaţia între punctele terminale.

Toate calculatoarele cuplate la Internet au cel puţin o adresă Internet, numită adresă IP; adresele sunt unice, şi identifică în mod ne-ambiguu calculatoarele. (Un calculator care este cuplat simultan la mai multe reţele va avea mai multe adrese; adresele sunt unice, în sensul că fiecare adresă se întîlneşte într-un singur loc în Internet.) O adresă IP este un simplu număr întreg pe 32 de biţi, care în mod tradiţional este scris indicînd valorile celor patru octeţi separate cu punct; de exemplu: 194.102.154.13.

Cînd un calculator vrea să comunice cu un altul, trebuie întîi să îi afle adresa IP. Pentru că utilizatorii în general numesc calculatoarele folosind nişte şiruri de caractere, de exemplu `www.netreport.ro`, un serviciu special din Internet, numit serviciul de nume, traduce fiecare astfel de şir de caractere într-o adresă IP.

După ce un calculator a aflat adresa destinaţiei cu care vrea să comunice, sparge datele pe care le are de transmis în pachete pe care le trimite în mod individual. Fiecare pachet conţine datele de transmis, adresele IP ale sursei şi destinaţiei, şi adesea şi alte informaţii utile, de exemplu cîte pachete au fost deja trimise şi dacă sursa vrea ca recepţia să fie confirmată. Acest pachet este dat unui ruter.

Ruterele fac doar două lucruri în viaţă: (1) discută între ele pentru a afla în care parte se află fiecare calculator cuplat la Internet (adică învaţă *topologia* Internetului) (2) cînd primesc pachete pentru o anumită adresă, folosesc informaţia despre topologie pentru a trimite pachetul spre destinaţie. Dacă totul funcţionează bine, un pachet de date sare din ruter în ruter, la fiecare pas fiind mai aproape de destinaţie, pînă cînd este livrat.

Destinatarul descifrează pachetul, şi dacă sursa se aşteaptă la un răspuns (de exemplu o confirmare), răspunde folosind aceeaşi metodă, construind un nou pachet de date. Pentru a afla care este sursa de unde i-a venit pachetul, destinatarul se uită la adresa IP a sursei, aflată în interiorul pachetului primit.

3 Atacuri distribuite de sabotare a serviciilor (DDoS)

Dacă aţi citit descrierea de mai sus cu atenţie, poate aţi observat o primă slăbiciune a Internetului: am zis că pachetul cu date este compus de sursă. Sursa pune înauntru toate informaţiile necesare pentru a trimite pachetul în cealaltă parte, inclusiv propria ei adresă. Asta implică însă ca avem încredere în sursă, ca nu va trimite pachete malformate, şi ca nu va minţi în ceea ce priveşte propria ei adresă.

Într-adevăr, ruterele nu verifică dacă sursa unui pachet pe care îl primesc este corectă, şi în general nici nu pot face aşa ceva, pentru că ruterele pot primi pe aceeaşi sîrmă pachete de la zeci de milioane de adrese diferite. Unul din ingredientele care face atacurile distribuite atît de ucigaşe este chiar aceasta: sursele pot minţi în ceea ce priveşte propria lor identitate, punînd valori arbitrare în pachet. Această tehnică se numeşte în jargon "spoofing" (în română asta s-ar traduce aproximativ prin escrocherie).

De ce este importantă tehnica de "spoofing"? Pentru că împiedică *filtrarea* pachetelor bazate pe sursă!

La ora actuală toate companiile care au o prezenţă importantă pe Internet (şi sunt din ce în ce mai multe astfel de companii) încearcă să se protejeze de atacurile informatice folosind "pereţi de foc" (firewalls). Un firewall este un fel de ruter special, care analizează traficul care trece spre companie, şi care elimină pachetele care arată suspect. Dacă un atacator naiv încearcă să inunde compania cu pachete, firewall-ul observă predominanţa pachetelor care vin de la o anumită adresă, şi le elimină în mod defensiv pe toate. În felul acesta, compania este protejată. Dacă atacatorul foloseşte însă spoofing, firewall-ul este neputincios, pentru că nu poate diferenţia pachetele de atac de cele legitime care ar veni de la acelaşi surse.

Atacatorii sunt însă şi mai malefici: pentru că, în general, companiile au servere foarte puternice, ele nu pot fi inundate dacă atacul porneşte de la un calculator obişnuit: acesta nu poate genera suficient trafic, şi adesea nu are destulă capacitate de reţea pentru a sufoca victima cu trafic[1]. Atacatorii au dezvoltat scule care funcţionează în două etape:

1. Atacatorii infiltrează viruşi sau viermi în zeci, sute sau chiar mii de calculatoare. Tehnologiile pentru acest gen de atac sunt cunoscute de foarte multă vreme, chiar dinainte de existenţa Internetului.

[1] În general, munca efectuată pentru a recepţiona un pachet este mult mai mare decît munca depusă pentru a-l trimite, deci atacatorii au un avantaj din pornire.

2. Calculatoarele infectate execută apoi un program de atac, care aşteaptă comenzi de la distanţă. Cînd primesc o astfel de comandă, toate aceste calculatoare pornesc simultan un atac concertat asupra victimei.

Aceste atacuri se numesc DDoS, de la Distributed Denial of Service. "Distributed" vine din faptul că atacul se face simultan de la multe calculatoare, iar "DoS" vine din faptul că atacul consumă resursele computaţionale ale victimei, şi nu fură sau distruge informaţie.

4 O evaluare a numărului de atacuri folosind "împrăştierea" (back-scatter)

În luna iulie 2001 va avea loc al Zecelea simpozion pentru securitate USENIX; acolo va fi prezentat un articol deosebit de interesant, care încearcă să estimeze numărul de atacuri DDoS din Internet. Cei trei autori sunt cercetători la universitatea din California din San Diego. Despre ultimul dintre autori, Stefan Savage, am mai scris chiar în PC Report, în contextul analizei unor slăbiciuni ale protocolului de transmisiune fiabilă a datelor în Internet, TCP.

Articolul despre DDoS se bazează pe o idee foarte simplă şi foarte elegantă: dacă pachetele de atac folosesc (spoof) adrese sursă absolut la întîmplare (uniform distribuite între 0 şi $2^{32}-1$), atunci cînd sursa va încerca să răspundă la un astfel de pachet, va trimite răspunsul unui calculator din Internet la întîmplare. Acest fenomen este numit de autori "împrăştiere" (back-scatter); o ilustraţie a sa este în figura 1 .

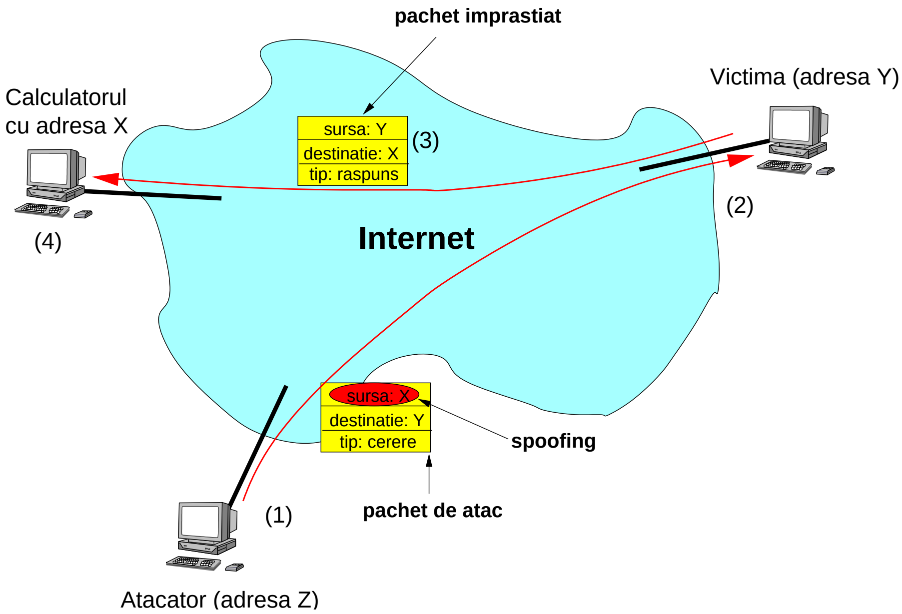

Figura 1: Împrăştierea pachetelor de răspuns la un atac. (1) Atacatorul inserează o adresă sursă arbitrară X în pachetul folosit pentru atac (2) Victima primeşte pachetul otrăvit (3) Victima răspunde calculatorului cu adresa X (4) Calculatorul de la adresa X primeşte un pachet de răspuns din senin

Această observaţie oferă cheia monitorizării atacurilor: dacă atacurile sunt suficient de multe ele vor putea fi observate de la orice calculator din Internet. Dacă aveţi un calculator care are adresa X, în medie la fiecare $2^{32} \approx 4$ miliarde de pachete de atac, acesta va primi un pachet-răspuns.

Asumpţia că adresele sunt generate la întîmplare este foarte importantă pentru a putea face o estimare statistică corectă; autorii au investigat toate pachetele software disponibile public pentru atacuri distribuite, şi în toate aceste programe adresa sursă este într-adevăr generată folosind numere aleatoare cu distribuţie uniformă (articolul citat discută pe larg şi alte scenarii posibile, şi trage concluzia că, dacă asumpţia de uniformitate nu e adevărată, rezultatele obţinute vor *subestima* numărul de atacuri, şi nu îl vor supraestima).

Autorii studiului au obţinut acces la un ruter care serveşte o reţea foarte mare (o reţea de clasă A, cum este numită), care conţine 2^{24} adrese, adică 1/256 din numărul total de adrese din Internet (ruterul este singura conexiune a acestei reţele la Internet). Lîngă acest ruter a fost instalat un PC, programat să noteze informaţii despre toate pachetele care circulă dinspre şi spre această reţea.

PC-ul a colectat date timp de trei săptămîni, în trei experimente de cîte o săptămînă, la scurt timp unul după altul. Datele colectate au fost apoi analizate separat (off-line), eliminînd traficul legitim, şi păstrînd numai pachetele împrăştiate (pachete de tip răspuns care vin fără o cerere iniţiată din interiorul reţelei).

Datorită asumpţiei de distribuţie uniformă, aceste pachete vor reprezenta în medie 1/256 din *întregul trafic din Internet* care reprezintă atacuri DDoS. Numărînd aceste pachete putem obţine estimarea amploarei fenomenului la scara mondială!

5 Numere îngrijorătoare

Rezultatele sunt foarte îngrijorătoare: în cele trei săptămîni au fost observate 200 de milioane de pachete de acest gen. Acest trafic trebuie înmulţit cu 256 pentru a obţine traficul din întregul Internet: 51 de miliarde de pachete! Considerînd că acest trafic este focalizat pe un număr relativ mic de victime, dimensiunile sunt înfricoşătoare.

(Să observăm că, din moment ce orice calculator din Internet primeşte pachete împrăştiate, şi că în medie fiecare calculator va primi unul din fiecare 4 miliarde de pachete, chiar şi calculatorul dumneavoastră observă în medie 1 pachet împrăştiat la fiecare două zile. Deci chiar şi dumneavoastră aţi putea efectua măsurători, ceva mai puţin precise, despre magnitudinea fenomenului, fără a avea la dispoziţie resursele din articolul descris!)

Dar pachetele captate conţin multe alte informaţii. De exemplu, conţin adresele victimelor, care răspund la pachetele-atac. Din tipul de pachet se poate infera tipul de atac. Folosind distribuţia pachetelor în timp, autorii au încercat să atribuie pachetele unor atacuri distincte şi să măsoare frecvenţa, durata şi intensitatea atacurilor.

Autorii deduc ca au asistat la 12800 de atacuri în această perioadă, asupra a 5000 de victime distincte. Cele mai lente atacuri aveau cîte 50 de pachete/secundă (observate la victimă), iar cele mai puternice peste 15000 de pachete/secundă. Cel mai intens avea peste două treimi de milion de pachete/secundă!

Studiind soluţiile disponibile comercial pentru a contracara atacurile de acest gen, autorii afirmă ca un atac de 500 de pachete pe secundă poate pune în genunchi un server mic, şi că un firewall sofisticat poate tolera pînă la 14000 pachete/secundă. Ca atare, multe din atacurile observate sunt ucigătoare pentru companii mici, şi unele dintre ele pot fi fatale şi pentru instalaţii deosebit de scumpe şi sofisticate.

Durata atacurilor este în medie scurtă: 50% din atacuri durează mai puţin de 10 minute, dar 2% din atacuri durează ore, cîteva zeci de atacuri fiind neîntrerupte timp de mai multe zile consecutive.

Cele mai multe victime (65%) au suferit un singur atac, 18% suferind două atacuri. Dar unele victime au suferit multiple atacuri, uneori mai multe atacuri diferite simultan!

Cele mai multe atacuri vizează sistemul de operare şi capacitatea lui de a procesa pachete[2]. Unele atacuri sunt însă direcţionate spre aplicaţiile care se execută pe calculatorul atacat, cum ar fi servere de web sau servere de chat. Un număr relativ mic de atacuri loveşte în puncte foarte importante pentru infrastructura Internetului: servere de nume şi rutere. Deşi aceste atacuri sunt puţine, impactul lor poate fi enorm, pentru că pot afecta toată porţiunea de reţea care depinde de serverul sau ruterul afectat. Cam 1-3% dintre atacuri sunt de acest tip.

6 România: locul I în lume pe ţări la atacuri distribuite

În pachetele împrăştiate se găseşte o mulţime de informaţie foarte interesantă. În mod ironic, lipseşte tocmai informaţia cea mai utilă, şi anume identitatea reală a atacatorului! La ora actuală *nu există nici o metodă prin care aceasta poate fi aflată*, cel puţin pentru atacurile care folosesc spoofing. Felul în care poate fi depistată sursa reală a acestor atacuri este un subiect fierbinte de cercetare, dar este destul de departe de a fi rezolvat în mod practic.

Pe lîngă toate aceste statistici, autorii au încercat să traducă adresele IP ale victimelor în adrese simbolice (nume) şi au clasificat atacurile după domeniul şi ţara de destinaţie ale victimelor.

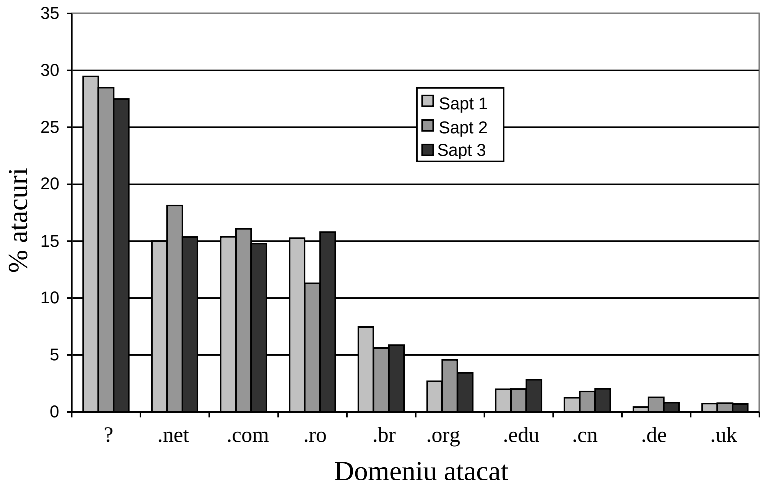

Figura 2: Procente din atacurile DDoS grupate după sufixul domeniului victimei. Semnul întrebării indică calculatoare pentru care nu a putut fi determinat numele pornind de la adresa IP.

Rezultatele sunt iarăşi deosebit de interesante. Figura 2 arată distribuţia atacurilor după sufixul domeniului atacat, pentru fiecare din cele trei săptămîni. După cum se vede, atacurile sunt relativ neschimbate de la o săptămînă la alta. Cam 30% din atacuri nu au putut fi clasificate (nu este

[2] Adică sunt trimise spre un port ales la întîmplare

întotdeauna posibil să se translateze o adresă IP într-un nume); e posibil ca în acest grup să fie calculatoare din domeniul militar cu sufixul `.mil`, care nu apare în această figură.

Domeniile `.net` şi `.com` sunt oarecum de aşteptat (cu cîte 15% fiecare), dar autorii îşi exprimă surpriza pentru poziţia a patra, prima care aparţine unei ţări: sufixul este `.ro`. Autorii nu îşi explică cum de o ţară, care în materie de infrastructură Internet este departe de a fi fruntaşă, conţine un număr atît de mare de victime. După noi urmează, la mare distanţă, în ordine Brazilia, domeniile ne-comerciale `.org` şi `.edu`, şi abia apoi China, Germania şi Marea Britanie.

Încercarea de a mapa adresele pe domenii administrative arată că pe locul 1 în lume ca număr de atacuri este domeniul Starnets, care este un ISP (Internet Service Provider) din România, care a fost victima a 5% din toate atacurile din Internet din perioada monitorizată.

Autorii articolului încearcă să depisteze şi genul de victimă; din faptul că multe din nodurile atacate sunt foarte mici, sau chiar calculatoare conectate prin modem sau cablu, ei presupun că unele atacuri sunt de fapt vendette între hackeri.

Îmi permit să ghicesc că, în ceea ce priveşte victimele din România, atacatorii sunt co-naţionali (nu vad motivaţia pentru care atacatori din exterior ar bombarda ţinte româneşti cu atîta statornicie). Asta înseamnă că suntem în top şi ca intensitate a activităţii distructive pe Internet. Dacă raportăm la populaţie, sau la numărul de calculatoare conectate, conjencturez că suntem clar pe poziţia întîi în lume.

7 Concluzii (în loc de soluţii)

Voi încheia acest text cu un citat dintr-o publicaţie recentă despre securitatea reţelelor; citatul aparţine domnului Bruce Schneier, un expert în domeniul securităţii informatice:

> În război informaţia este putere. Cu cît îţi înţelegi mai bine inamicul, cu atît vei fi mai capabil să-l înfrîngi. În războiul împotriva hacker-ilor duşmănoşi, a celor care "sparg" reţele, şi a altor "pălării negre" din ciber-spaţiu, cei de partea binelui au surprinzător de puţine informaţii. Cei mai mulţi profesionişti din securitate, chiar şi cei care proiectează scule de securitate, ignoră uneltele, tacticile şi motivaţiile inamicilor. Şi această stare de fapt este favorabilă inamicilor.

Un studiu precum cel prezentat în acest text nu oferă soluţii, dar chiar cuantificînd dimensiunea şi natura problemei avem o bază de pornire de la care putem proiecta eventuale metode de apărare.

La ora actuală nu există soluţii eficace împotriva atacurilor DDoS. O soluţie parţială, care ar reduce mult gravitatea acestor atacuri, constă în filtrarea traficului *la intrarea* în reţea (ingress filtering). De exemplu, un ruter plasat între o reţea cu adrese de forma 128.x.x.x şi Internet, nu ar trebui sa accepte pachete care vin din această reţea dar care au adrese de altă formă. Acest gen de filtrare se poate face doar la marginile reţelei; un ruter din centru are mult mai puţin control asupra direcţiei din care pot veni pachete. Filtrarea ar reduce enorm eficacitatea metodei "spoofing", pentru că marea majoritate e pachetelor ar fi distruse de rutere înainte de a intra în Internet.

Deşi filtrarea la intrare este relativ simplu de implementat, problema constă în marele număr de rutere deja existente care nu folosesc această metodă, şi în numărul enorm de ISP-uri (Internet Service Providers) care ignoră gravitatea acestor atacuri şi nu îşi reconfigurează ruterele în mod corespunzător.

La ora actuală nu există însă nici o soluţie practică pentru a determina cine a pornit atacul, şi nici măcar pentru a determina exact calculatoarele care efectuează atacul (care de obicei nu aparţin atacatorului ci au fost infectate).

Metode extra-tehnologice pot face parte din soluţie: dacă atacurile informatice sunt recunoscute ca activităţi ilegale, şi cei care le efectuează sunt aspru pedepsiţi (atunci cînd sunt descoperiţi), se poate eventual reduce motivaţia atacatorilor.

Dintr-un punct de vedere ştiinţific însă, fenomenul Internetului este absolut fascinant, iar evoluţia sa este plină de surprize. Şi suntem abia la început!

8 Alte surse de informaţie

- Articolul pe care este bazată această prezentare conţine multe alte informaţii foarte detaliate, şi poate fi găsit la `http://www.caida.org/outreach/papers/backscatter/index.xml`: "Inferring Internet Denial-of-Service Activity", de David Moore, Geoffrey M. Voelker şi Stefan Savage, de la universitatea California din San Diego. Acest articol va fi prezentat la a Zecelea simpozion de securitate USENIX în luna iulie, 2001.

- Citatul de la finalul articolului de faţă aparţine domnului Bruce Scheneier, un expert în probleme de securitate electronică; extrasul este din numărul din luna iunie 2001 a publicaţiei sale electronice lunare Criptogram: `http://www.counterpane.com/crypto-gram-0106.html`.

- Articolul meu despre rutarea în Internet, din PC Report din mai 1998: `http://www.cs.cmu.edu/~mihaib/articles/articles.html#internet`.

- Un articol de Iosif Fettich, care descrie primele atacuri distribuite înregistrate în Internet, în PC Report din martie 2000: `http://www.pcreport.ro/pcrep90/0192.shtml`.

- Povestea trepidantă despre disecţia unui atac distribuit de către o victimă administrator de sistem şi descoperirile acestuia despre tehnologiile atacatorilor: `http://grc.com/dos/grcdos.htm`

- Articolul meu din PC Report mai 2000, despre colaborare şi concurenţă în Internet, bazat pe o expunere a lui Stefan Savage (unul dintre autorii articolului pe care se bazează prezentarea de faţă): `http://www.cs.cmu.edu/~mihaib/articles/articles.html#tcp`.