COMPUTERWORLD

# Den ultimative anonymitet når du kommunikerer på Internettet.

## TOR er et rigtigt spændende projekt der arbejder med anonymitet for dagens Internetbrugere. Artiklen er ikke teknisk og indeholder ingen vejledning i brug, kun en beskrivelse af principper og historien bag.

Skrevet den **04. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Kryptering** | ★★★☆☆

**Den ultimative anonymitet når du kommunikerer på Internettet.**

Internettet er fyldt med spændende historier, projekter, organisationer, myter og ideer, en af de mere spændende er Tor. Tor handler om anonymitet, sikkerhed, integritet og fortrolighed, og vi kan alle være med til at udbrede og udvikle ideen.

**Et overblik**

Tor er i virkeligheden to ting. Det er dels et netværk af virtuelle tunneler hvorigennem personer eller grupper af personer kan kommunikere sikkert og anonymt over Internettet.
Tor er også en platform eller et idegrundlag for udviklere med hvilket de kan skabe nye kommunikations værktøjer, der har Tor's privacy features indbygget.

**Hvad kan Tor så bruges til**

Når du bruger Internettet via Tor, vil det have indflydelse på alt det du gør. De web sites du besøger, vil ikke kunne logge en IP adresse og dermed ikke tracke hvorfra du kommer. News group servere vil heller ikke kunne logge eller blokerer din IP adresse da denne skifter hele tiden, for instant messaging som MSN messenger eller ICQ vil det samme gælde, og du kan heller ikke IP blokeres i din egen ende, da svarene også kommer fra nye og hele tiden skiftende IP adresser.
Tor's netværk lader dig også publicere web sites eller Internet services uden at sitets eller servicens placering (i form af IP adressen) afsløres. Dette kunne f.eks. være relevant for services der håndterer socialt følsomme emner som f.eks. chat rooms for voldsofre eller for folk med forskellige sygdomme.

**Hvorfor Tor**
Det Tor gør er at umuliggøre det der kaldes Trafikanalyse. Trafikanalyse handler om at indsamle oplysninger om din opførsel og dine vaner på nettet. Når man ved hvorfra kommunikationen kommer og hvor den går hen, kan man skabe et detaljeret billede af dine interesser, vaner og præferencer, bl.a. som forbruger og dermed give organisationer og personer med mindre rene hensigter, muligheder ingen af os har lyst til eller behov for. Det kunne f.eks. være pris diskrimination, forskellige former for entrapment (hvor du lokkes til at begå kriminelle ting) eller direkte afpresning. På det normale Internet, vil selv brug af VPN og kryptering ikke kunne skjule hvorfra du kommer og hvor du skal til, kun indholdet af det der sendes, Tor går altså skridtet videre end VPN.

**Hvordan virker trafikanalyse det så?**
Alle pakker der bevæger sig rundt på Internettet består af to dele, data payload der indeholder det der sendes og header informationer, der bruges til at route pakken med. Normalt vil data payloadet være tilgængeligt i en eller anden form og selv når du krypterer, er det kun payloadet der krypteres, header informationerne (hvis du anvender en VPN gateway, vil din egne interne IP adresse være skjult, men VPN gatewayens IP adresse vil være fuldt tilgængelig) vil altid være synlig, da pakken ellers ikke kan routes. Dette betyder, at lige gyldigt hvad du gør, vil informationerne om, hvorfra du sender, og hvortil du sender

altid være fuldt synlige.
Det basale problem er derfor, at den du sender til, din Internet service provider, routere på vejen, samt maskiner der sidder på vejen mellem dig og modtageren, vil kunne indsamle oplysninger om kommunikationen.
Der findes selvfølgelig også mere sofistikerede metoder hvormed oplysninger fra forskellige knudepunkter opsamler og udsættes for avanceret statistik. Også dette kan anvendes på måder ingen af os er interesseret i.

**Løsningen, Det distribuerede, anonyme net**
IP protokollen er lavet sådan at pakkerne kan følge tilfældige veje igennem Internettet og så samles når de lander hos modtageren. I praksis styres den vej pakkerne går, således at de følger den vej, der bedst kan betale sig, altså korteste/hurtigste vej. Dette igen betyder, at pakkerne næsten altid følger samme vej gennem Internettet.
Tor reducere risikoen for både simpel og sofistikeret trafikanalyse ved at tvinge pakkerne over flere forskellige router, således at intet enkeltpunkt på nettet sidder med hele kommunikationen og kan linke dig til din destination.

> The Onion Router, Sikkerhed som et løg
>
> Onion Routing is a technique for pseudonymous (or anonymous) communication over a computer network, developed by David Goldschlag, Michael Reed, and Paul Syverson. It is based on David Chaum's Mix networks, though it includes a number of advances and modifications. Among these modifications is the concept of "routing onions", which encode routing information in a set of encrypted layers.
>
> http://en.wikipedia.org/wiki/Onion_Router

**Tor netværket opbygges således**
**Tor set fra surferens synsvinkel**

Når du har installeret Tor klienten (eller anden software der bygger på Tor's netværk) opbygges et netværk af krypterede forbindelser mellem servere på Internettet. Opbygningen sker incrementalt (et skridt af gangen) således, at hver server, kun kender den server eller klient den får pakker fra, og den server eller klient den skal afleverer pakkerne til. Ingen individuel server kender den komplette vej gennem nettet. Klienterne generere et separate sæt af krypteringsnøgler for hvert enkelt hop i nettet således, at intet "hop" kan spore kommunikationen når de passerer.

Når Tor netværket er etableret, kan mange forskellige slags kommunikation udveksles og fordi hver server/router kun ser et hop, vil hverken en sniffer eller en kompromitteret server/router kunne afslører oplysninger om destination eller source. Tor virker kun for TCP streams og kan bruges at enhver application der understøtter SOCKS

> A server running SOCKS acts as a proxy server that provides screening, authentication, and logging for application-level connections.
> http://literacynet.org/modules/netglossary.html

**Tor set fra udbyderen af tjenesters side**
Tor gør det også muligt at udbyde forskellige tjenester som fora, chatrooms, message boards , ICQ, web steder og meget mere. Tor opsætter såkaldte "rendezvous points" hvortil andre Tor brugere kan tilkoble

sig og på den made bruge disse services uden at kunne se deres IP adresser og uden at deres egen IP adresse kan logges, anonymiteten er, på godt og ondt, bevaret for alle parter.

**Tor den ultimative løsning?**
Det ultimative findes sjældent i den virkelige verden, og lad det være sagt med det samme, Tor løser heller ikke alle anonymitets problemer. Det vil eksempelvis stadig være muligt for de web steder du besøger at skrive cookies til din maskine, ligesom man også kan opfange browser typen. Ønsker du den slags beskyttelse kan du eksempelvis anvende proxy services som Privoxy.

Det er klart at Tor heller ikke beskytter mod ganske almindelig dumhed, hvis du selv opgiver dit navn, adresse og andre personlige informationer i forskellige web forms, ja så vil Tor ikke kunne redde dig.

Tor vil heller ikke kunne forhindre så kaldt end-to-end timing attacks. Hvis en angriber har adgang til at opfange både tidspunktet for din afsending af pakker samt tidspunktet for pakkernes ankomst, vil statisk analyse kunne afsløre om de er en del at den samme kommunikation. Denne angrebsform er dog lidt teoretisk endnu, men vil sagtens kunne finde anvendelse, hvis brugen af Tor bliver stor og hvis Tor på sigt bliver anvendt til meget væsentlig trafik som f.eks. militær kommunikation eller til kommunikation der er meget værdifuld.

**Hvem står bag Tor**
Tor bliver i dag drevet af The Free Haven Project, udviklerne bag er Roger Dingledine og Nick Mathewson med hjælp fra en stor gruppe af frivillige rundt omkring på Internettet og støttet af Electronic Frontier Foundation.
I den første tid (2002 til 2004) blev projektet sponseret af The Naval Research Lab medstøtte fra US Navy Office of Naval Research (ONR) og US Department of Defence Advanced Research Projects Agency (DARPA) sammen med Paul Syverson og bygget på de oprindelige ideer bag The Onion Router.

**Hvem bruger Tor**
Journalister anvender Tor til at beskytte deres kilder mod afslørelse. Selv ikke en retskendelse om udlevering af server- og routerlogs kan afsløre en kilde der kommunikerer via Tor.
Non-governmental organizations (NGOs) Anvender Tor til kommunikation i de lande der aktivt begrænser Internettet og befolkningernes muligheder for at kommunikere frit.
Grupper som f.eks. Indymedia og Electronic Frontier anbefaler og anvender Tor til beskyttelse at deres kommunikation og medlemmer, ligesom Tor oftere og oftere finder anvendelse kommercielt i firmaer rund om i verden.

> The Independent Media Center (aka Indymedia or the IMC) started as a vision for a global, open network of DIY journalists and alternative media activists. The overall network is decentralized, with core collectives formed at the local level or along themes such as Print Media or Biotech. Along with contributing their own media, these core organizers maintain the IMC's open publishing infrastructure, enabling different people throughout the internet to publish their news.
> http://en.wikipedia.org/wiki/Indymedia

**Hvordan gør du så**
Du kan downloade den nødvendige software fra Electronic Frontier's hjemmeside http://tor.eff.org/download.html og installere det nødvendige. Du skal huske at læse vejledningerne grundigt inden du downloader og installere, da Tor jo er et Open Source projekt på godt og ondt.
Inden du går i gang, bør du have gjort dig nogle overvejelser, da du får mulighed for at installere 2 grundlæggende forskellige pakker. Du kan installerer som klient og bruge Tor eller du kan installere som Onion Router og dermed være en del af selve netværket. Jeg vil bestemt anbefale, at du starter som klient

og kikker dig godt for, før du giver dig ud med at route. Ikke at jeg advare mod projektet, bestemt ikke, men der er flere uafklarede forhold, bl.a. lovlige, som jeg ikke er sikker på, så forsigtighed tilrådes.

Når du så har fået installeret klienten og det hele kører, så prøv at gå ind på http://www.myip.dk og reloade med lidt tidspause mellem, så vil du se at din IP adresse skifter hele tiden.

> Lige netop dette giver tilsyneladende lidt problemer og jeg er ved at undersøge hvorfor. Jeg kikker bl.a. om der skulle være ændret noget i forhold til da jeg arbejdede med Tor, om det skulle være cache problemer eller noget med IE; da jeg brugte firefox

Du skal også være opmærksom på at alle IP baserede tjenester kan have problemer med at din IP skifter så ofte.

Det var så Tor beskrevet. Prøv det selv og skriv gerne til mig på kim@bufferzone.dk om hvordan det går, hvilke positive som negative oplevelser du har. Dine erfaringer kunne sagtens finde vej til denne artikel. Hvis du har kommentarer og/eller spørgsmål, er du velkommen til at kontakte mig lige som jeg selvfølgelig er at finde på Eksperten. Jeg modtager kommentarer og rettelser (f.eks. af stavefejl) med tak. Jeg beder om at du ikke stiller spørgsmål i kommentarerne til artiklen, der kan jeg jo ikke besvare dem.

**Kommentar af coder d. 26. Oct 2007 | 1**

Du glemmer at fortælle hvor usikkert det er at bruge Tor, da enhver EndNode kan sniffe din trafik. Du glemmer jo at det skal ud af Tor netværket og hen til f.eks. en web-server .. og her kan din data sniffes af den computer Tor-netværket har valgt at bruge. Læs f.eks.: http://en.wikipedia.org/wiki/Tor_(anonymity_network)#Eavesdropping_by_exit_nodes

**Kommentar af philip d. 22. Oct 2005 | 2**

Velskrevet artikel. Bestemt 5 points værd. Kan godt se det smarte i det, men er også bange for at det vil blive brugt til fx. hacking. Dette kunne du godt skrive lidt om i artiklen.

**Kommentar af apj d. 10. Jul 2006 | 3**

Alt for mange siger at ToT ingen indflydelse har paa deres IP nummer. Saa er fidusen jo ligesom vaek, uanset hvor faa stavefejl der er i artiklen. :/

**Kommentar af casualty d. 23. Oct 2005 | 4**

Rigtig spændende læsning... Men lad os håbe at de pædofile stoddere derude er for dumme til at bruge det...

**Kommentar af lenk d. 07. Nov 2005 | 5**

Meget interessant projekt, der skal prøves. Lidt skræmmende muligheder, men der er desværre situationer hvor det kan være nødvendigt

**Kommentar af ilithanos d. 16. Nov 2007 | 6**

har lige siddet og testet tor systemet på min linux maskine, og jo min ip den bliver skiftet ind imellem via tor, de fungere fint, men som man jo regner med sløver det jo en del at bruge det da det skal igennem de mange tor nodes.

og hvad angår det at det kan misbruges, det kan alle ting der er udviklet til at forøge brugernes beskyttelse mod overvågningssamfundene vi får idag, den dag idag bliver alt internettrafik logget og gemt hos vores ISP med henblik på at politi og lignene kan få dem oplyst på forlangene, dette vil give meget store muligheder for vores stat til at udnytte det på andre måder også, jeg har personligt selv ikke noget at skjule, synes bare det er for latterligt at det forgår på denne måde.

tor systemet tog mig ca 10 min at få til at virke på min linux maskine, og fungere fint. det er meget simpelt at sætte op, og enhver da har lyst til det kan gøre det , også en pædefil eller terorist hvilket ligesom fjerne meningen med den overvågning.

**Kommentar af acid-head d. 03. May 2006 | 7**

Mon det med den ikke-skiftende IP har noget at gøre med følgnde (taget fra tor.eff.org):

"For efficiency, the Tor software uses the same circuit for connections that happen within the same minute or so. Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones."

Artiklen er udemærket, meget af den er dog direkte oversættelse af siden http://tor.eff.org/overview.html.en

**Kommentar af human d. 24. Oct 2005 | 8**

Fantastisk, han har gjort det igen! Og yderst interessant læsning, det skal prøves, skal lige se om dyndns.dk kan følge med ;)

EDIT: Tor har heller ikke nogen effekt på min IP adresse, den skifter simpelthen ikke.

**Kommentar af kreidlerhansen d. 23. Oct 2005 | 9**

Absolut en flot og velskrevet artikel. Umiddelbart lader TOR dog til ikke at have nogen indflydelse på min IP-adresse, men det har som sådan intet med artiklen at gøre. Derfor, topkaraktér.

**Kommentar af kenp d. 19. Oct 2005 | 10**

Intressant læsning.. Kunne være man skulle prøve det på et tidspunkt når man har tid nok :)

**Kommentar af jpvj d. 19. Oct 2005 | 11**

Sjovt projekt at læse om. Vil dog nok ikke kaste mig ud i det, da jeg pt. ikke har behovet, men det kan jo være at det kommer en dag :-)

**Kommentar af dreamless d. 12. Feb 2006 | 12**

http://www.freehaven.net/~arrakis/torpark.html <-- synes torpark skulle nævnes, en nem og god tor løsning.

**Kommentar af jojulha d. 20. Oct 2005 | 13**

Fint og velskrevet, det skal da prøves på et tidspunkt.

**Kommentar af limi d. 25. Jun 2006 | 14**

**Kommentar af cpn80 d. 19. Oct 2005 | 15**

Interessant og information artikel om en mulighed for at bevæge sig anonymt rundt på nettet.

**Kommentar af kelfe d. 03. May 2006 | 16**

Super artikkel der fik vækket min opmærksomhed.
Man kan få et plugin til firefox sådan, at man kan vælge om man vil gå på via tor netværket eller ej. Det skal siges at det er en del hurtigere direkte, hvilket nok ikke undrer en, da man jo kører gennem tor netværket før man får kontakt til siden og så igen tilbage igen.
http://www.freehaven.net/~squires/torbutton/
Tjekket med mozilla firefox version 1.5.0.2 og det kræver selvfølgelig at tor klienten er instaleret.

**Kommentar af spif2001 d. 21. Oct 2005 | 17**

Jeg kendte slet ikke til Tor - det skal da prøves.
God og velskreven artikel - en lille "eyeopener".

**Kommentar af huset d. 19. Oct 2005 | 18**

Meget spændende læsninbg endnu en gang :D