Tor för IT-forensiker

Linus Nordberg, NORDUnet

IT-forensiska seminariet 2012

Innehåll

Presentation

- Yrke programmerare
- Anställd av NORDUnet
- Tor-relaterat arbete inkluderar föreläsningar, drift av mättjänster och relän, utveckling (Tor på IPv6)
- Kontakt linus@nordu.net 0x23291265
  8C4C D511 095E 982E B0EF BFA2 1E8B F349 2329 1265

Presentation

- Yrke programmerare
- Anställd av NORDUnet
- Tor-relaterat arbete inkluderar föreläsningar, drift av mättjänster och relän, utveckling (Tor på IPv6)
- Kontakt linus@nordu.net 0x23291265
  8C4C D511 095E 982E B0EF BFA2 1E8B F349 2329 1265

Presentation

- Yrke programmerare
- Anställd av NORDUnet
- Tor-relaterat arbete inkluderar föreläsningar, drift av mättjänster och relän, utveckling (Tor på IPv6)
- Kontakt linus@nordu.net 0x23291265
  8C4C D511 095E 982E B0EF BFA2 1E8B F349 2329 1265

Presentation

- Yrke programmerare
- Anställd av NORDUnet
- Tor-relaterat arbete inkluderar föreläsningar, drift av mättjänster och relän, utveckling (Tor på IPv6)
- Kontakt linus@nordu.net 0x23291265
  8C4C D511 095E 982E B0EF BFA2 1E8B F349 2329 1265

Innehåll

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Ett protokoll och ett program

- Ett nätverksprotokoll
- Ett program – fri programvara, BSD-licensierad
- Öppna epostlistor, källkods-arkiv med specifikationer, förändringsförslag och kod, “bug tracker”, chatrum
- Teknik och urpsrunglig kod från NRL (U.S. Naval Research Laboratory) ==> “onion routing” 1996 ==> Tor 2002

Tre funktioner

- Anonym och skyddad åtkomst till internet
- Kringgå blockering
- Anonym och skyddad publicering

Tre funktioner

- Anonym och skyddad åtkomst till internet
- Kringgå blockering
- Anonym och skyddad publicering

Tre funktioner

- Anonym och skyddad åtkomst till internet
- Kringgå blockering
- Anonym och skyddad publicering

Ett ekosystem av applikationer

- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

Ett ekosystem av applikationer

- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

Ett ekosystem av applikationer

- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

Ett ekosystem av applikationer

- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

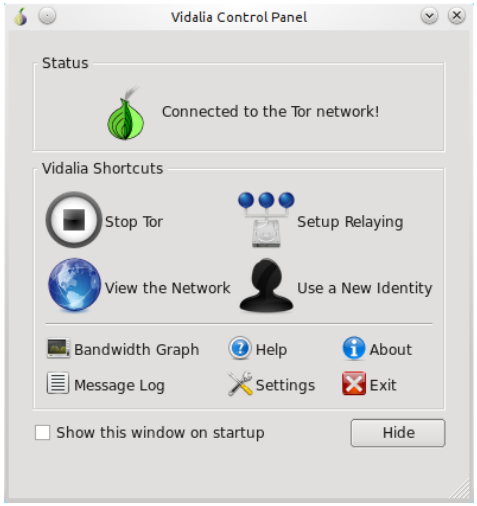
Ett ekosystem av applikationer

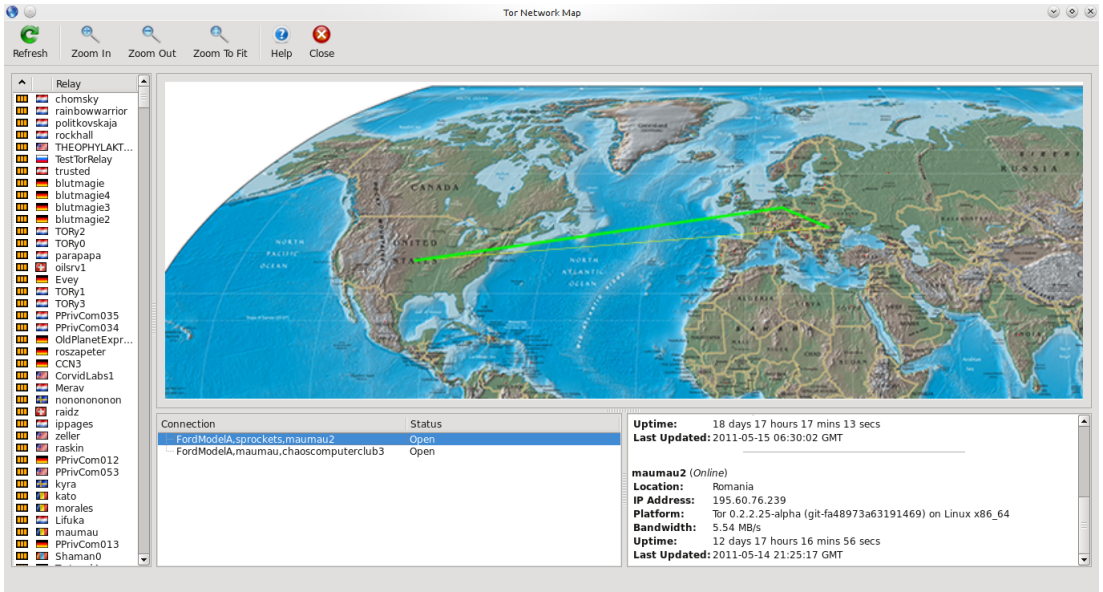
- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

Ett ekosystem av applikationer

- Browsern Aurora – Firefox + Torbutton
- Vidalia – en kontrollpanel
- Metrics – analysverktyg och information om nätet
- TBB (Tor Browser Bundle) – Vidalia + FF + Torbutton
- Tails – en live-CD/USB med TBB
- Orbot – Tor för Android

Vidalia – en kontrollpanel





En “non-profit org”

- 501(c)(3) – non-profit (ideell org) för forskning och utveckling av teknologi för anonymitet och skyddande av personlig integritet på nätet (2006)
- Historia – NRL, Electronic Frontier Foundation (EFF)

En “non-profit org”

- Finansiering – BBG, Sida, Internews, NSF, NLnet, NRL, individuals, Google, HRW (EFF, DARPa, Bell)
- Tor Project Inc (2011) – Kommersialisering för att hitta privata sponsorer

Community

- Forskare
  Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, MIT, National Science Foundation, Naval Research Labs, Cambridge (UK), Bamberg (Tyskland)
- Programutvecklare
  Ca 5 heltid + ca 20 deltid (betalda och obetalda) + 6 GSOC-studenter + många tillfälliga bugrapportörer, mindre patchar mm.

Community

- Forskare
  Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, MIT, National Science Foundation, Naval Research Labs, Cambridge (UK), Bamberg (Tyskland)
- Programutvecklare
  Ca 5 heltid + ca 20 deltid (betalda och obetalda) + 6 GSOC-studenter + många tillfälliga bugrapportörer, mindre patchar mm.

Community

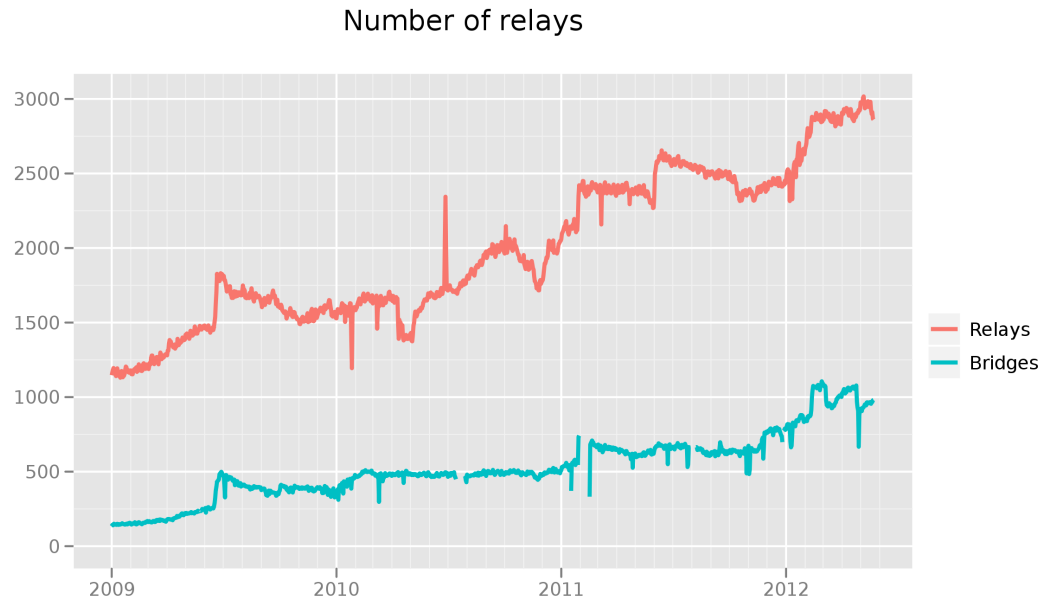
- Relä-operatörer
  2000-3000, framför allt i USA och Europa
- Användare
  Ca 400,000 dagliga användare
  https://metrics.torproject.org/users.html

Community

- Relä-operatörer
  2000-3000, framför allt i USA och Europa
- Användare
  Ca 400,000 dagliga användare
  `https://metrics.torproject.org/users.html`

Infrastruktur

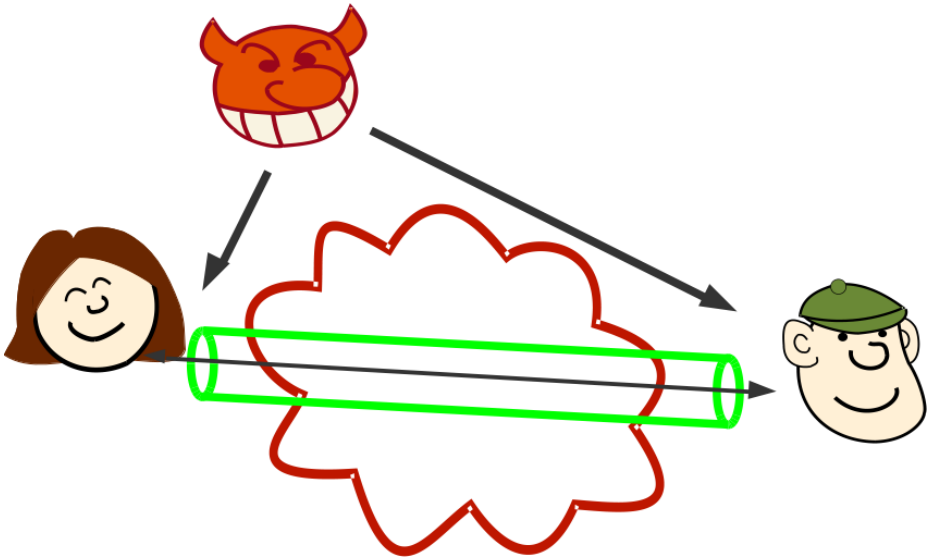
Ett frivillignätverk bestående av ca 3000 relän



The Tor Project - https://metrics.torproject.org/

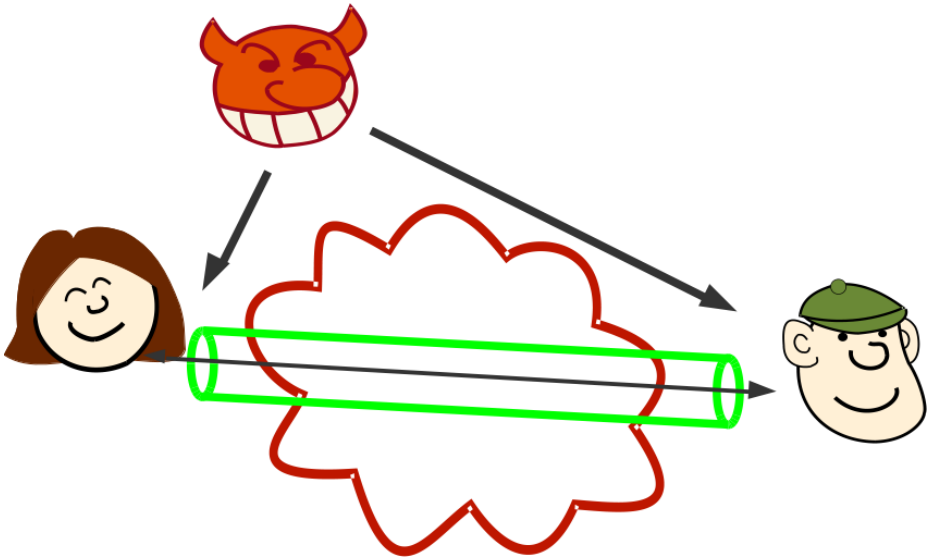
Innehåll

Enbart kryptering ger inte anonymitet



- Krypto skyddar data vid överföring
- Man kan fortfarande se vem som pratar med vem, hur ofta och hur mycket

Enbart kryptering ger inte anonymitet



- Krypto skyddar data vid överföring
- Man kan fortfarande se vem som pratar med vem, hur ofta och hur mycket

Steganografi ger inte anonymitet

- Stego döljer datat
- Man kan fortfarande se att Alice pratar med någon, hur ofta och hur mycket

Steganografi ger inte anonymitet

- Stego döljer datat
- Man kan fortfarande se att Alice pratar med någon, hur ofta och hur mycket

Önsketänkande ger inte anonymitet

- “Du kan inte bevisa att det var jag”
- “Lova att inte titta”
- “Lova att inte lagra”
- “Lova att inte berätta för någon”

Önsketänkande ger inte anonymitet

- Bevis – Behövs inte, statistisk analys räcker långt
- Löften – Kommer de hållas? Finns incitament och kompetens? Databaser läcker.
- ==> “Privacy by design, not privacy by policy”

Önsketänkande ger inte anonymitet

- Bevis – Behövs inte, statistisk analys räcker långt
- Löften – Kommer de hållas? Finns incitament och kompetens? Databaser läcker.
- ==> “Privacy by design, not privacy by policy”

Önsketänkande ger inte anonymitet

- Bevis – Behövs inte, statistisk analys räcker långt
- Löften – Kommer de hållas? Finns incitament och kompetens? Databaser läcker.
- ==> “Privacy by design, not privacy by policy”

Blanda sig med mängden

- Användaren måste gömmas i en massa
- Ett system för detta måste få användaren att se ut som alla andra
- Dölja vem som pratar med vem
- Även för operatörer av systemet

Blanda sig med mängden

- Användaren måste gömmas i en massa
- Ett system för detta måste få användaren att se ut som alla andra
- Dölja vem som pratar med vem
- Även för operatörer av systemet

Blanda sig med mängden

- Användaren måste gömmas i en massa
- Ett system för detta måste få användaren att se ut som alla andra
- Dölja vem som pratar med vem
- Även för operatörer av systemet

Blanda sig med mängden

- Användaren måste gömmas i en massa
- Ett system för detta måste få användaren att se ut som alla andra
- Dölja vem som pratar med vem
- Även för operatörer av systemet

Vem använder Tor

- Vanliga människor
  Reklamnätverk, sökmotorer, kringgå censur.
- Polisen
  Undersökning utan uniformen på, skydd av privatliv.
- Nätaktivister
  Blogga, personlig säkerhet, åtkomst till blockerade sidor.
- Militären
  I fält, separera privatliv och tjänstgöring.
- Personer med skyddad identitet
  Offer för kvinnofridsbrott behöver också internet, t.ex. för kontakt med andra.

Vem använder Tor

- Vanliga människor
  Reklamnätverk, sökmotorer, kringgå censur.
- Polisen
  Undersökning utan uniformen på, skydd av privatliv.
- Nätaktivister
  Blogga, personlig säkerhet, åtkomst till blockerade sidor.
- Militären
  I fält, separera privatliv och tjänstgöring.
- Personer med skyddad identitet
  Offer för kvinnofridsbrott behöver också internet, t.ex. för kontakt med andra.

Vem använder Tor

- Vanliga människor
  Reklamnätverk, sökmotorer, kringgå censur.
- Polisen
  Undersökning utan uniformen på, skydd av privatliv.
- Nätaktivister
  Blogga, personlig säkerhet, åtkomst till blockerade sidor.
- Militären
  I fält, separera privatliv och tjänstgöring.
- Personer med skyddad identitet
  Offer för kvinnofridsbrott behöver också internet, t.ex. för kontakt med andra.

Vem använder Tor

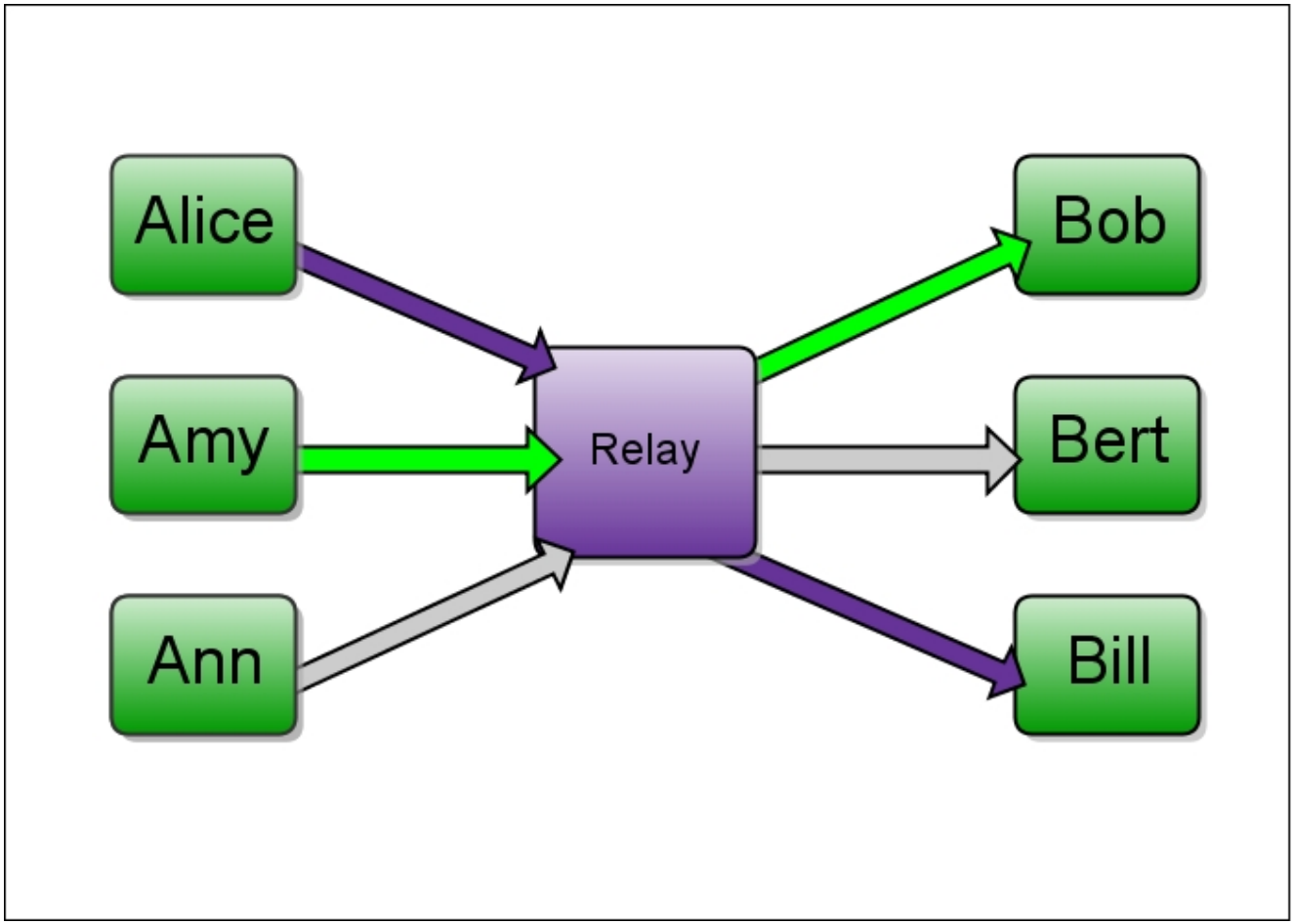
- Vanliga människor
  Reklamnätverk, sökmotorer, kringgå censur.
- Polisen
  Undersökning utan uniformen på, skydd av privatliv.
- Nätaktivister
  Blogga, personlig säkerhet, åtkomst till blockerade sidor.
- Militären
  I fält, separera privatliv och tjänstgöring.
- Personer med skyddad identitet
  Offer för kvinnofridsbrott behöver också internet, t.ex. för kontakt med andra.

Vem använder Tor

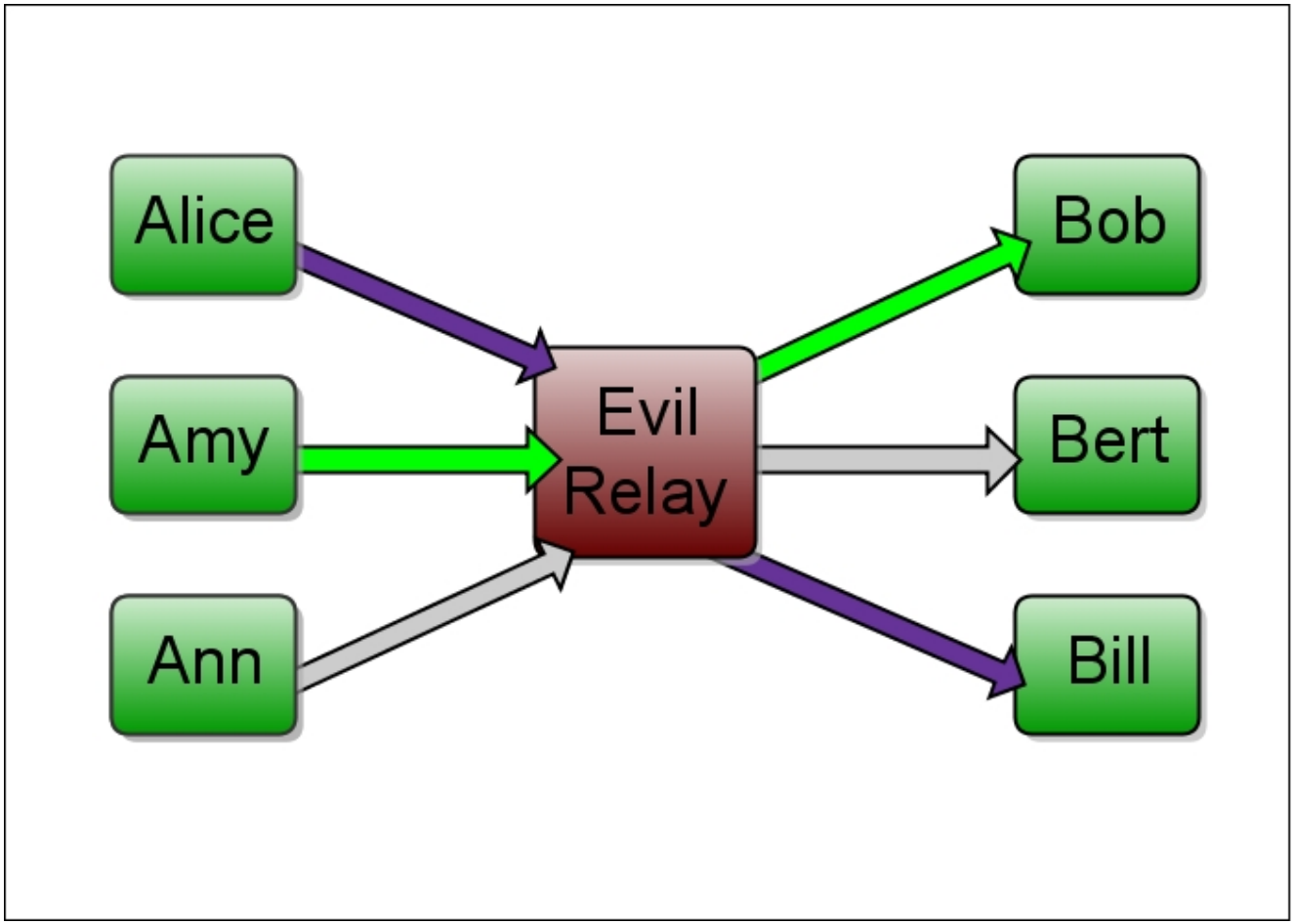
- Vanliga människor
  Reklamnätverk, sökmotorer, kringgå censur.
- Polisen
  Undersökning utan uniformen på, skydd av privatliv.
- Nätaktivister
  Blogga, personlig säkerhet, åtkomst till blockerade sidor.
- Militären
  I fält, separera privatliv och tjänstgöring.
- Personer med skyddad identitet
  Offer för kvinnofridsbrott behöver också internet, t.ex. för kontakt med andra.

Innehåll

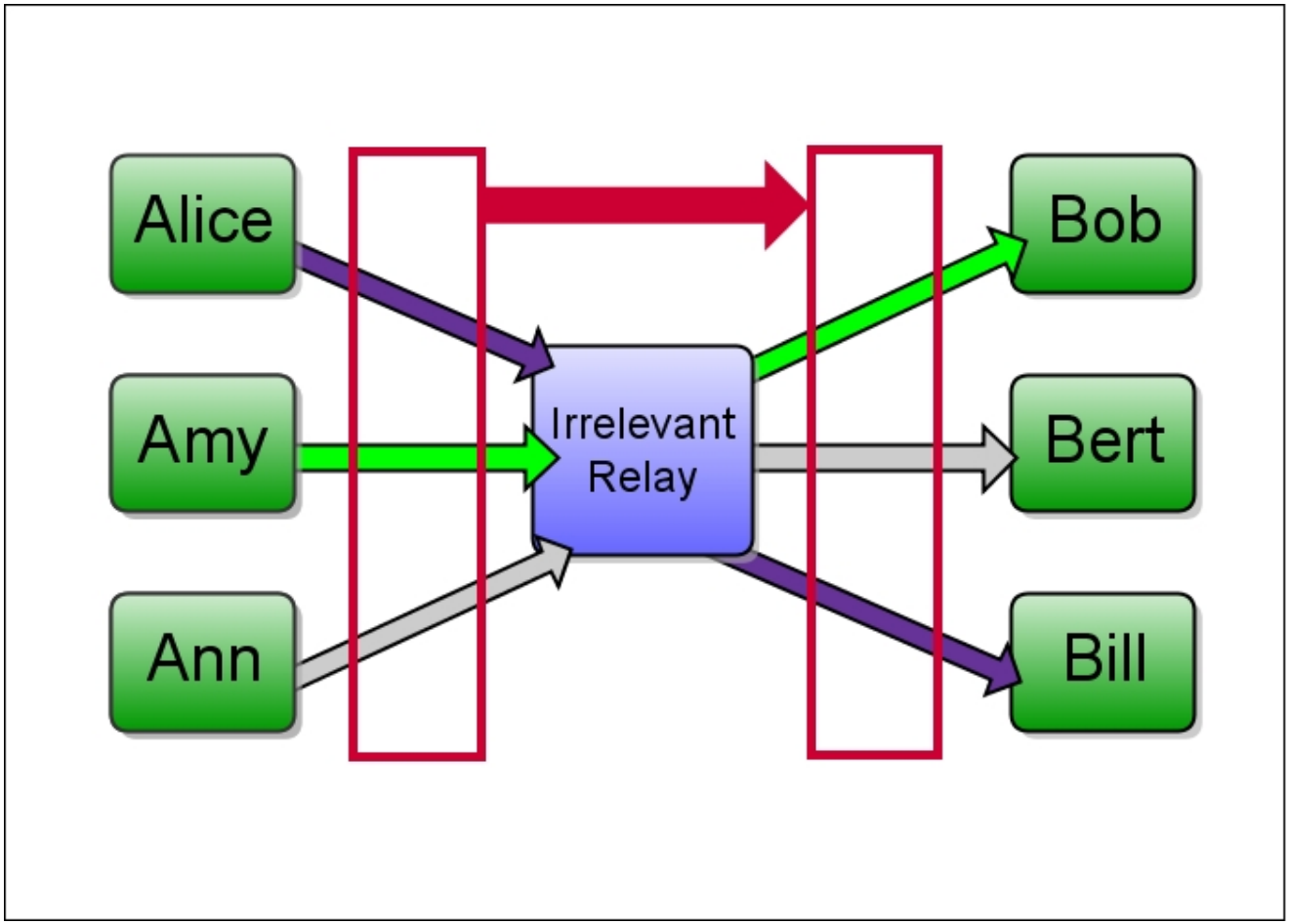
Enhopps-proxy



Enhopps-proxy



Enhopps-proxy



Tor gör tre hopp

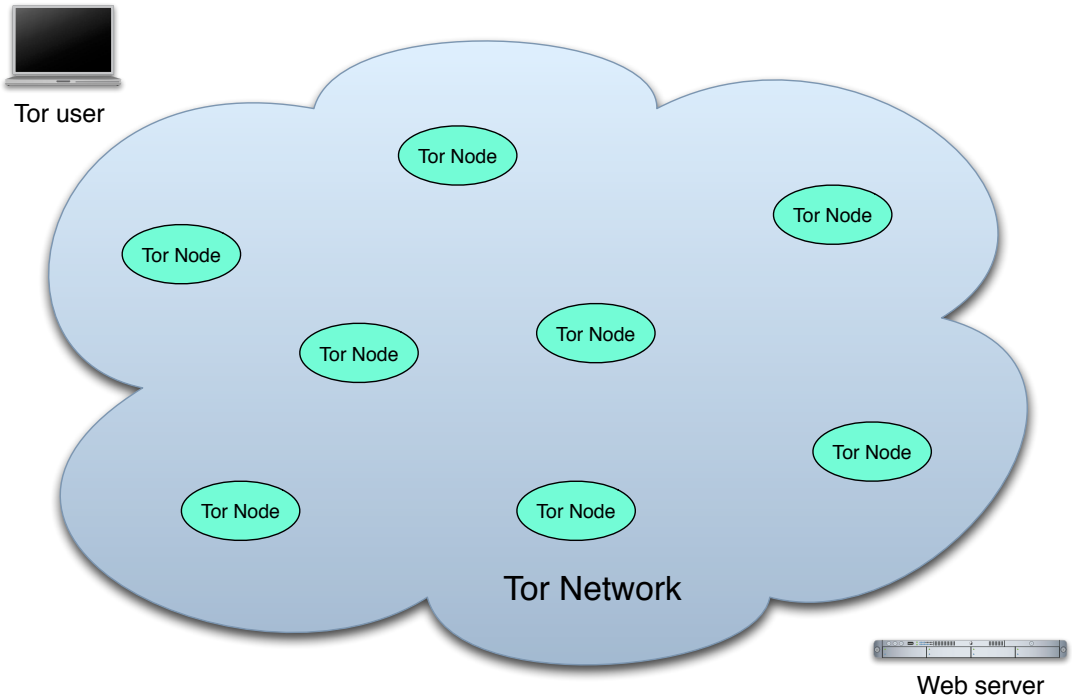


Diagram: Robert Watson

Tor gör tre hopp

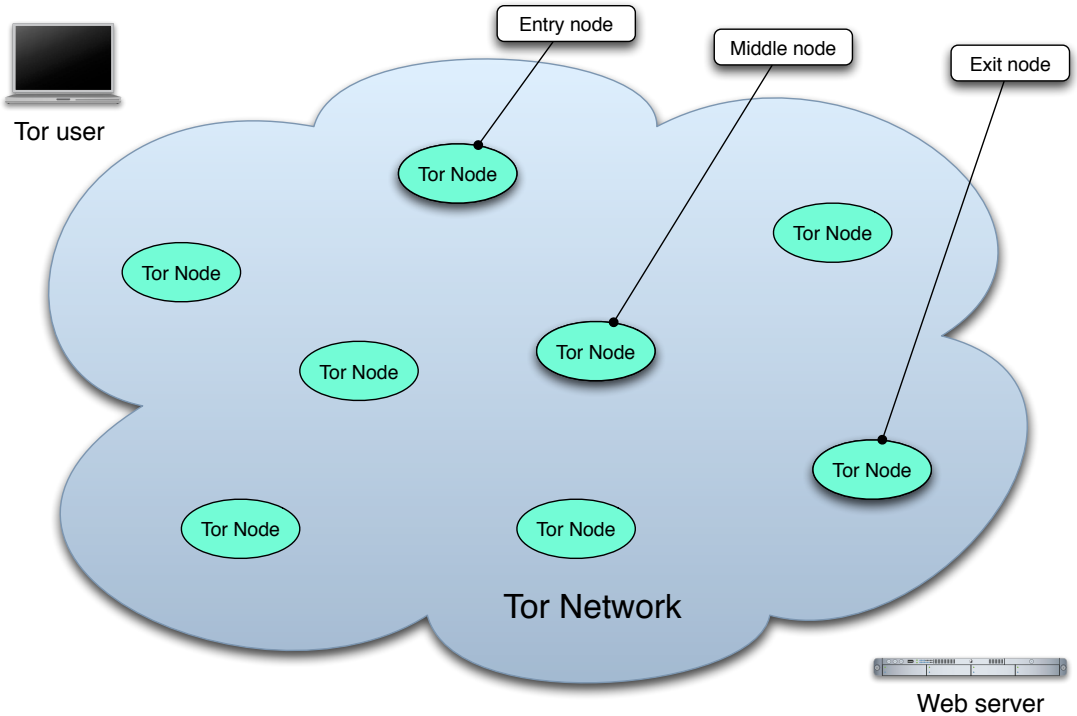


Diagram: Robert Watson

Tor gör tre hopp

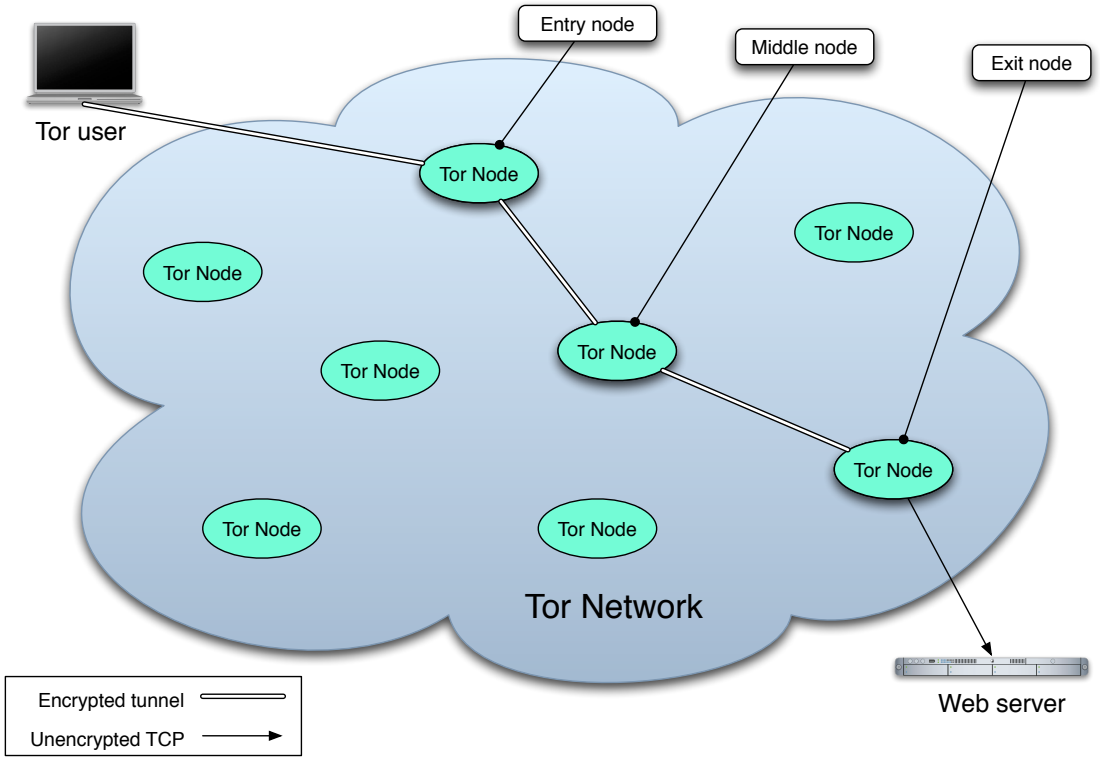


Diagram: Robert Watson

Tor gör tre hopp

- Ett komprometterat första hopp kan se att Alice pratar men inte med vem
- Ett komprometterat sista hopp kan se att någon pratar med Bob men inte vem

Tor gör tre hopp

- Ett komprometterat första hopp kan se att Alice pratar men inte med vem
- Ett komprometterat sista hopp kan se att någon pratar med Bob men inte vem

Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

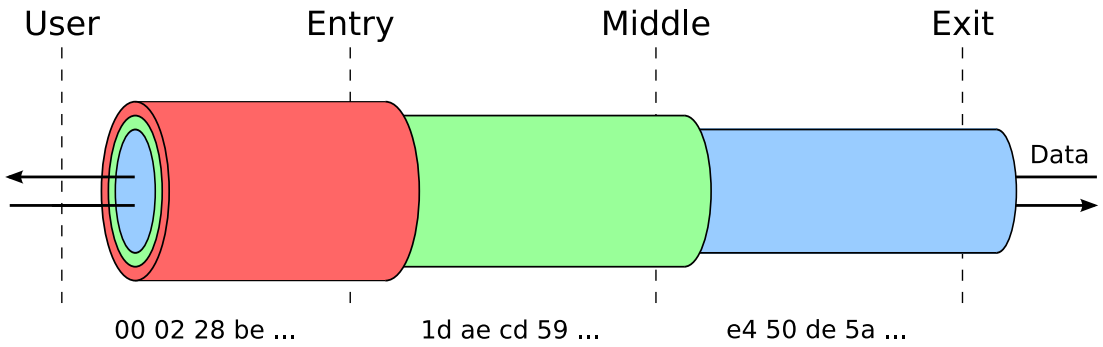
Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

Tre lager av kryptering

- Alice väljer tre relän ur nätverkslistan (konsensus)
- Exit-policyn hos sista relät tillåter uppkoppling till Bobs adress och port
- Alice förhandlar fram nycklar med det första relät (128-bits AES-CTR mha D-H) och sätter upp en “circuit” dit (CREATE/CREATED)
- Hoppar vidare till andra relät (EXTEND/EXTENDED –> CREATE/CREATED)
- Hoppar vidare till tredje och sista relät
- Sista relät sätter upp TCP-koppel till Bobs tjänst

Tre lager av kryptering



Kryptering av transportlager

- TLS/SSLv3 för kryptering och autenticering
- Tre versioner av handskakning förhandlar fram version
- v2 och v3: NETINFO, VERSIONS
- v3: CERTS AUTH_CHALLLENGE, AUTHENTICATE

Kryptering av transportlager

- TLS/SSLv3 för kryptering och autenticering
- Tre versioner av handskakning förhandlar fram version
- v2 och v3: NETINFO, VERSIONS
- v3: CERTS AUTH_CHALLLENGE, AUTHENTICATE

Kryptering av transportlager

- TLS/SSLv3 för kryptering och autenticering
- Tre versioner av handskakning förhandlar fram version
- v2 och v3: NETINFO, VERSIONS
- v3: CERTS AUTH_CHALLLENGE, AUTHENTICATE

Kryptering av transportlager

- TLS/SSLv3 för kryptering och autenticering
- Tre versioner av handskakning förhandlar fram version
- v2 och v3: NETINFO, VERSIONS
- v3: CERTS AUTH_CHALLLENGE, AUTHENTICATE

Nycklar och certifikat

- Varje relä har en “long term identity key” som signerar TLS-cert och “network documents (“server descriptors” och konsensus)
- En “medium term onion key” för dekryptering av EXTEND-celler
- En “short term connection key” för TLS-koppel

Nycklar och certifikat

- Varje relä har en “long term identity key” som signerar TLS-cert och “network documents (“server descriptors” och konsensus)
- En “medium term onion key” för dekryptering av EXTEND-celler
- En “short term connection key” för TLS-koppel

Nycklar och certifikat

- Varje relä har en “long term identity key” som signerar TLS-cert och “network documents (“server descriptors” och konsensus)
- En “medium term onion key” för dekryptering av EXTEND-celler
- En “short term connection key” för TLS-koppel

Server descriptors

- Ett reläs beskrivning av sig självt
- Innehåller nickname, annonserad kapacitet, timestamp, publik del av identity key, IP-adress och port(ar), onion key (publika delen), exit policy, family, m.m.
- Signeras med identity key
- Laddas upp till “directory authorities”
- Bakas ihop till “konsensus” – listan över de reläer som utgör Tor-nätverket för en timme framöver

Server descriptors

- Ett reläs beskrivning av sig självt
- Innehåller nickname, annonserad kapacitet, timestamp, publik del av identity key, IP-adress och port(ar), onion key (publika delen), exit policy, family, m.m.
- Signeras med identity key
- Laddas upp till “directory authorities”
- Bakas ihop till “konsensus” – listan över de reläer som utgör Tor-nätverket för en timme framöver

Server descriptors

- Ett reläs beskrivning av sig självt
- Innehåller nickname, annonserad kapacitet, timestamp, publik del av identity key, IP-adress och port(ar), onion key (publika delen), exit policy, family, m.m.
- Signeras med identity key
- Laddas upp till “directory authorities”
- Bakas ihop till “konsensus” – listan över de reläer som utgör Tor-nätverket för en timme framöver

Server descriptors

- Ett reläs beskrivning av sig självt
- Innehåller nickname, annonserad kapacitet, timestamp, publik del av identity key, IP-adress och port(ar), onion key (publika delen), exit policy, family, m.m.
- Signeras med identity key
- Laddas upp till “directory authorities”
- Bakas ihop till “konsensus” – listan över de reläer som utgör Tor-nätverket för en timme framöver

Server descriptors

- Ett reläs beskrivning av sig självt
- Innehåller nickname, annonserad kapacitet, timestamp, publik del av identity key, IP-adress och port(ar), onion key (publika delen), exit policy, family, m.m.
- Signeras med identity key
- Laddas upp till “directory authorities”
- Bakas ihop till “konsensus” – listan över de reläer som utgör Tor-nätverket för en timme framöver

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Directory authorities

- Åtta stycken i fem länder (plus en för bryggor)
- Röstar fram en s.k. konsensus varje timme
- Konsensus utgör nätverkskartan
- Signeras med “long term key”
- Klienter laddar ner konsensus och väljer relän ur denna för att bygga circuits
- Listan på directory authorities och deras long term keys finns inkompilerad i klienten (och relän)

Bryggor

- Bryggor är “semipublika” relän
- Fungerar som bryggor mellan internet och Tor-nätet för användare som inte kan nå publika relän p.g.a. blockering
- Tor-nätet har en “bridge authority” dit en brygga kan ladda upp sin deskriptor
- Bryggor sprids sedan av Tor-projektet via e-post, web, IM, kontakter
- Privata bryggor laddar inte upp deskriptorer utan operatören sprider själv bryggans address och port

Bryggor

- Bryggor är “semipublika” relän
- Fungerar som bryggor mellan internet och Tor-nätet för användare som inte kan nå publika relän p.g.a. blockering
- Tor-nätet har en “bridge authority” dit en brygga kan ladda upp sin deskriptor
- Bryggor sprids sedan av Tor-projektet via e-post, web, IM, kontakter
- Privata bryggor laddar inte upp deskriptorer utan operatören sprider själv bryggans address och port

Bryggor

- Bryggor är “semipublika” relän
- Fungerar som bryggor mellan internet och Tor-nätet för användare som inte kan nå publika relän p.g.a. blockering
- Tor-nätet har en “bridge authority” dit en brygga kan ladda upp sin deskriptor
- Bryggor sprids sedan av Tor-projektet via e-post, web, IM, kontakter
- Privata bryggor laddar inte upp deskriptorer utan operatören sprider själv bryggans address och port

Bryggor

- Bryggor är “semipublika” relän
- Fungerar som bryggor mellan internet och Tor-nätet för användare som inte kan nå publika relän p.g.a. blockering
- Tor-nätet har en “bridge authority” dit en brygga kan ladda upp sin deskriptor
- Bryggor sprids sedan av Tor-projektet via e-post, web, IM, kontakter
- Privata bryggor laddar inte upp deskriptorer utan operatören sprider själv bryggans address och port

Bryggor

- Bryggor är “semipublika” relän
- Fungerar som bryggor mellan internet och Tor-nätet för användare som inte kan nå publika relän p.g.a. blockering
- Tor-nätet har en “bridge authority” dit en brygga kan ladda upp sin deskriptor
- Bryggor sprids sedan av Tor-projektet via e-post, web, IM, kontakter
- Privata bryggor laddar inte upp deskriptorer utan operatören sprider själv bryggans address och port

Hidden services

- 2004, för anti-DoS och fysisk säkerhet
- Lasse Øverlier, FFI (Forsvarets forskningsinstitutt)

Hidden services

- 2004, för anti-DoS och fysisk säkerhet
- Lasse Øverlier, FFI (Forsvarets forskningsinstitutt)

Svagheter

- End-to-end timing correlation
- Applikationslagret – browsers läcker som såll
- Bittorent läcker – se bl.a. papper från NRIA 2010
  https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Svagheter

- End-to-end timing correlation
- Applikationslagret – browsers läcker som såll
- Bittorent läcker – se bl.a. papper från NRIA 2010
  https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Svagheter

- End-to-end timing correlation
- Applikationslagret – browsers läcker som såll
- Bittorent läcker – se bl.a. papper från NRIA 2010
  `https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea`

Innehåll

Metrics – mätdata, statistik, grafer

- Nätstatus – konsensus, söka på reläer
- Grafer – statistik för nät, användare, nedladdningar, prestanda
- Mätdata som ligger till grund för graferna
- Forskningspapper och tekniska rapporter
- Verktyg – TorDNSEL och ExoneraTor

Metrics – mätdata, statistik, grafer

- Nätstatus – konsensus, söka på reläer
- Grafer – statistik för nät, användare, nedladdningar, prestanda
- Mätdata som ligger till grund för graferna
- Forskningspapper och tekniska rapporter
- Verktyg – TorDNSEL och ExoneraTor

Metrics – mätdata, statistik, grafer

- Nätstatus – konsensus, söka på reläer
- Grafer – statistik för nät, användare, nedladdningar, prestanda
- Mätdata som ligger till grund för graferna
- Forskningspapper och tekniska rapporter
- Verktyg – TorDNSEL och ExoneraTor

Metrics – mätdata, statistik, grafer

- Nätstatus – konsensus, söka på reläer
- Grafer – statistik för nät, användare, nedladdningar, prestanda
- Mätdata som ligger till grund för graferna
- Forskningspapper och tekniska rapporter
- Verktyg – TorDNSEL och ExoneraTor

Metrics – mätdata, statistik, grafer

- Nätstatus – konsensus, söka på reläer
- Grafer – statistik för nät, användare, nedladdningar, prestanda
- Mätdata som ligger till grund för graferna
- Forskningspapper och tekniska rapporter
- Verktyg – TorDNSEL och ExoneraTor

TorDNSEL

- DNS-baserad lista av exitrelän
- Svarar snabbt på frågan “Är den här IP-addressen ett exitrelä just nu?”
- Används i applikationer för att t.ex. kräva autenticering eller en CAPTCHA
- Använd Tor-projektets tjänst eller kör den själv

TorDNSEL

- DNS-baserad lista av exitrelän
- Svarar snabbt på frågan “Är den här IP-addressen ett exitrelä just nu?”
- Används i applikationer för att t.ex. kräva autenticering eller en CAPTCHA
- Använd Tor-projektets tjänst eller kör den själv

TorDNSEL

- DNS-baserad lista av exitrelän
- Svarar snabbt på frågan “Är den här IP-addressen ett exitrelä just nu?”
- Används i applikationer för att t.ex. kräva autenticering eller en CAPTCHA
- Använd Tor-projektets tjänst eller kör den själv

TorDNSEL

- DNS-baserad lista av exitrelän
- Svarar snabbt på frågan “Är den här IP-addressen ett exitrelä just nu?”
- Används i applikationer för att t.ex. kräva autenticering eller en CAPTCHA
- Använd Tor-projektets tjänst eller kör den själv

ExoneraTor

- Svarar på frågan “Agerade den här IP-adressen och porten Tor-exitrelä vid den här tidpunkten?”
- Ladda ner verktyg och databas och ställ lokala frågor
- Tjänst tillhandahållen av Tor-projektet: `https://metrics.torproject.org/exonerator.html`

ExoneraTor

- Svarar på frågan “Agerade den här IP-adressen och porten Tor-exitrelä vid den här tidpunkten?”
- Ladda ner verktyg och databas och ställ lokala frågor
- Tjänst tillhandahållen av Tor-projektet: `https://metrics.torproject.org/exonerator.html`

ExoneraTor

- Svarar på frågan “Agerade den här IP-adressen och porten Tor-exitrelä vid den här tidpunkten?”
- Ladda ner verktyg och databas och ställ lokala frågor
- Tjänst tillhandahållen av Tor-projektet: `https://metrics.torproject.org/exonerator.html`

Innehåll

Källor, tillerkännanden

- Krypto skyddar data vid överföring (Alice, Bob och ondskan): Ilja Hallberg
- Trädet med katten i: GFDL
  `https://commons.wikimedia.org/wiki/GNU_Free_Documentation_License`
- Katten (utan träd): GFDL
  `https://commons.wikimedia.org/wiki/GNU_Free_Documentation_License`

Frågor

Frågor?