

Tecnologie per la comunicazione riservata ed anonima in rete Onion routing e Darknet

Gianni Bianchini <giannibi@dii.unisi.it>

Linux Day - 26 novembre 2005

©2005 Gianni Bianchini

Questo documento è rilasciato nei termini della GNU General Public License, versione 2 o successiva.

Per ottenere la versione in formato modificabile contattare l'autore.

Typeset using \LaTeX

Indice

- 1 **Introduzione**
 - Privacy ed anonimato
 - Tecnologie per la comunicazione anonima
- 2 Sistemi anonimi a bassa latenza
 - Onion routing
 - Tor
- 3 Darknet
 - Freenet
 - Freenet
 - GNUnet
 - Ants P2P
 - Waste
 - IIP (Invisible IRC Project)
- 4 Bibliografia

Indice

- 1 **Introduzione**
 - Privacy ed anonimato
 - Tecnologie per la comunicazione anonima
- 2 **Sistemi anonimi a bassa latenza**
 - Onion routing
 - Tor
- 3 **Darknet**
 - Freenet
 - Freenet
 - GNUnet
 - Ants P2P
 - Waste
 - IIP (Invisible IRC Project)
- 4 **Bibliografia**

Indice

- 1 **Introduzione**
 - Privacy ed anonimato
 - Tecnologie per la comunicazione anonima
- 2 **Sistemi anonimi a bassa latenza**
 - Onion routing
 - Tor
- 3 **Darknet**
 - Freenet
 - Freenet
 - GNUnet
 - Ants P2P
 - Waste
 - IIP (Invisible IRC Project)
- 4 **Bibliografia**

Indice

- 1 **Introduzione**
 - Privacy ed anonimato
 - Tecnologie per la comunicazione anonima
- 2 **Sistemi anonimi a bassa latenza**
 - Onion routing
 - Tor
- 3 **Darknet**
 - Freenet
 - Freenet
 - GNUnet
 - Ants P2P
 - Waste
 - IIP (Invisible IRC Project)
- 4 **Bibliografia**

Prologo. Quanta privacy c'è in Rete?

- In Rete, senza accorgimenti, *non esiste privacy*
 - L'origine e la destinazione di ogni comunicazione, ed anche il contenuto, sono identificabili presso ogni nodo di rete intermedio con elementari tecniche di *analisi del traffico*
- In Rete, senza accorgimenti, *nessuno è completamente libero di esprimersi*
 - La pubblicazione sul web è facilmente censurabile attaccando, per via informatica o legale, un singolo server, che è esposto alla censura come un'anatra zoppa al cacciatore
- In Rete, senza accorgimenti, *nessuno è anonimo*
 - Ogni connessione ad un provider comporta l'archiviazione di ora e numero di telefono in file di log
 - Recenti disposizioni di legge obbligano i gestori degli internet point ad identificare i clienti, altre obbligano i fornitori di accesso a conservare a lungo i file di log

Prologo. Quanta privacy c'è in Rete?

- In Rete, senza accorgimenti, *non esiste privacy*
 - L'origine e la destinazione di ogni comunicazione, ed anche il contenuto, sono identificabili presso ogni nodo di rete intermedio con elementari tecniche di *analisi del traffico*
- In Rete, senza accorgimenti, *nessuno è completamente libero di esprimersi*
 - La pubblicazione sul web è facilmente censurabile attaccando, per via informatica o legale, un singolo server, che è esposto alla censura come un'anatra zoppa al cacciatore
- In Rete, senza accorgimenti, *nessuno è anonimo*
 - Ogni connessione ad un provider comporta l'archiviazione di ora e numero di telefono in file di log
 - Recenti disposizioni di legge obbligano i gestori degli internet point ad identificare i clienti, altre obbligano i fornitori di accesso a conservare a lungo i file di log

Prologo. Quanta privacy c'è in Rete?

- In Rete, senza accorgimenti, *non esiste privacy*
 - L'origine e la destinazione di ogni comunicazione, ed anche il contenuto, sono identificabili presso ogni nodo di rete intermedio con elementari tecniche di *analisi del traffico*
- In Rete, senza accorgimenti, *nessuno è completamente libero di esprimersi*
 - La pubblicazione sul web è facilmente censurabile attaccando, per via informatica o legale, un singolo server, che è esposto alla censura come un'anatra zoppa al cacciatore
- In Rete, senza accorgimenti, *nessuno è anonimo*
 - Ogni connessione ad un provider comporta l'archiviazione di ora e numero di telefono in file di log
 - Recenti disposizioni di legge obbligano i gestori degli internet point ad identificare i clienti, altre obbligano i fornitori di accesso a conservare a lungo i file di log

Anonimato

- Definizione tecnica

Lo stato di non essere identificabile in un insieme

- Comunicazione anonima

Alice comunica un messaggio a Bob attraverso un mezzo M

- il mezzo M è *anonimo in avanti* se nessuno (neppure Bob) può conoscere l'identità di Alice
- il mezzo M è *anonimo all'indietro* se nessuno (neppure Alice) può conoscere l'identità di Bob

Accesso riservato/anonimo ad un servizio di rete

Bob predispone un servizio di rete S (sito web, file system condiviso, sistema di messaggistica...)

- Accesso *anonimo in avanti*: Alice accede a S senza che nessuno possa risalire all'indirizzo IP da cui ella ha generato la richiesta
- Accesso *anonimo all'indietro*: Alice accede a S senza che nessuno possa risalire all'indirizzo IP del server che ospita S
- Accesso *riservato*: Nessuno tranne Alice e Bob può conoscere il contenuto dei dati scambiati

Anonimato in rete: cui prodest?

- Cittadini che non vogliono farsi tracciare da siti web (caso Google Analytics) o profilare commercialmente
- Persone soggette a restrizione della libertà di espressione
- Persone che desiderino partecipare in modo anonimo a gruppi di discussione su argomenti sensibili
- Aziende che non vogliono rendere note relazioni strategiche
- Autorità giudiziarie che vogliono visitare siti senza lasciare IP governativi nei log
- Persone che desiderino offrire servizi senza rivelarne la locazione, allo scopo di prevenire attacchi
- Persone mal intenzionate naturalmente, e qui siamo tutti consapevoli che il problema è tutt'altro che tecnico...

La riservatezza passa per la crittografia

- Sistemi crittografici a chiave pubblica (o asimmetrica)
 - Alice possiede due chiavi, una segreta K_s^A ed una pubblica K_p^A , che ella condivide con Bob
 - Ogni messaggio che Bob cifra con K_p^A può essere decifrato solo impiegando K_s^A , quindi solo Alice può decifrarlo
 - Non è possibile risalire da K_p^A a K_s^A in tempi ragionevoli
- Sistemi crittografici a chiave simmetrica
 - Alice e Bob condividono un segreto K , usato da entrambi come chiave per cifrare e decifrare messaggi
- Gli algoritmi di ogni buon sistema crittografico *devono essere pubblici*, la riservatezza deve essere affidata alle sole chiavi

Tecnologie per la comunicazione anonima

- Sistemi anonimi ad alta latenza
 - Anonymous remailer
 - Server di pseudonimi

Garantiscono l'anonimato in avanti ed all'indietro nello scambio di messaggi, senza esigenze di comunicazione "in tempo reale", con latenze variabili

- Sistemi anonimi a bassa latenza
 - Onion routing

Mirano a rendere non tracciabile la fruizione di servizi di rete generici (WWW, IM, ecc.) in modo trasparente all'utente e garantendo latenze tollerabili e predicibili

- Darknet
 - "Reti nella Rete"

Tecnologie per la comunicazione anonima

- Sistemi anonimi ad alta latenza
 - Anonymous remailer
 - Server di pseudonimi

Garantiscono l'anonimato in avanti ed all'indietro nello scambio di messaggi, senza esigenze di comunicazione "in tempo reale", con latenze variabili

- Sistemi anonimi a bassa latenza
 - Onion routing

Mirano a rendere non tracciabile la fruizione di servizi di rete generici (WWW, IM, ecc.) in modo trasparente all'utente e garantendo latenze tollerabili e predicibili

- Darknet
"Reti nella Rete"

Tecnologie per la comunicazione anonima

- Sistemi anonimi ad alta latenza
 - Anonymous remailer
 - Server di pseudonimi

Garantiscono l'anonimato in avanti ed all'indietro nello scambio di messaggi, senza esigenze di comunicazione "in tempo reale", con latenze variabili

- Sistemi anonimi a bassa latenza
 - Onion routing

Mirano a rendere non tracciabile la fruizione di servizi di rete generici (WWW, IM, ecc.) in modo trasparente all'utente e garantendo latenze tollerabili e predicibili

- Darknet
 - "Reti nella Rete"

Il modello Mix-Net [Chaum, 1981]

- L'invio di un messaggio da Alice a Bob avviene attraverso una serie di nodi intermedi (paradigma delle buste chiuse)
- Il messaggio è inizialmente cifrato a chiave pubblica con tutte le chiavi dei nodi che deve attraversare a partire dall'ultimo
- Ogni nodo intermedio riceve, decifra ed inoltra il messaggio al nodo successivo
- L'anonimato in avanti è garantito a meno che tutti i nodi intermedi siano compromessi
- I moderni sistemi di anonimato sono raffinamenti e specializzazioni di questo modello di base

Il modello Mix-Net [Chaum, 1981]

- L'invio di un messaggio da Alice a Bob avviene attraverso una serie di nodi intermedi (paradigma delle buste chiuse)
- Il messaggio è inizialmente cifrato a chiave pubblica con tutte le chiavi dei nodi che deve attraversare a partire dall'ultimo
- Ogni nodo intermedio riceve, decifra ed inoltra il messaggio al nodo successivo
- L'anonimato in avanti è garantito a meno che tutti i nodi intermedi siano compromessi
- I moderni sistemi di anonimato sono raffinamenti e specializzazioni di questo modello di base

Il modello Mix-Net [Chaum, 1981]

- L'invio di un messaggio da Alice a Bob avviene attraverso una serie di nodi intermedi (paradigma delle buste chiuse)
- Il messaggio è inizialmente cifrato a chiave pubblica con tutte le chiavi dei nodi che deve attraversare a partire dall'ultimo
- Ogni nodo intermedio riceve, decifra ed inoltra il messaggio al nodo successivo
- L'anonimato in avanti è garantito a meno che tutti i nodi intermedi siano compromessi
- I moderni sistemi di anonimato sono raffinamenti e specializzazioni di questo modello di base

Onion routing

- Tecnologia di comunicazione anonima a bassa latenza resistente alle comuni tecniche di analisi di traffico
- Tunneling di stream TCP attraverso circuiti virtuali
 - Incapsulamento dei pacchetti TCP in strutture dati (*onion*) ripetutamente cifrate
 - Instradamento delle onion attraverso nodi successivi

- *Tor*. The second generation onion router

<http://tor.eff.org/>

Onion routing

- Tecnologia di comunicazione anonima a bassa latenza resistente alle comuni tecniche di analisi di traffico
- Tunneling di stream TCP attraverso circuiti virtuali
 - Incapsulamento dei pacchetti TCP in strutture dati (*onion*) ripetutamente cifrate
 - Instradamento delle onion attraverso nodi successivi

- *Tor*. The second generation onion router

<http://tor.eff.org/>

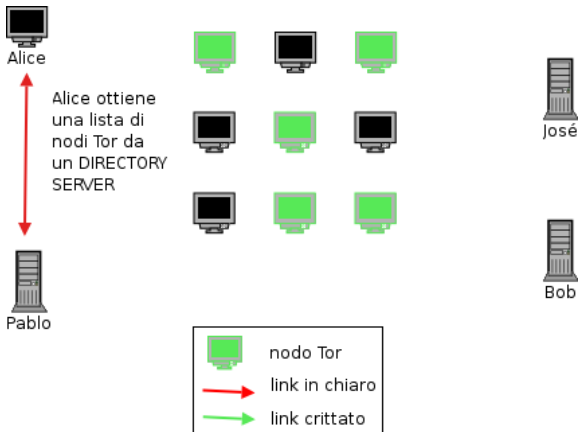
Onion routing

- Tecnologia di comunicazione anonima a bassa latenza resistente alle comuni tecniche di analisi di traffico
- Tunneling di stream TCP attraverso circuiti virtuali
 - Incapsulamento dei pacchetti TCP in strutture dati (*onion*) ripetutamente cifrate
 - Instradamento delle onion attraverso nodi successivi

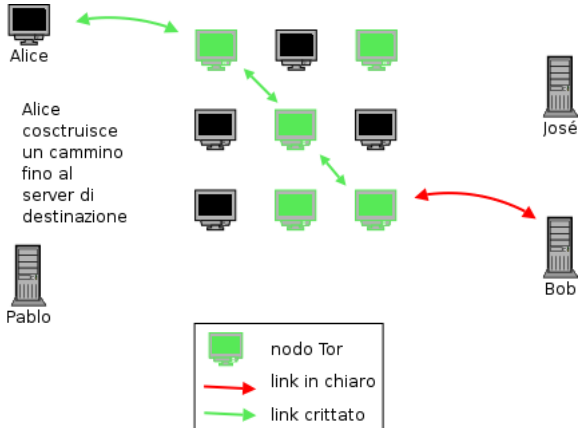
- *Tor*. The second generation onion router

<http://tor.eff.org/>

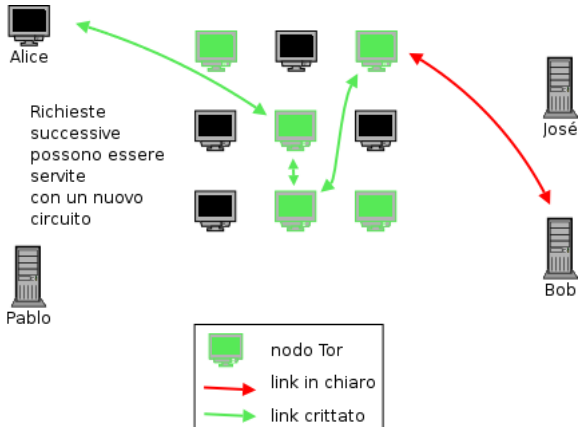
Tor: funzionamento di base (1/3)



Tor: funzionamento di base (2/3)



Tor: funzionamento di base (3/3)



Tor vs. progetto originale onion routing

- Anonimato in avanti “perfetto”
 - Costruzione incrementale del circuito mediante negoziazione di chiavi di sessione temporanee con ogni nodo successivo
 - Rinnovo periodico del circuito
- Possibilità di instradare più stream TCP sullo stesso circuito per ridurre le latenze
- Topologia *leaky pipe* del circuito virtuale
- Uso di TLS in qualunque transazione tra nodi (relay dati o messaggi di controllo)
 - Impossibilità di modificare i dati in transito
 - Impossibilità di impersonare un router
- Controllo di congestione decentralizzato mediante messaggi di acknowledgement end-to-end
- Controllo end-to-end di integrità dei dati

Tor: modello di minaccia

- Le caratteristiche di Tor mirano a neutralizzare un avversario capace di
 - osservare una frazione del traffico di rete
 - generare, modificare, ritardare il traffico di rete
 - gestire egli stesso nodi “rogue” (questo è una *costante* di ogni sistema anonimo!)
 - compromettere la sicurezza di una frazione dei nodi
- Nei sistemi anonimi a bassa latenza, un attaccante può ragionevolmente concludere che Alice sta comunicando con Bob se osserva e può correlare la temporizzazione ed il volume di traffico ai due estremi

Tor: caratteristiche

- Relaying di stream TCP con indipendenza dall'applicazione
- Interfacciamento con protocolli applicativi tramite protocollo SOCKS
- Possibilità di integrazione con proxy filtranti come *Privoxy*, <http://www.privoxy.org/>
- Software libero, scritto in C, disponibile per i sistemi operativi più comuni
- La rete attuale consta di 200-250 nodi con una banda disponibile di 60 Mbit/s

Tor: Hidden services

- Sistema integrato per servizi TCP anonimi, in cui l'IP del server host non viene rivelato
 - Bob comunica la localizzazione del servizio nascosto (es. `www.ing.ar.unisi.it:80`) ad un insieme di (*introduction points*) (IP) e lo indicizza sui directory server
 - Alice acquisisce in qualche modo la *handle* del servizio (es. `jdfh456j56fb.onion`)
 - Alice stabilisce un nodo come *rendez-vous point* (RP) per la connessione al servizio di Bob e ne annuncia la localizzazione ad uno degli IP
 - Bob riceve la richiesta dall'IP e si connette al RP, stabilendo così un circuito con Alice attraverso il RP
 - Alice e Bob rimangono anonimi l'una all'altro
- Protezione da attacchi DoS nei confronti del server host

Tor: Abusi ed exit policies

- Con l'uso di sistemi anonimi, non viene introdotta nessuna nuova classe di abusi rispetto a quelli normalmente perpetrabili in rete. Tuttavia questi possono essere compiuti in modo non tracciabile
 - Spammer ed altri “pirati della Rete” hanno già a disposizione migliaia di sistemi mal configurati in cui nascondersi!
- L'ultimo anello della catena di onion routing può essere tuttavia scambiato per l'originatore di eventuali abusi
- Per prevenire gli abusi, ogni nodo può impostare la propria *exit-policy*, ovvero l'insieme delle coppie `host:tcp_port` verso cui il nodo è autorizzato a connettersi quando è l'ultimo nodo del circuito
 - L'uso di Tor per l'invio di spam può essere prevenuto impedendo connessioni da ogni nodo della rete verso `*:25`

Tor: Abusi ed exit policies

- Con l'uso di sistemi anonimi, non viene introdotta nessuna nuova classe di abusi rispetto a quelli normalmente perpetrabili in rete. Tuttavia questi possono essere compiuti in modo non tracciabile
 - Spammer ed altri “pirati della Rete” hanno già a disposizione migliaia di sistemi mal configurati in cui nascondersi!
- L'ultimo anello della catena di onion routing può essere tuttavia scambiato per l'originatore di eventuali abusi
- Per prevenire gli abusi, ogni nodo può impostare la propria *exit-policy*, ovvero l'insieme delle coppie `host:tcp_port` verso cui il nodo è autorizzato a connettersi quando è l'ultimo nodo del circuito
 - L'uso di Tor per l'invio di spam può essere prevenuto impedendo connessioni da ogni nodo della rete verso `*:25`

Tor + Privoxy: the dynamic duo!

Privoxy: HTTP proxy con filtraggio avanzato

- Modifica di contenuti sospetti nelle pagine web
- Controllo dei cookie
- Rimozione di informazioni superflue o potenzialmente pericolose nelle richieste
- Controllo degli accessi
- Rimozione di banner pubblicitari
- Rimozione di pop-up

Tor + Privoxy: the dynamic duo!

- Possibilità di forward delle richieste attraverso Tor attraverso il protocollo SOCKS
- Problema del DNS lookup
 - Nella navigazione web è fondamentale impiegare Privoxy come HTTP proxy e non direttamente Tor come SOCKS proxy, in modo da ottenere il tunneling attraverso Tor anche delle richieste DNS

Privacy test sites

- `http://www.whatismyip.com`
- `http://ipid.shat.net`
- `http://showmyip.com`
- `http://www.noreply.org`

Darknet

Darknet: a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.

[Biddle et al., 2002]

- Permettono l'immissione e la fruizione di informazioni con mezzi interni alla darknet stessa
- Non solo file sharing scambio peer-to-peer di contenuti
 - Aspetto più sgradito e contrastato ma forse meno interessante
- Scopo delle darknet è creare comunità di utenti logicamente separate dalla Rete (e da tecnologie sempre più controllate)

Darknet

Darknet: a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.

[Biddle et al., 2002]

- Permettono l'immissione e la fruizione di informazioni con mezzi interni alla darknet stessa
- Non solo file sharing scambio peer-to-peer di contenuti
 - Aspetto più sgradito e contrastato ma forse meno interessante
- Scopo delle darknet è creare comunità di utenti logicamente separate dalla Rete (e da tecnologie sempre più controllate)

Darknet

Darknet: a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.

[Biddle et al., 2002]

- Permettono l'immissione e la fruizione di informazioni con mezzi interni alla darknet stessa
- Non solo file sharing scambio peer-to-peer di contenuti
 - Aspetto più sgradito e contrastato ma forse meno interessante
- Scopo delle darknet è creare comunità di utenti logicamente separate dalla Rete (e da tecnologie sempre più controllate)

Darknet

Darknet: a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.

[Biddle et al., 2002]

- Permettono l'immissione e la fruizione di informazioni con mezzi interni alla darknet stessa
- Non solo file sharing scambio peer-to-peer di contenuti
 - Aspetto più sgradito e contrastato ma forse meno interessante
- Scopo delle darknet è creare comunità di utenti logicamente separate dalla Rete (e da tecnologie sempre più controllate)

Una rete separata dalla Rete

- Separata come contenuti
- Separata come metodi di scambio
- Separata come tecnologie
 - Uso di crittografia forte
 - Indirizzi virtuali
 - Anonimato forte e identità pseudonime
- La Rete funziona da tecnologia ospite per la darknet, che la impiega essenzialmente come protocollo di trasporto

Una rete separata dalla Rete

- Separata come contenuti
- Separata come metodi di scambio
- Separata come tecnologie
 - Uso di crittografia forte
 - Indirizzi virtuali
 - Anonimato forte e identità pseudonime
- La Rete funziona da tecnologia ospite per la darknet, che la impiega essenzialmente come protocollo di trasporto

Freenet

- Freenet è un sistema anonimo per la pubblicazione e il recupero di informazioni (chiavi)
- Non è (ragionevolmente) possibile risalire a chi inserisce, conserva o recupera dati
- Non permette la cancellazione di contenuti
- Non ha funzionalità di ricerca, le informazioni sono indicizzate su richiesta su *freesite* specifici mantenuti da utenti
- L'informazione contenuta in Freenet può essere acceduta in HTTP attraverso un proxy
 - Freesites: DBR o ad edizioni
- Freenet non è un applicazione ma un protocollo: può essere utilizzato come strato di trasporto per applicazioni (FCP)
 - Message board con scambio sicuro file (Frost)
 - Messaggistica (ad alta latenza!)
 - Tool di pubblicazione

Freenet

- Freenet è un sistema anonimo per la pubblicazione e il recupero di informazioni (chiavi)
- Non è (ragionevolmente) possibile risalire a chi inserisce, conserva o recupera dati
- Non permette la cancellazione di contenuti
- Non ha funzionalità di ricerca, le informazioni sono indicizzate su richiesta su *freesite* specifici mantenuti da utenti
- L'informazione contenuta in Freenet può essere acceduta in HTTP attraverso un proxy
 - Freesites: DBR o ad edizioni
- Freenet non è un applicazione ma un protocollo: può essere utilizzato come strato di trasporto per applicazioni (FCP)
 - Message board con scambio sicuro file (Frost)
 - Messaggistica (ad alta latenza!)
 - Tool di pubblicazione

Freenet

- Freenet è un sistema anonimo per la pubblicazione e il recupero di informazioni (chiavi)
- Non è (ragionevolmente) possibile risalire a chi inserisce, conserva o recupera dati
- Non permette la cancellazione di contenuti
- Non ha funzionalità di ricerca, le informazioni sono indicizzate su richiesta su *freesite* specifici mantenuti da utenti
- L'informazione contenuta in Freenet può essere acceduta in HTTP attraverso un proxy
 - Freesites: DBR o ad edizioni
- Freenet non è un applicazione ma un protocollo: può essere utilizzato come strato di trasporto per applicazioni (FCP)
 - Message board con scambio sicuro file (Frost)
 - Messaggistica (ad alta latenza!)
 - Tool di pubblicazione

Freenet

- Modello decentralizzato: nessun indice globale delle informazioni e contatti mantenuti da una catena di intermediari
- Comportamento non deterministico: non consente di provare con certezza che un file presente localmente su un nodo sia stato richiesto dal nodo stesso
- Routing adattativo: i nodi si specializzano in classi di chiavi simili in senso crittografico
- Resilienza: la rete può perdere un rilevante numero di nodi con basso degrado delle prestazioni
- Comportamento ecologico: l'informazione frequentemente acceduta si moltiplica su più nodi
- Progetto GPL, necessita di implementazioni proprietarie di Java.

Freenet

- Modello decentralizzato: nessun indice globale delle informazioni e contatti mantenuti da una catena di intermediari
- Comportamento non deterministico: non consente di provare con certezza che un file presente localmente su un nodo sia stato richiesto dal nodo stesso
- Routing adattativo: i nodi si specializzano in classi di chiavi simili in senso crittografico
- Resilienza: la rete può perdere un rilevante numero di nodi con basso degrado delle prestazioni
- Comportamento ecologico: l'informazione frequentemente acceduta si moltiplica su più nodi
- Progetto GPL, necessita di implementazioni proprietarie di Java.

GNUnet

“L’ambiente P2P decentralizzato, anonimo e anticensura del Progetto GNU”

- Non solo file sharing. Mira a fornire un framework per protocolli generici di comunicazione P2P anonima e non censurabile
- Routing anonimo basato su source rewriting
 - Non è ragionevolmente possibile dedurre se una richiesta è generata da un nodo o inoltrata per conto di altri
- Comunicazione cifrata e autenticata tra nodi
 - Ogni nodo è identificato in rete solo dalla sua chiave pubblica
 - Può usare diversi meccanismi di trasporto (direttamente TCP ma anche HTTP, SMTP...)
 - Il binding tra chiave e protocollo trasporto: indirizzo corrente è comunicato da peer a peer mediante speciali messaggi

GNUnet

“L’ambiente P2P decentralizzato, anonimo e anticensura del Progetto GNU”

- Non solo file sharing. Mira a fornire un framework per protocolli generici di comunicazione P2P anonima e non censurabile
- Routing anonimo basato su source rewriting
 - Non è ragionevolmente possibile dedurre se una richiesta è generata da un nodo o inoltrata per conto di altri
- Comunicazione cifrata e autenticata tra nodi
 - Ogni nodo è identificato in rete solo dalla sua chiave pubblica
 - Può usare diversi meccanismi di trasporto (direttamente TCP ma anche HTTP, SMTP...)
 - Il binding tra chiave e protocollo trasporto: indirizzo corrente è comunicato da peer a peer mediante speciali messaggi

GNUnet

- Cifratura anche a livello di contenuti, per impedirne la censura
- Sistema a priorità per l'isolamento dei freeloaders ed il bilanciamento del carico di rete
- Possibilit' a di selezionare il livello di anonimato
 - Quantità di traffico di copertura
- Funzionalità di ricerca
- Progetto GPL molto ben documentato, vasta bibliografia di livello scientifico (anche sulle tecniche di compromissione)

GNUnet

- Cifratura anche a livello di contenuti, per impedirne la censura
- Sistema a priorità per l'isolamento dei freeloaders ed il bilanciamento del carico di rete
- Possibilit' a di selezionare il livello di anonimato
 - Quantità di traffico di copertura
- Funzionalità di ricerca
- Progetto GPL molto ben documentato, vasta bibliografia di livello scientifico (anche sulle tecniche di compromissione)

Ants P2P

- File sharing anonimo
- Route/peer discovery basato su algoritmi di “swarm” (paradigma della colonia di formiche)
- Funzionalità di ricerca decentralizzata
- Funzionalità di ricerca contenuti nei file indicizzati
- Mira a costituire un framework per applicazioni eterogenee
- GPL, beta release
- Similare come concetto ed orientata al solo file sharing: Mute

Ants P2P

- File sharing anonimo
- Route/peer discovery basato su algoritmi di “swarm” (paradigma della colonia di formiche)
- Funzionalità di ricerca decentralizzata
- Funzionalità di ricerca contenuti nei file indicizzati
- Mira a costituire un framework per applicazioni eterogenee
- GPL, beta release
- Similare come concetto ed orientata al solo file sharing: Mute

Ants P2P

- File sharing anonimo
- Route/peer discovery basato su algoritmi di “swarm” (paradigma della colonia di formiche)
- Funzionalità di ricerca decentralizzata
- Funzionalità di ricerca contenuti nei file indicizzati
- Mira a costituire un framework per applicazioni eterogenee
- GPL, beta release
- Similare come concetto ed orientata al solo file sharing: Mute

Waste

- Orientato alla creazione di reti di piccole dimensioni (10-50 nodi) tra utenti fidati
- Comunicazione P2P cifrata ed autenticata
- Funzionalità
 - Instant messaging
 - Chat
 - Ricerca e trasferimento file
- Progetto GPL (lasciato?) in fase poco più che embrionale, release ferme al 2004

Waste

- Orientato alla creazione di reti di piccole dimensioni (10-50 nodi) tra utenti fidati
- Comunicazione P2P cifrata ed autenticata
- Funzionalità
 - Instant messaging
 - Chat
 - Ricerca e trasferimento file
- Progetto GPL (lasciato?) in fase poco più che embrionale, release ferme al 2004

IIP (Invisible IRC Project)

- Realizza un sistema di messaggistica in tempo reale sul modello IRC (Internet Relay Chat) con architettura distribuita e caratterizzato da
 - Anonimato dei relay server e degli utenti
 - Riservatezza del contenuto della comunicazione
- Tra utenti e server è interposta una serie di relay in modo che l'IP dell'uno sia nascosto all'altro (IRC è normalmente un sistema centralizzato)
- Ogni messaggio è cifrato a chiave simmetrica, con rekeying D-H. Cifratura nodo-nodo ed end-to-end per contrastare nodi rogue
- Utilizzabile con ogni client IRC attraverso un proxy locale
- Progetto con alterne vicende, release ferme al 2004, GPL.

IIP (Invisible IRC Project)

- Realizza un sistema di messaggistica in tempo reale sul modello IRC (Internet Relay Chat) con architettura distribuita e caratterizzato da
 - Anonimato dei relay server e degli utenti
 - Riservatezza del contenuto della comunicazione
- Tra utenti e server è interposta una serie di relay in modo che l'IP dell'uno sia nascosto all'altro (IRC è normalmente un sistema centralizzato)
- Ogni messaggio è cifrato a chiave simmetrica, con rekeying D-H. Cifratura nodo-nodo ed end-to-end per contrastare nodi rogue
- Utilizzabile con ogni client IRC attraverso un proxy locale
- Progetto con alterne vicende, release ferme al 2004, GPL.

IIP (Invisible IRC Project)

- Realizza un sistema di messaggistica in tempo reale sul modello IRC (Internet Relay Chat) con architettura distribuita e caratterizzato da
 - Anonimato dei relay server e degli utenti
 - Riservatezza del contenuto della comunicazione
- Tra utenti e server è interposta una serie di relay in modo che l'IP dell'uno sia nascosto all'altro (IRC è normalmente un sistema centralizzato)
- Ogni messaggio è cifrato a chiave simmetrica, con rekeying D-H. Cifratura nodo-nodo ed end-to-end per contrastare nodi rogue
- Utilizzabile con ogni client IRC attraverso un proxy locale
- Progetto con alterne vicende, release ferme al 2004, GPL.

IIP (Invisible IRC Project)

- Realizza un sistema di messaggistica in tempo reale sul modello IRC (Internet Relay Chat) con architettura distribuita e caratterizzato da
 - Anonimato dei relay server e degli utenti
 - Riservatezza del contenuto della comunicazione
- Tra utenti e server è interposta una serie di relay in modo che l'IP dell'uno sia nascosto all'altro (IRC è normalmente un sistema centralizzato)
- Ogni messaggio è cifrato a chiave simmetrica, con rekeying D-H. Cifratura nodo-nodo ed end-to-end per contrastare nodi rogue
- Utilizzabile con ogni client IRC attraverso un proxy locale
- Progetto con alterne vicende, release ferme al 2004, GPL.

Fine della prima parte, inizio della seconda parte...

Vediamo se funziona...

Bibliografia (1/2)

-  Tor website, <http://tor.freehaven.net/>
-  Roger Dingledine, Nick Mathewson, Paul Syverson, *Tor: The Second-Generation Onion Router*.
-  D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudo-nyms*, Communications of the ACM, 4(2), 1981.
-  Privoxy website, <http://www.privoxy.org/>
-  P. Biddle, P. England, M. Peinado, B. Willman, *The Darknet and the Future of Content Distribution*, proc. ACM Workshop on Digital Rights Management, 2002.

Bibliografia (2/2)

-  M. A. Calamari, *Sono le darknet il futuro della rete? Innovazione e libertà al confine tra ordine e caos*, proc. E-Privacy 2005, <http://e-privacy.firenze.linux.it>.
-  The Freenet Project, <http://www.freenetproject.org>
-  Invisible IRC Project, <http://www.invisiblenet.net/iip>
-  GNUnet, <http://gnunet.org>
-  Ants, <http://antisp2p.sourceforge.net>
-  MUTE File sharing, <http://mute-net.sourceforge.net>
-  Waste, <http://waste.sourceforge.net>