Invisible Irc Project

Anonymous real time communication

Yvette (vodka) Agostini - vodka@s0ftpj.org

E-Privacy 2003 Firenze 14 giugno 2003

Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

Radici del progetto

- creare un ambiente di lavoro collaborativo che garantisse la privacy e la riservatezze della comunita' di sviluppatori impegnati in progetti legati alla privacy e alla liberta' di parola
- freenet non possiede una caratteristica importante: un sistema di comunicazione real time
- il progetto è nato nell'autunno del 2001 per interesse di un programmatore: Intel Nop 0x90
- il codice è in ANSI C, e gira su *BSD, OSX, WIN*, linux, MacOS9
- l'architettura a 3 livelli tende a garantire l'anonimato degli utenti, dei server e delle comunicazioni

Linee guida

liberta’ di parola nel pieno rispetto di:

- privacy
- sicurezza
- anonimato

Freenet e IIP

- freenet è destinata a supportare contenuti statici, bassa velocita' , grandi volumi
- queste caratteristiche mal si prestano alla messaggistica e alla comunicazione real time
- freenet e iip sono simili solo per i seguenti aspetti:
  - peer to peer
  - architettura distribuita
  - utilizzo della crittografia

Sintesi delle caratteristiche

- Cifratura da nodo a nodo e tra estremi
- Traffico spurio per confondere l'analisi del traffico
- Architettura a 3 livelli per garantire anonimato degli utenti e dei server
- Nickserv e chanserv (qualcosa di simile): trent
- File dei nodi di riferimento si autoaggiorna
- Compatibilità con tutti i client IRC
- Interfaccia grafica per windows
- controllo del livello di flood del nodo
- multipiattaforma

Come funziona (molto in sintesi) IIP

Tra utenti e server esiste una rete di relays, di modo che:

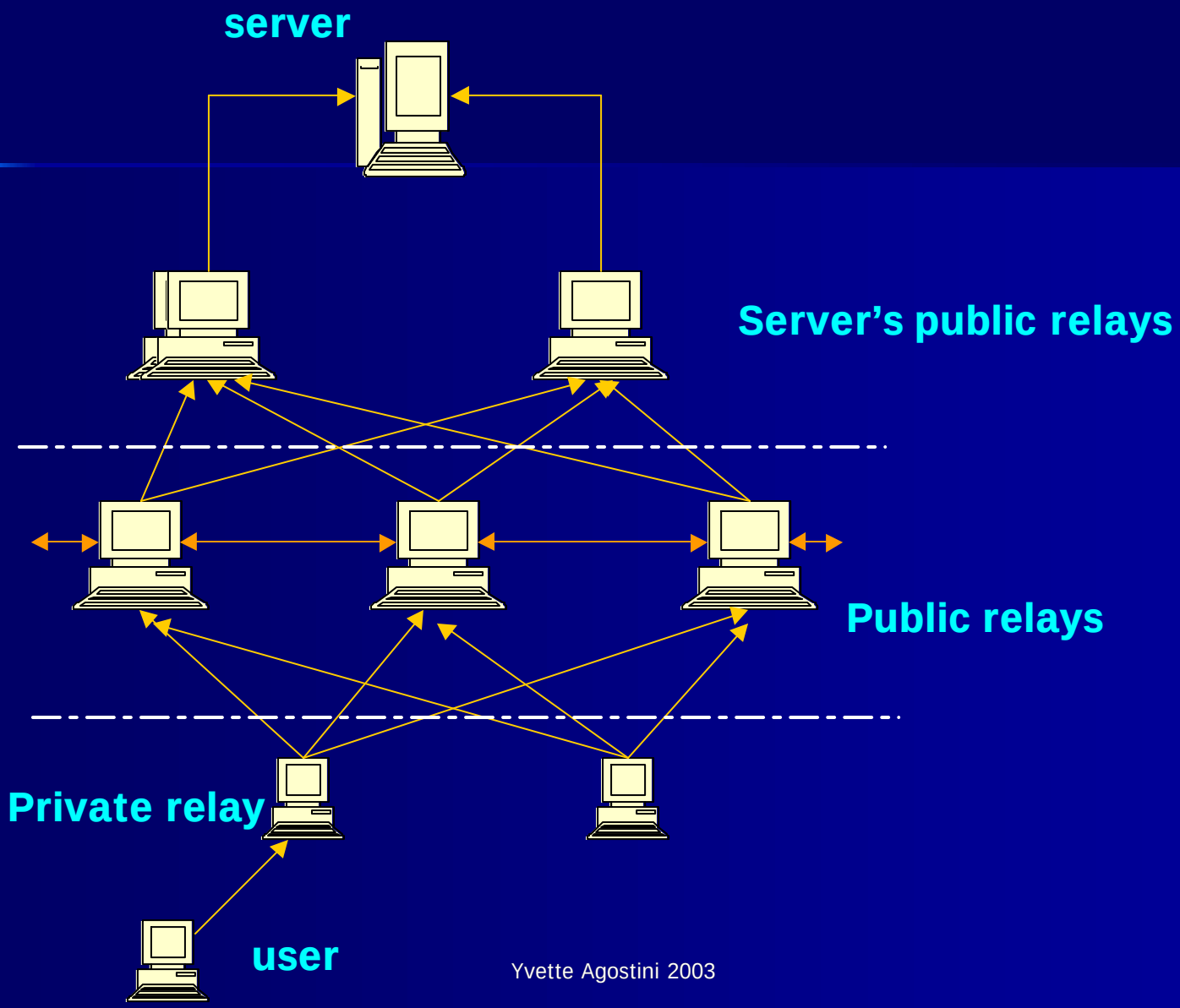
- gli utenti non conoscono l'indirizzo IP del server e il server non conosce gli indirizzi IP degli utenti
- ogni comunicazione nella rete è cifrata a non meno di 128 bit (Diffie-Hellman, SHA-1, Blowfish)
- ogni 52 blocchi di dati, la chiave di cifratura viene ruotata
- periodicamente viene generato traffico falso
- nel server IRC non esistono i comandi CTCP che consentono di conoscere l'indirizzo IP degli utenti

Architettura (1)

- avendo un server (ircd) e dei client (BitchX, mIRC, Xchat,ecc), siamo in presenza di una struttura centralizzata
- attraverso l'uso di una rete di relays si nasconde di fatto il server agli utenti e anche gli utenti rimangono anonimi per il server

IN pratica l'utente non ha modo di conoscere l'indirizzo IP del server, ne' il server ha modo di conoscere l'IP del client

Architettura (2)



Utilizzo della crittografia a protezione della privacy (1): da nodo a nodo

- Ogni connessione tra i differenti nodi della rete e' cifrata.
- L'algoritmo utilizzato e' Blowfish a 128 bit (tosto!!!)
- La chiave di sessione e' scambiata utilizzando il Protocollo di scambio della chiave pubblica di Diffie-Hellman (utilizzato anche in IPSEC)
- Le chiavi pubbliche dei nodi vengono mantenute nel file nodes.ref

PROTEZIONE DAL MONITORAGGIO ESTERNO, MA NESSUNA PROTEZIONE NEI CONFRONTI DI UN SERVER "AVVELENATO"

Utilizzo della crittografia a protezione della privacy (2): end to end

- Per contrastare il rischio dei nodi avvelenati viene aggiunto un livello aggiuntivo di cifratura

- La comunicazione tra utente e server viene cifrata prima con la chiave del server IRC (che viene letta dal file nodes.ref), poi con la chiave del relay (anche essa letta dal file nodes.ref)

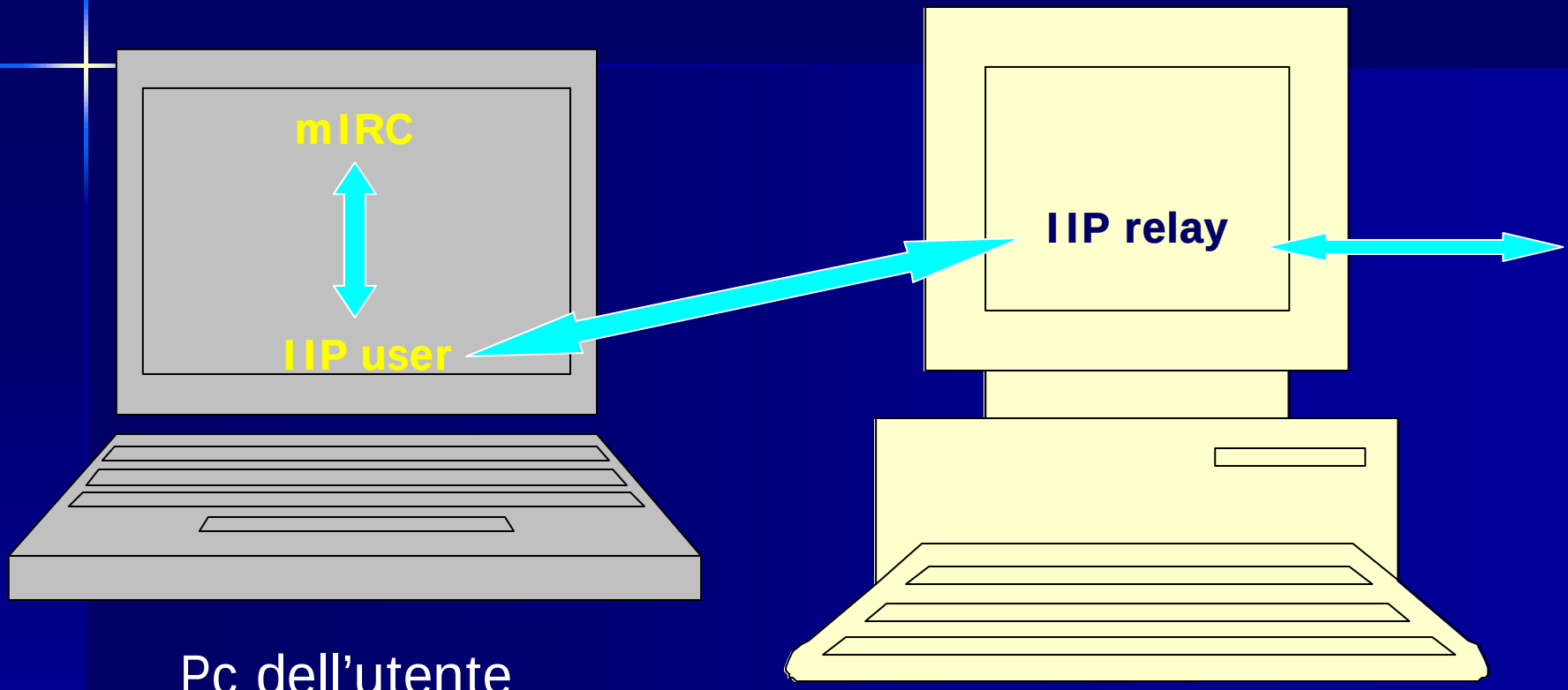
- se anche la trasmissione dovesse essere decifrata in un nodo avvelenato, rimarrebbe cmq protetta dalla cifratura end to end tra utente e server

FORZA DELLA CIFRATURA ASIMMETRICA E DELLA DOPPIA CIFRATURA

IIP dal punto di vista utente (1)

- la connessione all'irc server avviene tramite una specie di proxy: isproxy (*NIX) o IIP (Winx)
- il proxy e' multipiattaforma e di facile installazione e configurazione
- una volta installato il proxy si accede a IRC tramite il client solito (mIrc, BitchX, ecc..) impostandogli l'uso del proxy locale
- e' il proxy che si fa carico della parte crittografica e dei vari meccanismi di sicurezza: per l'utente la cosa e' totalmente trasparente

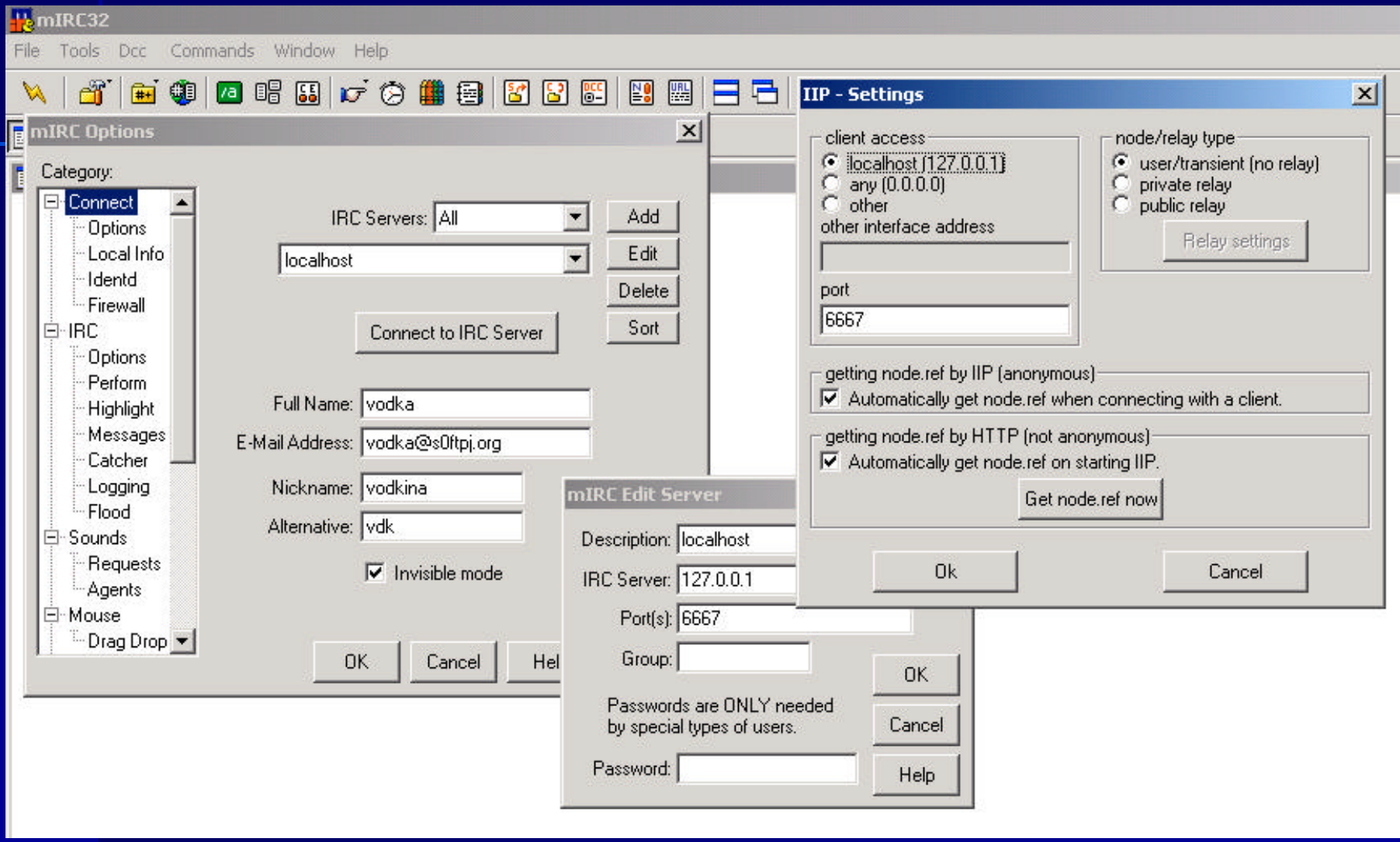
IIP dal punto di vista utente (2)



Pc dell'utente

PC che funge da Relay

Schermata di esempio IIP (win2k)



Altre funzionalita' di IIP

- esiste un servizio di registrazione dei nick e dei canali: trent
- i nick registrati tramite trent possono fruire della funzionalita' di **anonymail**
- indirizzo di mail nella forma nickname@iipmail.net
- possibilita' di ricevere messaggi mail da utenti interni ed esterni al network iip e spedire solo a utenti interni al network iip

Utilizzi particolari: yodelbank (1)

- yodelbank (http://www.yodelbank.com) e' un servizio bancario online che dovrebbe garantire il completo anonimato delle transazioni che si svolgono al suo interno
- e' un servizio basato su IIP, DMT (Digital Money Trust), FreeTraders (una sorta di ebay basata su denaro digitale quotato in oro e sul concetto di scambio)
- IIP viene utilizzata come "sportello" della banca attraverso il chan #yodel e utilizzando il bankbot ovvero un bot adattato a impiegato di banca automatico e virtuale

Utilizzi particolari: yodelbank (2)

- bankbot e' in pratica un front-end IRC
- la comunicazione tra il front-end (bankbot) e il back-end yodel e' realizzata in XML-RPC
- non tutto il codice di yodelbank e' pubblico
- le divise trattate da yodelbank sono: euro, dollaro americano, e-gold (valuta digitale quotata in oro), DRAN (valuta digitale del Digital Money Trust quotata su un mix di assets differenti), GOD (Goods On Demand, un "diritto di credito" per lo scambio di beni/servizi in FreeTraders)

Reperire IIP

- Il software e' distribuito sotto licenza Berkely Software/Standard Distribution (BSD)
- il sito di riferimento e':

http://www.invisiblenet.net/iip/

- l'applicazione e' disponibile per piattaforme diverse: *NIX, MACOSX, WINx
- la documentazione e' tutta in inglese ma il software e' di semplicissimo utilizzo

Risorse utili per approfondire o esplorare

Digital Monetary Trust: http://dmt.orlingrabbe.com/

E-gold: http://www.e-gold.com

FreeTraders: http://www.freetraders.org/

Canali interessanti in IIP:

#iip dove si incontrano gli utenti e gli sviluppatori di iip

#anonymous conversazioni generiche

#yodel dove chiarirsi dubbi e parlare con i fondatori e gestori di yodelbank

Invisible Irc Project

Anonymous real time communication

Yvette (vodka) Agostini - vodka@s0ftpj.org

E-Privacy 2003 Firenze 14 giugno 2003