

TOR

Enrico Cherubini
<kevin@bestkevin.com>

- Presidente del Linux User Group di Verona
- Lavora per Multilink Spa/Infracom Spa come amministratore dei server di produzione linux based
- E' libero professionista con la propria società InfoSysNet Snc

TOR

Obiettivi: In questa presentazione analizzeremo gli aspetti fondamentali e di utilizzo della rete anonimizzatrice distribuita TOR – The Second Generation Onion Router

TOR

La necessita' di avere privacy

- Non voglio che vengano tracciate le mie abitudini (google analytics, referrer incrociati)
- Voglio poter partecipare a forum specifici (aids, droga)
- Voglio poter dialogare con amici in Cina
- Non voglio lasciare traccia durante un controllo giudiziario su server illegali

TOR

TOR e' un sistema a bassa latenza, garantisce quindi la possibilita' di un uso funzionale anche con sistemi interattivi (ssh, telnet, http...)

TOR

Senza accorgimenti in rete non c'e' privacy !!! Chiunque si trovi nel mezzo di una comunicazione in chiaro ne puo' analizzare i contenuti (sniffing), ed anche le connessioni criptate possono essere "facilmente" compromesse "man in the middle"

TOR

Senza accorgimenti chiunque puo' essere soggetto a censura, sia bloccando la persona che posta le proprie idee, sia scollegando il server che ospita il forum, il blog, etc...

TOR

Senza accorgimenti nessun accesso alla rete puo' essere anonimo: tracciatura delle connessioni dialup/ADSL, log dei mailserver e dei server web, etc...

TOR

Alcune definizioni:

Anonimato significa non poter essere riconosciuti in un insieme. Insiemi più numerosi aumentano la qualità dell'anonimato, ovvero il “grado di anonimato”

TOR

Tipi di comunicazione anonima:

Alice comunica con Bob attraverso il mezzo M.

- M e' anonimo in avanti se nessuno (nemmeno Bob) puo' risalire all'identita' di Alice.
- M e' anonimo all'indietro se nessuno, nemmeno Alice, puo' ricondursi a Bob.

TOR

Questo vale anche per i servizi:

- Alice accede ad un servizio in maniera anonima in avanti quando nessuno puo' sapere l'IP del client;
- Bob offre un servizio anonimo all'indietro se nessuno puo' sapere l'indirizzo IP del server che offre tale servizio;
- Si dice riservato un accesso i cui dati scambiati siano noti solo ad Alice e Bob.

TOR

Qual'e' la base della sicurezza ?

Crittografia !!!

- **assimmetrica:** chiave pubblica e privata
- **simmetrica:** le parti condividono la chiave segreta
- **Open Source:** e' fondamentale che il codice di cifratura sia pubblico

TOR

Il problema dell'usabilità
Affinche' un sistema si diffonda deve
essere usabile, e per essere usabile
deve avere **bassa latenza**
Il remailer anonimo mixmaster e' un
esempio di alta latenza

TOR

Onion Router invece...

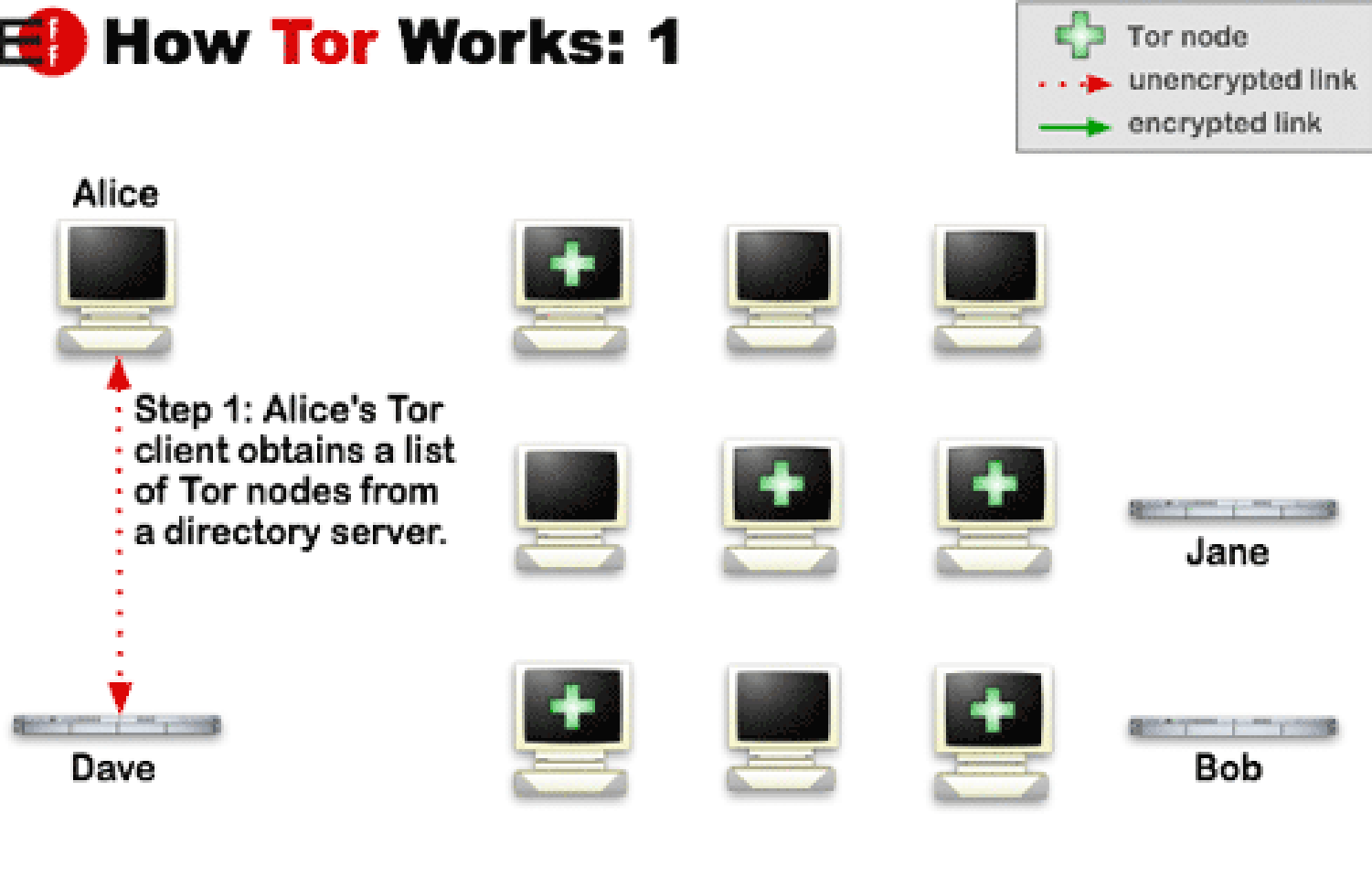
Gli Onion Router garantiscono una **bassa latenza** (o almeno accettabile), permettendo quindi un'interazione in tempo reale (http, ssh, etc)

TOR

- Resiste alle piu' comuni tecniche di analisi del traffico: tutti i router devono essere compromessi;
- Viene incapsulato il traffico TCP in strutture dati (onion) di volta in volta cifrate;
- Instradamento dei pacchetti attraverso vari nodi;

TOR

How Tor Works: 1

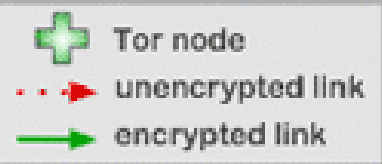


TOR

Alice ottiene da Dave (il Directory Server) la lista degli Onion Router e delle loro chiavi pubbliche (il link **non** e' criptato)

TOR

How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



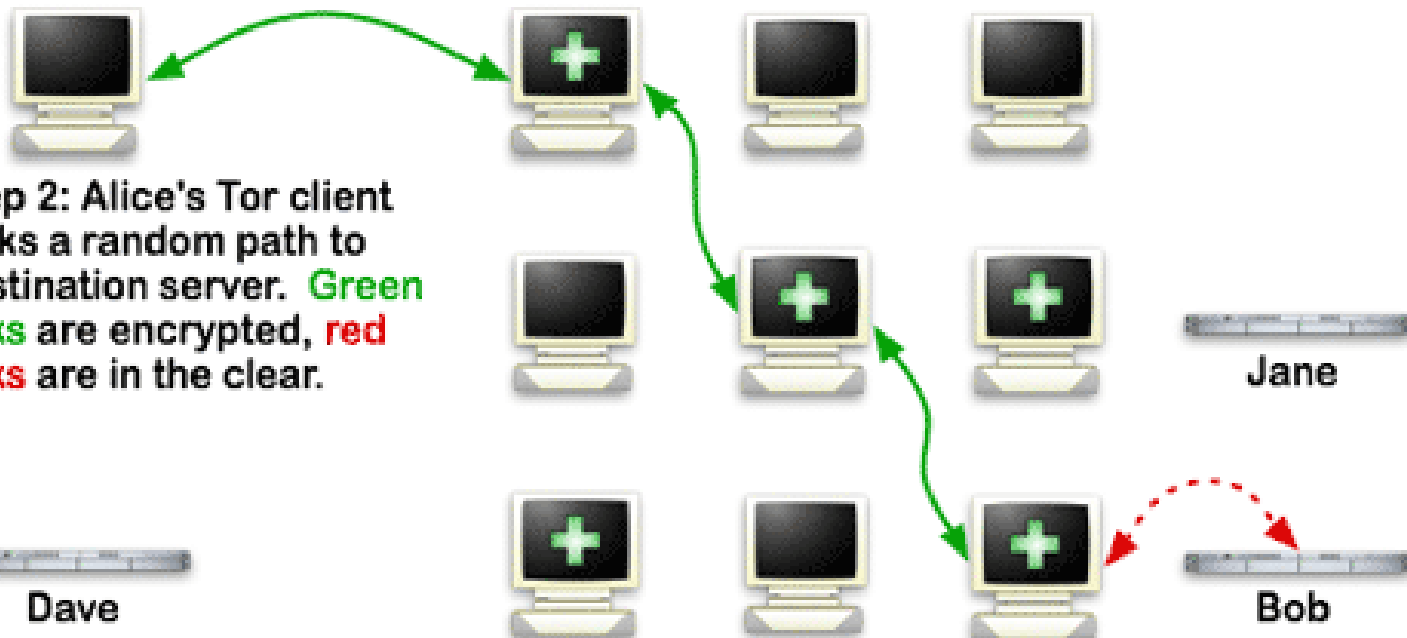
Jane



Dave



Bob

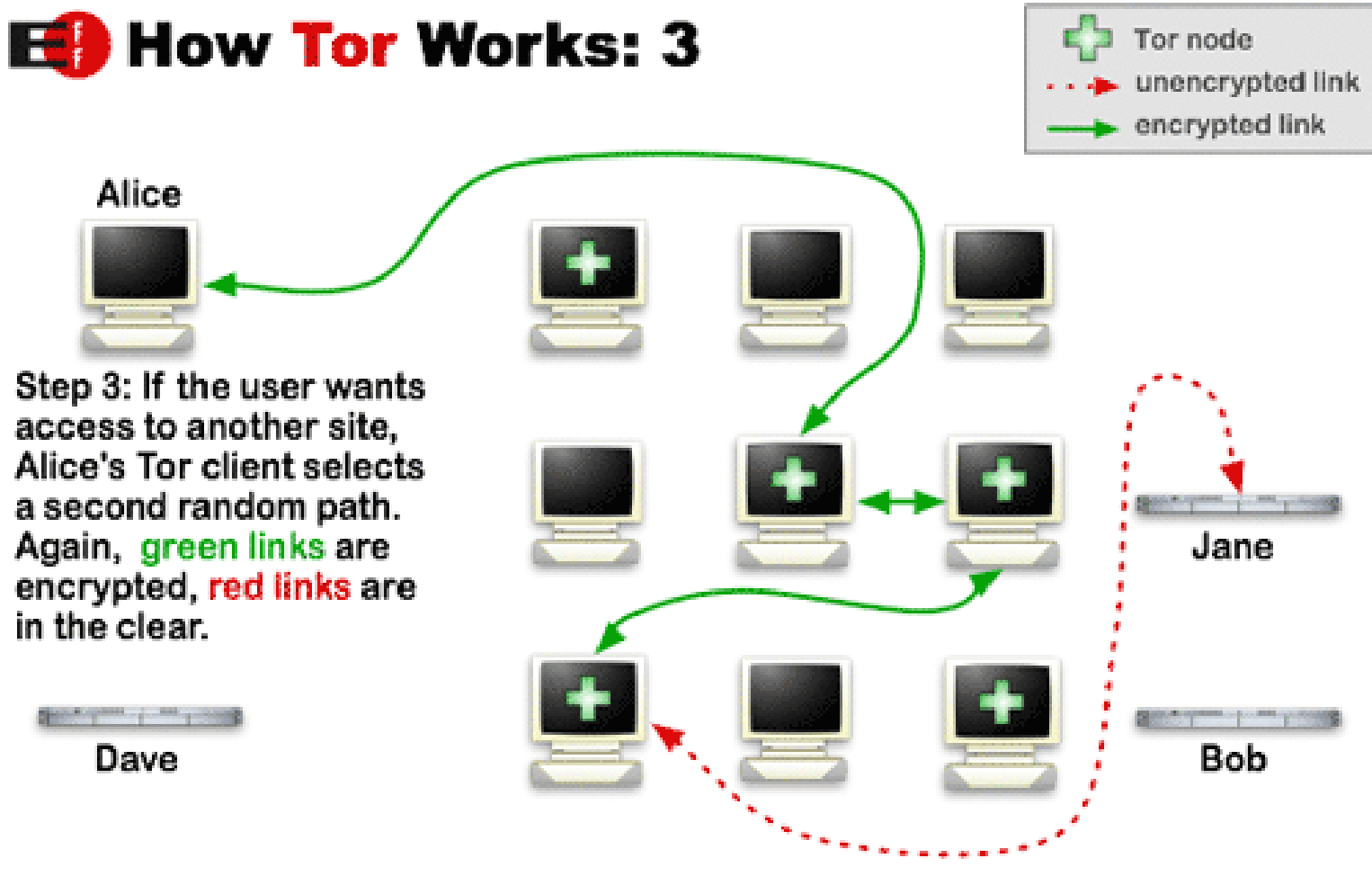


TOR

Alice crea un percorso attraverso vari nodi TOR, tutti criptati. L'unica connessione non criptata e' dal nodo di uscita verso il server di destinazione.

TOR

How Tor Works: 3



TOR

Se Alice vuole accedere ad un'altra risorsa tramite TOR viene creato un nuovo percorso tra Onion Router diversi

TOR

Quali vantaggi ?

- Anonimato in avanti “perfetto” grazie alla costruzione incrementale di percorsi tra server diversi, con chiavi diverse ed effimere;
- Variazione nel tempo dei percorsi;

TOR

ancora...

- Possibilita' di instradare varie connessioni sullo stesso percorso (riduzione delle latenze);
- Topologia Leaky Pipe per ridurre la possibilita' di analisi dei percorsi;

TOR

...ed ancora...

- Uso di TLS a chiave asimmetrica, per impedire che i messaggi vengano modificati in transito (cambiare un *ls* in *rm*) o che qualcuno impersoni un router;
- Controllo della congestione mediante messaggi end-to-end;
- Controllo dell'integrita' dei dati end-to-end;

TOR

Con TOR evitiamo l'attaccante che possa:

- Controllare il traffico su parte della connessione;
- Generare, modificare o alterare il traffico;
- Gestire lui stesso un Onion Router;
- Compromettere una parte dei nodi.

TOR

Il problema sorge con i sistemi a bassa latenza, proprio analizzando l'interezza della connessione facendo collimare richieste e risposte in spazi temporali

TOR

Caratteristiche interessanti

- E' indipendente dall'applicazione (basta che sia uno stream TCP);
- Si interfaccia tramite SOCKS;
- Puo' essere usato con Privoxy, un proxy anonimizzatore filtrante.

TOR

Hidden Services

Sono classici servizi TCP (ad esempio web) forniti in maniera anonima, senza rendere noto l'IP destinatario. E' così possibile offrire servizi senza rischi di censura o DoS.

TOR

Hidden Services: come ?

- Bob rende noto ai router il proprio servizio che viene indicizzato, otterra' cosi' il suo indirizzo onion:
`http://w5jddmtglec2rgaz.onion`
- Alice viene a conoscenza di tale indirizzo;
- Alice contatta un RVP (Rendez Vous Point) e chiede di essere messa in contatto con l'indirizzo dell'HS;

TOR

Hidden Services: come ?

- Il RVP contatta quindi Bob e apre una connessione con l'HS;
- A questo punto Alice puo' utilizzare l'HS attraverso il RVP: Alice non sa dove si trova Bob e viceversa.

TOR

Abusi ?

- Di per se' TOR non introduce nuovi sistemi di abuso delle reti: gli spammer hanno altri sistemi di lavoro meno onerosi, i terroristi possono benissimo usare GPG o altri algoritmi;
- Ci sono tante macchine con OS proprietario gia' compromesse da usare per attacchi;

TOR

Exit Point

Il verso problema e' l'exit point che risulta nei log. Ci sono regole per decidere quali servizi offrire e quali negare: *:25

TOR

Exit Point non etici

- Un problema potrebbero essere gli EP che sniffano e fanno proxying del traffico;
- man-in-the-middle ?

TOR

Privoxy

Privoxy e' un proxy filtrante da usare nella navigazione assieme a TOR.

E' fondamentale per evitare la tracciatura tramite DNS.

TOR

Esempi pratici

- File di configurazione (torrc, tsocks.conf, privoxy config, firefox)
- Analisi del traffico senza e con;
- Risultati via web;
- Esempi di Hidden services;
- Esempio di abuso come EP

TOR

Domande ?!?

TOR

Grazie !!!

Arrivederci presso l'ITIS Marconi il

28 maggio 2006

per la conferenza

GNU/Linux e la sicurezza personale

TOR

Si ringraziano:

- L'Universita' di Verona per l'ospitalita';
- Il Prof. Quaglia;
- Gianni Bianchini e Marco A. Calamari, autori originali delle slides da cui queste sono state tratte;

Lavoro rilasciato secondo la licenza GPL v.2 o successiva.