Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2015/16

Lezione XXI: TOR

Onion Routing

Onion Routing (OR) è una tecnica sviluppata dal Naval Research Laboratory di Washington.
Il traffico viene instradato in una serie (mutevole) di *onion router* in maniera tale da rendere difficile il tracciamento delle attività.
Gli onion router costituiscono dei mix di Chaum.

Mix di Chaum

Mix di Chaum

Un mix riceve messaggi di lunghezza fissa, li cripta, aspetta di averne in numero sufficiente da garantire un certo livello di anonimato e inoltra i messaggi (in ordine arbitrario) ad altri mix.

Onion router

- Gli onion router intermedi non hanno informazione sufficiente per tracciare mittente/destinatario e traffico
- Rimane una certa criticità degli exit node e (minore) dei nodi d'entrata

Riassumendo

L'anonimato nella navigazione web è un problema piuttosto complesso. Varie difese:

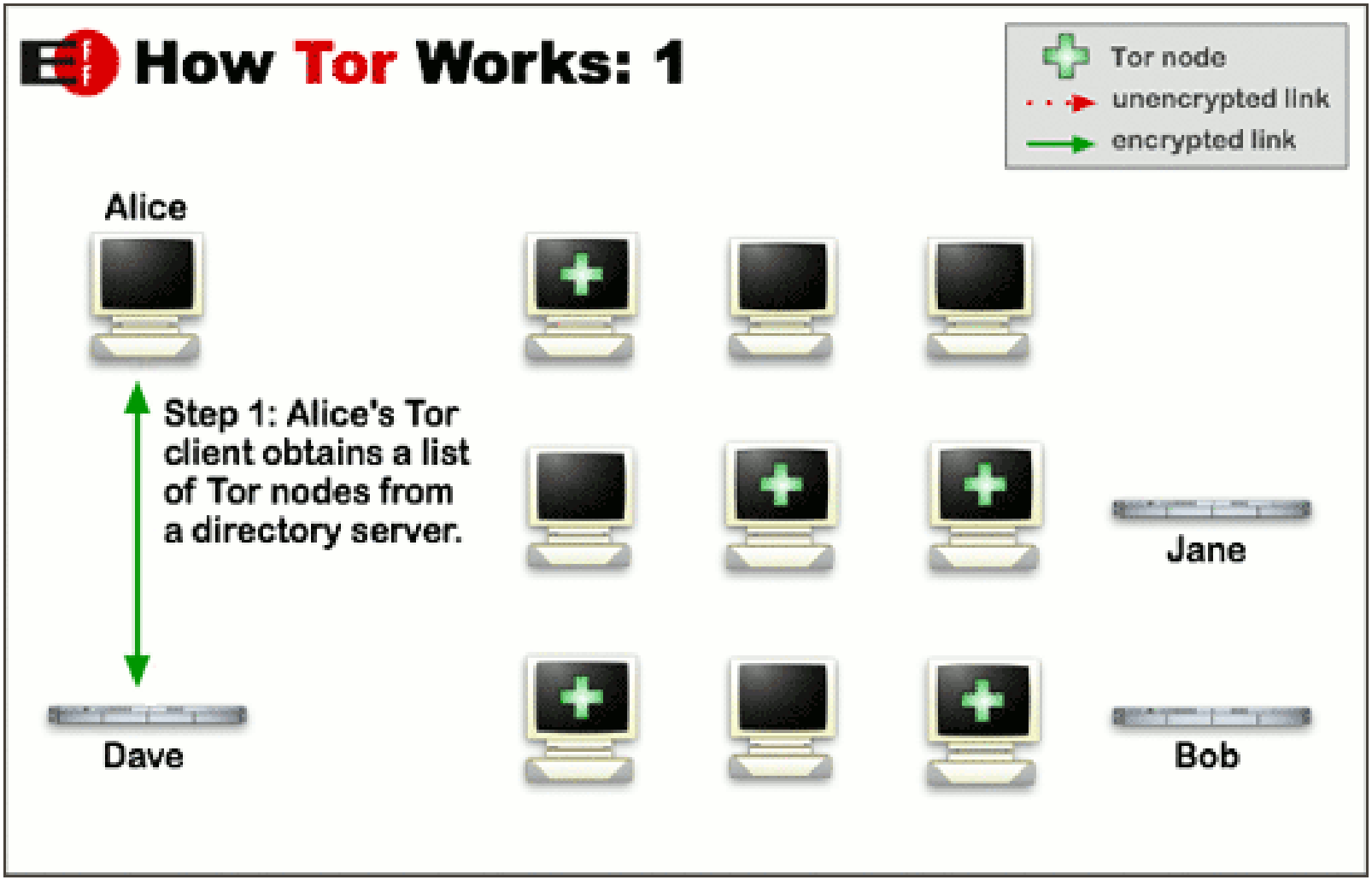
- HTTPS
- Proxy
- Onion Routing

TOR

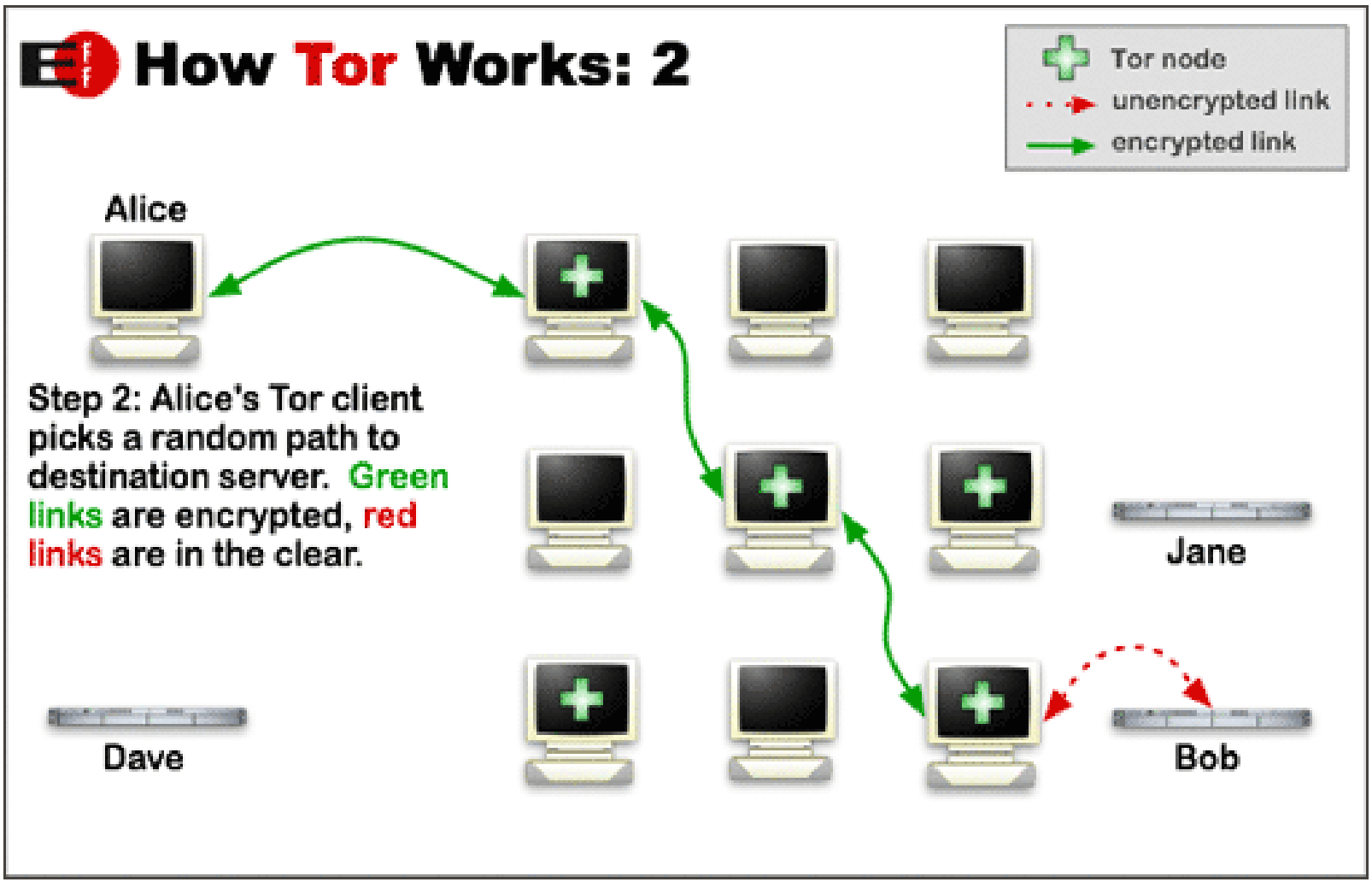
TOR (The Onion Router project) è l'evoluzione piú recente del concetto di OR. Sviluppato da NRL, open source, supportato da EFF.

Il progetto fa parecchi sforzi per rendere il prodotto comprensibile e utilizzabile anche da utenti inesperti (il numero di utenti è un valore per l'anonimato).

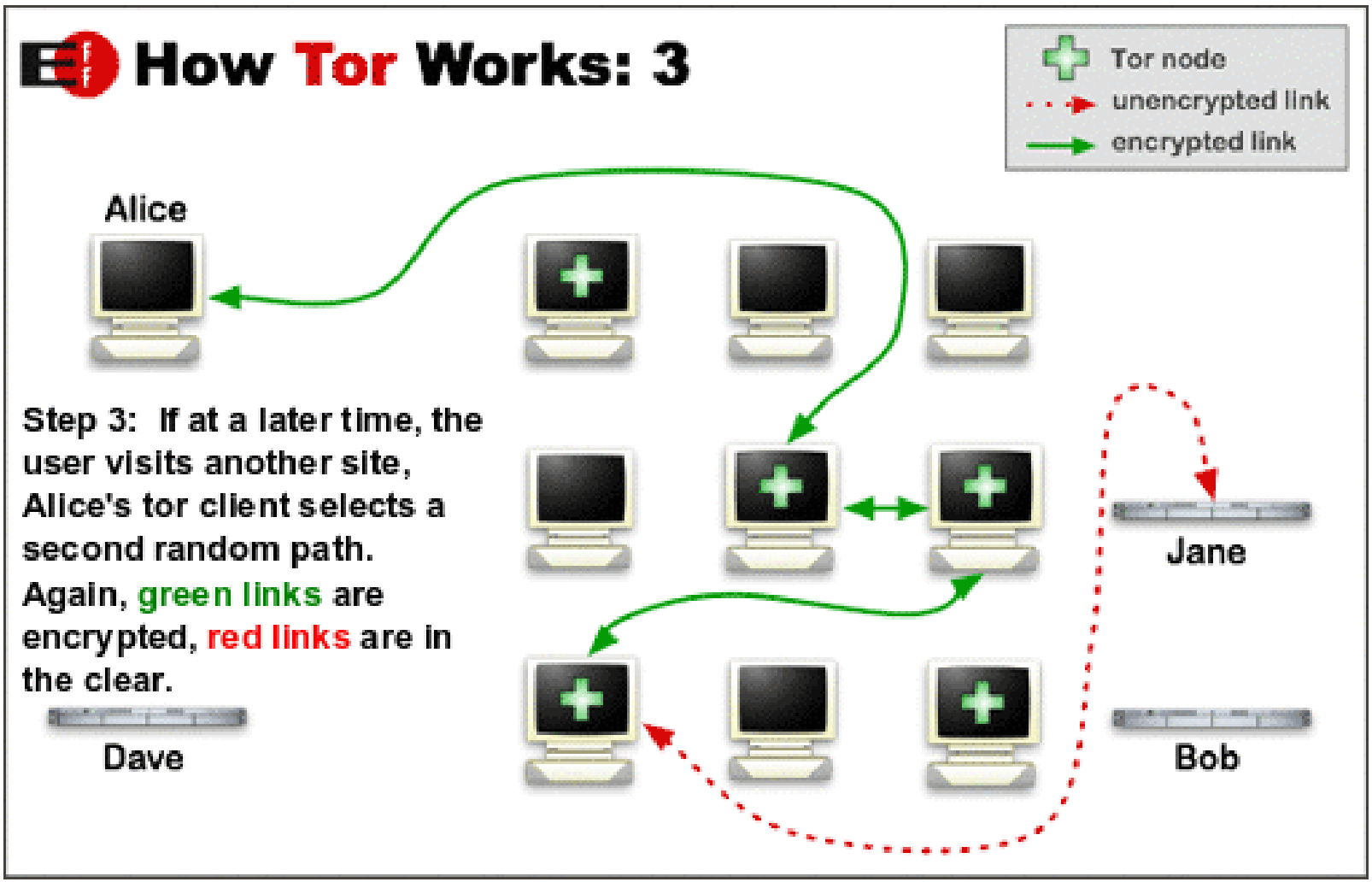
Onion routing con TOR



Onion routing con TOR



Onion routing con TOR



Circuiti

L'instradamento di ogni messaggio viene detto circuito

- Ogni nodo del circuito conosce solo il nodo precedente e successivo (non origine e destinazione)
- Molte richieste diverse vengono multiplexate in un unico circuito
- Robusto rispetto alla compromissione o l'introduzione di onion router malevoli
- Nodi trusted operano da *directory server* iniziali

Struttura di una rete TOR

- Nodi utenti hanno un Onion Proxy (OP)
- Onion Router (OR) connessi tra loro con TLS
- Gli OR hanno una long-term key e short-term "onion" key
- L'unità di trasmissione è la cella, di dimensione fissa di 512 byte

Uso delle chiavi

La *long-term identity key* viene usata per

- firmare la descrizione del router: certificati TLS, chiavi, metadati, *exit policy*
- firmare gli elenchi di router

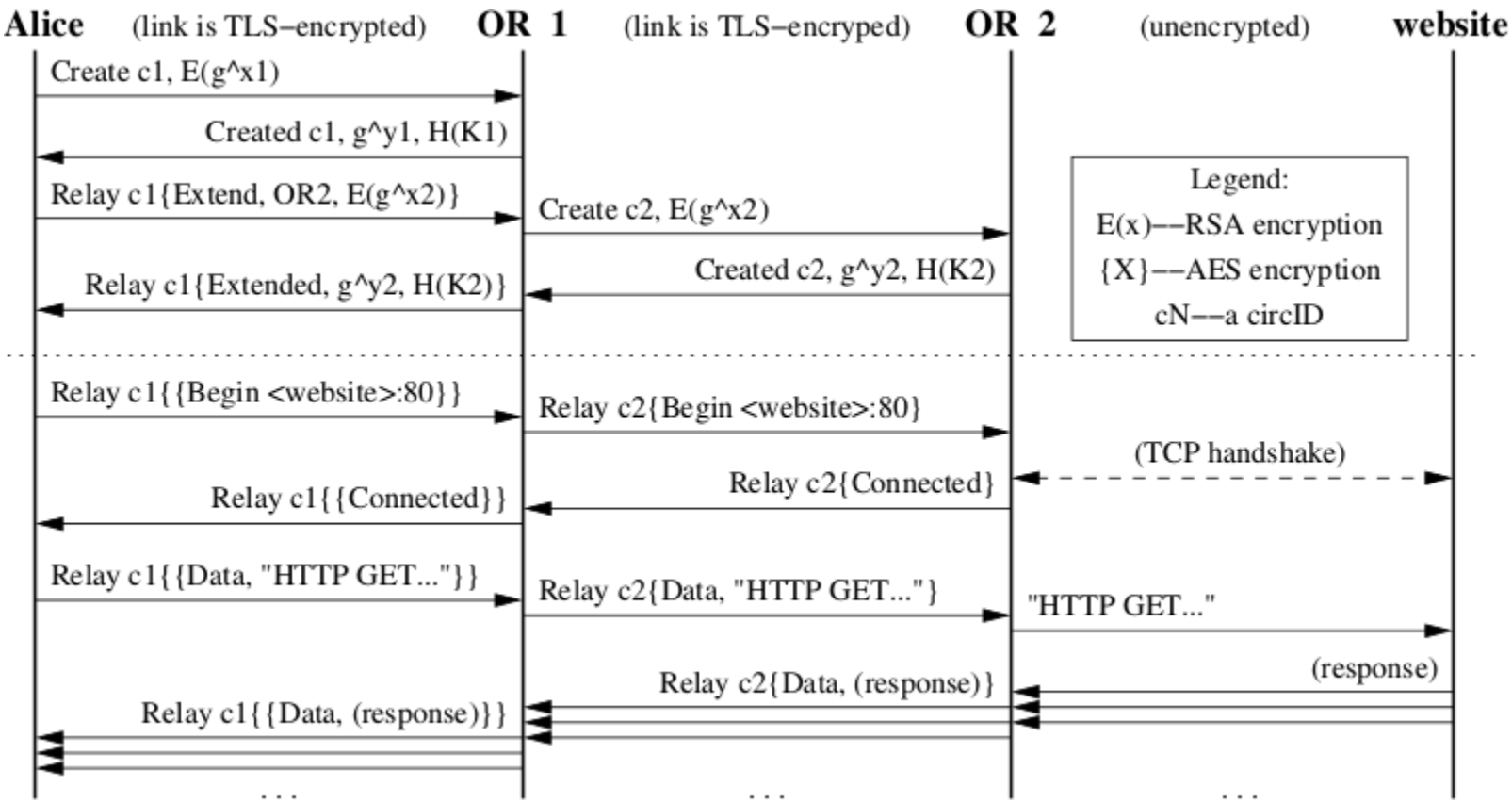
La *short-term key* (onion key) per:

- decrittare le richieste di circuiti
- negoziare chiavi una tantum (ephemeral key) che garantiscono la *forward secrecy*

Circuiti

- l'OP costruisce un circuito in background, e diversi stream utente vengono multiplexati sullo stesso circuito
- Ogni minuto viene creato un nuovo circuito

Creazione di un circuito



La prima fase *estende* il circuito, poi c'è il relay del traffico

Creazione dello stream

L'OP sceglie quale OR può fare da exit node (ognuno ha una *exit policy*)
Solo TCP stream possono essere creati (UDP, e quindi le risouzioni DNS, rimangono problematiche: vedi `http://code.google.com/p/torsocks/` per una soluzione)
Un protocol cleaner è necessario per evitare che informazioni rilevanti finiscano nello stream.

Riassumendo

TOR

- il maggior progetto di Onion Routing
- permette la creazione di circuiti anonimi
- necessita di un protocol cleaner