E-PRIVACY 2010

Mixminion: il ritorno

PREMESSA

Prima di tutto: che tipo di presentazione?

Presentazione descrittiva dello stato attuale e degli sviluppi futuri che si vogliono raggiungere;

Descrizione della qualità del lavoro in gioco e delle competenze necessarie;

Propaganda-Promozione-Divulgazione interessata

MOTIVI: IL TRAFFICO

Andamento in costante aumento del traffico in rete a prescindere dal momento difficile, l'aumento è indotto anche dal mutare dei contenuti;

Analogo costante aumento del numero di messaggi di posta elettronica scambiati;

Qualità delle informazioni veicolate dal flusso di email;

SALVAGUARDIA TRAFFICO MAIL

I motivi che inducono la necessità di anonimizzare il traffico standard di Internet sono validi anche per il flusso di dati email;

L'informazione trasportata dal flusso email è più ricca di significato anche se di entità inferiore rispetto al flusso degli altri protocolli internet;

UNA SOLUZIONE: IL REMAILER

Una possibile soluzione per lo scopo di rendere anonimo il traffico è l'adozione di un REMAILER;

Il REMAILER è un server che, posizionato tra mittente e destinatario, riceve e ritrasmette il messaggio email nel suo cammino;

L'operazione di ritrasmissione avviene utilizzando informazioni contente nel messaggio e senza rivelare dati del mittente;

TIPI DI REMAILER

Nel tempo i REMAILER si sono evoluti per garantire un livello sempre maggiore di sicurezza nell'anonimato della trasmissione;

Esistono tre passi evolutivi dell'implementazione di questi componenti software:

- Tipo I – Cypherpunk
- Tipo II – Mixmaster
- Tipo III - Mixminion

Tipo I - Cypherpunk

Meccanismi adottati:

- Sostituzione header
- Cifratura del contenuto con chiave pubblica del server
- Riordino casuale dei messaggi in uscita
- Ritardo nella trasmissione
- Catene di server
- Risposta con recapito anonimo (reply-block)

Tipo II: Mixmaster

A carico del client:

- Scomposizione messaggio
- Cifratura delle parti
- Incapsulazione in pacchetti di uguale dimensione

Trasmissione su server distinti

Riordino

Non esiste bidirezionalità

Compatibilità con Cypherpunk

Tipo III: Mixminion

- Al posto dell'SMTP usa delle connessioni SSL tra server e per accettare i messaggi dagli utenti
- I messaggi inviati e quelli di risposta risultano indistinguibili
- Ricezione di risposte anonime usando dei reply-block a uso singolo, "Single Use Reply Blocks" o "SURBs"

Stato del progetto Mixminion

Il progetto, il cui software è in fase beta, è stato sviluppato fino al 2007

in seguito il team di sviluppatori si è focalizzato su TOR e quindi lo sviluppo di Mixminion si è arrestato lasciando due componenti non implementati

Interfaccia grafica e directory server

COMPONENTI DA SVILUPPARE 1

l'interfaccia grafica verrà creata in un ambiente di sviluppo grafico multipiattaforma e fornirà lo strumento di contatto amichevole con il client;

il directory server è un server che all'interno della rete mixminion fornisce ai client informazioni sulle chiavi correnti, sulle capacità e sullo stato dei nodi mix

COMPONENTI DA SVILUPPARE 2

Questi server di directory devono essere sincronizzati e ridondanti: si perde sicurezza se i client hanno informazioni differenti sulla topologia della rete e sulla risponibilità dei nodi

Quindi non essendo una semplice questione di convenienza per i client ottenere informazioni aggiornate sui mix server,il servizio di directory è specificato come parte dello standard.

COMPONENTI DA SVILUPPARE 3

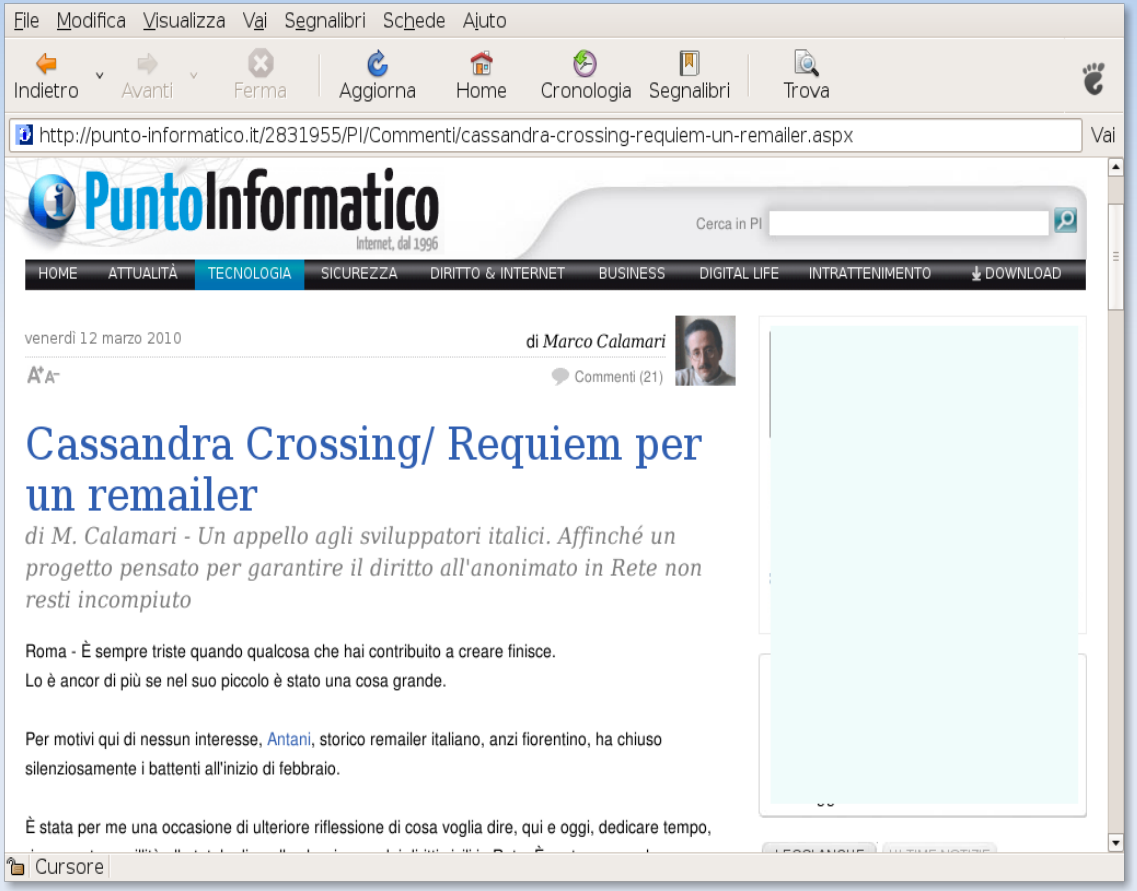
I directory server lavorano assieme per assicurare dati completi e corretti → sicurezza che un dato certificato di un mix è stato validato da un numero minimo di altri mix server;

Lo scopo è quello di trovare un bilanciamento tra

a) fornire ai client informazioni accurate ed aggiornate e

b) evitare che un exploit di directory server possa manipolare il comportamento dei client

ADESIONI AL PROGETTO



Il progetto è appena partito

L'avvio coincide con la pubblicazione su PI di una articolo di MC

ADESIONI AL PROGETTO 2

Allo stato attuale a quell'appello hanno risposto Francesco, Andrea, Luigi, Giovanni (il sottoscritto), Lorenzo

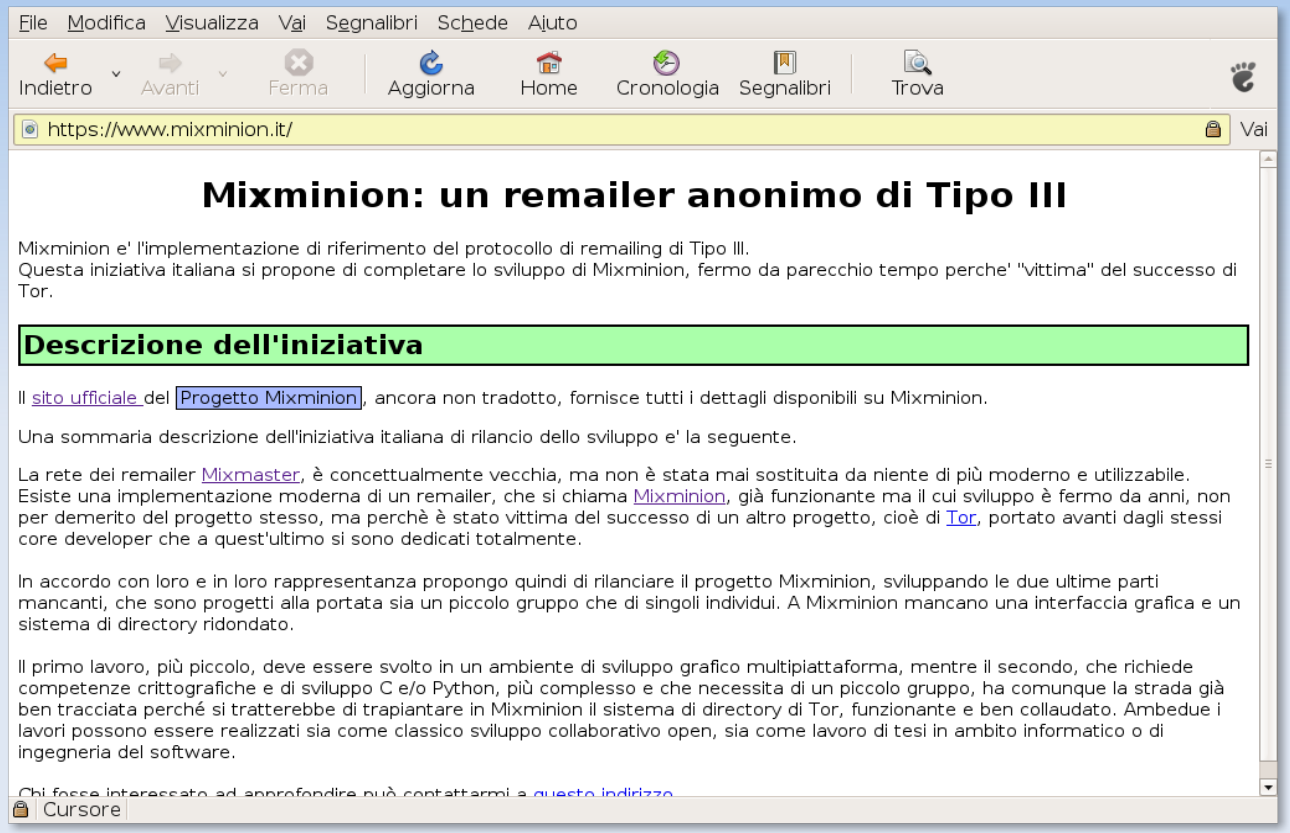
L'estrazione dei partecipanti è varia

Il nucleo di aggregazione è la lista

La lista del gruppo di sviluppo italiano di Mixminion

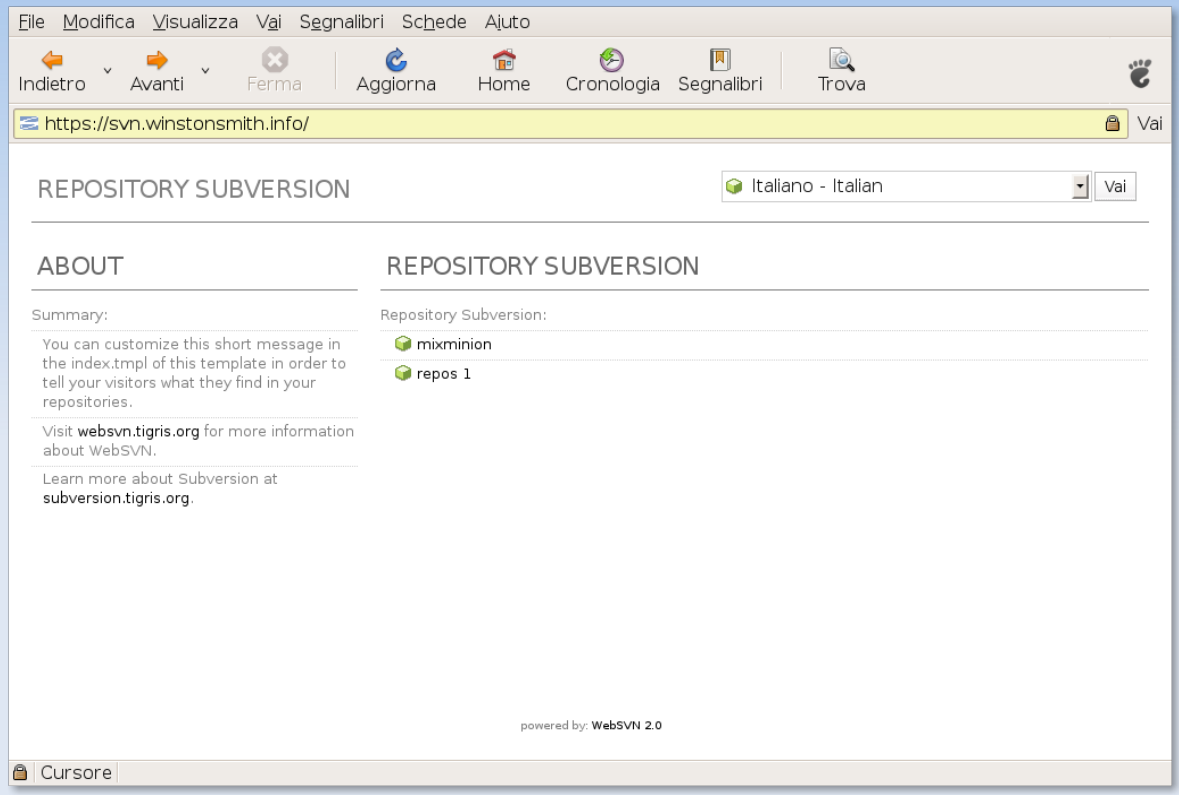
<mixminion-it@winstonsmith.org>

GLI STRUMENTI 1



Nucleo iniziale del sito italiano su Mixminion

GLI STRUMENTI 2



Sito con il repository subversion destinato ad accogliere il codice

CONCLUSIONI

Due speranze:

> "[Agente Smith] Allora siamo d'accordo Sig. Reagan"
> "[Cypher] Vede io so che questa bistecca non esiste. So che quando la infilerò in bocca Matrix suggerirà al mio cervello che è succosa e deliziosa. Dopo nove anni sa che cosa ho capito? Che l'ignoranza è un bene"

che un numero sempre maggiore di persone capisca la deriva a cui andiamo incontro senza antidoti: abbiamo bisogno di chiunque, ciascuno con le proprie capacità

CONCLUSIONI 2

Speriamo di portare tra un anno risultati tangibili di questo impegno

GRAZIE A TUTTI!