

Anonimato e Privacy su Internet



Moreno Marzolla
INFN Sezione di Padova
moreno.marzolla@pd.infn.it
<http://www.dsi.unive.it/~marzolla>

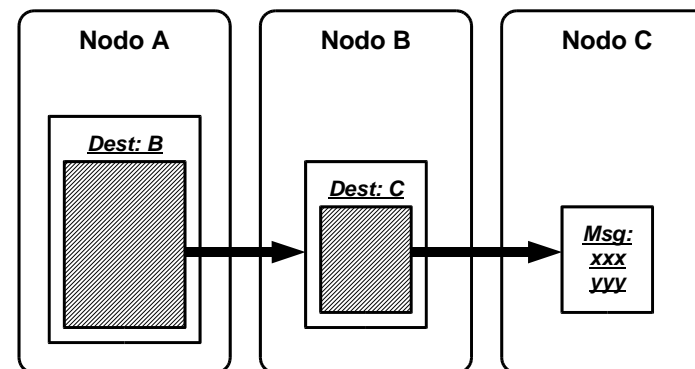
Riferimenti

- Lorrie Faith Cranor, *“Introduction to P3P”*, <http://p3pbook.com/p3p-intro0702.ppt>
- David Chaum, *“Security without Identification: Card Computers to make Big Brother Obsolete”*
- Anonymity Bibliography, <http://freehaven.net/anonbib/topic.html>

Aspetti negativi del WWW

- Totale assenza di privacy
 - Nell'implementazione “di default”
 - La privacy può essere implementata “in cima” al web
 - Onion Routing (www.onion-router.net)
 - Tor (tor.eff.org)
- Onion Routing: idea di base
 - Ciascun nodo possiede una sua chiave crittografica
 - Ciascun nodo è in grado di decifrare l'id del prossimo nodo della catena...
 - ...ma non è in grado di decifrare l'id dei successivi, né può espere dove è transitato il messaggio prima di arrivare a lui
 - Anche in TV: “Portami dal tuo capo”, episodio della serie “Agente Speciale”

Esempio



Osservazioni

- Ogni volta che si elimina un layer di crittografia, la dimensione del messaggio diminuisce
 - Ciascun nodo deve aggiungere padding casuale in fondo al messaggio decrittato per mantenerne la dimensione

Formalmente / 1

- Supponiamo che un nodo all'indirizzo X voglia comunicare un messaggio T ad un nodo Y
- Caso semplificato: Esiste un nodo intermedio (*mix*) M1 con chiave pubblica K1. X invia al mix il seguente messaggio:

$K1(R1, KY(R0, T), Y)$

Ove R1, R0 sono stringhe casuali

Formalmente / 2

- Il mix opera la seguente trasformazione

$K1(R1, KY(R0, T), Y) \rightarrow KY(R0, T)$

- In pratica, decifra con la propria chiave privata, scarta R1 e passa a Y il messaggio $KY(R0, T)$

Formalmente / 3

- In generale, usando N mix:

$K1(R1, K2(R2, \dots KN(RN, T), Y), KN-1 \dots)$

Formalmente / 4

- Come gestire le risposte?
- Il mittente X inserisce come parte del messaggio T il seguente *reply onion*

$K_1(R_1, X), K_x$

con K_x chiave pubblica scelta per l'occasione

Formalmente / 5

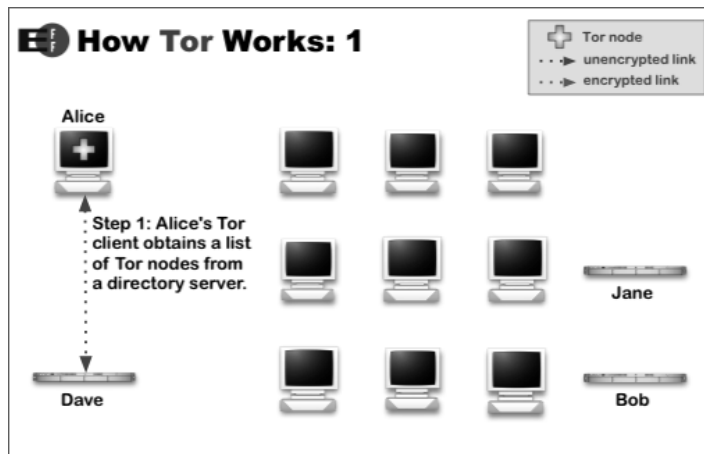
- Y usa il *reply onion* per mandare la risposta W preparando il seguente messaggio:

$K_1(R_1, X), K_x(R_0, W)$

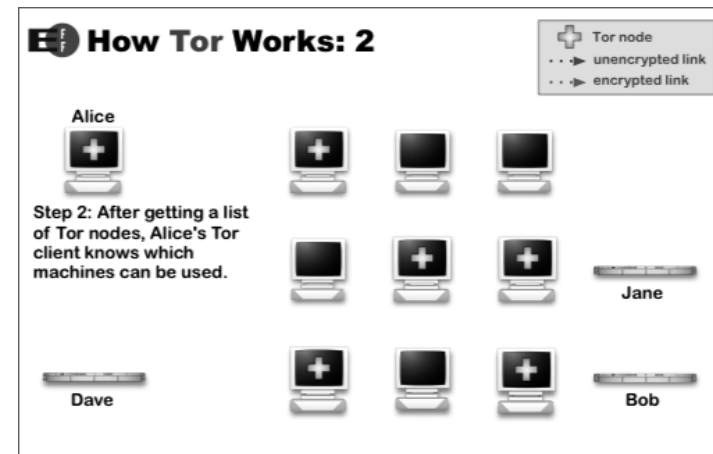
- Il mix M1 effettua la seguente trasformazione

$K_1(R_1, X), K_x(R_0, W) \rightarrow R_1(K_x(R_0, W))$

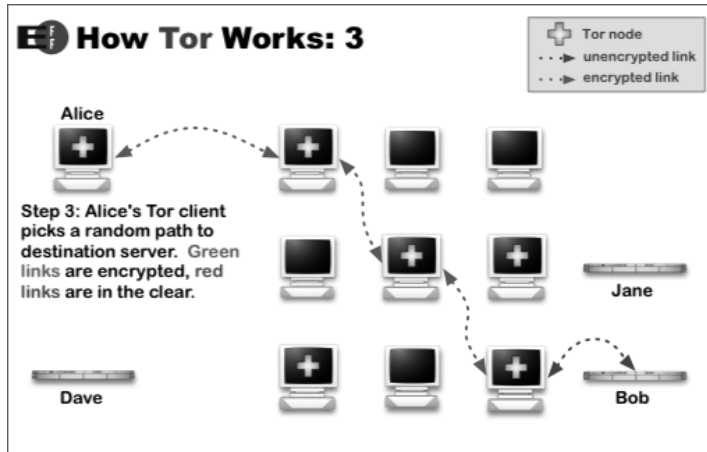
Tor / 1



Tor / 2



Tor / 3

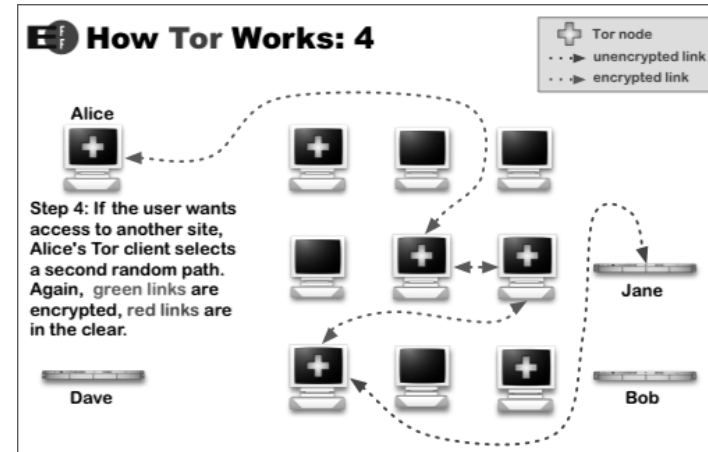


Moreno Marzolla

Tecnologie Web

13

Tor / 4



Moreno Marzolla

Tecnologie Web

14

Platform for Privacy Preferences (P3P)

- Developed by the World Wide Web Consortium (W3C) <http://www.w3.org/p3p/>
 - Final P3P1.0 Recommendation issued 16 April 2002
- Offers an easy way for web sites to communicate about their privacy policies in a standard machine-readable format
 - Can be deployed using existing web servers
- Enables the development of tools (built into browsers or separate applications) that
 - Summarize privacy policies
 - Compare policies with user preferences
 - Alert and advise users

Moreno Marzolla

Tecnologie Web

15

Componenti di base

- P3P provides a standard XML format that web sites use to encode their privacy policies
- Sites also provide XML “policy reference files” to indicate which policy applies to which part of the site
- Sites can optionally provide a “compact policy” by configuring their servers to issue a special P3P header when cookies are set
- No special server software required
- User software to read P3P policies called a “P3P user agent”

Moreno Marzolla

Tecnologie Web

16

Esempio di Policy Reference File

```

<META xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY-REFERENCES>
  <EXPIRY max-age="172800"/>

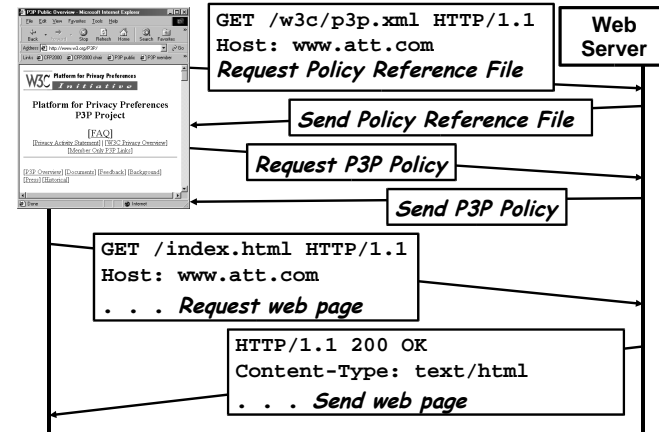
  <POLICY-REF about="/P3P/Policies.xml#first">
    <INCLUDE> /* </INCLUDE>
    <EXCLUDE> /catalog/* </EXCLUDE>
    <EXCLUDE> /cgi-bin/* </EXCLUDE>
    <EXCLUDE> /servlet/* </EXCLUDE>
  </POLICY-REF>

  <POLICY-REF about="/P3P/Policies.xml#second">
    <INCLUDE> /catalog/* </INCLUDE>
  </POLICY-REF>

  <POLICY-REF about="/P3P/Policies.xml#third">
    <INCLUDE> /cgi-bin/* </INCLUDE>
    <INCLUDE> /servlet/* </INCLUDE>
    <EXCLUDE> /servlet/unknown </EXCLUDE>
  </POLICY-REF>
</POLICY-REFERENCES>
</META>

```

Usare P3P in pratica

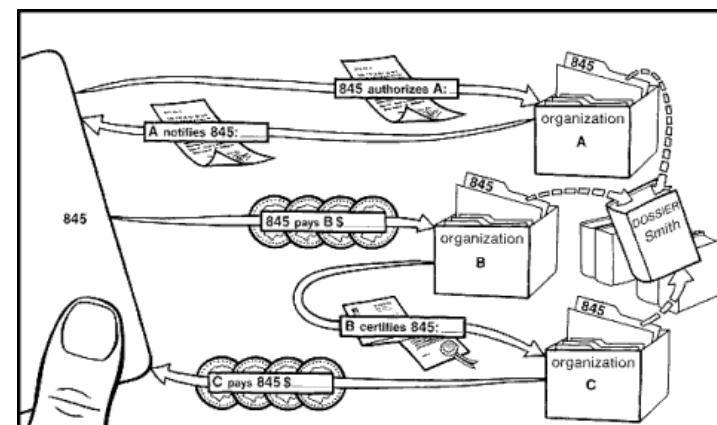


Cosa c'è in una policy P3P?

- Name and contact information for site
- The kind of access provided
- Mechanisms for resolving privacy disputes
- The kinds of data collected
- How collected data is used, and whether individuals can opt-in or opt-out of any of these uses
- Whether/when data may be shared and whether there is opt-in or opt-out
- Data retention policy

Transazioni economiche e anonimato

http://www.chaum.com/articles/Security_Without_Identification.htm



Transazioni economiche e anonimato

http://www.chaum.com/articles/Security_Without_Identification.htm

- “UNIVERSALLY IDENTIFYING NUMBERS or other equivalent identifying information is presented by the individual card holder to each organization---in the current approach. Unrelated generic examples are shown of three kinds of transactions: commutation, in which the individual sends an authorizing message and receives a notifying message; payment in which the individual pays an organization or receives a payment; and credential, in which a certification that an individual has some credential is transferred from an organization B to an organization C. The identifying information—845—allows all transactions to be linked together into a dossier on the individual.”

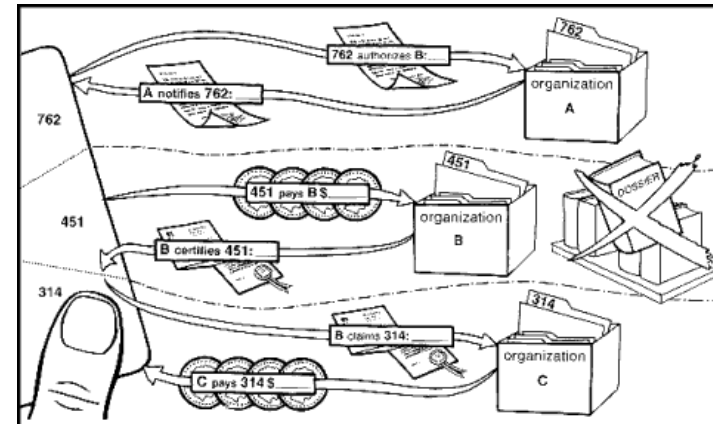
Moreno Marzolla

Tecnologie Web

21

Transazioni economiche e anonimato

http://www.chaum.com/articles/Security_Without_Identification.htm



Moreno Marzolla

Tecnologie Web

22

Transazioni economiche e anonimato

http://www.chaum.com/articles/Security_Without_Identification.htm

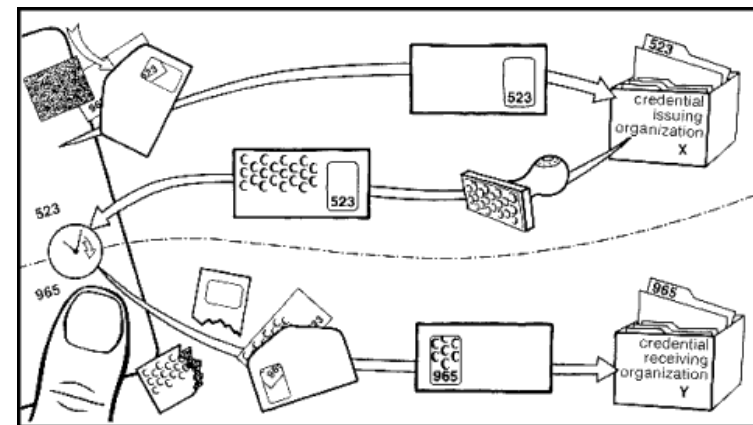
- “DIFFERENT NUMBERS OR DIGITAL PSEUDONYMS are used with each organization by a personal card computer that the individual completely controls---under the new approach. The credential transfer is no longer just between organizations: it must now go through the card where the pseudonym, 451, used with the issuing organization 3 is transformed to the pseudonym, 314, used with the receiving organization C. Systems using this approach can provide organizations with improved protection against abuses by individuals, and also allow individuals to ensure that pseudonyms cannot be traced across the dashed boundary lines, thereby preventing dossier compilation.”

Moreno Marzolla

Tecnologie Web

23

Credenziali anonime

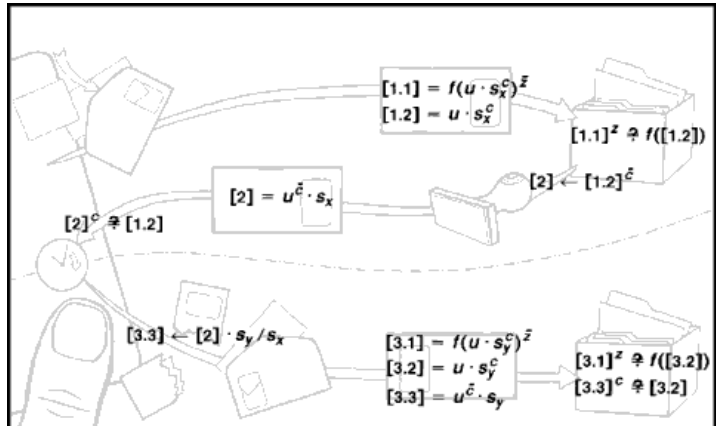


Moreno Marzolla

Tecnologie Web

24

Credenziali anonime



Moreno Marzolla

Tecnologie Web

25