

Steganografia e Covert Channel

Claudio Agosti - vecna@delirandom.net

Politecnico di Milano – **POuL** – 10 Giugno 2009

<http://www.delirandom.net>

Steganografia, dove la si è vista ?

- The core: Il ratto e la chiave di numeri primi.
- Contact: trasmissione televisiva da parte degli alieni.

Information Hiding

- Information hiding è l'area di ricerca che studia tecnologie in grado di rendere invisibili le informazioni.
- sviluppata in quattro forme:
 - differenti problemi da superare.
 - l'analisi del modello di minaccia va sempre fatta in ogni contesto.

Information Hiding

Information Hiding

```
graph TD; A[Information Hiding] --> B[Steganografia]; A --> C[Copyright Marking]; A --> D[Anonimato]; A --> E[Covert Channel];
```

Steganografia

Copyright Marking

Anonimato

Covert Channel

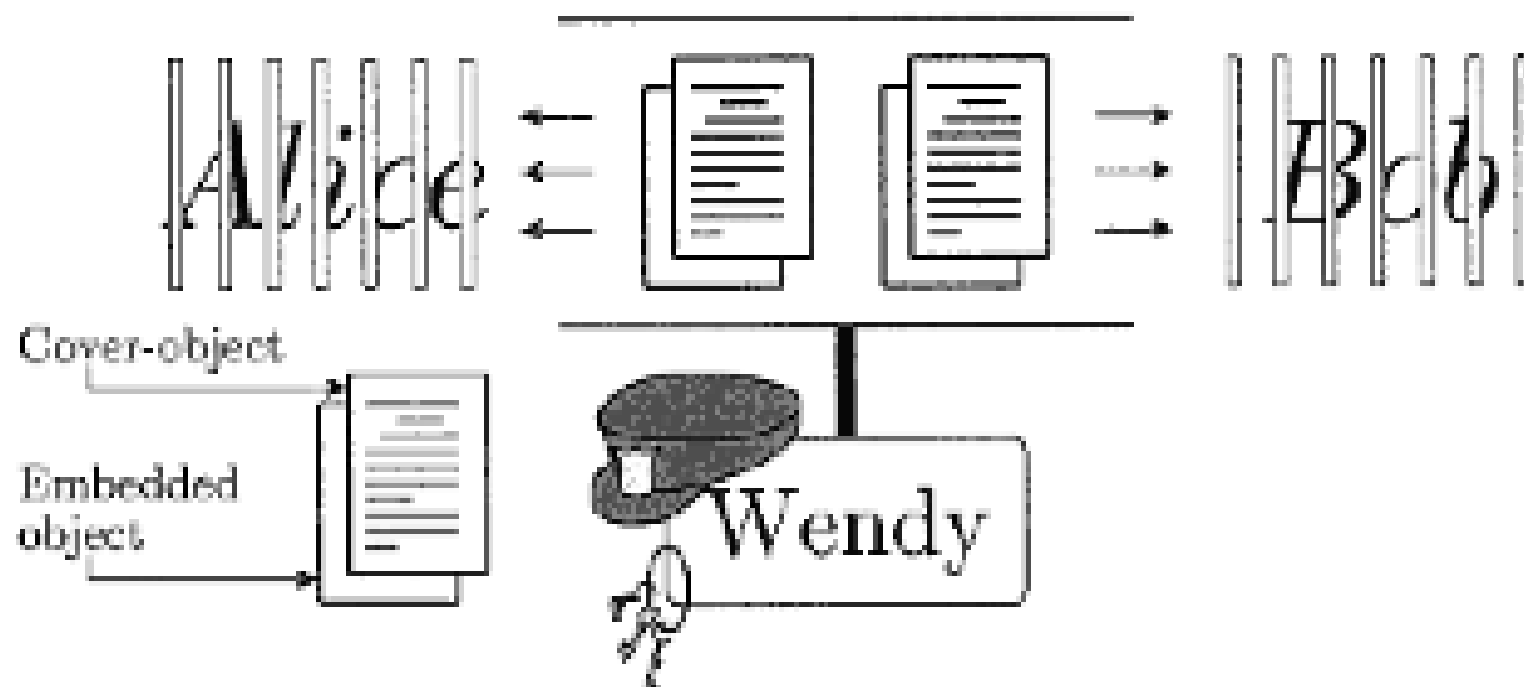
Quello di cui non parleremo: Anonimato

- L'anonimato è una caratteristica della connessione; Spesso viene fraintesa con delle caratteristiche di conservazione dei dati.
- Lo si ottiene tramite reti peer to peer con protocolli anonimi.
- E' uno strumento necessario per l'equilibrio democratico.

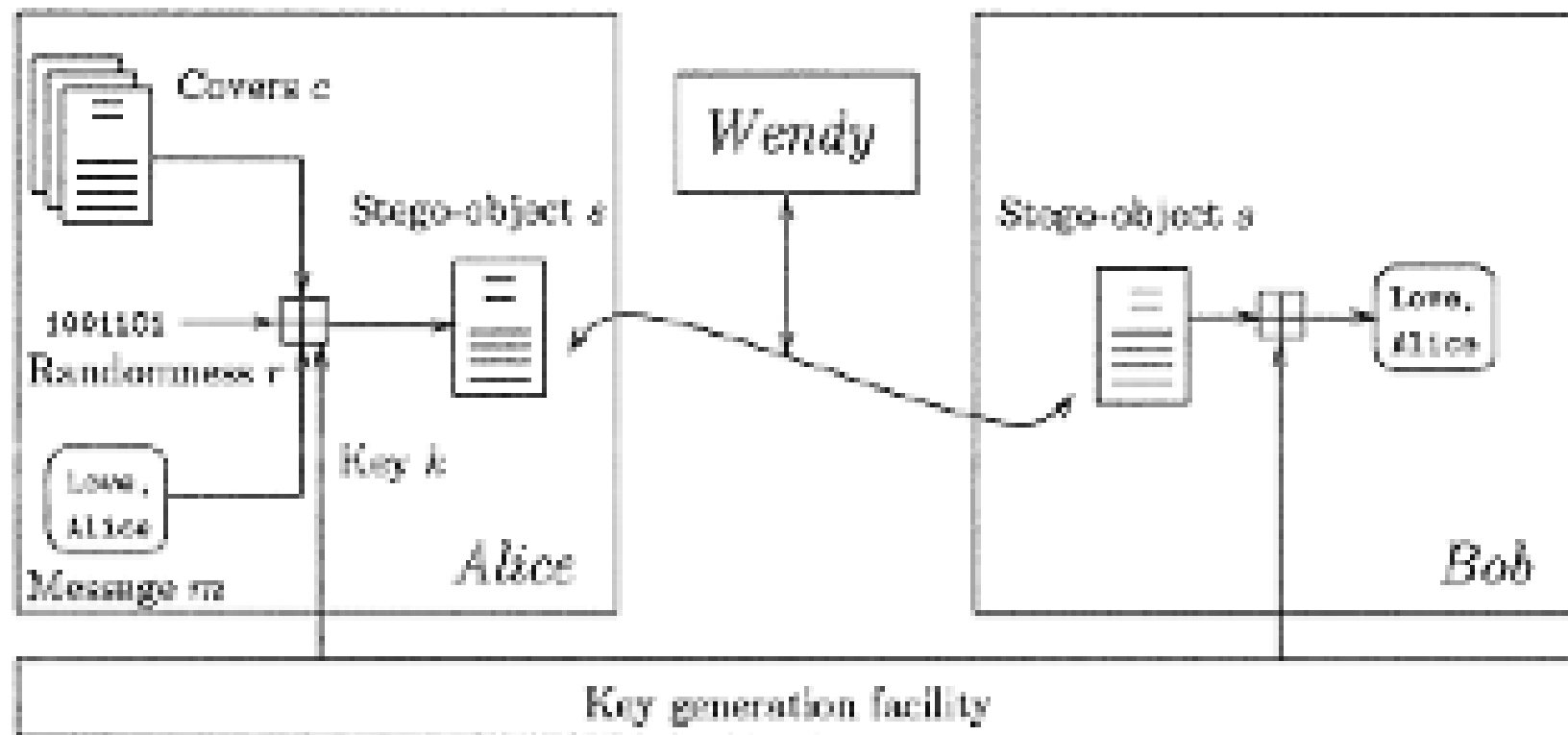
L'altro del quale non parleremo: copyright marking / watermarking

- Marcatura univoca in file generati in funzione dell'utente a cui è destinato:
 - Può essere visibile o invisibile
 - Serve come deterrente efficace per la fuga di informazioni protette
 - Si misura in quanto è **robusto**.

Steganografia e il problema che vuole risolvere.



Come lo risolve ?



Steganografia vs Crittografia

- le loro forme classiche, sono entrambe: $P(K) = E$, $E(K) = P$
- la crittografia vuole proteggere il dato
- la steganografia vuole proteggerne l'individuazione (e siccome non puo' sparire, si affida ad un contenitore)

Steganografia nella sua accezione convenzionale



+



=



formati multimediali – basata
su contenitore – l'organo umano
non nota le differenze

Ma sono molte di più le condizioni in cui la steganografia può essere usata

- **Con covert:** Sostituzione di informazioni ridondanti o irrilevanti.
- **Con covert:** Distorsione nella fase (sinonimi, allineamento, punteggiatura, spazi)
- **Senza covert:** Generazione nel dominio (generazione di spam, generazione di click)

Sostituzione informazioni ridondanti

- Ogni contenuto multimediale che può essere degradato di qualità in modo non percettibile, utilizzando lo spazio risparmiato per lo stegomessaggio.
- Utilizzare questi bit in toto o a seconda di una chiave pre-condivisa.

Sostituzione informazioni ridondanti

- outguess e la sua saga
- VOIP, RTP, e il primo attacco attivo
- StegoVideo
- ... l'applicazione steganografica dipende dal formato contenitore
- <http://www.stegoarchive.org>

Distorsione nella fase

- Quando un dato generato da un utente può assumere diversi stati, e sono tutti legittimi.
- La scelta di uno stato o di un altro, è data dal dizionario dello stegomessaggio.

Distorsione nella fase

(sarà il 19-20-21 Giugno, <http://it.hackmeeting.org>)

■ SNOW: steganography nature of whitespace.

“quando sarà hackmeeting a milano ?”

“ quando sarà hackmeeting a milano ?”

■ numero di possibili combinazioni =
numero di bit disponibile.

Distorsione nella fase

- esistono sistemi ben più efficienti (spazi per testi "giustificati", utilizzo dei sinonimi)
- Applicato all'HTML in varie salse
 - utilizzo di TAG in relazione ad un dizionario
 - utilizzo degli spazi bianchi fuori dalle tag (mod_stego)

Generazione nel dominio

■ Quando un dato può essere descritto da un dizionario di riferimento, e le generazioni anche casuali sono accettabili, è sufficiente perché l'attaccante si trovi un dato plausibile.

Generazione nel dominio

- Lo spam viene spesso descritto tramite keyword riconosciute
- Si associa ad ognuna di queste keyword un valore specifico (si crea così il dizionario)
- Si genera spam su necessità
- Si sparpagliano articoli e punteggiatura.

Generazione nel dominio

- Un utente che naviga su un sito, ha la possibilità di scegliere qualunque link ?
- Ogni percorso di navigazione, descrive una serie molto ampia di possibilità ?
- StegoClick 1.0, ad hackmeeting 2009:
<http://it.hackmeeting.org>

Attacchi alla steganografia

- La verifica di un sistema steganografico viene fatta sottoponendolo a steganalisi
- La steganalisi ha successo quando si può scoprire, con ragionevole certezza, quali messaggi sono contenitori steganografici.

Attacchi alla steganografia

- Differenti livelli di attacco possono essere assunti, in relazione a ciò di cui l'attaccante dispone:
 - Solo lo stegomessaggio ?
 - Hai il software ?
 - Ha il contenitore originale ?
 - Ha il dato steganografato ?
 - Ha la password ?

covert channel

(anche noto come “lo strumento che stronca le politiche di filtro”)

- Se la steganografia utilizza una chiave e presuppone un attaccante umano o informatico
- Il covert channel è la sua variante semplice, che consiste nel “mettere dati dove questi non sono previsti”, o “mettere dati diversi da quelli previsti”

covert channel

(anche noto come “lo strumento che stronca le politiche di filtro”)

- Filtro del traffico basato su pattern non approfonditi (porta TCP, stringhe note)
 - Filtro del web solo se verso un determinato host (socks/proxy è un cover channel)
 - Permesso solo traffico DNS ? (dnstunnel è il covert channel)

• *Comparazione dei rami di Information Hiding*

- Steganografia
 - comunicazione tra N elementi, non è necessario sia “robusto”, (dovrebbe) essere pubblicato, necessariamente invisibile.
- Copyright Marking
 - non necessariamente invisibile, robusto su necessità, molte permutazioni devono essere possibili.
- Anonymity
 - anonimizzazione del mittente (opzionalmente, del destinatario), utile quando il dato sensibile è l'esistenza di uno scambio tra A e B. Ottenuto tramite una rete collaborativa.
- Covert Channel
 - bypass di strumenti di filtro automatici.

Grazie dell'attenzione

<http://www.sikurezza.org> - mailing list e community di sicurezza informatica

<https://www.winstonsmith.info> - “la paranoia è una virtù”
(Anonimo)

<http://www.delirandom.net> - sito personale

<http://it.hackmeeting.org> - tra 9 giorni!