

**SICUREZZA INFORMATICA: QUESTA (S)CONOSCIUTA**

Corrado Giustozzi

# TECHNOINTELLIGENCE



**CORRADO GIUSTOZZI**  
*ZETA RETICULI*

19 novembre 2007      Convegno Mensa-Consip      1 

## Gli argomenti che tratteremo

Corrado Giustozzi

- Considerazioni di scenario
- La technointelligence: scienza o fantascienza?
- Le tipologie di attuazione
- L'intelligence "casereccia"
- Technointelligence esoterica
- Contro la stupidità...

19 novembre 2007      Convegno Mensa-Consip      2 

## Considerazioni di scenario (1/2)

Corrado Giustozzi

- Oggi la maggior parte delle informazioni di valore viene elaborata ed archiviata su sistemi informativi, personali o non, generalmente connessi tra loro in modo sempre meno estemporaneo e sempre più integrato grazie alla crescente pervasività delle reti
- Il numero e le tipologie degli strumenti informatici utilizzati per gestire e scambiare informazioni sono aumentati enormemente
- Gli apparati hanno assunto una dimensione anche personale (palmari, PDA), con grande capacità di comunicazione e di integrazione di reti diverse (bluetooth, cellulare, Internet, ...)

19 novembre 2007

Convegno Mensa-Consip

3



## Considerazioni di scenario (2/2)

Corrado Giustozzi

- La convergenza fra informatica e telefonia ha reso assai comune anche l'utilizzo delle reti cellulari (GSM, GPRS, UMTS) per il trasporto di dati e informazioni multimediali integrate
- L'utilizzo delle reti wireless è cresciuto, e si è esteso ad ambiti geografici estremamente variegati quali:
  - **MAN**: Metropolitan Area Network
  - **WAN**: Wide Area Network
  - **LAN**: Local Area Network
  - **PAN**: Personal Area Network
- Questo scenario apre prospettive importanti alla cosiddetta *technointelligence*, o **intelligence delle informazioni tecno-mediate**

19 novembre 2007

Convegno Mensa-Consip

4



## Aspettative, miti, realtà

Corrado Giustozzi

- False concezioni sulla technointelligence:
  - Tutto è sorvegliato sempre e comunque grazie alle tecnologie avanzate (foto satellitari, log onnipresenti, ...)
  - Si può fare intelligence globale senza muoversi dalla propria scrivania (Echelon, ...)
  - Tutti i sistemi tecnologici sono vulnerabili, basta saper imporre le mani al modo giusto
- La realtà:
  - La technointelligence è un utile supporto ma non una alternativa alle forme di intelligence più tradizionali (agenti sul territorio, social engineering, intercettazione ambientale, scavenging, ...)
  - È comunque sorprendente quello che si può fare con metodi caserecci e strumenti di pubblico dominio!

19 novembre 2007

Convegno Mensa-Consip

5



## Tipologia di azione

Corrado Giustozzi

- Le due modalità di azione della technointelligence:
  - **passiva**: raccogliere ed analizzare le informazioni che un determinato soggetto raccoglie, elabora, scambia con altri o trasmette in pubblico, volontariamente o involontariamente
  - **attiva**: acquisire informazioni non basandosi sull'analisi dei flussi di rete ma agendo direttamente sul sistema "bersaglio"
- Tipologie di technointelligence passiva:
  - analisi delle fonti aperte di Internet
  - sniffing su reti tradizionali o wireless
  - SIGINT, EMINT, ...
- Tipologie di technointelligence attiva:
  - spyware, keyloggers, ...
  - backdoor, rootkit, ...

19 novembre 2007

Convegno Mensa-Consip

6



## La technointelligence... casereccia

Corrado Giustozzi

- Il paradosso della intelligence in Rete:
  - quella “professionale” è difficile, costosa e poco efficace
  - quella “amatoriale” è piuttosto facile e dà risultati interessanti
- Le motivazioni sono molteplici:
  - spesso le reti di computer ed i sistemi di comunicazione sono vulnerabili ad attacchi volti solo a raccogliere informazioni
    - chi pensa di non avere nulla da nascondere non si protegge a sufficienza
    - chi pensa di essersi protetto non sempre lo ha fatto davvero!
  - alcuni protocolli sono assai loquaci o possono essere resi tali...
  - certe informazioni “tecniche” sono pubbliche: basta chiedere...
  - la Rete ha una lunga memoria (*wayback machine*, ...)
  - i motori di ricerca sono sempre più efficaci (ricerca in profondità, dentro molteplici tipi di documenti, nei gruppi, ...)
  - molti dati pubblici “anonimi” spesso non lo sono!

19 novembre 2007

Convegno Mensa-Consip

7



## Inferenza nei database (1/2)

Corrado Giustozzi

NAME	RANK	SALARY	YEARS
Brown	Clerk	34.000	5
Evan	Clerk	34.000	3
Hammer	Director	65.000	3
Joels	Clerk	34.000	3
Smith	Accountant	41.000	6
Small	Secretary	28.000	8

- Un tipico database “protetto”:
  - Lo stipendio (SALARY) è legato al ruolo (RANK)
  - Per motivi di privacy, nessuna query può accedere ai campi NAME e SALARY contemporaneamente

19 novembre 2007

Convegno Mensa-Consip

8



## Inferenza nei database (2/2)

Corrado Giustozzi

- Query 1: elenca RANK e SALARY di tutto il personale con 3 anni di anzianità

RANK	SALARY
Clerk	34.000
Director	65.000

- Query 2: elenca NAME e RANK di tutto il personale con 5 anni di anzianità

NAME	RANK
Brown	Clerk

- Inferenza:  
Brown → Clerk → 34.000

19 novembre 2007

Convegno Mensa-Consip

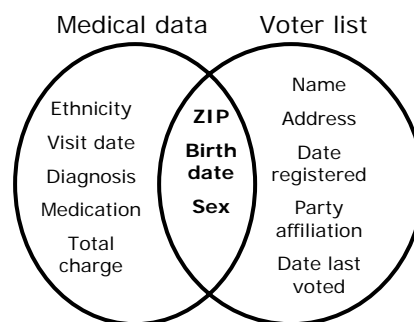
9



## Esperimento Sweeney (2001) (1/2)

Corrado Giustozzi

- Dataset 1: medical records resi disponibili agli istituti di ricerca dalla "US National Association of the Health Data Organizations", ritenuti anonimi
- Dataset 2: liste elettorali della contea di Cambridge, Massachusetts (54.805 elettori), liberamente acquistabili
- Campi in comune: data di nascita, genere, ZIP code



87% unique US-wide with ZIP, date and sex!

19 novembre 2007

Convegno Mensa-Consip

10



## Esperimento Sweeney (2001) (2/2)

Corrado Giustozzi

- Ha utilizzato i due dataset precedentemente descritti
- Ha preso in esame pochi dati personali pubblicamente noti relativi al governatore dello Stato del Massachusetts:
  - soltanto sei persone avevano la sua stessa data di nascita
  - soltanto tre erano maschi
  - soltanto uno risiedeva in un'area con lo stesso ZIP code
- I dati clinici del governatore (presenti nel dataset sanitario) perdevano immediatamente la (presunta) caratteristica di anonimato attingendo a fonti legalmente accessibili!

19 novembre 2007

Convegno Mensa-Consip

11



## Potenza dei motori di ricerca...

Corrado Giustozzi

Il giornale statunitense Chicago Tribune rintraccia 2653 nomi. Il direttore dell'agenzia Goss "inorridito"

### Migliaia di agenti Cia smascherati su internet

di RICCARDO STAGLIANO

ALLE pagine bianche su internet Valerie Plame non risulta. Niente numeri di telefono per la spia il cui nome venne rivelato per vendetta dando vita allo scandalo del Cia-gate. Ma mentre White Pages si scusa ("sorry, niente risultati") nella stessa pagina spunta fuori un annuncio di US Search, un servizio concorrente: "Abbiamo questo nome nel nostro database". Con 20 dollari si può scoprire indirizzo e telefono. Spendendo il doppio anche eventuali coinquilini, valore dell'immobile, grane fiscali sino alla bancarotta, storia giudiziaria, matrimoni e divorzi. Con la garanzia "soddisfatti o rimborsati": l'addebito sulla carta di credito avviene solo se le informazioni saltano fuori.

Dura la vita degli agenti segreti al tempo di Google. Basta sapere come cercare e le "coperture" degli 007 diventano trasparenti come veli di organza. Come ha dimostrato un'inchiesta del Chicago Tribune che ha identificato come dipendenti della Central Intelligence Agency ben 2653 persone, oltre ad aver localizzato una cinquantina di aziende fantoccio dove costoro figuravano lavorare. Il tutto utilizzando solo informazioni pubbliche (elenchi telefonici, registri di compravendite immobiliari o sentenze di tribunale e così via) che vari servizi a pagamento online aggregano. Il direttore dell'agenzia Porter Goss si è detto "inorridito". "Non so se Al Qaeda sia in grado di arrivare agli indirizzi, i cinesi certamente possono" ha commentato un alto funzionario di Langley. E non si capisce il motivo della distinzione dal momento che basta un accesso a internet, una carta di credito e qualche familiarità con le banche dati.

la Repubblica.it



Fonte: Repubblica.it, 13 marzo 2006

19 novembre 2007

Convegno Mensa-Consip

12



## Esempio: la telefonia cellulare

Corrado Giustozzi

- La rete di prima generazione (TACS):
  - non era protetta contro le intercettazioni
  - non era protetta contro l'impersonazione
- Le reti di generazioni successive (GSM, GPRS, UMTS):
  - si basano sull'uso di tecniche crittografiche
  - sono sicure e protette contro abusi e violazioni
- Vulnerabilità nella rete TACS:
  - modulazione analogica e non digitale
  - trasmissione in chiaro della comunicazione
    - permette di intercettare le comunicazioni
    - consente la violazione della privacy degli utenti
  - trasmissione in chiaro dell'handshake/handover
    - permette di ricostruire l'identità del cellulare (clonazione)
    - consente le truffe ai danni del gestore della rete

19 novembre 2007

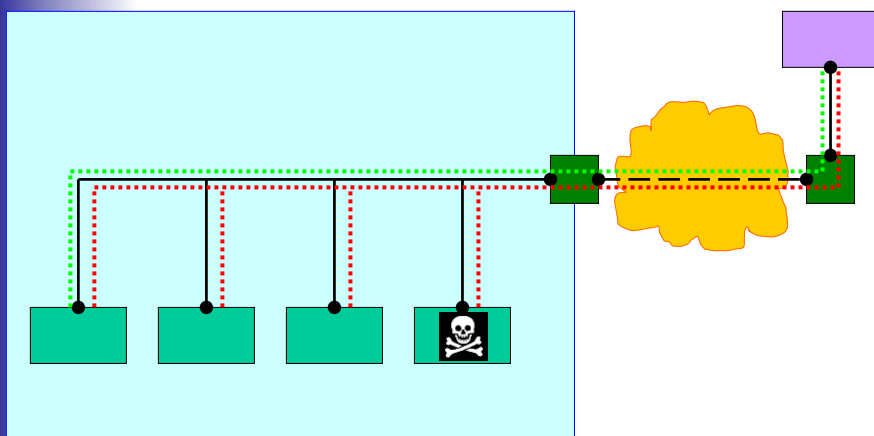
Convegno Mensa-Consip

13



## Sniffing su rete locale

Corrado Giustozzi



19 novembre 2007

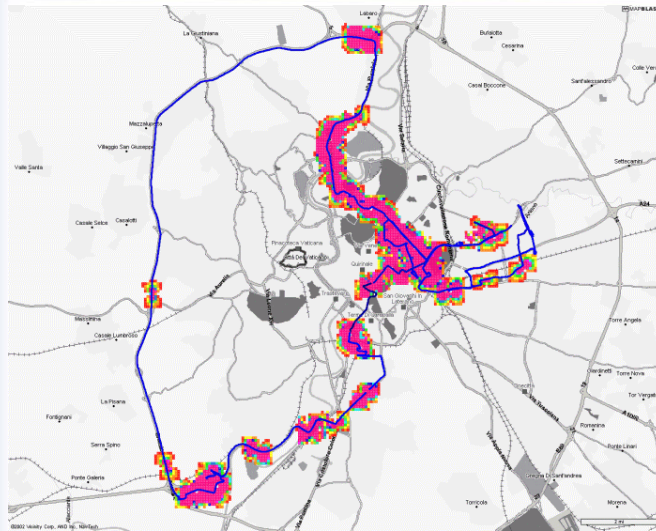
Convegno Mensa-Consip

14



## Wardriving a Roma (fine 2002)

Corrado Giustozzi



Fonte: SecLab gennaio 2003.

19 novembre 2007

Convegno Mensa-Consip

15



## Una *cantenna* ad alto guadagno

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

16



## Tews, Weinmann, Pyshkin (2007)

Corrado Giustozzi

- Breaking 104 bit WEP in less than 60 seconds
  - We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40.000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85.000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately 220 RC4 key setups, which on current desktop and laptop CPUs is negligible.

19 novembre 2007

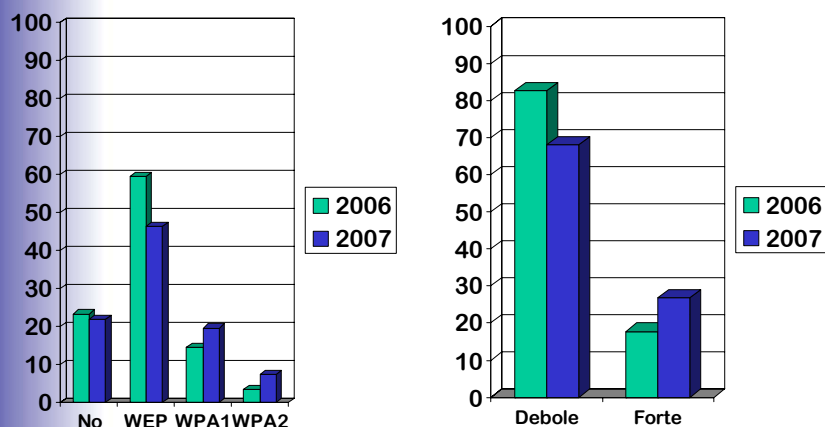
Convegno Mensa-Consip

17



## Protezione Wi-Fi (Germania)

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

18



## E il bluetooth?...

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

19



## Technointelligence esoterica...

Corrado Giustozzi

- Emanazioni radio
  - TEMPEST
- Emanazioni ottiche
  - LED emanations
    - Joe Loughry, Lockheed Martin Space Systems
    - David A. Umphress, Auburn University
  - Luminosità diffusa per riflessione
    - Markus J. Kuhn, University of Cambridge
- Emanazioni acustiche
  - Crittanalisi dattilografica
    - Li Zhuang, Feng Zhou, J. D. Tygar, University of California, Berkeley
  - Crittanalisi acustica
    - Shamir, Tromer

19 novembre 2007

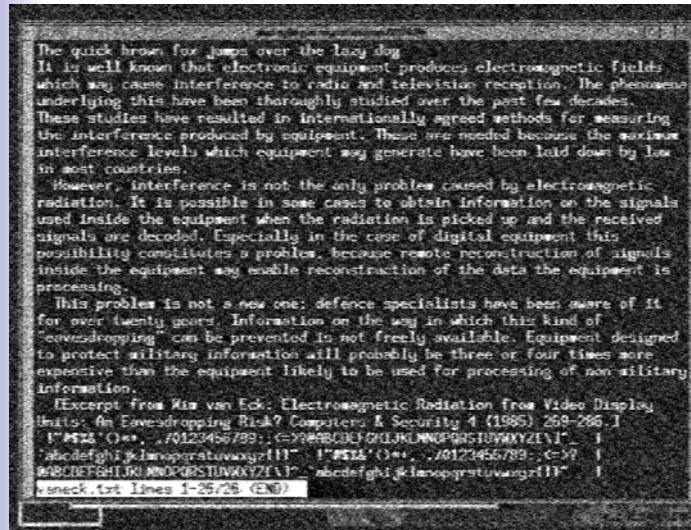
Convegno Mensa-Consip

20



## TEMPEST di un LCD...

Corrado Giustozzi



19 novembre 2007

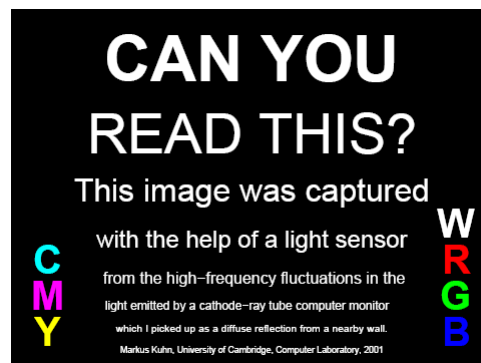
Convegno Mensa-Consp

21



## Luminosità riflessa su un muro (1/3)

Corrado Giustozzi



19 novembre 2007

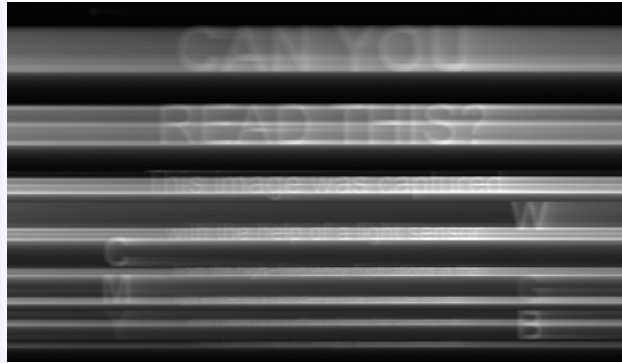
Convegno Mensa-Consp

22



## Luminosità riflessa su un muro (2/3)

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

23



## Luminosità riflessa su un muro (3/3)

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

24



## Zhuang, Zhou, Tygar (2005)

Corrado Giustozzi

- Keyboard Acoustic Emanations Revisited
  - We present a novel attack taking as input a 10-minute sound recording of a user typing English text using a keyboard, and then recovering up to 96% of typed characters. There is no need for a labeled training recording. Moreover the recognizer bootstrapped this way can even recognize random text such as passwords: In our experiments, 90% of 5-character random passwords using only letters can be generated in fewer than 20 attempts by an adversary; 80% of 10-character passwords can be generated in fewer than 75 attempts. Our attack uses the statistical constraints of the underlying content, English language, to reconstruct text from sound recordings without any labeled training data. The attack uses a combination of standard machine learning and speech recognition techniques, including cepstrum features, Hidden Markov Models, linear classification, and feedback-based incremental learning.

19 novembre 2007

Convegno Mensa-Consip

25



## Un esempio reale

Corrado Giustozzi

- Testo acquisito
  - the big money fight has drawn the shoporo od dosens of companies in the entertainment industry as well as attorneys gnnerals on states, who fear the fild shading softwate will encourage illegal acvivity, srem the grosth of small arrists and lead to lost cobs and dimished sales tas revenue.
- Testo corretto
  - the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys generals in states, who fear the film sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and finished sales tax revenue.
- Testo originale
  - the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys gnnerals in states, who fear the file sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and dimished sales tax revenue.

19 novembre 2007

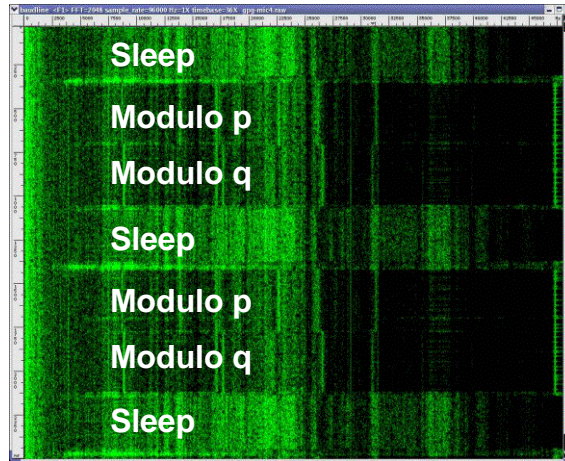
Convegno Mensa-Consip

26



## Shamir, Tromer (2004)

Corrado Giustozzi



Source: Shamir and Tromer

19 novembre 2007

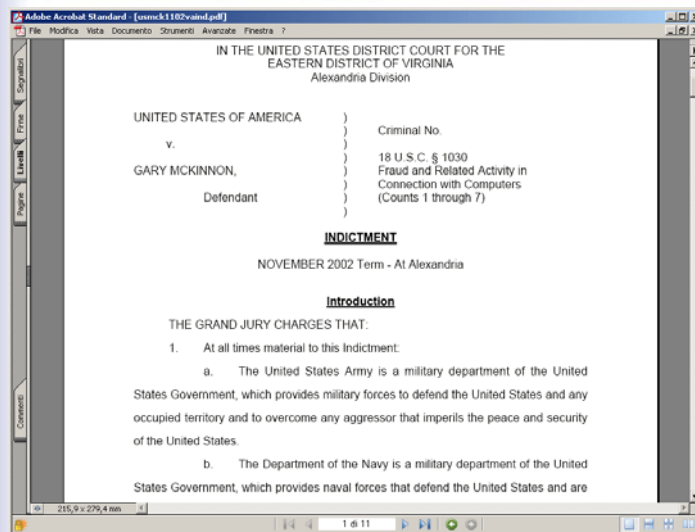
Convegno Mensa-Consip

27



## Contro la stupidità... (1/2)

Corrado Giustozzi



19 novembre 2007

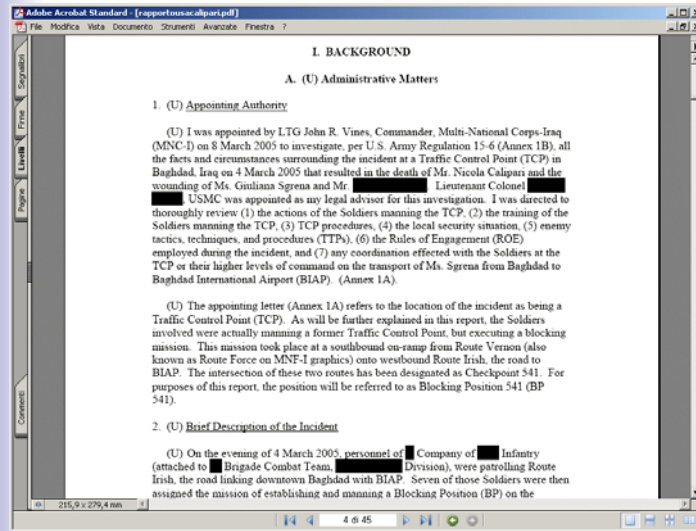
Convegno Mensa-Consip

28



## Contro la stupidità... (2/2)

Corrado Giustozzi



19 novembre 2007

Convegno Mensa-Consip

29



## SICUREZZA INFORMATICA: QUESTA (S)CONOSCIUTA

Corrado Giustozzi

## GRAZIE PER L'ATTENZIONE



**TECHNOINTELLIGENCE**

19 novembre 2007

Convegno Mensa-Consip

30

