Intercettazioni *telematiche* e data retention

Due diverse strategie di contrasto, analizzate in mezz'ora

vecna@winstonsmith.org
Claudio Agosti – http://www.delirandom.net

AK Vorrat

- Si fanno conoscere con Freedom Not Fear
- Sono una costola del CCC motivata a contrastare la date retention ed il controllo incondizionato per finalità di sicurezza
  - In the field of telecommunications, **data retention** (or **data preservation**) generally refers to the storage of call detail records (CDRs) of telephony and internet traffic and transaction data (IPDRs) by governments and commercial organisations.
    - http://en.wikipedia.org/wiki/Telecommunications_data_retention

Febbraio 2009

- Nel Febbraio 2009, vengono riconosciute le basi legali per la scrittura di una normativa per la data retention a livello europeo
  - http://www.statewatch.org/news/2009/feb/eu-ecj-ireland-datret-judgment-prel.pdf
- E' l'inizio della mobilitazione di AK vorrat
  - http://www.statewatch.org/news/2009/feb/04eu-datret-ecj-german-wgdr.htm
- Viene stilata un'analisi su ogni stato europeo
  - Timeline, documentazione, lettere e risposte: http://www.statewatch.org/eu-data-retention.htm

Giugno 2009

- Per AK vorrat, Patrick Breyer, organizza una lettera aperta da mandare a 3 MEP.
- Firmata da più di un centinaio di esponenti di NGOs, spingeva queste argomentazioni:
  - Distruzione della confienzialità
  - Costi gravosi sulla società
  - Aumento di sicurezza solo illusorio
  - Accumulo di dati potenzialmente abusabili
    - https://www.privacyinternational.org/article/civil-society-groups-call-end-telecommunications-data-retention

Luglio 2009

- Cecilia Malmstrom risponde in modo non ufficiale che
  - Ha votato nel 2005 contro, e non è del tutto convinta
  - Ma si concentrerebbe sulle tempistiche massime
    - Anche Pizzetti si è detto attento a questo
- Viviane Reading da una risposta pressoché simile
  - http://www.vorratsdatenspeicherung.de/images/reply_reding.pdf

Agosto 2009

- Risposta ufficiale di CM
- http://www.vorratsdatenspeicherung.de/images/reply_malmstroem.pdf
  - Vuole dati dimostrativi che la DR non incrementi la frequenza di successo delle indagini
  - AK Vorrat si mobilita per fornire queste informazioni
- Discussione delle strategie di DR
  - Uno degli obiettivi è abbassare la barriera d'ingresso alle tecnologie di collezione dei dati

Germania, statistiche

- before the introduction of data retention legislation 96% of police requests for traffic data were successful
- before the introduction of data retention legislation the crime clearance rate was just as high as with data retention in effect
- before the introduction of data retention legislation the clearance rate for Internet crime was significantly above average.

Ottobre 2009

- Veniva studiato l'action plan decentralizzato
  - http://twiturl.de/DR-Action-Plan
- Questo è il loro stile di lavoro: un contatto, un coordinamento, vari contatti con realtà localizzate che possano soddisfare le varie esigenze
  - Noi siamo una di queste, e sovente non abbiamo il tempo per seguir questa vicenda! Help!

Anno 2010

- Viene reso pubblico uno studio sull'impatto tra la DR e l'effettiva utilità investigativa
- http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf
- Germany has certainly not lead to a larger share of registered crime being cleared than in previous years.
- There is no proof that the number of cleared cases, the crime rate or the number of convictions, acquittals or closed cases significantly depends on whether a blanket data retention scheme is in operation in a given country or not.
- There is no evidence that countries using targeted investigation techniques clear less crime or suffer from more criminal acts than countries operating a blanket communications data retention scheme.

Novembre 2010

- German Minister wants to end EU-wide communications data retention
- German Minister of Justice Sabine Leutheusser-Schnarrenberger has informed us this week that she supports our position that if the EU Commission wants to uphold the policy of mandatory retention of all call records ("data retention") at all […]
- **Durante il 2010 la commissione per la DR è stata a studiare l'effettiva utilità per la sicurezza.**

Dicembre 2010

- http://www.vorratsdatenspeicherung.de/content/view/415/79/lang,en/
- Esposizione in commissione europea del perché la data retention è superflua

Anno 2011, prosecuzione

- There was no agreement on whether blanket telecommunications data retention is necessary
- or whether "quick freeze" should be seriously examined and discussed as an alternative
  - http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2010/22_%22QuickFreeze%22.html?nn=410156

Schedule

- Nel mese di giugno, la commissione europa incontrerà rappresentati di:
  - Società civile / NGO (8/6/2011)
  - Industria (17/6/2011)
  - Rappresentanti Data protection authority (DPA) e European Data Protection Supervisor (EDPS) (22)
  - Rappresentati stati membri UE (30)
  - Per la fine del 2011: concludere la direttiva

Strategia di influenza

- Divulgare e promuovere l'impedimento della data retention massiva, entro l'8, verso le NGOs ed associazioni.
- Diffondere "EDRi shadow evaluation report"
  - http://www.edri.org/files/shadow_drd_report_110417.pdf
- Per il 17, ridondare la stessa cosa verso i rappresentati dell'industria (ISP, AIIP)
- Per il 22, ridondare al Garante della Privacy

Data retention e Massive traffic analysis

- La diffusione di tecnologie per l'acquisizione massiva di traffico "raw" cresce e si stabilizza con la crescita della rete
- Ha preso il termine di DPI
  - Che è la tecnologia alla base di:
    - **Lawful interception**
    - **Policy definition and enforcement**
    - **Targeted advertising**
    - **Tiered services**
    - **Censorship**

Cos’hanno in comune tutti i DPI ?

- “Riassemblano” il traffico in sessioni

- Andare su YouTube, scrivere una ricerca, fare invio:
  - in media 900 pacchetti scambiati,
  - verso 3 indirizzi differenti,
  - suddivisi in circa 20 connessioni differenti

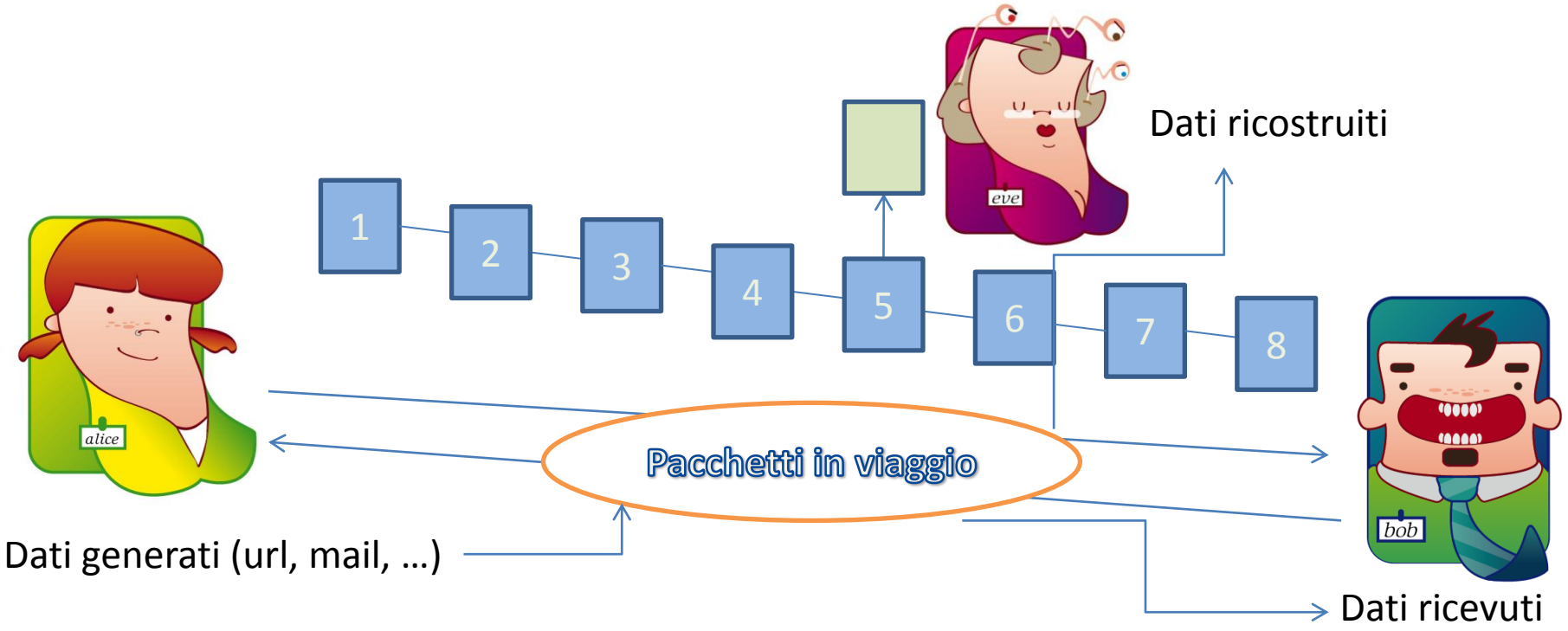
Crescita di Internet e della DPI

- Le tecnologie trasmissive migliorano (lineare)
- Il numero di servizi aumenta (lineare)
- Il numero di ISP aumenta (lineare)

- Le tecnologie di DPI devono
  - Imporsi limiti tecnologici (anni 2000: 1gb, 2006: 10gb, in uscita 2011: 100gb)
  - Cercare di scalare (senza crescere come armadi!)

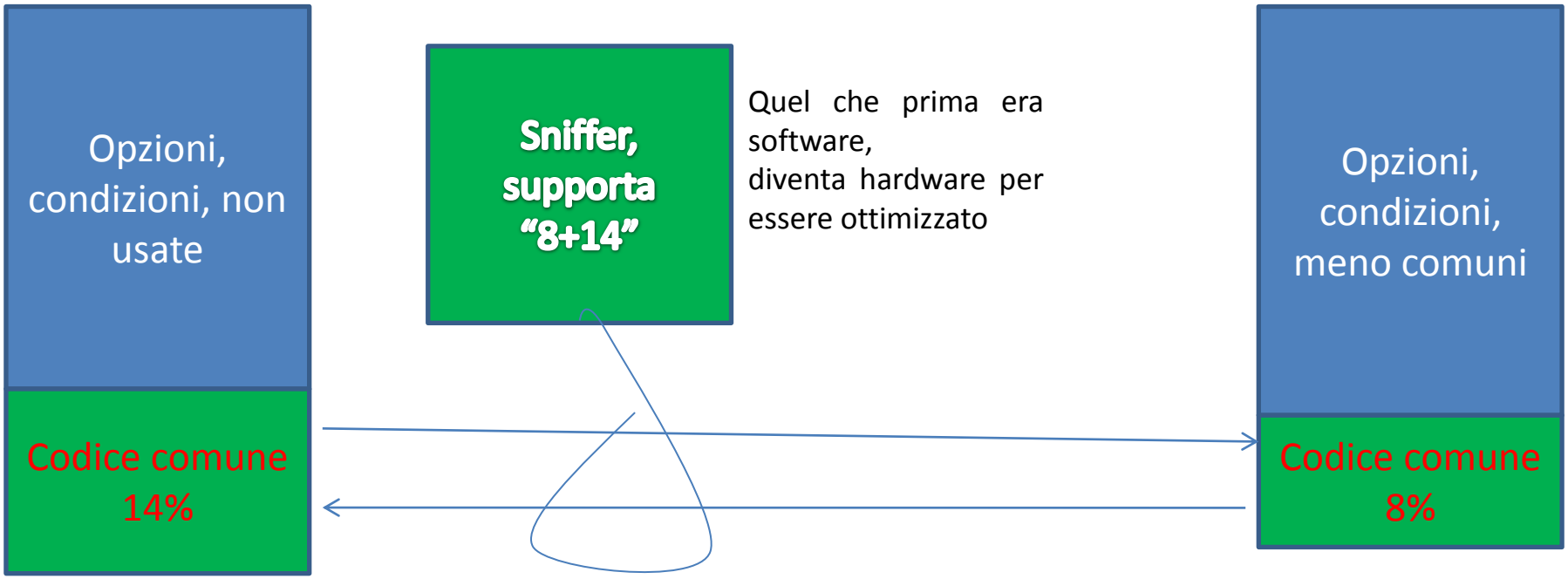
Cosa devono ricostruire

- Riconoscere le sessioni e derivarle
  - Viene fatto in hardware
  - E' l'operazione apparentemente più semplice



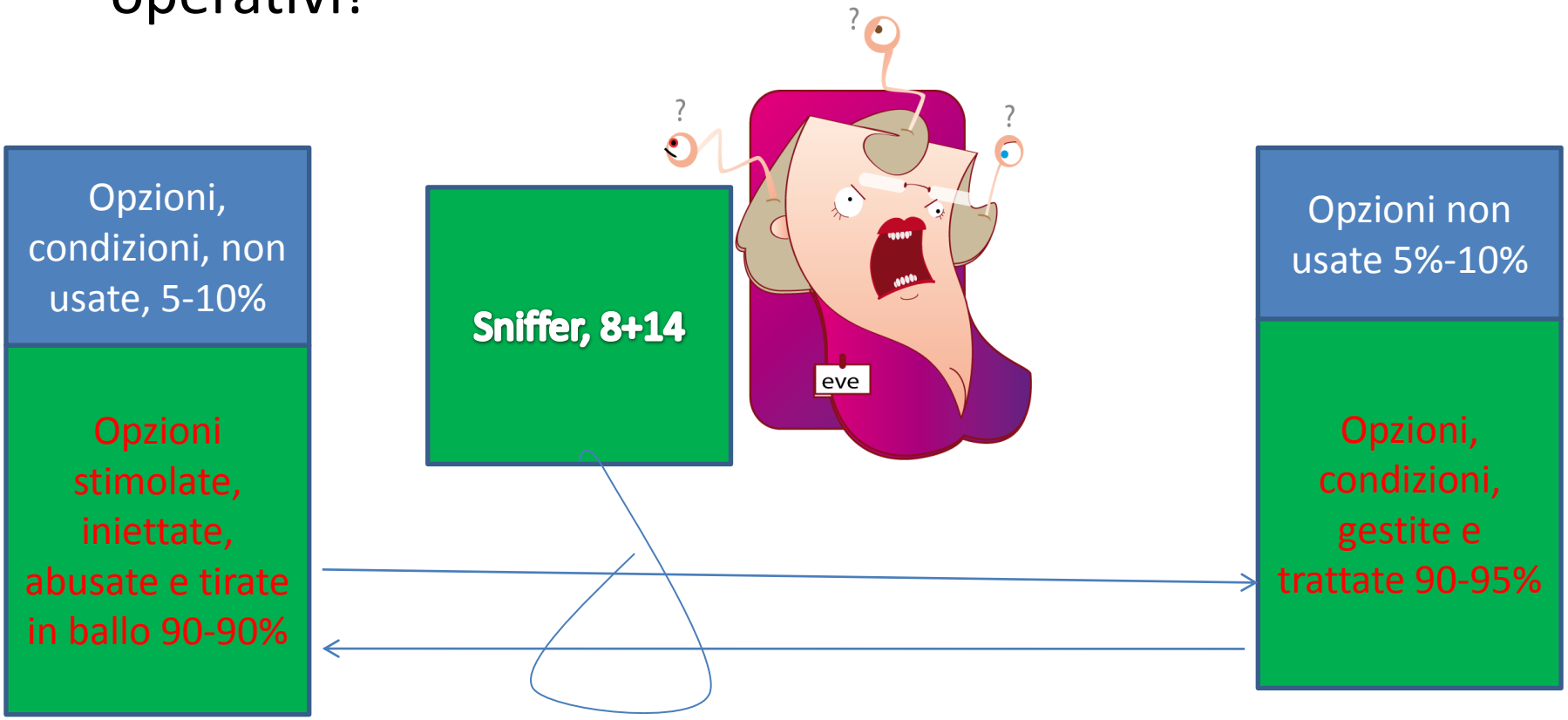
Ma cosa succede, la sotto ?

- Il client usa circa l'8% del codice dello stack di rete
- Il server ne usa circa il 14% (derivati da OProfile)
- Tutte le altre, sono opzioni e condizioni rare (ma del tutto legittime!)



Progetto SniffJoke, la base

- Spinge l'uso di tutte le condizioni previste di sistemi operativi!



Progetto SniffJoke, 2/3

- Sfrutta le differenze nascoste tra i sistemi operativi
  - Ed uno sniffer multigigabit, dovrebbe “emulare ogni singolo sistema operativo” per aver la certezza di ricostruire quello che succede tra i due comunicatori

Progetto SniffJoke 3/3

- Non c’è la garanzia che un dato transitato, sia effettivamente stato ricevuto dall’elemento remoto
  - Questo accade con bassa probabilità
  - **SniffJoke mette sempre in questa condizione di ambiguità**
- La voce, nelle indagini forensi, è considerato un dato biometrico con parametri statistici e contenuti certi
  - SniffJoke sconvolge queste assunzioni

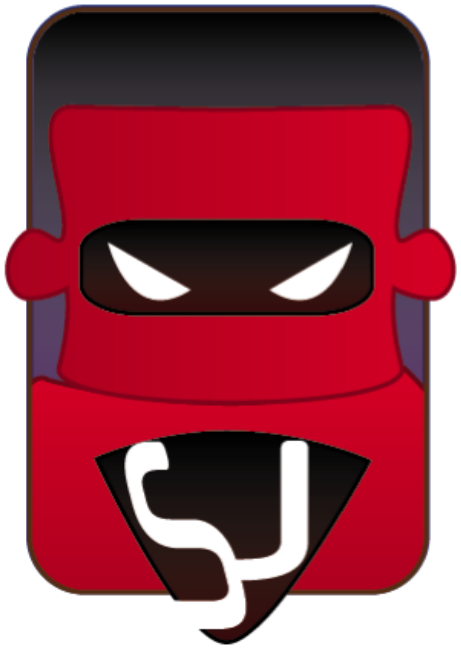
Obiettivi del progetto

- Rendere la deep packet inspection un’azione molto meno scontata e *meno proficua*
- Evidenziare la differenza legislativa e ideologica da applicare tra reti telefoniche e telematiche
- Sostenere le argomentazioni in contrasto alla DPI come metodologia securitaria

Prossimi passi

- (Poiché che c'è già documentazione scientifica in merito…)
- Documentare evidenze sia in laboratorio che in casi reali
- Trovare finanziamenti di qualche tipo
- Coprire un bacino di utenti maggiore
- Danneggiare l'equazione "*controllo = sicurezza != privacy, ma tutto sommato, ok*"

Grazie! Domande ?



http://www.delirandom.net/sniffjoke