Intelligenze artificiali nell'informatica forense

DIGITAL FORENSICS LAB
UNIVERSITY OF PAVIA

Pavia, 26 novembre 2021

Chi vi parla

Davide ‘Rebus’ Gabrini

- Professore a contratto in Informatica e Sicurezza Informatica presso il Dipartimento di Giurisprudenza dell’Università degli Studi di Pavia, A.A. 2021/2022
- Collaboratore del Laboratorio di Informatica Forense dell’Università degli Studi di Pavia, afferente al Laboratorio Nazionale di Cyber Security
- Membro del Comitato Scientifico dell’Area di Diritto e Informatica del Centro Ricerca e Didattica Universitaria del Collegio Ghislieri di Pavia
- Contributor di Tsurugi Linux
- Project Manager di Bento
- Socio fondatore di Inclusive Hacker Framework, già *Italian Gr.A.P.P.A.*
- Socio fondatore del Linux User Group di Pavia
- Curatore della newsletter Rebus’ Digest

Artificial Intelligence for law enforcement

Artificial intelligence and robotics for law enforcement

- Dal 2018 l'Istituto interregionale delle Nazioni Unite per la ricerca sul crimine e la giustizia (UNICRI) e Interpol promuovono annualmente il "*Global Meeting on the Opportunities and Risks of Artificial Intelligence and Robotics for Law Enforcement*"
- Ai meeting vengono presentati e discussi i contributi che IA e robotica possono dare alle attività di polizia e si esaminano casi d'uso a vari stadi di sviluppo da parte delle forze dell'ordine nazionali

unicri
United Nations
Interregional Crime and Justice
Research Institute

CENTRE FOR
ARTIFICIAL
INTELLIGENCE
AND ROBOTICS

INTERPOL

Artificial intelligence and robotics for law enforcement

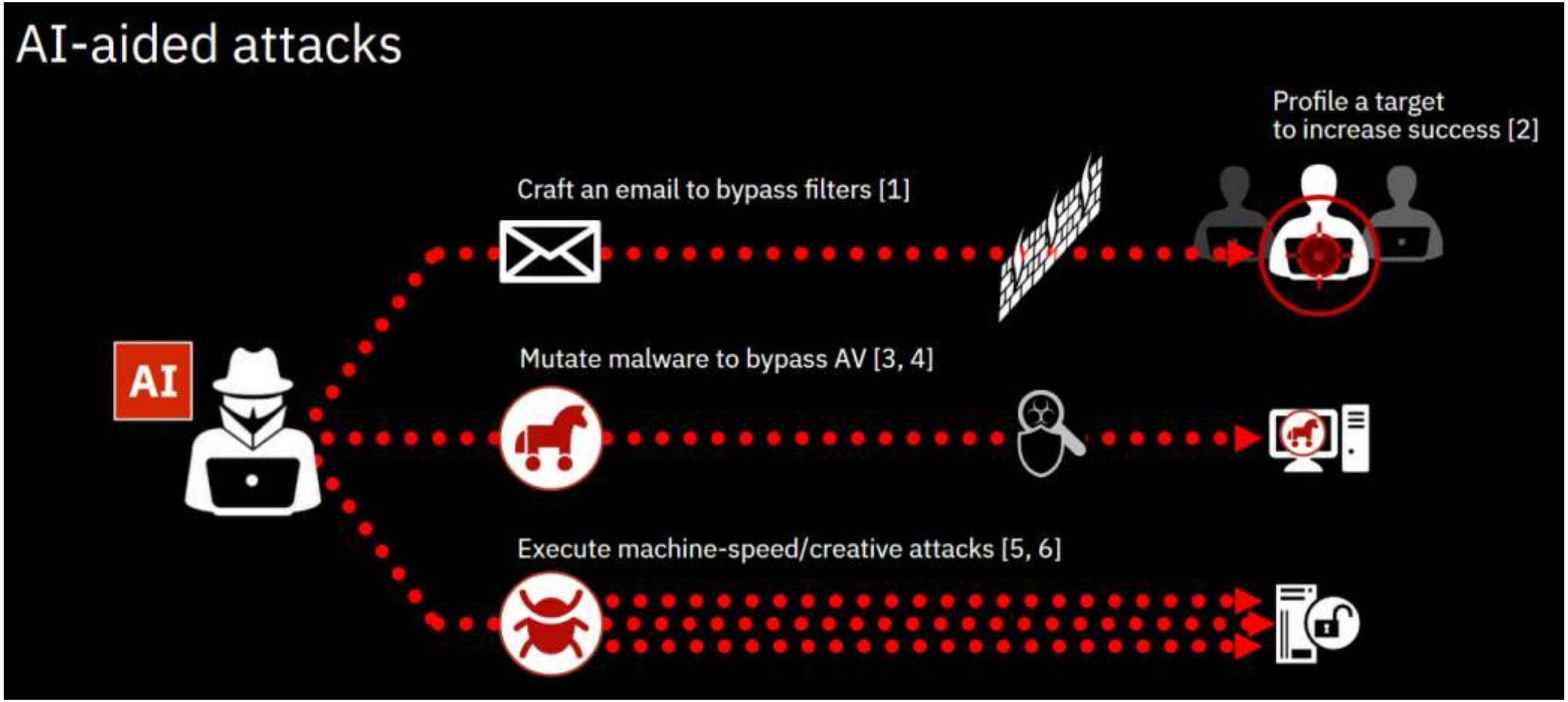
- Tra i più interessanti impieghi considerati ci sono:
  - Strumenti avanzati per l'autopsia virtuale, che aiutino a determinare le cause del decesso
  - Sistemi robotici autonomi di pattugliamento
  - Sistemi predittivi riguardo a luogo e tipologia dei reati che potrebbero compiersi
  - Software di visione artificiale per identificare le auto rubate
  - Strumenti analitici per immagini, video e audio
  - Sistemi di riconoscimento avanzato dei volti
  - Strumenti per identificare i bambini sfruttati o a rischio
  - Strumenti di rilevamento comportamentale, per individuare taccheggiatori
  - Strumenti totalmente autonomi per identificare truffe online
  - Sistemi di realtà aumentata per le forze di polizia

Artificial intelligence and robotics for law enforcement

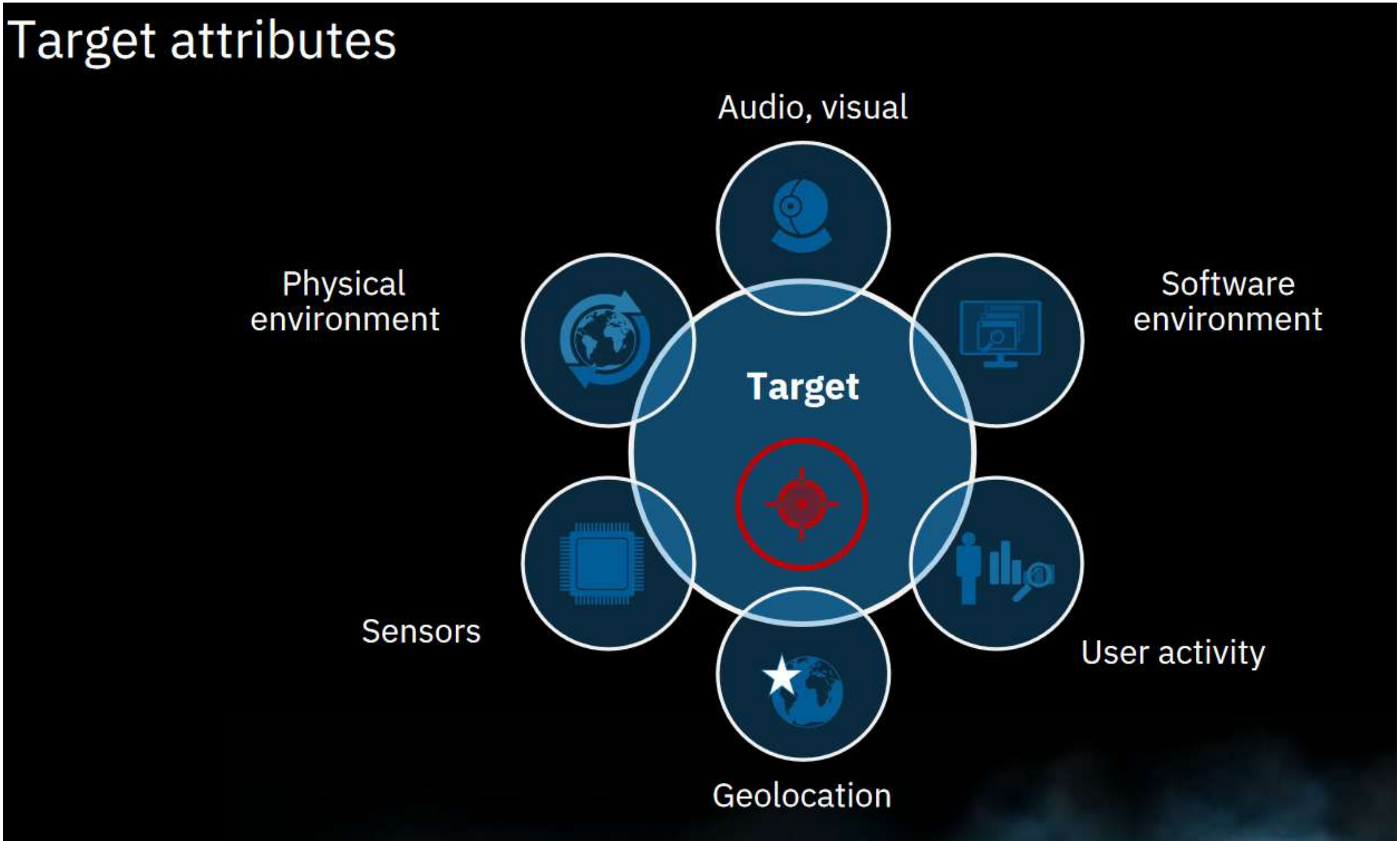
- Tra i possibili usi malevoli sono stati considerati:
  - cyber-attachi condotti da IA
    - spear phishing, exploiting automatizzati, ddos…
  - Attacchi di natura politica
    - proliferazione di fake news, propaganda, disinformazione, deepfake…
  - Attacchi cinetici
    - con l'uso di droni impiegati per colpire persone
  - Una IA potrebbe essere utilizzata anche per contrastare o sovvertire un altro sistema di IA
    - ad esempio per avvelenare il dataset

Un PoC di utilizzo malevole: DeepLocker

- A BlackHat 2018, ricercatori IBM presentano DeepLocker, un malware sperimentale per condurre attacchi altamente mirati ed evasivi basato su tecnologia AI

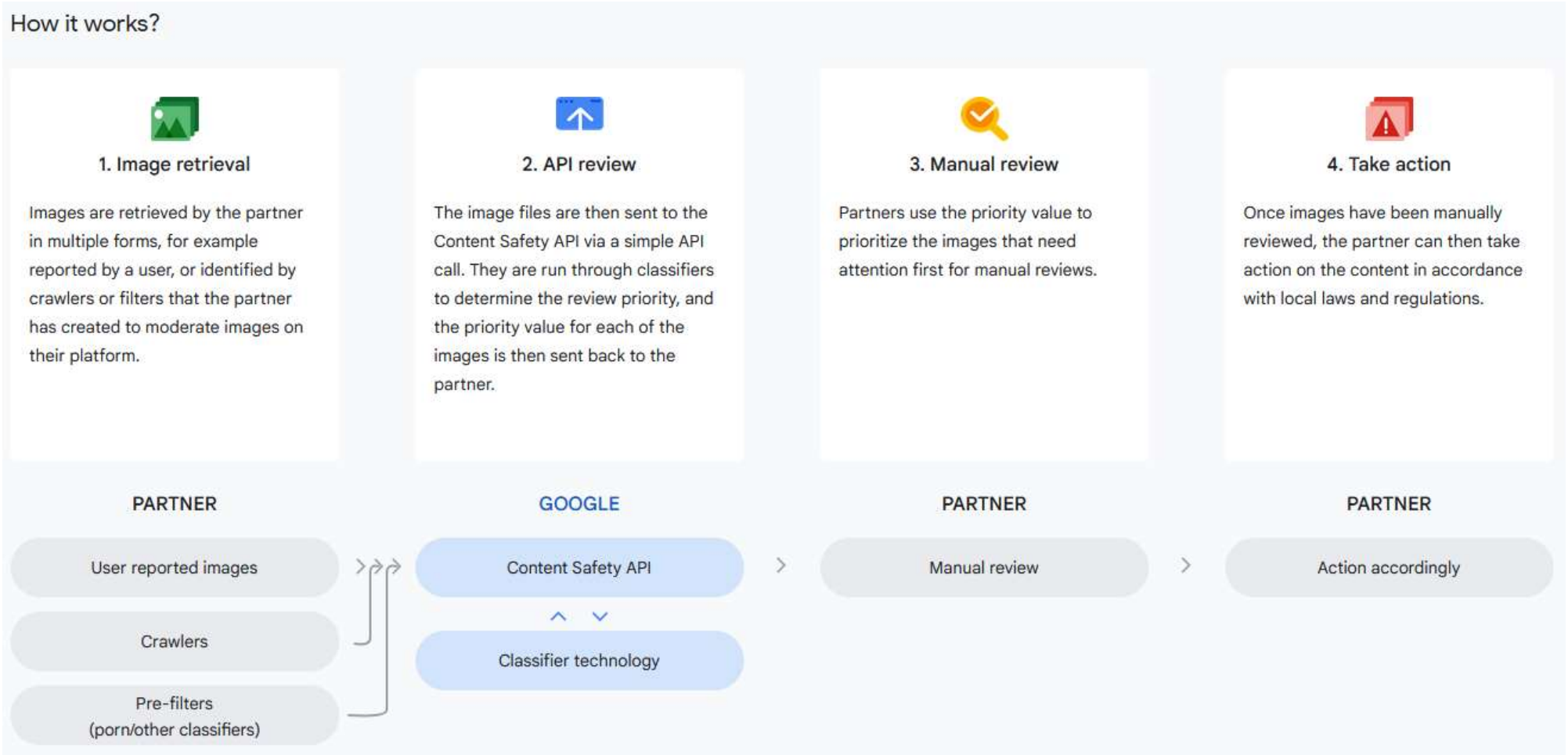


Un PoC di utilizzo malevole: DeepLocker



Un utilizzo virtuoso: Content Safety API di Goole

- Toolkit di Google messo gratuitamente a disposizione delle ONG partner per agevolare il riconoscimento di *child sexual abuse material* (CSAM)
- Anziché basarsi sul riconoscimento di contenuti già noti (comunque disponibile), impiega una IA per identificare contenuti ancora sconosciuti



Artificial Intelligence for digital forensics

Il peso dei dati sui laboratori

- Tutti i reati sono in qualche modo informatici
  - Aumentano i casi
  - Aumentano i reperti per caso
- La capienza degli storage aumenta
  - Quant'è un megabyte?
- L'accesso a risorse in cloud aumenta
- I dispositivi smart aumentano
- L'integrazione e i metadati aumentano
- Tutto questo rischia di causare un DDoS sui laboratori di digital forensics

Si fa presto a dire "big data"

- Nel 2001, gli analisti si trovarono a fronteggiare circa mezzo milione di email relative al caso Enron

  Ricorrendo a tecniche di Social Network Analysis hanno potuto:

  - Scoprire gruppi nascosti ("*a group of individuals planning an activity over a communication medium without announcing their intentions*");
  - Scoprire la struttura organizzativa;
  - Dimostrare il modificarsi delle dinamiche comunicative durante situazioni di emergenza.
- Nel 2008, il caso TJX ha richiesto di elaborare 45 milioni di numeri di carte di credito.
  - Il CERT della Carnegie Mellon University sviluppò il programma CCFinder, che applicava tecniche di data mining e data reduction al fine di tracciare gli utilizzi abusivi, risalire al furto originale e agevolare la notifica alle vittime.

Si fa presto a dire "big data"

- Nel 2020 dal dump di un singolo smartphone può anche saltare fuori 1 milione di messaggi WhatsApp. True story.
- Abbiamo già provato in ogni modo a fronteggiare il problema con intelligenza:
  - Data mining
  - Data reduction
  - Link Analysis
  - Processing power
  - Distributed processing
  - Elastic cloud

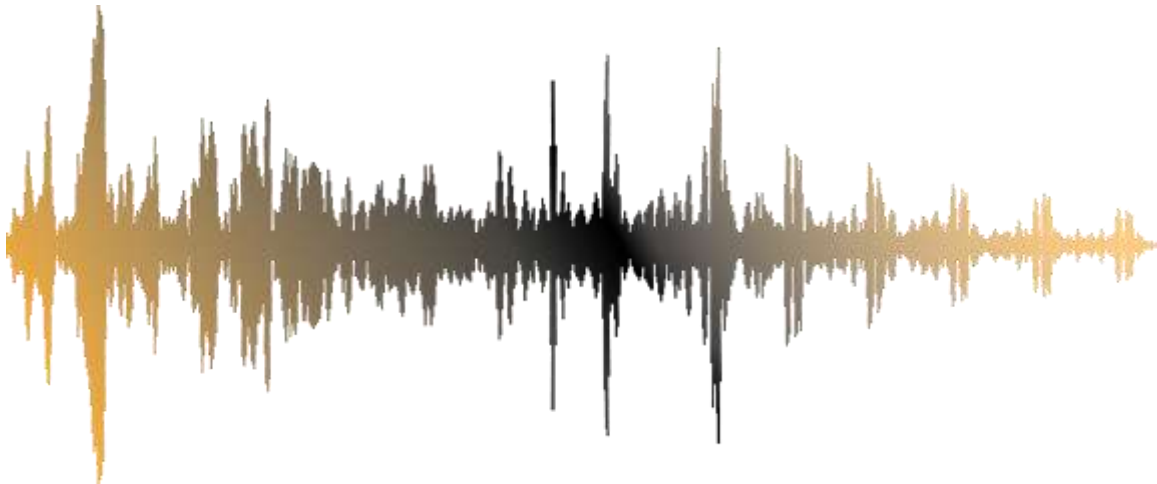
- Tutto ancora utile, ma serve più intelligenza :-)

IA per la digital forensics

- L'uso di IA in analisi forense è un salto di paradigma
- Finora sono stati impiegati algoritmi sempre più sofisticati
  - Modelli deterministici
  - Elevato livello di specializzazione
  - Fondati su profonda comprensione del fenomeno da analizzare
- Gli algoritmi di IA invece sono basati sui dataset di addestramento
  - Imparano da esempi, non hanno necessità di comprendere il fenomeno e i suoi principi
- Coesisteranno entrambi gli approcci
- Le IA possono dare ausilio per:
  - risolvere problemi complessi, che con algoritmi ordinari sono intrattabili
  - risolvere meglio problemi che con algoritmi ordinari sono solubili, ma in modo insoddisfacente

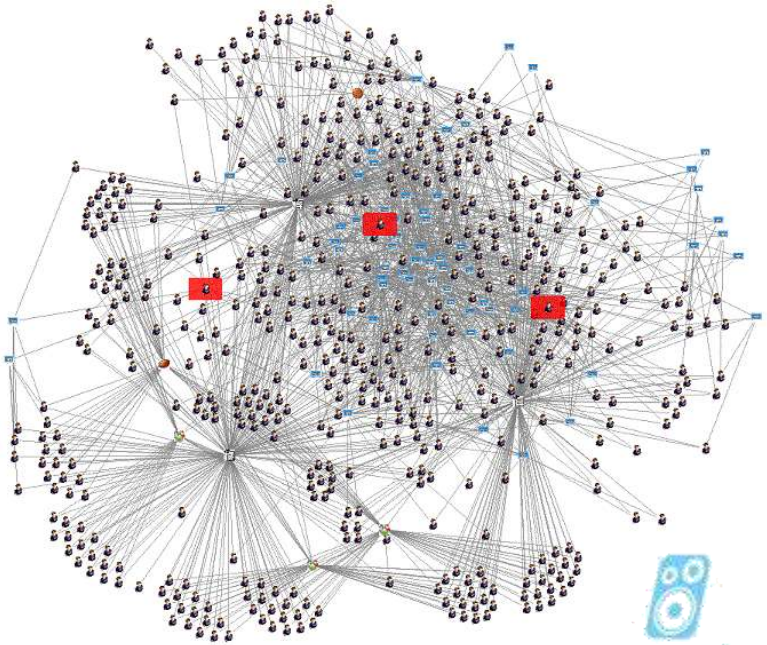
Campi di applicazione per la digital forensics

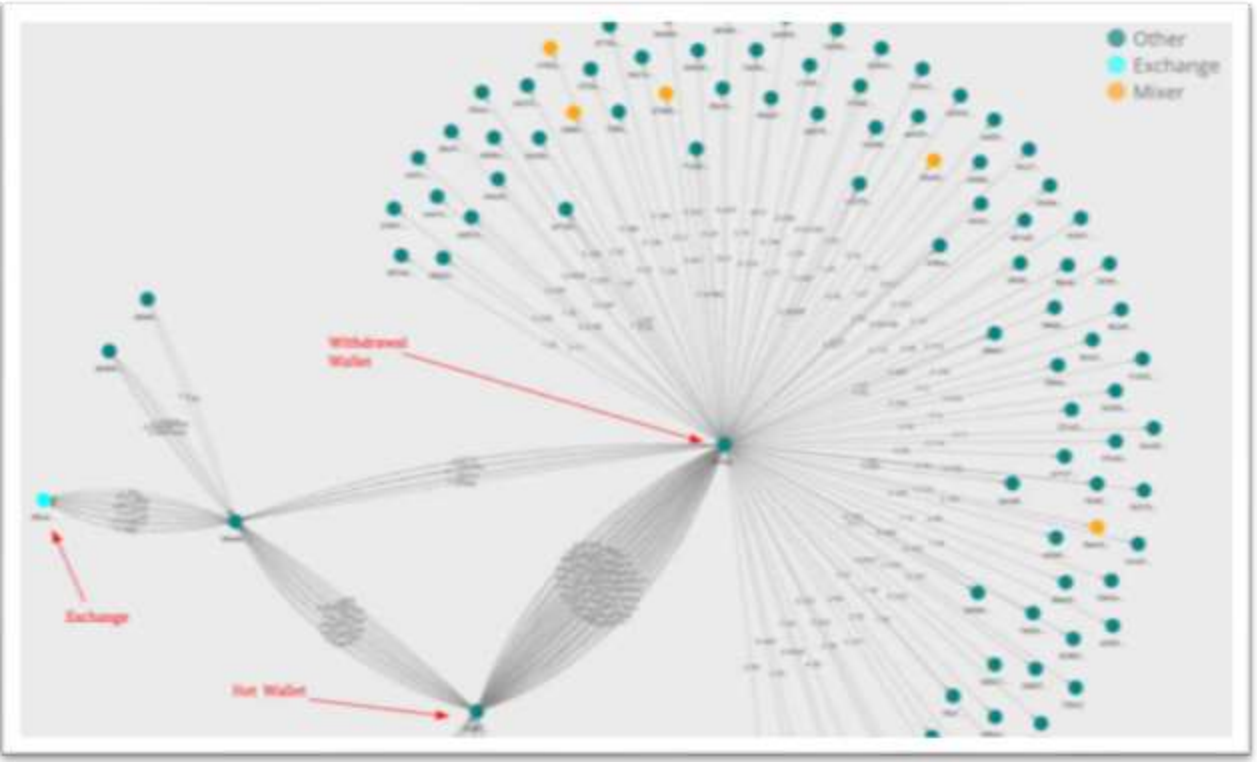
- Analisi semantica dei testi
  - Riassunto
  - Individuazione *key evidence*
  - Traduzione
  - Ricerche per significato
- Analisi file audio
  - Trascrizione messaggi vocali da diverse lingue
  - Riconoscimento del parlante
  - Rilevamento anomalie



Campi di applicazione per la digital forensics

- Link analisys
- Triage
- Blockchain intelligence





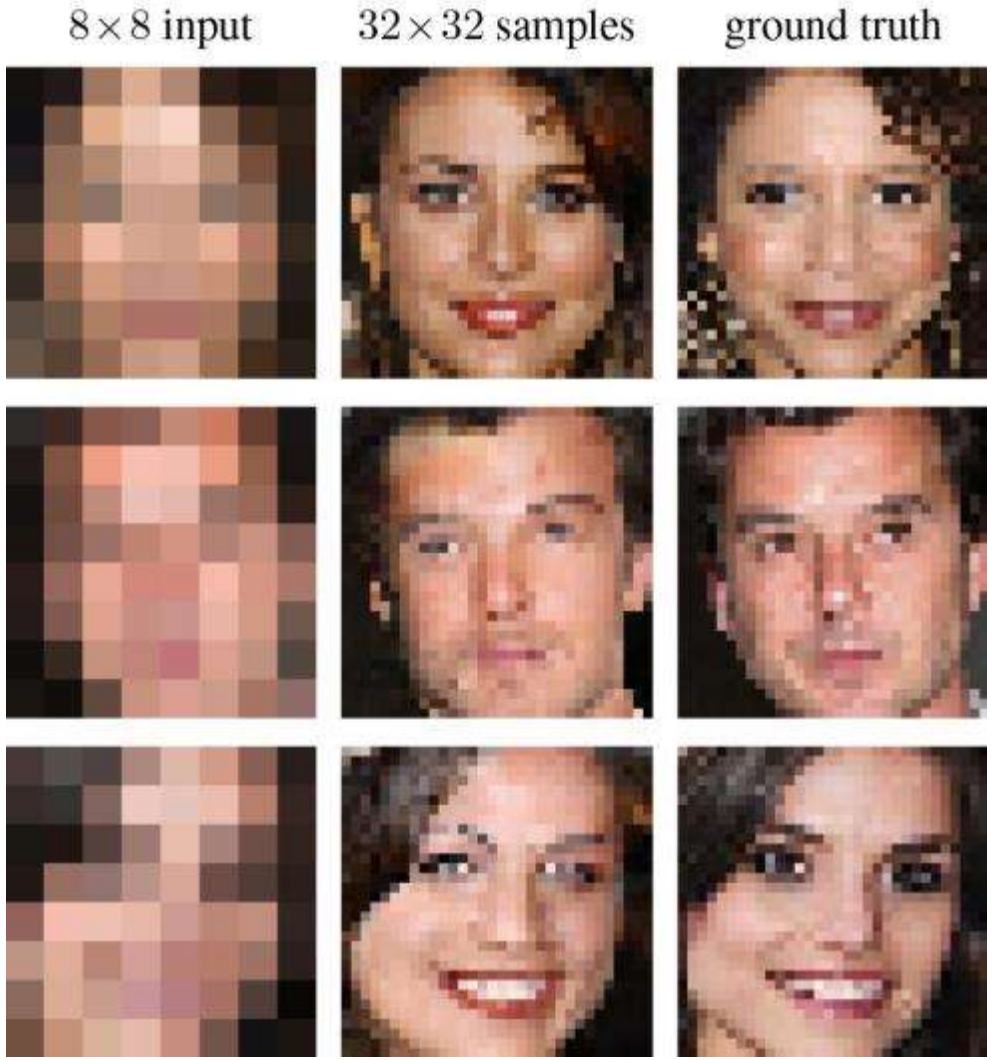
Campi di applicazione per la digital forensics

- Analisi immagini e video
  - Stima similarità
    - Ricostruzione serie
  - Riconoscimento volti
    - Rilevamento, individuazione, aggregazione, categorizzazione…
  - Riconoscimento elementi
    - Persone, armi, droga, soldi, veicoli, targhe, documenti, mappe, pornografia, screenshot…
  - Trascrizione testi
  - Rilevamento contraffazioni

- I video hanno una dimensione temporale:
  - Comprensione degli eventi dinamici

Miglioramento di immagini e video

- Si possono fare informazioni che non ci sono



Utilizzabilità

- Le elaborazioni di una IA difficilmente potranno avere una qualche rilevanza probatoria
  - Per quello sarà sempre richiesta la valutazione di un perito qualificato
- Possono invece essere uno spunto investigativo importante o addirittura necessario

Altrettanto come ausilio al giudice:

- Non possiamo lasciare che prendano decisioni sulle persone
- Ma possono essere un validissimo supporto decisionale
  - Possono fornire una stima di affidabilità
  - Possono mitigare i bias umani

Teniamoci in contatto...

Davide Rebus Gabrini

e-mail: davide.gabrini@unipv.it

GPG Public Key: www.tipiloschi.net/rebus.asc

KeyID: 0x176560F7

DIGITAL FORENSICS LAB
UNIVERSITY OF PAVIA

Queste e altre cazzate su

www.tipiloschi.net

facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus

- **Rebus' Digest**
  newsletter su cybercrime, hacking, digital forensics...
- **EventiLoschi**
  calendario delle conferenze pubbliche in materia