



Cybercrimes.it

Computer Forensics & Crime Informatico

Maurizio Anconelli

Introduzione al

Digital Profiling

Uno degli aspetti paradossali dell'universo digitale è come la lotta al crimine informatico sia ostacolata dallo sviluppo e dal miglioramento di quelle stesse tecnologie di sicurezza che hanno come obiettivo principale proprio il contenimento dei danni derivanti dall'utilizzo criminale di computer ed apparati.

L'adattamento delle realtà criminali alle tecnologie software ed hardware più complesse rappresenta il motivo principale di un rinato interesse verso l'impiego di tecniche umano-psicologiche come mezzo per la persecuzione del crimine informatico, così come l'importanza delle procedure di investigazione digitale e computer forensics cresce di pari passo alle difficoltà di analisi dei sistemi coinvolti nei crimini informatici.

Nuovi software ed apparati che necessitano giornate di apprendimento, algoritmi crittografici e programmi steganografici alla portata della nonna, ostici slalom fra norme e principi a tutela della privacy, terabyte di hard disk dai quali estrarre miliardi di dati nei quali è magari nascosta un'unica manciata binaria di reale rilevanza forense.

Quando una particolare tecnologia informatica non facilmente aggirabile è sfruttata dal criminale per coprire le proprie azioni o le possibili prove derivanti, la prosecuzione delle indagini attraverso canali investigativo-psicologici si dimostra in molti casi il principale sistema che consente il raggiungimento di risultati concreti nonostante la mancanza di elementi di connessione fisici.

Ecco quindi come, travolti da una valanga di dati, log ed aspetti tecnici riguardanti casi inerenti una o più tra le varie tipologie di crimine informatico, rammentiamo di colpo che un computer, per quanto evoluto, sia comunque un semplice sistema automatizzato controllato dalla mente umana, un mezzo per commettere il crimine o l'oggetto stesso del crimine ed in nessun caso la mente che pianifica ed esegue le operazioni realizzate.

Il "Digital Profiling" si inserisce in questo contesto come metodologia primaria per l'isolamento e l'analisi delle caratteristiche umane in una determinata serie di eventi informatici, utilissima nelle indagini su reati già commessi, indispensabile nella pianificazione e strutturazione di sistemi di sicurezza realmente efficaci.

Ad oggi in gran parte ignorato, sia dagli addetti alla sicurezza informatica che dagli organi istituzionali, sta acquisendo rapidamente importanza, trasformandosi da inutile pratica semi-esoterica in reale strumento di prevenzione e persecuzione del crimine informatico, in particolare grazie all'utilizzo di un approccio scientifico e metodologico dove spesso giocavano facoltà ed improvvisazioni del singolo esperto informatico, psicologo o investigatore.

Il Digital Profiling comprende una serie di sistemi e metodologie utili al tracciamento dei profili psicologici, anagrafici e comportamentali delle persone coinvolte in un determinato evento criminale, per mezzo di procedure induttive e deduttive applicate agli elementi emersi dalle indagini preliminari, dall'analisi vittimologica, della scena del crimine e dalle adatte procedure di computer forensics.

Definizione

La definizione "Digital Profiling" abbraccia le combinazioni di sistemi e tecniche volte ricavare informazioni e caratteristiche sugli autori di reati coinvolgenti sistemi informatici, analizzando le strutture comportamentali emergenti dalle prove digitali, dalla vittima e dal contesto nel quale il crimine è commesso.

Altre espressioni utilizzate a livello internazionale quali Cybercrime Profiling, Offender Characterization, Digital Behavioral ecc... suggeriscono una trasposizione in campo informatico di quella che in tempi recenti è stata una delle più discusse e travisate tecniche investigative: il Criminal Profiling.

La stretta correlazione con il Profiling Criminale nato nell'FBI ed utilizzato ormai con risultati tangibili dalle forze di polizia di tutto il mondo suggerisce come nella realtà digitale, il profiling sia utile in particolare per trovare i collegamenti tra due o più soggetti, tra un soggetto ed un determinato crimine, per ridurre il gruppo di possibili sospettati, per condurre operazioni sotto copertura e nella valutazione vittimologica.

Nonostante ciò, pur condividendone il fine ed il concetto di base, ovvero l'impiego di procedure parallele all'investigazione tradizionale per riuscire a tracciare le caratteristiche ed un profilo psicologico del/i criminale/i, il DP non costituisce una semplice rielaborazione delle tecniche utilizzate nel profiling tradizionale.

L'accostamento delle tecniche di profiling al mondo digitale ha origine come supporto nei casi di hacking di siti e di reti, negli episodi di defacement ed in situazioni in cui risultavano evidenti caratteristiche utili quali signature, modus operandi ed attributi vittimologici particolari, nella creazione del profilo di cosiddetti hacker operanti nell'underground, o di gruppi organizzati ai quali era facilmente associabile una

firma comportamentale evidente e riscontrabile in altre attività in rete, spesso catalogate in database organizzati di azioni di cracking o defacement.

Questa tipologia di profiling (che chiameremo Hacker Profiling) rappresenta attualmente solo un aspetto del Digital Profiling.

Lo sviluppo delle tecniche di investigazione informatica e l'accresciuta complessità delle tipologie criminali hanno contribuito infatti a ad una diversa specializzazione e ad una ramificazione strutturale del DP.

Non più solo defacement ed intrusioni ma anche insiding, pedofilia, frode, terrorismo e forensics; non più solo reazione ma anche prevenzione, valutazione e controllo.

Insita Diffidenza

Nonostante le favorevoli aspettative e le potenzialità dimostrate, il profiling digitale incontra tuttora difficoltà nell'essere adottato sia come elemento costitutivo dell'architettura di sicurezza informatica, sia come valido strumento per la prevenzione ed il perseguimento dei reati informatici.

I motivi principali di questa diffidenza sono i seguenti:

- Carente documentazione sull'argomento
- Astrazione dalla natura umana propria dell'ambiente informatico
- Diffidenza manifesta nei confronti delle tecniche tradizionali di investigazione psicologica o profiling criminale generico
- Risultati discrepanti nel profiling criminale generico (non digitale)

Proprio i risultati contrastanti derivati dall'utilizzo di queste tecniche come ausilio alle investigazioni di crimini seriali quali omicidio, stupro, rapina, molestie sessuali, unitamente alla sistematica distorsione/mistificazione operata da letteratura e cinematografia moderna hanno infatti relegato le tecniche di profiling in un contesto figurato di pratica quasi 'esoterica', professata da investigatori dotati di particolare intuito e capacità medianiche nei confronti delle menti criminali.

E' facile inoltre comprendere come in un contesto "virtuale" sia ulteriormente amplificata la sensazione di metodologia eterea.

Ancor più che nel mondo reale, quindi, la comprensione della reale validità del profiling nel mondo digitale, necessita di un approccio scientifico e metodologico spesso in prima analisi trascurato dagli stessi addetti al settore.

Breve introduzione al Criminal Profiling tradizionale

Introduciamo brevemente la storia e le caratteristiche del profiling tradizionale, in modo da chiarire alcuni concetti poco conosciuti ed eliminare ogni errata interpretazione che coinvolgerebbe la corrispondente controparte digitale.

Tralasciando Bertillon, Lombroso e la remota Antropologia Criminale, la nascita del criminal profiling moderno risale convenzionalmente al 1972, quando viene istituita a Quantico la "Behavioral Science Unit"(BSU), o unità delle scienze comportamentali, reparto speciale dell'FBI dedicato all'implementazione di tecniche psicologiche, sociologiche ed investigative per ricavare un profilo della personalità criminale.

Dopo una decina di anni caratterizzata da risultati incoraggianti, all'interno della Behavioral Science Unit, viene organizzato il progetto V.I.C.A.P., Violent Criminal Apprehension Program. Il maggior valore di questo programma risiede nell'aver creato il primo concreto modello di analisi organizzata degli elementi psico-comportamentali nelle indagini criminali o, informaticamente parlando, il primo framework di sviluppo decisionale.

E' sempre all'interno della BSU che nel 1992 Douglas, Burges e Ressler redigono il Crime Classification Manual, un testo nel quale vengono analizzati crimini violenti quali omicidio, stupro ed incendio ponendo particolare attenzione al fattore motivazionale fornendo un'utile classificazione per il lavoro sul campo ed una terminologia standardizzata per facilitare la gestione dei dati. Nel 1997 il testo è stato aggiornato e rivisto dagli stessi autori.

Le caratteristiche ed i principi generali delle scienze comportamentali studiate negli Stati Uniti sono stati implementati ad oggi in molti paesi, nella maggior parte dei quali, comunque, il criminal profiling non ha raggiunto la stessa rilevanza e lo stesso impiego costante.

Nonostante il continuo miglioramento ed affinamento delle tecniche, lo sviluppo del criminal profiling ha

mantenuto inalterato l'obiettivo di partenza, ovvero delineare un tipo psicologico utile a restringere la rosa dei possibili sospetti ed indirizzare gli investigatori verso tipologie individuali specifiche. ma è stato ed è tuttora caratterizzato dal contrasto di due approcci differenti, uno fondamentalmente deduttivo, l'altro induttivo.

Adattamento modello Profiling di Douglas, Ressler, Burgess ed Hartman

Per comprendere meglio le analogie tra il profiling tradizionale e quello digitale utilizzeremo la seguente trasposizione in ambito informatico degli elementi presenti nel modello delineato da Douglas, Ressler, Burgess ed Haltman.

Le linee generali di applicazione mostrate hanno l'unico scopo di rendere comprensibile il percorso generale del processo di profiling che nella realtà deve adattarsi al contesto d'utilizzo. Seppur estremamente semplificato quindi, questo modello permette un confronto visivo immediato.

Fasi	Profiling Tradizionale	Digital Profiling
Profiling Input	Acquisizione di dati ed informazioni riguardanti il crimine, istantanee, testimonianze e caratteristiche dei soggetti coinvolti	Acquisizione dati delle strutture e delle figure coinvolte, architettura dei sistemi, procedure di Incident Response ed acquisizione in Computer Forensics, raccolta dei dettagli fisici e delle prove
Decision Process Models	Organizzazione delle informazioni acquisite attraverso schemi precostituiti, classificazioni e domande pertinenti il caso in oggetto	Raccolta ed inserimento datie file di log in software di analisi e database, elaborazione dati, suddivisione in categorie, creazione di un modello di dati appropriato alle caratteristiche informatiche dell'indagine
Crime Assessment	Ricostruzione comportamentale di criminale e vittima	Valutazione delle caratteristiche informatiche dei sistemi coinvolti, delle metodologie e degli strumenti utilizzati per il crimine ed impatto conseguente. Analisi di eventuali collegamenti e caratteristiche socio/politiche. Estrazione dati comportamentali significativi RPE (Reverse Profile Engineering)
Criminal Profiling	Elaborazione di un profilo iniziale sulla base delle informazioni ricavate dai passaggi precedenti (Razza, sesso, età, stile di vita, caratteristiche psicologiche) Confronto di ogni ipotesi con i dati relativi alla fase due. Analisi induttiva ed elaborazione attraverso storico dati	Link analysis, Data Mining, elaborazione del profilo informatico e dei collegamenti psicologici.
Investigation	Passaggio del profilo supposto alla controparte investigativa per il confronto con i sospetti. Eventuali altri dati emergenti dalla fase di investigazione verranno utilizzati per un aggiornamento del profilo.	Razionalizzazione e scrematura dei link ottenuti. Approfondimento dei collegamenti e degli elementi risultanti dalla precedente fase. Elaborazione dei dati comportamentali e trasposizione nella fase investigativa. Eventuale report di feedback per procedure investigative e di Computer Forensics
Apprehension	Arresto ed interrogatorio del sospettato. Integrazione dei dati nelle basi dati

		Estrazione dati comportamentali significativi Integrazione RPE (Reverse Profiling Engineering)
--	--	---------------------------------------------------------------------------------------------------

Tab.1 Parallelismi con Profiling Model tradizionale

Nella realtà le procedure di profiling applicate all'informatica sono complesse e differenti a seconda dei casi in esame, mostrando differenti livelli di integrazione con le procedure informatiche.

La maggior parte dei problemi e degli scarsi risultati nell'impiego del DP derivano proprio dall'applicazione errata di schemi rigidi che spesso risultano non idonei al frangente nei quali sono utilizzati.

Il DP utilizzato come risposta ad un incidente informatico ha regole, dati ed applicazione differenti dal sistema impiegato, ad esempio, in operazioni anti-terrorismo o intelligence, così come le caratteristiche di un processo di valutazione delle minacce in ambito di security aziendale variano molto da quelle relative ad un'operazione anti-pedofilia.

Gli interventi richiedono in molti casi un differente bilanciamento delle competenze di profiling, esistono infatti situazioni che richiedono metodologie per la maggior parte psico-analitiche (pedofilia, stalking, undercover...) contro altre che necessitano di competenze in gran parte tecniche (es. Incident Response, defacement, computer forensics...)

Per quanto riguarda la progettazione di sistemi informatici di supporto, questa circostanza suggerisce lo sviluppo di framework dedicati ad ogni macro-area di applicazione o alla realizzazione di strutture estremamente modulari, sia per quanto riguarda la base dati che gli algoritmi ed i sistemi di analisi.

Campi di Applicazione

La aree di applicazione del profiling in ambito informatico sono numerose e spaziano dagli ambiti di sicurezza infrastrutturale alle operazioni antiterrorismo, il seguente elenco fornisce una lista degli impieghi più comuni:

- Investigazione informatica generica
- Incident Response
- Computer Forensics
- Prevenzione del crimine informatico
- Operazioni sotto copertura
- Valutazione delle minacce (threat assessment)
- Security Engineering tradizionale
- Security Engineering del software
- Crimini commessi da Insider
- Reati commessi con l'utilizzo di social engineering
- IRC intelligence
- Antiterrorismo
- Cyberstalking e violenza sessuale
- PedoPornografia
- Truffe Informatiche
- Intelligence tradizionale

Ogni ambito presenta caratteristiche peculiari che obbligano conoscenze e strumenti specifici, bisogna in ogni caso tener presente che la correlazione e l'interazione dei campi di applicazione è la norma nella

maggior parte dei casi coinvolgenti procedure di Digital Profiling.

In figura 1 è riportato uno schema visuale degli ambiti di applicazione.

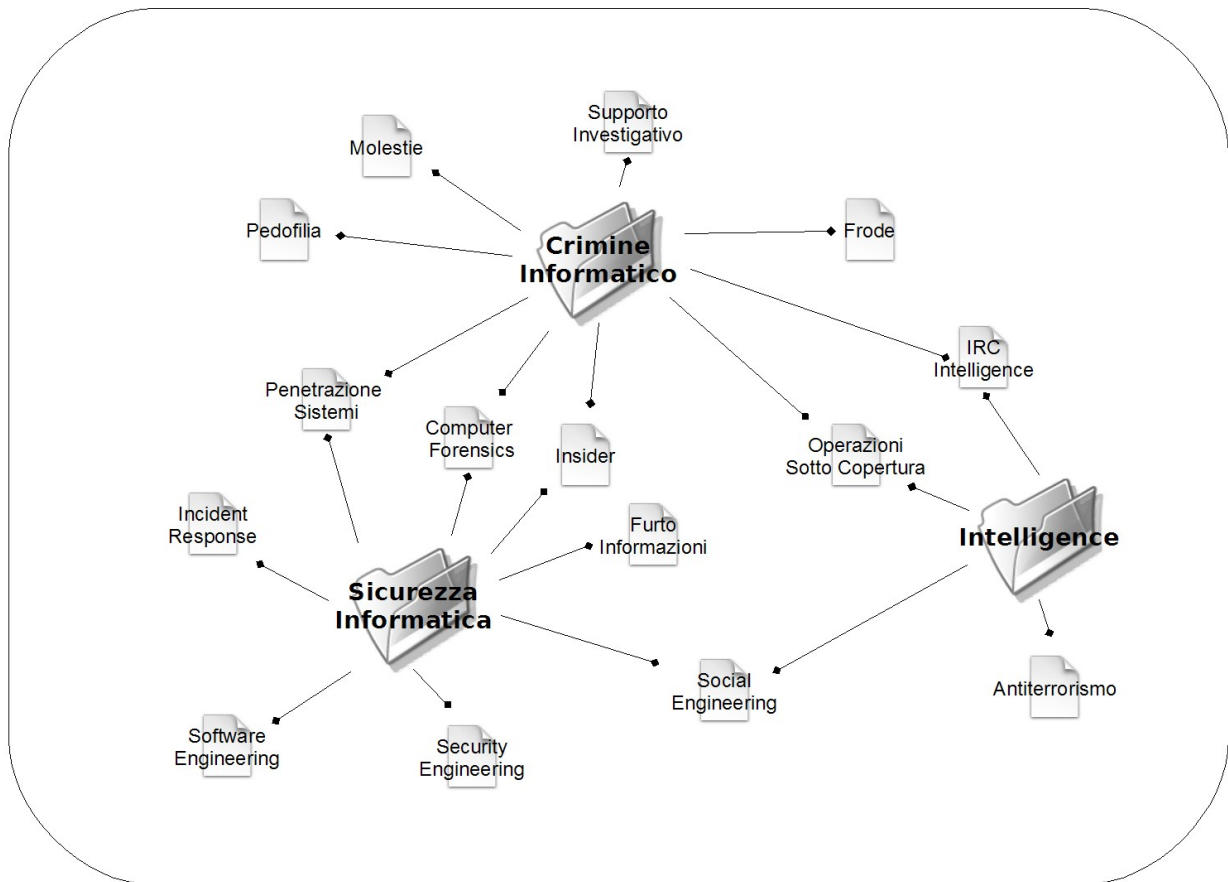


Fig. 1 Campi di Applicazione del Digital Profiling

Elementi del Digital Profiling

La maggior parte degli elementi presenti nel profiling tradizionale trova applicazione anche in campo informatico. La trasposizione comporta una modifica a volte sostanziale delle caratteristiche di ogni elemento, pur conservandone le caratteristiche di base.

Vediamo in breve gli elementi principali:

- **SIGNATURE** – E' la caratteristica più utile in fase di linking e profiling. Come dice il nome stesso si tratta di una "firma" propria dell'autore del crimine, riscontrabile sulla scena del crimine o connessa in altro modo al sospettato. Può essere lasciata a livello conscio o meno e a differenza del Modus Operandi non cambia nella reiterazione del crimine. Non si tratta della classico "Re di cuori" lasciato sulla scena del delitto dal serial killer di turno (anche se nei defacement la firma grafica è praticamente una costante), bensì di modelli comportamentali univoci e ripetuti, spesso non necessari alla dinamica del crimine.

In campo informatico esempi di signature possono essere dettagli linguistici ed aggiunte particolari nei messaggi e-mail o IRC, l'utilizzo di particolari forme di violenza verbale nei casi di cyberstalking, dettagli grafici non necessari nei casi di defacement, caratteristiche forme di commento del codice, denominazione inconsueta di file e cartelle ecc...

- **MODUS OPERANDI** – Solitamente confuso con la Signature, consiste nelle modalità attraverso le quali il crimine è commesso. Nonostante sia utile nella correlazione di casi o individui, il Modus Operandi può variare nel tempo e ciò è molto evidente soprattutto in campo informatico, visto il tasso di accrescimento delle tecnologie ed il parallelo incremento di esperienza da parte del criminale.

Soprattutto nel DP, quindi, il Modus Operandi può condurre a falsi positivi o mancato link psicologico. Appartengono al MO il sistema di penetrazione in un server, le tecniche di occultamento dei log, i programmi utilizzati, le tecniche di scansione, i fattori temporali, le tecniche di avvicinamento ad una preda in chat, il sistema di probing delle vulnerabilità di un sito ed in generale le caratteristiche comportamentali e strumentali dell'individuo che commette il crimine.

- VITTIMOLOGIA – Studio delle caratteristiche della vittima per ottenere l'identificazione del colpevole o dei possibili collegamenti con l'identità criminale. Evidente l'utilità nei casi di molestie sessuali e minacce, in ambito digitale trova primaria applicazione nelle analisi preventive di reti o strutture informatiche.
- MOTIVAZIONE – Elementi psicologici, economici, politici o sociali che spingono l'individuo a commettere un reato. Come esempio possiamo pensare alle convinzioni politiche che spingono un gruppo di hacker a defacciare un particolare sito propagandistico, alle pulsioni sessuali che spingono il pedofilo a contattare ragazzine in chat o ai fattori economici che spingono l'insider a vendere un progetto all'azienda concorrente.
- FATTORI DI RISCHIO – Possono riferirsi al livello di rischio al quale si espone l'individuo che compie l'atto criminale o al risultato della valutazione psicologica durante la fase vittimologica. Il pedofilo che si espone in chat fornendo indicazioni personali ha un fattore di rischio elevato proporzionalmente all'urgenza delle pulsioni, un hacker avrà un indice di rischio più o meno elevato a seconda degli obiettivi scelti. Dal lato vittimologico una ragazzina che inserisce la propria foto in comunità virtuale e la rete di un'azienda contestata per le politiche inquinanti avranno entrambe un fattore di rischio elevato
- STAGING – Consiste nell'alterazione della scena del crimine o di elementi ad essa correlati. Può essere effettuato dal criminale, per evidenti ragioni di depistaggio, o da persone legate in qualche modo al crimine in oggetto. Immaginiamo la madre che cancella dal computer le foto hard della figlia durante un'indagine di stalking o, in caso di intrusione, l'amministratore di sistema che modifica le regole sul firewall per nascondere i propri errori in fase di configurazione.

Analisi

Lo studio e la caratterizzazione dei crimini informatici, dell'ambiente e delle tipologie comportamentali costituisce la base fondamentale per una corretta applicazione dei modelli di profiling e la regolare gestione di azioni preventive e responsive.

Possiamo dividere l'analisi in due tipologie fondamentali : **passiva ed attiva**.

Analisi Passiva

L'analisi passiva è costituita da vittimologia, analisi del movente o motivazione, del Modus Operandi, della scena del crimine e delle caratteristiche del criminale, e dalle altre tecniche analitiche applicabili ad un evento criminale già avvenuto o in fase di svolgimento.

Analisi Attiva

L'analisi attiva è caratterizzata dallo studio dell'ambiente e dei patterns comportamentali propri dell'ambiente digitale, attraverso l'interazione personale o automatizzata, in forma mirata nel caso sia attuata nei confronti di un crimine specifico. A differenza della passiva, questo tipo di analisi non necessita l'applicazione nel contesto di un crimine informatico anzi, spesso è utilizzata come mezzo di prevenzione e creazione di piattaforme di dati utili o statiche. Gli stessi elementi utili in analisi passiva (vittimologia, modus operandi ecc...) vengono rielaborati ed utilizzati in ottica proattiva. Pur essendo sottovalutata, questa tipologia di analisi conduce spesso a risultati maggiormente evidenti.

Attraverso entrambe le tipologie di analisi è possibile estrarre dati che possono essere utilizzati come successivo riferimento o essere elaborati in modelli comportamentali da validare ed applicare nelle varie forme di profiling.

Conclusione

Il Digital Profiling è un campo vasto e controverso, caratterizzato da diverse correnti di pensiero abbinate a differenti tecniche di applicazione, che crescerà di importanza in maniera direttamente proporzionale all'aumento delle difficoltà tecnologiche presenti nell'investigazione informatica.

Attraverso una serie di articoli e testi rilasciati sotto la licenza Creative Commons, porteremo avanti lo studio delle tecniche e dei procedimenti di caratterizzazione utilizzabili con profitto nel dominio del crimine informatico, cercando di eliminare i contrasti ideologici attraverso un approccio, per quanto possibile, pratico ed esemplificativo.

Bibliografia ed Approfondimenti

Brent Turvey – Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques – Knowledge Solutions Library, January 1998

E. Eugene Schultz, Russell Shumway - Incident Response: A Strategic Guide to Handling System and Network Security Breaches – Sams 2002

Brent Turvey – Criminal Profiling: an introduction to behavioural evidence analysis – Academic Press 1999

J. Douglas, A. Burgess, A. Burgess, R. Ressler – Crime Classification Manual – Jossey-Bass Publishers 1992

M. Picozzi, A. Zappalà – Criminal Profiling: Dall'analisi della scena del delitto al profilo psicologico del criminale – McGraw-Hill 2002

Marco Strano – Nuove frontiere delle tecniche di criminal profiling – ANFP Forze Civili Anno 3 N.1 2005

Roberta Bruzzone – Introduzione al Criminal Profiling - ANFP Forze Civili Anno 3 N.1 2005

