CPF Mathematical Formalization Series - Paper 3: Social Influence Vulnerabilities: Modelli di Reciprocità, Impegno e Prova Sociale

Giuseppe Canale, CISSP
Independent Researcher
g.canale@cpf3.org
ORCID: 0009-0007-3263-6897

November 18, 2025

Abstract

Presentiamo la formalizzazione matematica completa degli indicatori della Categoria 3 del Cybersecurity Psychology Framework (CPF): Vulnerabilità di Influenza Sociale. Ciascuno dei dieci indicatori (3.1-3.10) è definito matematicamente attraverso l'analisi delle reti sociali, modellazione della reciprocità e funzioni di escalation dell'impegno. La formalizzazione attinge dai principi di influenza di Cialdini, dalla ricerca di psicologia sociale e dalla teoria delle reti per quantificare come le dinamiche sociali creano sistematicamente vulnerabilità di sicurezza sfruttabili. Forniamo algoritmi espliciti per il rilevamento dell'influenza sociale in tempo reale, la valutazione delle vulnerabilità di rete e la modellazione dell'escalation. Questo lavoro stabilisce il fondamento matematico per l'operazionalizzazione delle tattiche di manipolazione sociale che costantemente aggirano i controlli di sicurezza tecnici attraverso meccanismi di influenza psicologica.

Keywords: Applied Mathematics, Interdisciplinary Psychology, Computational Statistics, Mathematical Modeling, Cybersecurity Research

1 Introduzione e Contesto CPF

Il Cybersecurity Psychology Framework (CPF) affronta il divario critico tra le realtà psicologiche umane e le strategie di difesa della cybersecurity [1]. Mentre le Categorie 1 e 2 si sono concentrate rispettivamente sulle vulnerabilità di autorità e temporali, la Categoria 3 esamina come i meccanismi di influenza sociale compromettono sistematicamente la sicurezza attraverso pattern di conformità psicologica prevedibili.

Le vulnerabilità di influenza sociale rappresentano il vettore di attacco più costantemente sfruttato nella cybersecurity moderna. A differenza delle vulnerabilità tecniche che richiedono conoscenze o risorse specifiche, gli attacchi di influenza sociale sfruttano meccanismi psicologici umani universali che operano attraverso culture e demografiche. I sei principi di influenza di Cialdini [2] forniscono un framework scientificamente validato per comprendere questi meccanismi.

Questo articolo fornisce la formalizzazione matematica completa per tutti i dieci indicatori di vulnerabilità di influenza sociale, consentendo il rilevamento e la previsione sistematici dei tentativi di manipolazione sociale. Ogni indicatore riceve funzioni di rilevamento esplicite che catturano la relazione non lineare tra pressione sociale e comportamento di conformità.

I modelli matematici integrano tre approcci complementari: (1) analisi delle reti sociali per la mappatura delle relazioni, (2) modelli game-theoretic per le dinamiche di reciprocità, e (3) funzioni di escalation dell'impegno per lo sfruttamento della coerenza. Questo approccio multifaccettato garantisce una copertura completa dei meccanismi di vulnerabilità di influenza sociale.

2 Fondamento Teorico: Psicologia dell'Influenza Sociale

Le vulnerabilità di influenza sociale emergono dall'intersezione della psicologia evoluzionistica [3], della teoria delle reti sociali [4] e della psicologia della conformità [5]. La cognizione sociale umana si è evoluta per ambienti di piccoli gruppi, creando punti ciechi sistematici quando applicata a contesti organizzativi moderni e comunicazioni digitali.

Il meccanismo fondamentale coinvolge euristiche di conformità sociale che aggirano il pensiero analitico. Queste euristiche si sono evolute come scorciatoie adattive per navigare ambienti sociali complessi ma diventano vulnerabilità sfruttabili quando gli avversari le attivano deliberatamente [2].

La ricerca dimostra che l'influenza sociale opera attraverso sei canali primari: reciprocità (obbligo di restituire favori), impegno/coerenza (pressione ad allinearsi con posizioni precedenti), prova sociale (tendenza a seguire il comportamento altrui), simpatia (preferenza per fonti gradevoli), autorità (deferenza all'expertise percepita) e scarsità (attribuzione di valore a opportunità rare) [2].

I modelli matematici presentati catturano questi meccanismi attraverso funzioni di propagazione dell'influenza, curve di escalation dell'impegno e fattori di amplificazione della prova sociale. Ogni indicatore quantifica aspetti specifici della vulnerabilità sociale mantenendo l'efficienza computazionale per il monitoraggio in tempo reale.

3 Formalizzazione Matematica

3.1 Framework di Rilevamento dell'Influenza Sociale Universale

Ogni indicatore di vulnerabilità di influenza sociale impiega la funzione di rilevamento unificata con ponderazione della rete sociale:

$$D_i(t) = w_1 \cdot R_i(t) + w_2 \cdot A_i(t) + w_3 \cdot N_i(t) + w_4 \cdot S_i(t) \tag{1}$$

dove $D_i(t)$ rappresenta il punteggio di rilevamento, $R_i(t)$ denota il rilevamento basato su regole, $A_i(t)$ rappresenta il punteggio di anomalia, $N_i(t)$ rappresenta il fattore di influenza di rete, e $S_i(t)$ rappresenta il modificatore di contesto sociale.

L'evoluzione della rete sociale incorpora effetti di propagazione dell'influenza:

$$S_i(t) = \alpha \cdot D_i(t) + \beta \cdot S_i(t-1) + \gamma \cdot \sum_{j \in N(i)} w_{ij} \cdot S_j(t) \tag{2}$$

dove γ cattura gli effetti di influenza di rete e w_{ij} rappresenta i pesi degli archi nel grafo di influenza sociale.

3.2 Indicatore 3.1: Sfruttamento della Reciprocità

Definizione: Manipolazione attraverso la creazione di relazioni di obbligo artificiali che portano a compromessi di sicurezza.

Modello Matematico:

La funzione di squilibrio della reciprocità:

$$R_i(t) = \sum_{j \in N(i)} \frac{Favors_{j \to i}(t) - Favors_{i \to j}(t)}{Favors_{j \to i}(t) + Favors_{i \to j}(t) + \epsilon} \tag{3}$$

dove ϵ previene la divisione per zero e $N(i)$ rappresenta il vicinato di rete dell'individuo i.

Modello di Pressione alla Conformità:

$$P_{comply}(R, T) = \frac{1}{1 + e^{-\beta(R \cdot \alpha + T \cdot \gamma - \theta)}} \tag{4}$$

dove R è lo squilibrio di reciprocità, T è il tempo trascorso dalla ricezione del favore, e θ è la soglia di conformità.

Funzione di Rilevamento:

$$D_{3.1}(t) = \begin{cases} 1 & \text{se } R_i(t) > \tau_{recip} \text{ e } Request\_Anomaly > \sigma \\ 0 & \text{altrimenti} \end{cases} \tag{5}$$

Analisi della Reciprocità di Rete: Utilizzando l'indice di reciprocità ponderata per le reti organizzative:

$$WRI = \frac{\sum_{i,j} w_{ij} \cdot \frac{min(x_{ij}, x_{ji})}{max(x_{ij}, x_{ji})}}{\sum_{i,j} w_{ij}} \tag{6}$$

dove x_{ij} rappresenta la frequenza di interazione e w_{ij} rappresenta il peso della relazione.

3.3 Indicatore 3.2: Trappole di Escalation dell'Impegno

Definizione: Aumento progressivo dell'impegno attraverso piccoli accordi iniziali che portano a compromessi di sicurezza importanti.

Modello Matematico:

Funzione di escalation dell'impegno:

$$C(n) = C_0 \cdot \prod_{i=1}^{n} (1 + \alpha_i \cdot consistency\_pressure_i) \tag{7}$$

dove C_0 è il livello di impegno iniziale e α_i rappresenta il fattore di escalation per il passo i.

Modello dell'Effetto Foot-in-the-Door:

$$P_{accept}(n) = P_0 \cdot \left(\frac{C(n)}{C_0} \right)^{\beta} \tag{8}$$

dove β cattura la forza della relazione impegno-conformità.

Analisi della Sequenza di Richieste:

$$ESI = \frac{\sum_{i=1}^{n-1} \log \left(\frac{Risk_{i+1}}{Risk_i} \right)}{n-1} \tag{9}$$

dove ESI è l'Indice di Sequenza di Escalation che misura l'aumento medio del rischio per passo.

Soglia di Rilevamento:

$$R_{3.2}(t) = \begin{cases} 1 & \text{se } ESI > 0.2 \text{ e } Sequence\_Length > 3 \\ 0 & \text{altrimenti} \end{cases} \tag{10}$$

3.4 Indicatore 3.3: Manipolazione della Prova Sociale

Definizione: Sfruttamento della tendenza a seguire il comportamento di gruppo percepito nelle decisioni di sicurezza.

Modello Matematico:

Funzione di influenza della prova sociale:

$$SP(p, s) = \frac{p^{\alpha}}{p^{\alpha} + (1-p)^{\alpha}} \cdot s^{\beta} \tag{11}$$

dove p è la proporzione che rivendica conformità, s è la similarità percepita al gruppo di riferimento, e α, β sono parametri di scala.

Rilevamento del Falso Consenso:

$$FC = \frac{Claimed\_Compliance - Actual\_Compliance}{Actual\_Compliance + \epsilon} \tag{12}$$

Modello dell'Effetto Bandwagon:

$$P_{join}(t) = \frac{N_{participants}(t)}{N_{total}} \cdot \frac{1}{1 + e^{-\gamma(t-t_0)}} \tag{13}$$

dove γ controlla il tasso di adozione e t_0 rappresenta il punto di svolta.
Algoritmo di Rilevamento:

$$D_{3.3}(t) = SP(p, s) \cdot FC \cdot \mathbb{I}[Claims\_Verification\_Failed] \tag{14}$$

3.5 Indicatore 3.4: Override della Fiducia Basato sulla Simpatia

Definizione: Compromesso di sicurezza attraverso lo sfruttamento della preferenza per fonti gradevoli o simili.

Modello Matematico:
Funzione di fiducia basata sulla simpatia:

$$T_{liking}(similarity, agreeability) = w_1 \cdot S + w_2 \cdot A + w_3 \cdot S \cdot A \tag{15}$$

dove S rappresenta il punteggio di similarità, A rappresenta il punteggio di gradevolezza, e w_3 cattura gli effetti di interazione.

Indice di Sfruttamento della Similarità:

$$SEI = \frac{\sum_{traits} |User_{trait} - Attacker_{claimed\_trait}|}{\sum_{traits} User_{trait}} \tag{16}$$

Probabilità di Override della Fiducia:

$$P_{override}(T, V) = \sigma\left(\alpha \cdot T_{liking} - \beta \cdot Verification\_Strength + \gamma\right) \tag{17}$$

dove V rappresenta la forza di verifica e σ è la funzione sigmoide.
Framework di Rilevamento:

$$R_{3.4}(t) = \begin{cases} 1 & \text{se } SEI < 0.3 \text{ e } P_{override} > 0.7 \\ 0 & \text{altrimenti} \end{cases} \tag{18}$$

3.6 Indicatore 3.5: Decisioni Guidate dalla Scarsità

Definizione: Compromesso di sicurezza attraverso rivendicazioni di urgenza artificiale e disponibilità limitata.

Modello Matematico:
Funzione di valutazione della scarsità:

$$V_{perceived} = V_{base} \cdot \left(\frac{1}{1 + Availability}\right)^{\alpha} \cdot (1 + \beta \cdot Urgency) \tag{19}$$

dove V_{base} è il valore di base, e α, β controllano la sensibilità alla scarsità e all'urgenza.
Amplificazione dell'Avversione alla Perdita:

$$LA = \lambda \cdot Loss_{potential} - Gain_{potential} \tag{20}$$

dove $\lambda > 1$ rappresenta il coefficiente di avversione alla perdita (tipicamente 2.25).

Degradazione della Qualità Decisionale:

$$DQ(t) = DQ_0 \cdot e^{-\gamma \cdot Urgency\_Level(t)} \cdot \left(\frac{Time_{available}}{Time_{needed}} \right)^{\delta} \tag{21}$$

Rilevamento della Manipolazione della Scarsità:

$$D_{3.5}(t) = \max \left(0, \frac{V_{perceived} - V_{rational}}{V_{rational}} - \tau_{scarcity} \right) \tag{22}$$

3.7 Indicatore 3.6: Sfruttamento del Principio di Unità

Definizione: Manipolazione attraverso appelli all'identità condivisa, scopo comune o appartenenza al gruppo.

Modello Matematico:

Forza dell'influenza di unità:

$$U(identity, purpose) = w_1 \cdot I_{shared} + w_2 \cdot P_{common} + w_3 \cdot \sqrt{I_{shared} \cdot P_{common}} \tag{23}$$

dove I_{shared} quantifica la forza dell'identità condivisa e P_{common} misura l'allineamento dello scopo comune.

Quantificazione del Bias In-Group:

$$IGB = \frac{Trust_{ingroup} - Trust_{outgroup}}{Trust_{baseline}} \tag{24}$$

Amplificazione dell'Identità di Gruppo:

$$GIA(t) = \sum_{markers} w_{marker} \cdot Presence_{marker}(t) \cdot Authenticity_{marker} \tag{25}$$

dove i marcatori includono linguaggio, simboli, esperienze condivise e riferimenti culturali.

Funzione di Rilevamento:

$$R_{3.6}(t) = \begin{cases} 1 & \text{se } U > \tau_{unity} \text{ e } IGB > 0.5 \\ 0 & \text{altrimenti} \end{cases} \tag{26}$$

3.8 Indicatore 3.7: Conformità alla Pressione dei Pari

Definizione: Compromesso di sicurezza attraverso pressione esplicita o implicita del gruppo di pari per la conformità.

Modello Matematico:

Funzione di intensità della pressione dei pari:

$$PP(n, d, c) = \frac{n^{\alpha}}{1 + e^{-\beta(c - c_0)}} \cdot \frac{1}{1 + \gamma \cdot d} \tag{27}$$

dove n è il numero di pari, d è la distanza sociale, c è il livello di consenso, e c_0 è la soglia di consenso.

Modello di Probabilità di Conformità:

$$P_{conform}(PP, personality) = \frac{PP^{\delta}}{PP^{\delta} + (Resistance_{personal})^{\delta}} \tag{28}$$

Calcolo della Distanza Sociale:

$$SD_{ij} = \sqrt{\sum_{k} w_k \cdot (attribute_{i,k} - attribute_{j,k})^2} \tag{29}$$

Algoritmo di Rilevamento:

$$D_{3.7}(t) = PP(t) \cdot P_{conform}(t) \cdot \mathbb{I}[Behavioral\_Change\_Detected] \tag{30}$$

3.9 Indicatore 3.8: Conformità a Norme Insicure

Definizione: Adozione di pratiche organizzativamente prevalenti ma insicure attraverso l'influenza sociale normativa.

Modello Matematico:

Forza dell'influenza normativa:

$$NI = \frac{\sum_i w_i \cdot Norm\_Adherence_i}{\sum_i w_i} \cdot Visibility_{factor} \tag{31}$$

dove w_i rappresenta il peso dell'influenza dei pari e la visibilità cattura l'osservabilità del comportamento.

Tasso di Stabilimento della Norma:

$$\frac{dN}{dt} = \alpha \cdot Adoption\_Rate \cdot (1 - N) - \beta \cdot N \tag{32}$$

dove N rappresenta la forza della norma, α è il coefficiente di adozione, e β è il tasso di decadimento.

Normalizzazione del Rischio di Sicurezza:

$$SRN(t) = \int_0^t Risk\_Acceptance\_Rate(\tau) \cdot e^{-\lambda(t-\tau)} d\tau \tag{33}$$

Rilevamento di Soglia:

$$R_{3.8}(t) = \begin{cases} 1 & \text{se } NI > 0.7 \text{ e } SRN > \tau_{norm} \\ 0 & \text{altrimenti} \end{cases} \tag{34}$$

3.10 Indicatore 3.9: Minacce all'Identità Sociale

Definizione: Compromesso di sicurezza attraverso minacce all'identità sociale individuale o di gruppo e alla reputazione.

Modello Matematico:

Intensità della minaccia all'identità sociale:

$$SIT = \sum_{dimensions} w_d \cdot \frac{|Identity_{current,d} - Identity_{threatened,d}|}{Identity_{current,d} + \epsilon} \tag{35}$$

dove d indicizza le dimensioni dell'identità (professionale, culturale, personale).

Modello di Risposta Difensiva:

$$DR(SIT, resources) = \frac{SIT^{\alpha}}{1 + e^{-\beta(Resources - R_0)}} \tag{36}$$

dove $Resources$ include capitale sociale, reputazione e capacità difensive.

Prioritizzazione della Protezione dell'Identità:

$$IPP = \frac{Identity\_Protection\_Effort}{Total\_Available\_Effort} \tag{37}$$

Valutazione della Vulnerabilità:

$$D_{3.9}(t) = SIT \cdot (1 - DR) \cdot IPP \tag{38}$$

3.11 Indicatore 3.10: Conflitti di Gestione della Reputazione

Definizione: Compromesso di sicurezza derivante da conflitti tra requisiti di sicurezza e preservazione della reputazione.

Modello Matematico:

Funzione di trade-off reputazione-sicurezza:

$$RST = \frac{Reputation_{Risk}}{Security_{Risk} + Reputation_{Risk}} \tag{39}$$

Modello del Capitale di Reputazione:

$$RC(t) = RC_0 \cdot e^{-\alpha \cdot Negative_{Events}(t)} + \beta \cdot \int_0^t Positive_{Actions}(\tau) \cdot e^{-\gamma(t-\tau)} d\tau \tag{40}$$

Bias di Risoluzione dei Conflitti:

$$CRB = \frac{Decisions_{reputation\_favoring} - Decisions_{security\_favoring}}{Total_{Conflict\_Decisions}} \tag{41}$$

Funzione di Rilevamento:

$$R_{3.10}(t) = \begin{cases} 1 & \text{se } RST > 0.6 \text{ e } CRB > 0.3 \\ 0 & \text{altrimenti} \end{cases} \tag{42}$$

4 Matrice di Interdipendenza

Gli indicatori di vulnerabilità di influenza sociale mostrano interdipendenze complesse catturate attraverso la matrice di correlazione $\mathbf{R}_3$:

$$\mathbf{R}_3 = \begin{pmatrix} 1.00 & 0.65 & 0.45 & 0.70 & 0.40 & 0.55 & 0.60 & 0.50 & 0.35 & 0.45 \\ 0.65 & 1.00 & 0.50 & 0.60 & 0.45 & 0.40 & 0.55 & 0.45 & 0.30 & 0.35 \\ 0.45 & 0.50 & 1.00 & 0.55 & 0.60 & 0.75 & 0.80 & 0.85 & 0.40 & 0.50 \\ 0.70 & 0.60 & 0.55 & 1.00 & 0.35 & 0.65 & 0.50 & 0.45 & 0.55 & 0.60 \\ 0.40 & 0.45 & 0.60 & 0.35 & 1.00 & 0.30 & 0.35 & 0.40 & 0.25 & 0.30 \\ 0.55 & 0.40 & 0.75 & 0.65 & 0.30 & 1.00 & 0.70 & 0.65 & 0.50 & 0.55 \\ 0.60 & 0.55 & 0.80 & 0.50 & 0.35 & 0.70 & 1.00 & 0.85 & 0.45 & 0.50 \\ 0.50 & 0.45 & 0.85 & 0.45 & 0.40 & 0.65 & 0.85 & 1.00 & 0.40 & 0.45 \\ 0.35 & 0.30 & 0.40 & 0.55 & 0.25 & 0.50 & 0.45 & 0.40 & 1.00 & 0.75 \\ 0.45 & 0.35 & 0.50 & 0.60 & 0.30 & 0.55 & 0.50 & 0.45 & 0.75 & 1.00 \end{pmatrix} \tag{43}$$

Le interdipendenze chiave includono:

- Forte correlazione (0.85) tra Prova Sociale (3.3) e Conformità a Norme (3.8)
- Alta correlazione (0.85) tra Pressione dei Pari (3.7) e Conformità a Norme (3.8)
- Significativa correlazione (0.80) tra Prova Sociale (3.3) e Pressione dei Pari (3.7)
- Forte correlazione (0.75) tra Minacce all'Identità Sociale (3.9) e Conflitti di Reputazione (3.10)

Dipendenze Inter-Categoria: Relazioni critiche con le vulnerabilità di Autorità (Categoria 1) e le vulnerabilità Temporali (Categoria 2):

- $R_{1.1,3.3} = 0.75$: Conformità all'autorità amplificata dalla prova sociale
- $R_{1.9,3.3} = 0.85$: Prova sociale basata sull'autorità correla direttamente con la prova sociale generale
- $R_{2.1,3.5} = 0.70$: Aggiramento per urgenza correla con decisioni guidate dalla scarsità
- $R_{1.6,3.9} = 0.65$: Effetti del gradiente di autorità correlano con minacce all'identità sociale

5 Algoritmi di Implementazione

Algorithm 1 Valutazione della Vulnerabilità di Influenza Sociale

Inizializza i parametri della rete sociale $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$
Carica il grafo sociale organizzativo e i pattern di comunicazione
for ogni passo temporale t **do**
  Estrai il contesto sociale: network_state(t), communication_flows(t)
  Calcola i coefficienti di propagazione dell'influenza sociale
  for ogni indicatore $i \in \{3.1, 3.2, \ldots, 3.10\}$ **do**
    Calcola le metriche di pressione sociale $SP_i(t)$
    Calcola il rilevamento basato su regole $R_i(t)$
    Calcola il punteggio di anomalia ponderato dalla rete $A_i(t)$
    Valuta il modificatore di contesto sociale $S_i(t)$
    Calcola il punteggio di rilevamento $D_i(t)$
    Applica il modello di propagazione dell'influenza sociale
    Aggiorna lo stato di influenza di rete $N_i(t)$
  end for
  Calcola le correzioni di interdipendenza usando $\mathbf{R}_3$
  Applica le correlazioni inter-categoria con Categorie 1 e 2
  Genera avvisi consapevoli dell'influenza con previsioni di propagazione
  Aggiorna i modelli di evoluzione della rete sociale
  Registra i risultati per la raffinazione dei pattern di influenza
end for

6 Framework di Validazione

La validazione della vulnerabilità di influenza sociale richiede metriche specializzate che tengono conto degli effetti di rete e delle dinamiche sociali:

Metriche di Classificazione Consapevoli della Rete:

$$Precision_{network} = \frac{\sum_{clusters} |TP_{cluster}| \cdot w_{cluster}}{\sum_{clusters} |TP_{cluster} + FP_{cluster}| \cdot w_{cluster}} \tag{44}$$

$$Recall_{network} = \frac{\sum_{clusters} |TP_{cluster}| \cdot w_{cluster}}{\sum_{clusters} |TP_{cluster} + FN_{cluster}| \cdot w_{cluster}} \tag{45}$$

dove $w_{cluster}$ fornisce la ponderazione basata su cluster per la struttura di rete.

Validazione della Propagazione dell'Influenza: Accuratezza della previsione per la diffusione dell'influenza:

$$IPA = 1 - \frac{|Predicted\_Influence\_Set \triangle Actual\_Influence\_Set|}{|Actual\_Influence\_Set|} \tag{46}$$

Accuratezza della Prova Sociale: Misura del rilevamento del falso consenso:

$$SPA = \frac{TP_{false\_consensus}}{TP_{false\_consensus} + FN_{false\_consensus}} \tag{47}$$

Previsione dell'Escalation dell'Impegno: Errore Assoluto Medio per le sequenze di escalation:

$$MAE_{escalation} = \frac{1}{n} \sum_{i=1}^{n} |Risk_{predicted,i} - Risk_{actual,i}| \tag{48}$$

Algorithm 2 Mappatura della Vulnerabilità della Rete Sociale

Input: Rete sociale $G(V, E)$, pattern di influenza P
Inizializza i punteggi di vulnerabilità dei nodi $V_{vuln}[|V|]$
for ogni nodo $v \in V$ **do**
    Calcola le misure di centralità: grado, betweenness, closeness
    Calcola il punteggio di capitale sociale $SC(v)$
    Valuta la suscettibilità all'influenza $IS(v)$
    Valuta la vulnerabilità della posizione di rete $NPV(v)$
    Calcola la vulnerabilità composita $V_{vuln}[v] = f(SC, IS, NPV)$
end for
for ogni arco $(u, v) \in E$ **do**
    Calcola la capacità di flusso di influenza $IFC(u, v)$
    Valuta la resistenza alla manipolazione $MR(u, v)$
    Calcola la vulnerabilità dell'arco $E_{vuln}(u, v)$
end for
Identifica i percorsi di influenza critici usando algoritmi di cammino minimo
Calcola le metriche di vulnerabilità a livello di rete
Genera raccomandazioni di mitigazione mirate
Restituisci la mappa di vulnerabilità con punteggi di confidenza

Validazione Incrociata con Stratificazione Sociale: Garantire che i set di training e test preservino la struttura sociale:

$$Social\_Preservation = \frac{Network\_Properties_{test}}{Network\_Properties_{total}} \tag{49}$$

Il punteggio di preservazione target si avvicina a 1.0 per il mantenimento ottimale della struttura sociale.

Validazione della Resistenza all'Influenza: Misura dell'efficacia dell'intervento:

$$Resistance_{gain} = \frac{Vulnerability_{baseline} - Vulnerability_{post\_intervention}}{Vulnerability_{baseline}} \tag{50}$$

7 Conclusione

Questa formalizzazione matematica delle vulnerabilità di influenza sociale fornisce un fondamento rigoroso per comprendere e rilevare le debolezze di sicurezza basate sulla manipolazione. L'integrazione dell'analisi di rete, della modellazione della reciprocità e della teoria dell'escalation dell'impegno crea un framework completo per la valutazione delle vulnerabilità sociali.

La matrice di interdipendenza rivela forti correlazioni tra gli indicatori di influenza sociale e effetti significativi inter-categoria con le vulnerabilità di autorità e temporali. Questo dimostra che l'influenza sociale agisce come un moltiplicatore di forza per altre vulnerabilità psicologiche, enfatizzando l'importanza critica delle strategie di sicurezza consapevoli del sociale.

Gli algoritmi di implementazione consentono il monitoraggio dell'influenza sociale in tempo reale con capacità predittive per la propagazione dell'influenza. Le organizzazioni possono anticipare le cascate di vulnerabilità basate sulla topologia di rete, i pattern di comunicazione e gli indicatori di pressione sociale, consentendo misure di sicurezza proattive piuttosto che reattive.

Il lavoro futuro estenderà questo approccio di modellazione sociale alle restanti categorie CPF, con particolare attenzione agli effetti di amplificazione sociale sul sovraccarico cognitivo (Categoria 5) e le dinamiche di gruppo (Categoria 6). Il rigore matematico qui stabilito fornisce un fondamento per strategie di sicurezza sociale basate sull'evidenza che tengono conto dei pattern prevedibili della cognizione sociale umana.

La categoria di influenza sociale dimostra che la sicurezza è fondamentalmente un fenomeno sociale, non meramente tecnico. Formalizzando matematicamente queste dinamiche sociali, consentiamo sistemi di sicurezza che comprendono e tengono conto delle realtà sociali umane piuttosto che aspettarsi che gli esseri umani operino al di fuori dei loro framework psicologici evoluti.

References

[1] Canale, G. (2024). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences. *Preprint*.

[2] Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. New York: Harper Business.

[3] Buss, D. M. (1999). *Evolutionary Psychology: The New Science of the Mind*. Boston: Allyn & Bacon.

[4] Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *Nature*, 393(6684), 440-442.

[5] Kelman, H. C. (1958). Compliance, identification, and internalization: Three processes of attitude change. *Journal of Conflict Resolution*, 2(1), 51-60.