CPF Mathematical Formalization Series - Paper 2: Temporal Vulnerabilities: Time-Pressure Models and Temporal Cognitive Load

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

September 24, 2025

Abstract

We present the complete mathematical formalization of Category 2 indicators from the Cybersecurity Psychology Framework (CPF): Temporal Vulnerabilities. Each of the ten indicators (2.1-2.10) is mathematically defined through time-dependent detection functions incorporating urgency modeling, temporal cognitive load assessment, and circadian rhythm analysis. The formalization draws from Kahneman and Tversky's prospect theory and temporal discounting research to quantify how time pressure systematically degrades security decision-making quality. We provide explicit algorithms for real-time temporal vulnerability assessment, interdependency matrices capturing temporal cascade effects, and validation metrics for organizational chronotype calibration. This work establishes the mathematical foundation for operationalizing time-based psychological vulnerabilities that create predictable windows of security weakness.

1 Introduction and CPF Context

The Cybersecurity Psychology Framework (CPF) addresses the critical gap between human psychological realities and cybersecurity defense strategies [1]. While Category 1 focused on authority-based vulnerabilities, Category 2 examines how temporal factors systematically degrade security effectiveness through predictable psychological mechanisms.

Temporal vulnerabilities represent one of the most quantifiable aspects of human security weakness. Unlike authority dynamics that vary by organizational culture, temporal effects follow universal patterns rooted in evolutionary psychology and circadian biology. Attackers consistently exploit these patterns through deadline-driven social engineering, end-of-day attacks, and time-pressure manipulation.

This paper provides complete mathematical formalization for all ten temporal vulnerability indicators, enabling systematic detection and prediction of time-based security weaknesses. Each indicator receives explicit detection functions that capture the nonlinear relationship between time pressure and security decision quality.

The mathematical models integrate three complementary approaches: (1) hyperbolic discounting functions for future threat valuation, (2) cognitive load modeling for time-pressure effects, and (3) circadian analysis for temporal performance variation. This multi-faceted approach ensures comprehensive coverage of temporal vulnerability mechanisms.

2 Theoretical Foundation: Temporal Psychology

Temporal vulnerabilities emerge from the intersection of prospect theory [2], cognitive load theory [3], and chronobiology [4]. Human temporal cognition exhibits systematic biases that create predictable security vulnerabilities when exploited by adversaries.

The fundamental mechanism involves hyperbolic discounting, where immediate rewards receive disproportionate weighting compared to delayed consequences [5]. In security contexts, this manifests as present bias in risk assessment: immediate operational needs consistently override future security consequences when time pressure increases.

Research demonstrates that cognitive performance follows predictable circadian patterns, with peak performance occurring 2-4 hours after awakening and significant degradation during circadian low points [6]. Security decision quality correlates strongly with these biological rhythms, creating systematic vulnerability windows.

The mathematical models presented capture these mechanisms through temporal weighting functions, cognitive load modifiers, and circadian performance curves. Each indicator quantifies specific aspects of temporal vulnerability while maintaining computational efficiency for real-time monitoring.

3 Mathematical Formalization

3.1 Universal Temporal Detection Framework

Each temporal vulnerability indicator employs the unified detection function with temporal weighting:

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

where $D_i(t)$ represents detection score, $R_i(t)$ denotes rule-based detection, $A_i(t)$ represents anomaly score, $T_i(t)$ represents temporal pressure indicator, and $C_i(t)$ represents circadian performance modifier.

The temporal evolution incorporates momentum effects:

$$S_i(t) = \alpha \cdot D_i(t) + \beta \cdot S_i(t-1) + \gamma \cdot \frac{dD_i}{dt} \tag{2}$$

where γ captures velocity effects in temporal vulnerability evolution.

3.2 Indicator 2.1: Urgency-Induced Security Bypass

Definition: Circumvention of security controls under perceived time pressure to meet deadlines.

Mathematical Model:

The urgency acceleration function:

$$U_i(t) = \frac{\Delta t_{normal} - \Delta t_{urgent}}{\Delta t_{normal}} \tag{3}$$

where Δt_{normal} represents baseline task completion time and Δt_{urgent} represents accelerated completion time under pressure.

Bypass Probability Model:

$$P_{bypass}(U, D) = \frac{1}{1 + e^{-\beta(U \cdot \alpha + D \cdot \gamma - \theta)}} \tag{4}$$

where U is urgency level, D is deadline proximity, and θ is the decision threshold.

Detection Function:

$$R_{2.1}(t) = \begin{cases} 1 & \text{if } U_i(t) > 0.5 \text{ and } N_{bypass} > \tau_{bypass} \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

Temporal Regression Model: Using Poisson regression for bypass rate prediction:

$$\log(\lambda) = \beta_0 + \beta_1 \cdot pressure + \beta_2 \cdot deadline\_proximity + \beta_3 \cdot circadian \tag{6}$$

3.3 Indicator 2.2: Time Pressure Cognitive Degradation

Definition: Systematic reduction in cognitive capacity under temporal constraints leading to security errors.

Mathematical Model:

Cognitive capacity function under time pressure:

$$C(t,p) = C_0 \cdot e^{-\alpha p(t)} \cdot (1 + \beta \sin(\frac{2\pi(t-\phi)}{24})) \tag{7}$$

where C_0 is baseline capacity, $p(t)$ is time pressure, and the sinusoidal term captures circadian variation.

Error Rate Model:

$$E(t) = E_{baseline} \cdot \left(\frac{C_0}{C(t,p)}\right)^{\gamma} \tag{8}$$

Detection Through Performance Metrics:

$$D_{2.2}(t) = \frac{E(t) - \mu_E}{\sigma_E} \cdot \frac{RT(t) - \mu_{RT}}{\sigma_{RT}} \tag{9}$$

where RT represents response time degradation under pressure.

3.4 Indicator 2.3: Deadline-Driven Risk Acceptance

Definition: Acceptance of elevated security risks to meet project deadlines.

Mathematical Model:

Hyperbolic discounting function for risk assessment:

$$V(R,D) = \frac{R}{1 + k \cdot D} \tag{10}$$

where V is perceived risk value, R is actual risk magnitude, D is deadline distance, and k is the organization-specific discount rate.

Risk Acceptance Threshold:

$$P_{accept}(R,D) = \sigma\left(\frac{V(R,D) - \theta_{risk}}{\sigma_{noise}}\right) \tag{11}$$

Project Management Integration:

$$DD_{score}(t) = \frac{\sum_i Risk_i \cdot Accepted_i(t)}{\sum_i Risk_i \cdot Proposed_i(t)} \tag{12}$$

Detection Condition:

$$R_{2.3}(t) = \begin{cases} 1 & \text{if } DD_{score}(t) > \mu + 2\sigma \text{ and } D < 7 \text{ days} \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

3.5 Indicator 2.4: Present Bias in Security Investments

Definition: Systematic undervaluation of future security benefits relative to immediate costs.

Mathematical Model:

Present bias coefficient in security ROI calculations:

$$NPV_{biased} = \sum_{t=1}^{T} \frac{B_t}{(1+r)^t \cdot (1+\delta)^t} - C_0 \tag{14}$$

where δ represents present bias parameter beyond standard discounting rate r.

Investment Decision Model:

$$P_{invest}(NPV, PB) = \frac{e^{\alpha \cdot NPV_{biased}}}{1 + e^{\alpha \cdot NPV_{biased}}} \tag{15}$$

Bias Detection:

$$PB_{indicator} = \frac{NPV_{standard} - NPV_{biased}}{NPV_{standard}} \tag{16}$$

Threshold Function:

$$D_{2.4}(t) = \max(0, PB_{indicator} - \theta_{pb}) \tag{17}$$

3.6 Indicator 2.5: Hyperbolic Discounting of Future Threats

Definition: Disproportionate weighting of immediate threats over future risks in resource allocation.

Mathematical Model:

Hyperbolic vs. exponential discounting comparison:

$$V_{exp}(t) = V_0 \cdot e^{-rt} \tag{18}$$

$$V_{hyp}(t) = \frac{V_0}{1 + kt} \tag{19}$$

Discounting Inconsistency Measure:

$$DI(t_1, t_2) = \frac{V_{hyp}(t_1)/V_{hyp}(t_2)}{V_{exp}(t_1)/V_{exp}(t_2)} \tag{20}$$

Threat Prioritization Analysis:

$$TP_{score} = \sum_i w_i \cdot \frac{T_{immediate,i}}{T_{future,i}} \tag{21}$$

where w_i represents threat weight and T represents resource allocation.

Detection Algorithm:

$$R_{2.5}(t) = \begin{cases} 1 & \text{if } DI > 1.5 \text{ and } TP_{score} > \tau_{tp} \\ 0 & \text{otherwise} \end{cases} \tag{22}$$

3.7 Indicator 2.6: Temporal Exhaustion Patterns

Definition: Systematic degradation of security vigilance during extended work periods.

Mathematical Model:

Vigilance decay function:

$$V(t) = V_0 \cdot e^{-\alpha t} + V_{min} \tag{23}$$

where V_0 is initial vigilance, α is decay rate, and V_{min} is minimum sustainable vigilance.

Circadian Modulation:

$$V_{circ}(t) = V(t) \cdot (1 + A \sin(\frac{2\pi(t - \phi)}{24} + \psi)) \tag{24}$$

where A is circadian amplitude, ϕ is phase shift, and ψ is individual chronotype.

Cumulative Fatigue Model:

$$F(t) = \int_0^t W(\tau) \cdot e^{-\lambda(t-\tau)} d\tau \tag{25}$$

where $W(\tau)$ is workload function and λ is recovery rate.

Detection Threshold:

$$D_{2.6}(t) = \frac{F(t)}{F_{threshold}} \cdot \left(1 - \frac{V_{circ}(t)}{V_0}\right) \tag{26}$$

3.8 Indicator 2.7: Time-of-Day Vulnerability Windows

Definition: Predictable periods of reduced security effectiveness based on circadian rhythms.

Mathematical Model:

Circadian performance function:

$$P_{circ}(h) = P_0 + A_1 \cos\left(\frac{2\pi(h - \phi_1)}{24}\right) + A_2 \cos\left(\frac{4\pi(h - \phi_2)}{24}\right) \tag{27}$$

where h is hour of day, P_0 is baseline performance, and A_1, A_2 are harmonic amplitudes.

Individual Chronotype Integration:

$$\phi_{individual} = \phi_{population} + \Delta\phi_{chronotype} + \Delta\phi_{age} \tag{28}$$

Vulnerability Window Detection:

$$VW(h) = \begin{cases} 1 & \text{if } P_{circ}(h) < P_0 - \sigma_{threshold} \\ 0 & \text{otherwise} \end{cases} \tag{29}$$

Aggregated Organizational Metric:

$$D_{2.7}(t) = \frac{\sum_{i=1}^{N} VW_i(hour(t))}{N} \cdot Incident\_Rate(hour(t)) \tag{30}$$

3.9 Indicator 2.8: Weekend/Holiday Security Lapses

Definition: Reduced security vigilance during non-business periods leading to exploitation windows.

Mathematical Model:

Weekend effect function:

$$WE(d) = \begin{cases} \beta_{weekend} & \text{if } d \in \{Saturday, Sunday\} \\ \beta_{holiday} & \text{if } d \in Holiday\_Set \\ 1.0 & \text{otherwise} \end{cases} \tag{31}$$

Staffing Impact Model:

$$S_{effective}(d, h) = S_{nominal} \cdot WE(d) \cdot Coverage(h) \tag{32}$$

Attack Success Probability:

$$P_{success}(d, h) = P_{baseline} \cdot \left(\frac{S_{nominal}}{S_{effective}(d, h)}\right)^{\gamma} \tag{33}$$

Detection Algorithm:

$$R_{2.8}(t) = \begin{cases} 1 & \text{if } WE(day(t)) < 0.7 \text{ and } Incident\_Count > \tau_{weekend} \\ 0 & \text{otherwise} \end{cases} \tag{34}$$

3.10 Indicator 2.9: Shift Change Exploitation Windows

Definition: Vulnerability periods during personnel transitions and handover processes.

Mathematical Model:

Shift transition vulnerability function:

$$STV(t) = \sum_i A_i \cdot e^{-\frac{(t - t_{shift,i})^2}{2\sigma^2_{transition}}} \tag{35}$$

where $t_{shift,i}$ represents shift change times and A_i represents transition severity.

Information Transfer Efficiency:

$$ITE(t) = \frac{Information_{received}(t)}{Information_{available}(t)} \cdot Quality\_Factor(t) \tag{36}$$

Coverage Gap Model:

$$CG(t) = \max(0, 1 - \frac{Staff_{effective}(t)}{Staff_{required}}) \tag{37}$$

Combined Detection:

$$D_{2.9}(t) = STV(t) \cdot (1 - ITE(t)) \cdot CG(t) \tag{38}$$

3.11 Indicator 2.10: Temporal Consistency Pressure

Definition: Pressure to maintain consistent response times leading to security shortcuts.

Mathematical Model:

Consistency pressure index:

$$CPI(t) = \frac{Var(Response\_Times)}{Mean(Response\_Times)^2} \cdot Penalty\_Factor \tag{39}$$

Shortcut Probability Model:

$$P_{shortcut}(CPI, deadline) = \sigma(\alpha \cdot CPI + \beta \cdot deadline\_pressure - \theta) \tag{40}$$

Quality Degradation Function:

$$QD(t) = Q_0 \cdot (1 - \gamma \cdot P_{shortcut}(t)) \tag{41}$$

where Q_0 is baseline quality and γ represents shortcut impact severity.

Detection Threshold:

$$R_{2.10}(t) = \begin{cases} 1 & \text{if } CPI(t) > \tau_{cpi} \text{ and } QD(t) < Q_{min} \\ 0 & \text{otherwise} \end{cases} \tag{42}$$

4 Interdependency Matrix

The temporal vulnerability indicators exhibit complex interdependencies captured through correlation matrix $\mathbf{R}_2$:

$$\mathbf{R}_2 = \begin{pmatrix} 1.00 & 0.75 & 0.60 & 0.45 & 0.50 & 0.65 & 0.55 & 0.40 & 0.35 & 0.70 \\ 0.75 & 1.00 & 0.55 & 0.40 & 0.35 & 0.80 & 0.50 & 0.30 & 0.25 & 0.65 \\ 0.60 & 0.55 & 1.00 & 0.70 & 0.75 & 0.45 & 0.35 & 0.40 & 0.30 & 0.50 \\ 0.45 & 0.40 & 0.70 & 1.00 & 0.85 & 0.30 & 0.25 & 0.35 & 0.20 & 0.40 \\ 0.50 & 0.35 & 0.75 & 0.85 & 1.00 & 0.40 & 0.30 & 0.45 & 0.25 & 0.35 \\ 0.65 & 0.80 & 0.45 & 0.30 & 0.40 & 1.00 & 0.75 & 0.60 & 0.55 & 0.50 \\ 0.55 & 0.50 & 0.35 & 0.25 & 0.30 & 0.75 & 1.00 & 0.85 & 0.70 & 0.40 \\ 0.40 & 0.30 & 0.40 & 0.35 & 0.45 & 0.60 & 0.85 & 1.00 & 0.65 & 0.30 \\ 0.35 & 0.25 & 0.30 & 0.20 & 0.25 & 0.55 & 0.70 & 0.65 & 1.00 & 0.45 \\ 0.70 & 0.65 & 0.50 & 0.40 & 0.35 & 0.50 & 0.40 & 0.30 & 0.45 & 1.00 \end{pmatrix} \tag{43}$$

Key interdependencies include:

- Strong correlation (0.85) between Present Bias (2.4) and Hyperbolic Discounting (2.5)
- High correlation (0.80) between Cognitive Degradation (2.2) and Exhaustion Patterns (2.6)
- Significant correlation (0.85) between Time-of-Day Windows (2.7) and Weekend Lapses (2.8)
- Moderate correlation (0.75) between Urgency Bypass (2.1) and Cognitive Degradation (2.2)

Cross-Category Dependencies: Critical relationships with Authority vulnerabilities (Category 1):

- $R_{1.5,2.1} = 0.70$: Fear-based compliance amplified by time pressure
- $R_{1.10,2.3} = 0.65$: Crisis escalation increases deadline-driven risk acceptance
- $R_{1.1,2.6} = 0.55$: Exhaustion increases unquestioning compliance

5 Implementation Algorithms

Algorithm 1 Temporal Vulnerability Assessment

```
Initialize temporal parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$
Load circadian profiles and organizational chronotypes
for each time step $t$ do
    Extract temporal context: $hour(t)$, $day(t)$, $workload(t)$
    Calculate circadian performance modifier $C_{circ}(t)$
    for each indicator $i \in \{2.1, 2.2, \ldots, 2.10\}$ do
        Compute temporal pressure $TP_i(t)$
        Calculate rule-based detection $R_i(t)$
        Compute anomaly score $A_i(t)$ with temporal weighting
        Evaluate Bayesian posterior $B_i(t)$
        Calculate detection score $D_i(t)$
        Apply temporal smoothing with momentum
        Update temporal state $S_i(t)$
    end for
    Compute interdependency corrections using $\mathbf{R}_2$
    Apply cross-category correlations with Category 1
    Generate temporal-aware alerts with time-to-vulnerability estimates
    Update circadian and fatigue models
    Log results for chronotype refinement
end for
```

6 Validation Framework

Temporal vulnerability validation requires specialized metrics accounting for time-dependent phenomena:

Temporal Classification Metrics:

$$Precision_t = \frac{\sum_i TP_i \cdot w_t(i)}{\sum_i (TP_i + FP_i) \cdot w_t(i)} \tag{44}$$

$$Recall_t = \frac{\sum_i TP_i \cdot w_t(i)}{\sum_i (TP_i + FN_i) \cdot w_t(i)} \tag{45}$$

where $w_t(i)$ provides temporal weighting based on detection timing.

Algorithm 2 Circadian Vulnerability Prediction

```
Input: Current time $t$, prediction horizon $h$
Initialize vulnerability forecast array $V_{forecast}[h]$
for each future time $t_f = t + \Delta t$ to $t + h$ do
    Calculate circadian performance $P_{circ}(t_f)$
    Estimate workload $W_{est}(t_f)$ from historical patterns
    Compute fatigue accumulation $F_{acc}(t_f)$
    Predict staff availability $Staff(t_f)$
    Calculate combined vulnerability $V(t_f)$
    Store in forecast array
end for
Identify peak vulnerability windows
Generate preemptive alerts for high-risk periods
Return vulnerability timeline with confidence intervals
```

Circadian Validation: Phase accuracy measurement:

$$\phi_{error} = \min(|\phi_{predicted} - \phi_{observed}|, 24 - |\phi_{predicted} - \phi_{observed}|) \tag{46}$$

Temporal Stability Analysis: Autocorrelation function for temporal consistency:

$$R(\tau) = \frac{E[(X_t - \mu)(X_{t+\tau} - \mu)]}{\sigma^2} \tag{47}$$

Predictive Accuracy: Mean Absolute Error for vulnerability timing:

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

Cross-Validation with Temporal Stratification: Ensuring training and test sets maintain temporal representativeness:

$$Stratification_{score} = \frac{\text{Var}(temporal\_distribution_{test})}{\text{Var}(temporal\_distribution_{total})} \tag{49}$$

Target stratification score approaches 1.0 for optimal temporal balance.

Chronotype Adaptation Validation: Measuring personalization effectiveness:

$$Adaptation_{gain} = \frac{Accuracy_{personalized} - Accuracy_{generic}}{Accuracy_{generic}} \tag{50}$$

7 Conclusion

This mathematical formalization of temporal vulnerabilities provides a rigorous foundation for understanding and detecting time-based security weaknesses. The integration of hyperbolic discounting, circadian modeling, and cognitive load theory creates a comprehensive framework for temporal vulnerability assessment.

The interdependency matrix reveals strong correlations between temporal indicators and significant cross-category effects with authority-based vulnerabilities. This demonstrates that temporal pressure acts as a force multiplier for other psychological vulnerabilities, emphasizing the critical importance of time-aware security strategies.

The implementation algorithms enable real-time temporal vulnerability monitoring with predictive capabilities. Organizations can anticipate vulnerability windows based on circadian patterns, workload forecasts, and fatigue accumulation models, enabling proactive rather than reactive security measures.

Future work will extend this temporal modeling approach to the remaining CPF categories, with particular attention to temporal amplification effects on cognitive overload (Category 5) and stress responses (Category 7). The mathematical rigor established here provides a foundation for evidence-based temporal security strategies that account for the predictable patterns of human temporal cognition.

The temporal vulnerability category demonstrates that security is not just about what people know, but when they apply that knowledge. By formalizing these temporal dynamics mathematically, we enable security systems that adapt to human temporal realities rather than expecting humans to maintain constant vigilance across all time periods.

References

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

[2] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-291.

[3] Sweller, J. (1988). Cognitive load during problem solving. *Cognitive Science*, 12(2), 257-285.

[4] Roenneberg, T., & Merrow, M. (2016). The circadian clock and human health. *Current Biology*, 26(10), R432-R443.

[5] Ainslie, G. (2001). *Breakdown of Will*. Cambridge University Press.

[6] Schmidt, C., Collette, F., Cajochen, C., & Peigneux, P. (2007). A time to think: Circadian rhythms in human cognition. *Cognitive Neuropsychology*, 24(7), 755-789.