Browser Hygiene Risk Assessment Model

Introduction

This mathematical model assesses the security risk level of a web browser based on various hygiene factors. It produces a risk score as a percentage, indicating how vulnerable a browser is to potential security threats.

Equation

$$R\% = \min\left(100, \frac{100\left(\frac{CLw_{10}}{3} + MEw_2 + MFw_4 + PAw_8 + PMw_5 + SBw_9 + TCw_6 + UPw_3 + \frac{100w_1 \sum_{i-1}^{n} CVSSEPSS}{MaxCVSSn} + \frac{w_7}{CC}\right)}{ME_{max}w_2 + MF_{max}w_4 + TC_{max}w_6 + 100w_1 + w_{10} + w_3 + w_5 + w_7 + w_8 + w_9}\right)$$

Weightage Coefficients

These are important factors assigned to each risk factor. They sum up to 1, representing the relative importance of each factor in the overall risk assessment.

W	Telemetry	Weightage Coefficient
w1	Deprecated Browser Versions	0.139650873
w2	Malicious Extensions	0.19201995
w3	Unsecure Protocol	0.039900249
w4	Malicious File Download	0.089775561
w5	Weak Password Management	0.089775561
w6	3rd party Cookies	0.144638404
w7	Cache management	0.064837905
w8	Pop-ups/ Adds	0.064837905
w9	Disabled safe browsing	0.099750623
w10	Camera/ Microphone/Location	0.074812968

Variables and Their Meanings (10 risk factors in total):

- RDB: Risk from Deprecated Browser versions
- RME: Risk from Malicious Extensions
- RMF: Risk from Malicious File downloads
- RCC: Risk from infrequent Cache Clearing
- RTC: Risk from Third-party Cookies

- RUP: Risk from Unsecure Protocols
- RPM: Risk from Poor Password Management
- RPA: Risk from allowing Pop-ups and Ads
- RCL: Risk from Camera/microphone/Location access
- RSB: Risk from disabled Safe Browsing

Explanation of Risk Factors

a) RDB (Deprecated Browser Risk):

Calculated as: $(\Sigma(CVSS_i * EPSS_i) / (n * MaxCVSS)) * 100\%$

$$RDB = \frac{100 \sum_{i=1}^{n} CVSSEPSS}{MaxCVSSn}$$

- CVSS: Common Vulnerability Scoring System
- EPSS: Exploit Prediction Scoring System
- n: Number of vulnerabilities
- MaxCVSS: Maximum possible CVSS score (typically 10)

b) RME (Malicious Extensions Risk): Direct count of detected malicious extensions

c) RMF (Malicious File Downloads Risk): Count of detected malicious file downloads

d) RCC (Cache Clearing Risk): Inverse of the frequency of cache clearing (in days)

e) RTC (Third-party Cookies Risk): Count of third-party cookies present

f) RUP, RPM, RPA, RSB: Binary values (0 or 1) indicating the presence or absence of the risk

g) RCL (Camera/Location Access Risk): Proportion of permissions granted (0 to 1)