Separating attacker skills from TTCs

Pontus Johnson

January 2025

Mathematical Model

Let

$A = \{\text{attackers}\}, \quad T = \{\text{attack steps}\}, \quad \mathcal{S} = \{s_1, s_2, \ldots, s_m\} \quad \text{(set of skill categories).}$

Each attacker $a \in A$ has a skill profile

$$\boldsymbol{\alpha}(a) = \big(\alpha_1(a), \alpha_2(a), \ldots, \alpha_m(a)\big) \in \mathbb{R}^m,$$

where $\alpha_i(a)$ is attacker a's proficiency in skill s_i.

For each attack step $t \in T$, define a function

$$g_t : \mathbb{R}^m \;\to\; \Theta,$$

where Θ is a set of parameters for a family of distributions (for example, the rate parameter of an exponential distribution). Then the time to compromise $X_{a,t}$, when attacker a carries out attack step t, follows the distribution

$$X_{a,t} \;\sim\; F\big(\,\cdot\;\big|\; g_t(\boldsymbol{\alpha}(a))\big),$$

where $F(\cdot \mid \theta)$ is the cumulative distribution function (CDF) parameterized by $\theta \in \Theta$.

Equivalently, if $F_{a,t}$ denotes the CDF of $X_{a,t}$, then

$$F_{a,t}(\tau) \;=\; \Pr\!\big(X_{a,t} \le \tau\big) \;=\; F\big(\tau \mid g_t(\boldsymbol{\alpha}(a))\big).$$

Example

Suppose we have two skills:

$$\mathcal{S} = \{\textit{binary\_exploitation},\; \textit{social\_engineering}\},$$

and we denote

$$\boldsymbol{\alpha}(a) = \big(\alpha_{\text{bin}}(a),\; \alpha_{\text{soc}}(a)\big).$$

Consider an attack step

$$t = \texttt{CVE-2020-1057.exploit\_vulnerability}.$$

We might assume that only the *binary_exploitation* proficiency influences this step. Concretely, define

$$g_t(\alpha_{\text{bin}}, \alpha_{\text{soc}}) \;=\; \theta_0 \;+\; \theta_1\, \alpha_{\text{bin}},$$

where θ_0 and θ_1 are constants, and α_{soc} does not appear.

If F is, for instance, an exponential distribution CDF with rate parameter λ, then

$$X_{a,t} \;\sim\; \text{Exponential}\Big(\lambda = \exp\big(g_t(\boldsymbol{\alpha}(a))\big)\Big).$$

Hence, higher $\alpha_{\text{bin}}(a)$ (i.e., higher *binary_exploitation* proficiency) reduces the expected time to compromise, while *social_engineering* proficiency is irrelevant for this particular step.