Appendix

Proof of Lemma 1

Lemma 1. $u \in \Gamma(\pi_x)$ if and only if $x_u a_u k_u L > c_u$.

Proof. First we show that $V^*(s) \geq 0 \quad (\forall s \in S)$:

\[ V^*(s) = \arg \max_{a \in A^s} Q(s, a) \geq Q(s, a = \text{stop}) = 0. \]

If direction: Consider state $s = \{u\}$, we have

\[ V^*(s) = (1 - x_u)(V^*(s) - c_u) + a_u x_u k_u (L - c_u) \]

\[ + x_u (1 - a_u k_u) (V^*(s) - c_u) \geq (1 - x_u)(V^*(s) - c_u) + a_u x_u k_u (L - c_u) \]

\[ + x_u (1 - a_u k_u) (0 - c_u). \]

If $x_u a_u k_u L > c_u$, then $V^*(s) > 0$, which means that $s$ is a reachable state and the optimal action at state $s$ is to attack user $u$ instead of stop attacking. Therefore, $u$ belongs to the potential attack set $\Gamma(\pi_x)$.

Only if direction: If we restrict the attacker’s policy so that he never attacks $u$, then $s$ and $s^{-u}$ are indifferent so that $V^*(s) = V^*(s^{-u})$.

Without the restriction, we have $V^*(s) \geq V^*(s^{-u})$. In other words, adding a user to a state does not decrease its value. We prove that if $\pi_x(s) = u$, then $x_u > \frac{c_u}{a_u k_u}$. By definition we have:

\[ V^*(s) = (1 - x_u)(V^*(s) - c_u) + a_u x_u k_u (L - c_u) \]

\[ + x_u (1 - a_u k_u) (V^*(s) - c_u) \leq 0. \]

By adjusting the terms we have:

\[ V^*(s) = -\frac{c_u}{a_u x_u} + L k_u + (1 - k_u) V^*(s^{-u}). \]

Since $V^*(s) \geq V^*(s^{-u})$, then:

\[ -\frac{c_u}{a_u x_u} + L k_u \geq k_u V^*(s^{-u}) \geq 0 \]

Note that if $-\frac{c_u}{a_u x_u} + L k_u = 0$, we have $V^*(s) = V^*(s^{-u}) = 0$ and $s = \{u\}$. Due to the setting that the attacker always prefers stopping attack rather than launching another attack, we have $\pi_x(s) = u$, which contradicts the assumption that $\pi_x(s) = u$. Therefore, $-\frac{c_u}{a_u x_u} + L k_u > 0$, equivalently, $x_u > \frac{c_u}{a_u k_u}$.

Proof of Lemma 2

Lemma 2.

\[ \theta(x, \pi_x) = \begin{cases} 1 - \prod_{u \in \Gamma(\pi_x)} (1 - a_u k_u), & \text{if } \Gamma(\pi_x) \neq \emptyset \text{ and } \Gamma(\pi_x) = \emptyset. \end{cases} \]

Proof. If $\Gamma(\pi_x) = \emptyset$, meaning that the attacker stops attacking at the initial state $s_0$, therefore the probability that the credential accessed is 0. Otherwise, we write the reachable states set as $\Delta(\pi_x) = \{s_0, s_1, \ldots, s_r\} \cup \{s^n, s^\nu\}$. We denote by $M_{\Delta(\pi_x)}$ the transition probability matrix, whose entry $M_{ij}$ represents the probability that state $s_i$ transitions to $s_j$ under policy $\pi_x$.

If case (1), $s_r$ could transition to itself, $s^n$ or $s^\nu$. Hence $M_{\Delta(\pi_x)}$ has the form like (denote $d_i = a_u k_u$, and $x_i = x_u$):

\[
\begin{bmatrix}
1 - x_0 (1 - d_0) & 0 & \cdots & 0 \\
1 - x_1 (1 - d_1) & d_1 x_1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
1 - x_r (1 - d_r) & d_r x_r & \cdots & 1
\end{bmatrix}
\]

Precisely, $M_{\Delta(\pi_x)}$ can be represented as:

\[ M_{\Delta(\pi_x)} = \begin{bmatrix} A & B \\ 0 & I_2 \end{bmatrix} \]

where $A$ is $r+1$ dimensional square matrix, $I_2$ is $2$ dimensional unit diagonal matrix and $B$ is $(r+1) \times 2$ matrix. We introduce a $(r+1) \times 2$ matrix $E$:

\[ E = F B, \quad \text{where } F = (I_{r+1} - A)^{-1} \]

Note that $s^n$ and $s^\nu$ are absorbing states. According to the properties of absorbing Markov chain, $s_0$ will eventually end in state $s^n$ or $s^\nu$ with probability $E_{11}$ and $E_{12}$ respectively, and $E_{11} + E_{12} = 1$. Therefore, the probability of losing the credential is equal to the probability that the attacker eventually ends in state $s^\nu$, i.e., $\theta(x, \pi_x) = E_{12}$. We can directly calculate $E_{11}$ based on the rules of matrix calculation:

\[
E_{11} = \sum_{i=1}^{r+1} F_i B_{i1} = F_{1, r+1} B_{r+1, 1} = \prod_{i=0}^{r-1} \frac{1 - d_i}{x_r (1 - d_r)} = \prod_{i=0}^{r} (1 - d_i) = \prod_{u \in \Gamma(\pi_x)} (1 - a_u k_u)
\]

Then $E_{12} = 1 - E_{11} = 1 - \prod_{u \in \Gamma(\pi_x)} (1 - a_u k_u)$.

If case (2), $s_r$ transitions to $s^n$ with probability 1. Thus $M_{\Delta(\pi_x)}$ has the form like ($d_i = a_u k_u$, and $x_i = x_u$):
Then, we still have
\[
E_k = \begin{bmatrix}
1 - x_0(1 - d_0) & x_0k_0 \\
1 - x_1(1 - d_1) & x_1k_1 \\
\vdots & \vdots \\
1 - x_{r-1}(1 - d_{r-1}) & x_{r-1}d_{r-1} \\
1 & 1
\end{bmatrix}
\]

Based on the result of Lemma 1, \( \Gamma(\pi) \) is constant for any \( x_u \in [0, \frac{c_u}{L\alpha_u k_u}] \) since the potential attack set \( \Gamma(\pi_x) \) remains the same when \( x_u \) varies among \( [0, \frac{c_u}{L\alpha_u k_u}] \). Therefore, any point in \( \arg \min_{x_u \in [0, \frac{c_u}{L\alpha_u k_u}]} \Lambda_u \) maximizes \( P_d(x, \pi_x) \). Similarly, \( \theta(x, \pi_x) \) is constant for any \( x_u \in \left( \frac{c_u}{L\alpha_u k_u}, 1 \right] \). Therefore, any points in \( \arg \min_{x_u \in \left( \frac{c_u}{L\alpha_u k_u}, 1 \right]} \Lambda_u \) maximizes \( P_d(x, \pi_x) \).}

\[
E_{11} = \sum_{i=1}^{r+1} F_{1i}B_{11}
= F_1 x_{r+1}
= \prod_{i=0}^{r-1} (1 - d_i)
= \prod_{u \in \Gamma(\pi_x)} (1 - a_u k_u)
\]

Then, we still have \( E_{12} = 1 - E_{11} = 1 - \prod_{u \in \Gamma(\pi_x)} (1 - a_u k_u) \).

**Proof of Theorem 1**

**Theorem 1.** The defender’s expected utility remains the same no matter how the attacker breaks ties, i.e., choosing any optimal policy.

**Proof.** Recall that in single-credential case the defender’s utility function is
\[ P_d(x, \pi_x) = -\rho^T \theta(x, \pi_x) L - \sum_{u \in U} \Lambda_u(x_u). \]

Based on the result of Lemma 1, \( \Gamma(\pi_x) \) can be represented as \( \{ u \in U | x_u > \frac{c_u}{L\alpha_u k_u} \} \), then \( \theta(x, \pi_x) \) can be represented as
\[ \theta(x, \pi_x) = 1 - \prod_{u \in \{ u \in U | x_u > \frac{c_u}{L\alpha_u k_u} \}} (1 - k_u). \]

For any other optimal policy \( \pi_x' \), we have
\[ \theta(x, \pi_x') = 1 - \prod_{u \in \{ u \in U | x_u > \frac{c_u}{L\alpha_u k_u} \}} (1 - k_u). \]

Note that \( \theta(x, \pi_x) = \theta(x, \pi_x)' \), which indicates that the defender’s expected utility will be the same when the attacker chooses any other optimal policy.