Exercises - Password metrics

COMP 6224 Foundations of Cyber Security

8th December 2016

Dr Mu Yang

Outline of the tasks

- NIST suggested entropy
- Shannon entropy, Hartley entropy and Min-entropy
- Guesswork, success-rate, work-factor, α-guesswork

Task 1: NIST suggested entropy (5 mins)

- Please estimate the entropy of the following password using the NIST approach.

  FcnXmCyB9h

Task 1: NIST suggested entropy (5 mins)

- Please estimate the entropy of the following password using the NIST approach.

  FcnXmCyB9h

- Solution: 4+2*7+1.5*2+6=27

Task 2: Shannon entropy (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the Shannon entropy $H_1(\mathcal{Z})$

Task 2: Shannon entropy (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the Shannon entropy $H_1(\mathcal{Z})$

- Solution:

$$H_1(\mathcal{Z}) = \sum_{i=1}^{9} -p_i \lg p_i = 2.94$$

Task 3: Min-entropy (5 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the Min-entropy H_∞

Task 3: Min-entropy (5 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the Min-entropy H_∞

- Solution:

$$H_\infty = -\lg p_1 = 2$$

Task 4: Hartley entropy (5 mins)

- An attacker has probabilities of success in guessing password. We assume a uniform distribution $\mathcal{Z}$ with probabilities 1/9.
- Please compute the Hartley entropy H_0

Task 4: Hartley entropy (5 mins)

- An attacker has probabilities of success in guessing password. We assume a uniform distribution $\mathcal{Z}$ with probabilities 1/9.

- Please compute the Hartley entropy H_0

- Solution:

$$H_0 = lg9 = 3.17$$

Task 5: Guesswork (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the guesswork $G_1(\mathcal{Z})$

Task 5: Guesswork (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute the guesswork $G_1(\mathcal{Z})$

- Solution:

$$G_1(\mathcal{Z}) = \sum_{i=1}^{9} p_i \cdot i = 3.65$$

Task 6: $\beta\text{-}success\text{-}rate$ (7 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute $\beta\text{-}success\text{-}rate$ where beta is 4: $\lambda_{\beta}(\mathcal{Z})$

Task 6: $\beta\text{-}success\text{-}rate$ (7 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\tfrac{1}{4}, \tfrac{1}{5}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{20}, \tfrac{1}{20}, \tfrac{1}{20}\}$$

- Please compute $\beta\text{-}success\text{-}rate$ where beta is 4: $\lambda_\beta(\mathcal{Z})$

- Solution:

$$\lambda_4(\mathcal{Z}) = \sum_{i=1}^{4} p_i = \frac{13}{20}$$

Task 7: α-work-factor (7 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute α-work-factor where alpha is 0.7: $\mu_\alpha(\mathcal{Z})$

Task 7: α-work-factor (7 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\tfrac{1}{4}, \tfrac{1}{5}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{20}, \tfrac{1}{20}, \tfrac{1}{20}\}$$

- Please compute α-work-factor where alpha is 0.7: $\mu_\alpha(\mathcal{Z})$

- Solution:

$$\mu_{0.7}(\mathcal{Z}) = \min\{j \mid \sum_{i=1}^{j} p_i \geq 0.7\} = 5$$

Task 8: α-guesswork (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute α-guesswork where alpha is 0.7: $G_\alpha(\mathcal{Z})$

Task 8: α-guesswork (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}\}$$

- Please compute α-guesswork where alpha is 0.7: $G_\alpha(\mathcal{Z})$

- S

If I have 100 accounts to crack, what is the average number of tries to crack 70% of the accounts.

$$= (1 - \frac{1}{20}) \cdot 3 + (\frac{1}{4} \cdot 1 + \frac{1}{5} \cdot 2 + \cdots + \frac{1}{10} \cdot 3)$$

$$= 3.1$$

Task 8: α-guesswork (10 mins)

- An attacker has probabilities of success in guessing password. We assume a toy distribution $\mathcal{Z}$ with probabilities

$$P_{\mathcal{Z}} = \{\tfrac{1}{4}, \tfrac{1}{5}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{10}, \tfrac{1}{20}, \tfrac{1}{20}, \tfrac{1}{20}\}$$

- Please compute α-guesswork where alpha is 0.7: $G_\alpha(\mathcal{Z})$

- Solution:

$$\begin{aligned} G_{0.7}(\mathcal{Z}) &= (1 - \lambda_{\mu_\alpha}) \cdot \mu_\alpha + \textstyle\sum_{i=1}^{\mu_\alpha} p_i \cdot i \\ &= (1 - \tfrac{15}{20}) \cdot 5 + (\tfrac{1}{4} \cdot 1 + \tfrac{1}{5} \cdot 2 + \cdots + \tfrac{1}{10} \cdot 5) \\ &= 3.1 \end{aligned}$$