Discussion of “Merchants of Vulnerabilities: Bug Bounty Programs and Their Impact on Software”

Daniil Larionov

ZEW Mannheim

June 27, 2024

Comments

Winner-take-all contest with different types of agents

- Agent types: eWHHs, neWHHs, BHHs
  - look for bugs in software;
- Principal: software firm
  - designs a bug bounty program.

Comments

Winner-take-all contest with different types of agents

- Agent types: eWHHs, neWHHs, BHHs
  - look for bugs in software;
- Principal: software firm
  - designs a bug bounty program.

Optimal design of (some aspects of) the contest

- The optimal number of WHHs (> 0, increases in $\#$BHHs)
  $\Rightarrow$ Profitable for firms to have a bug bounty program.
- Bug bounty programs $\Rightarrow$ software is released earlier (with more bugs).

Comments

Winner-take-all contest with different types of agents

- Agent types: eWHHs, neWHHs, BHHs
  - look for bugs in software;
- Principal: software firm
  - designs a bug bounty program.

Optimal design of (some aspects of) the contest

- The optimal number of WHHs (> 0, increases in $\#$BHHs)
  $\Rightarrow$ Profitable for firms to have a bug bounty program.
- Bug bounty programs $\Rightarrow$ software is released earlier (with more bugs).

Other aspects of the contest (e.g. general prize rules)?

Comments

Winner-take-all contest with different types of agents

- Agent types: eWHHs, neWHHs, BHHs
  - look for bugs in software;
- Principal: software firm
  - designs a bug bounty program.

Optimal design of (some aspects of) the contest

- The optimal number of WHHs (> 0, increases in #BHHs)
  $\Rightarrow$ Profitable for firms to have a bug bounty program.
- Bug bounty programs $\Rightarrow$ software is released earlier (with more bugs).

Other aspects of the contest (e.g. general prize rules)?

Literature on contests: Tullock (1980), . . . , Drugov et al. (2024).

Questions on the modeling approach

Where do the "winning" probabilities come from?

- eWHH i finds an SVV first (against $n-1$ eWHHs and m BHHs)

$$\text{with prob. } \mathbb{P}^s_{ie} = \frac{1}{n+m} + \frac{1}{n+m}\left(\alpha_{is} - \underbrace{\frac{(n-1)\alpha^*_s + m\mu^*_s}{(n-1)+m}}_{\text{Mean effort of others}}\right).$$

- What is the underlying distribution of individual success over time?

Questions on the modeling approach

Where do the "winning" probabilities come from?

- eWHH i finds an SVV first (against $n-1$ eWHHs and m BHHs)

$$\text{with prob. } \mathbb{P}^{s}_{ie} = \frac{1}{n+m} + \frac{1}{n+m}\left(\alpha_{is} - \underbrace{\frac{(n-1)\alpha^{*}_{s} + m\mu^{*}_{s}}{(n-1)+m}}_{\text{Mean effort of others}}\right).$$

- What is the underlying distribution of individual success over time?

How should the "winning" probabilities be interpreted?

- Let $\alpha^{*}_{s} = \mu^{*}_{s} \approx 0$ and $\alpha_{is} \approx 1 \Rightarrow \mathbb{P}^{s}_{ie} \approx \frac{2}{n+m} < 1.$
- Let $\alpha^{*}_{s} = \mu^{*}_{s} \approx 0$ and $\alpha_{is} \approx 0 \Rightarrow \mathbb{P}^{s}_{ie} \approx \frac{1}{n+m} > 0.$

Questions on the modeling approach

Where do the "winning" probabilities come from?

- eWHH i finds an SVV first (against $n-1$ eWHHs and m BHHs)

$$\text{with prob. } \mathbb{P}^s_{ie} = \frac{1}{n+m} + \frac{1}{n+m}\left(\alpha_{is} - \underbrace{\frac{(n-1)\alpha^*_s + m\mu^*_s}{(n-1)+m}}_{\text{Mean effort of others}}\right).$$

- What is the underlying distribution of individual success over time?

How should the "winning" probabilities be interpreted?

- Let $\alpha^*_s = \mu^*_s \approx 0$ and $\alpha_{is} \approx 1 \Rightarrow \mathbb{P}^s_{ie} \approx \frac{2}{n+m} < 1$.
- Let $\alpha^*_s = \mu^*_s \approx 0$ and $\alpha_{is} \approx 0 \Rightarrow \mathbb{P}^s_{ie} \approx \frac{1}{n+m} > 0$.

Isn't it important when the bug is found?

- Intoduce discounting?
- Impossible without explicit probabilistic model.

A more explicit model?

Suppose bug discovery times are exponentially distributed:

- For eWHH i, we have $T_i^{\text{eWHH}} \sim F(t; \alpha_i) = 1 - \exp(-\alpha_i t)$.
- For BHH j, we have $T_j^{\text{BHH}} \sim F(t; \mu_j) = 1 - \exp(-\mu_j t)$.

A more explicit model?

Suppose bug discovery times are exponentially distributed:

- For eWHH i, we have $T_i^{\text{eWHH}} \sim F(t;\alpha_i) = 1 - \exp(-\alpha_i t)$.
- For BHH j, we have $T_j^{\text{BHH}} \sim F(t;\mu_j) = 1 - \exp(-\mu_j t)$.

The winning probability of eWHH 1 is then given by:

$$\mathbb{P}\Big[\underbrace{T_1^{\text{eWHH}} \le T_2^{\text{eWHH}}, \dots, T_1^{\text{eWHH}} \le T_n^{\text{eWHH}}}_{n-1 \text{ remaining eWHHs}}; \underbrace{T_1^{\text{eWHH}} \le T_1^{\text{BHH}}, \dots, T_1^{\text{eWHH}} \le T_m^{\text{BHH}}}_{m \text{ BHHs}}\Big]$$

$$= \int_0^{+\infty} \mathbb{P}\Big[t \le T_2^{\text{eWHH}}, \dots, t \le T_n^{\text{eWHH}}; t \le T_1^{\text{BHH}}, \dots, t \le T_m^{\text{BHH}}\Big] \alpha_1 \exp\big(-\alpha_1 t\big)\, dt$$

$$= \int_0^{+\infty} \prod_{i=2}^{n} \mathbb{P}\big[t \le T_i^{\text{eWHH}}\big] \prod_{j=1}^{m} \mathbb{P}\big[t \le T_j^{\text{BHH}}\big] \alpha_1 \exp\big(-\alpha_1 t\big)\, dt$$

$$= \int_0^{+\infty} \big[\exp(-\alpha^* t)\big]^{n-1} \big[\exp(-\mu^* t)\big]^{m} \alpha_1 \exp\big(-\alpha_1 t\big)\, dt = \frac{\alpha_1}{\alpha_1 + (n-1)\alpha^* + m\mu^*}.$$