Equitable Security: Optimizing Distribution of Nudges and Resources

Elissa M. Redmiles, John P. Dickerson, Krishna Gummadi and Michelle L. Mazurek
eredmiles@cs.umd.edu

Presented by Dhruv Kuchhal

How can firms optimize the tradeoff between security nudges and levels of risk and investment for end-users, keeping fairness in mind?

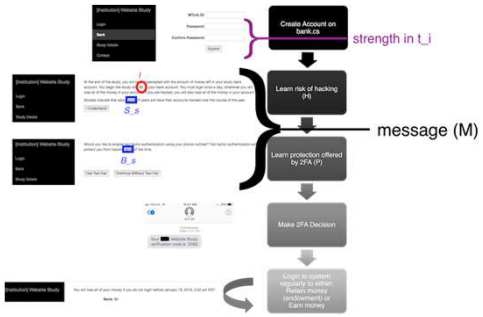
Motivation & Method

We ran **behavioral economics games on AMT** and were able to model user security decisions with high accuracy (R^2=0.61).

Users make **boundedly rational cost benefit optimized security decisions** [1]. Yet, sometimes security nudges encourage users toward irrational behavior.

Users have a limited compliance budget. We present a **mechanism design** to mathematically select values of different system features, maximizing utility for both users and online services.

Behavioral Economics Experimental System



Cost is defined as wage-earning time loss

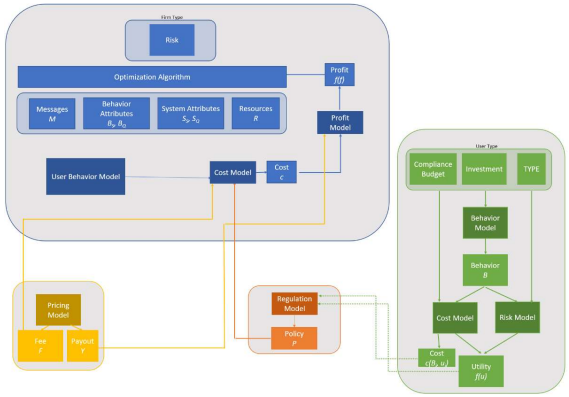
$$C_{2fa} = (T_{signup} + \sum T_{login}) * wage_{mturk}$$

Utility of 2FA is defined the $$$ savings if a hack occurred

$$U_{2fa} = P[(H) * Max_{bank}]$$

Rational behavior achieved when choice utility > cost

Mechanism Design



Firm wants to select optimal values for it's parameters in order to maximize profit. Firm can invest money to improve (up to some limits of engineering):

- B_s: security of the protective behaviors (e.g., app based 2FA vs. SMS)
- B_q: quality of behaviors (speed/ease of 2FA)
- S_s: overall security of any account
- S_q: overall quality of accounts (speed/ease of login)

They can also offer, on a per user basis:

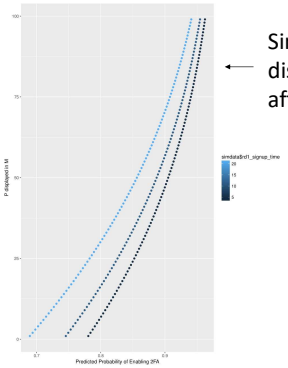
- *M*: messages that might reveal B_s, B_q, S_s, or S_q or are otherwise customized
- *R*: resources to reduce user costs e.g., ubikeys

Firm's Utility function: $f^s(B_i, u_i)_{i=1\ldots n} = \sum_{i=1}^{n} g(B_i, u_i) - c(B_i, u_i)$ $\quad f^s : (B, U)^n = \mathbb{R}$

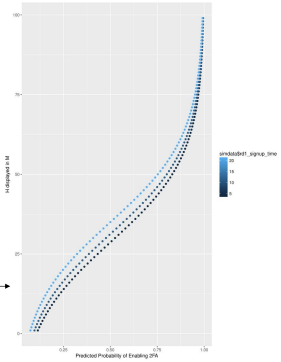
User's Utility function: $f^u : (TYPE, B, R) = g(B_i, t_i, R_i) - c(B_i, t_i, R_i)$ where u_i has some $t_i \in TYPE$

User behavior Adjustment: $if(\sum_{d=0}^{e} budget) < \sum_{t=0}^{e} cost(B_i, U_i) : m_i \times t_i \times r_i$

where *budget* is the users' overall "compliance budget" across digital accounts (see Beautment et al. 2009)

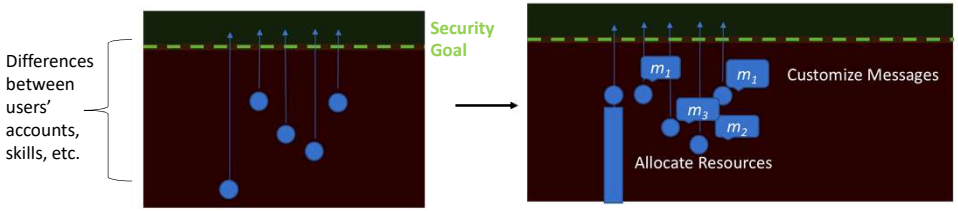


Simulation - varying the B_s value displayed to participants in m would affect their probability of enabling 2FA.



Simulation - varying the S_s value displayed to participants in m would affect their probability of enabling 2FA.

Firm solves for optimal values of B_s, B_q, S_s, S_q, and m_i, r_i for some user u_i **for *max(profit)***



Future work: impose fairness constraints, simulate impact on profit & overall user security

- **Risk fairness**: all people in the system should have as equal as possible risk of a negative outcome.
- **Effort fairness**: assignment of resources / messages to minimize user variance in cost (effort).

References

[1] Elissa M Redmiles, Michelle L Mazurek, and John P Dickerson. **Dancing Pigs or Externalities?: Measuring the Rationality of Security Decisions**. ACM EC2018.