NARA INSTITUTE OF SCIENCE AND TECHNOLOGY
- Outgrow your limits -

IARIA

Cost-benefit Analysis Toward Designing Efficient Education Programs for Household Security

N’guessan Yves-Roland Douha[1], Bernard Ousmane Sane[2], Masahiro Sasabe[1], Doudou Fall[1], Yuzo Taenaka[1], Youki Kadobayashi[1]

[1]Division of Information Science, Nara Institute of Science and Technology (Japan)

[2]Faculty of Science and Technology, University Cheikh Anta Diop (Sénégal)

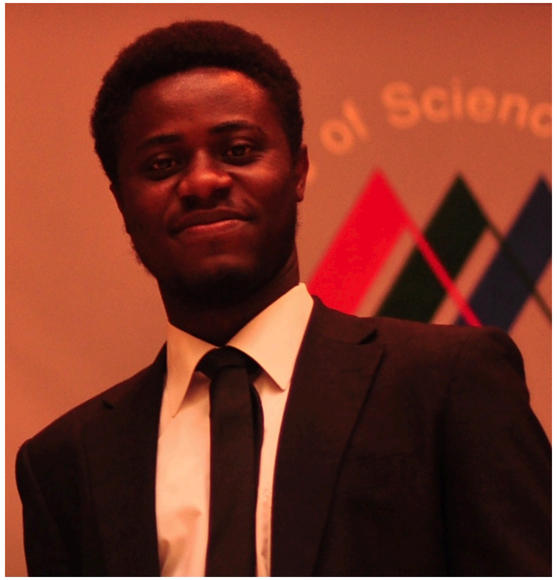
Presenter’s email address: douha.nguessan_yves-roland.dn6@is.naist.jp

iplab
Laboratory for
Cyber Resilience

__N’guessan Yves-Roland Douha__ received the Master’s degree of Engineering - MEng, Information Science and Engineering at Nara Institute of Science and Technology (NAIST), Japan, in 2020.

He is currently a doctoral student majoring in cybersecurity at the Division of Information Science, NAIST.

His research interests include risk management, machine learning, anomaly detection, game theory, and smart-home security.



INTRODUCTION

❑ Human is often known as the weakest link in the security chain.

❑ People are getting interested in the Internet of Things (IoT) applications such as smart homes.

❑ Worldwide revenue of smart homes :

- US$78.9 billion (2020) and US$182.3 billion (2025) [1]

❑ Smart homes use many technologies (e.g., the internet of things) to improve the quality of life of people at home.

❑ However, this smart environment faces many security challenges such as insecure software/firmware, and poor physical security.

❑ Furthermore, home users (e.g., children) are not necessarily aware of network security management and cyber threats such as phishing attacks.

INTRODUCTION

❑ Cybersecurity awareness education could be an effective solution to empower households, including children and senior citizens, with knowledge and skills to reduce the success rate of cyberattacks exploiting human vulnerabilities in homes.

❑ However, a serious obstacle to adopting those cybersecurity education programs is the financial costs and resources [2].

- Companies seek to minimize their budget regarding costs that are not tight to their operations.
- Individuals are willing to take cybersecurity awareness training only if their employers sponsor them [3].

INTRODUCTION

❑ Problem

- How can we encourage households to engage in cybersecurity awareness education considering financial challenges?

❑ Proposed solution

- Cost-benefit analysis
  - ✓ Help to figure out whether the benefits outweigh the cost
  - ✓ Remove any emotional element and help to overcome biases
  - ✓ Help to make a rational decision.

RELATED WORK

❑ *Z. Zuo, Y. Fang, L. Liu, F. Fang, and X. Hu [4]* used a game-theoretic approach to analyze information security cost investment to improve network security

❑ *Z. J. Zhang, W. He, W. Li, and M. Abdous [5]* introduced a new theoretical framework for conducting a cost-benefit analysis of cybersecurity awareness training programs to evaluate different costs and benefits on a company's optimal degree of security

❑ Limitations: Prior research have not studied households' perspectives regarding the cost-benefit of cybersecurity awareness training.

METHOD AND CONTRIBUTIONS

❑ Method

- Use a game-theoretic approach to analyze the cybersecurity awareness cost-benefit for households and smart-home security.

❑ Contributions

- Providing a decision-support system for households to understand the cost effectiveness of investing in cybersecurity awareness education.
- Identifying pure and mixed Nash equilibria to discover households' and attackers' payoffs following a cyberattack.
- Analyzing the proposed game through numerical results.

PROPOSED GAME MODEL

- ❑ Our smart home comprises three types of households: adults (User1), children (User2), and senior citizens (User3).
- ❑ This house is composed of many IoT devices that are convenient for every household.
  - User 1 uses IP cameras and smart door locks to ensure the house's physical security.
  - User 2 uses a smart TV and smart speakers for advertisement.
  - User 3 could use a smart pill dispenser or smartwatch for healthcare.
  - An attacker would like to deceive User1, User2, or User3.

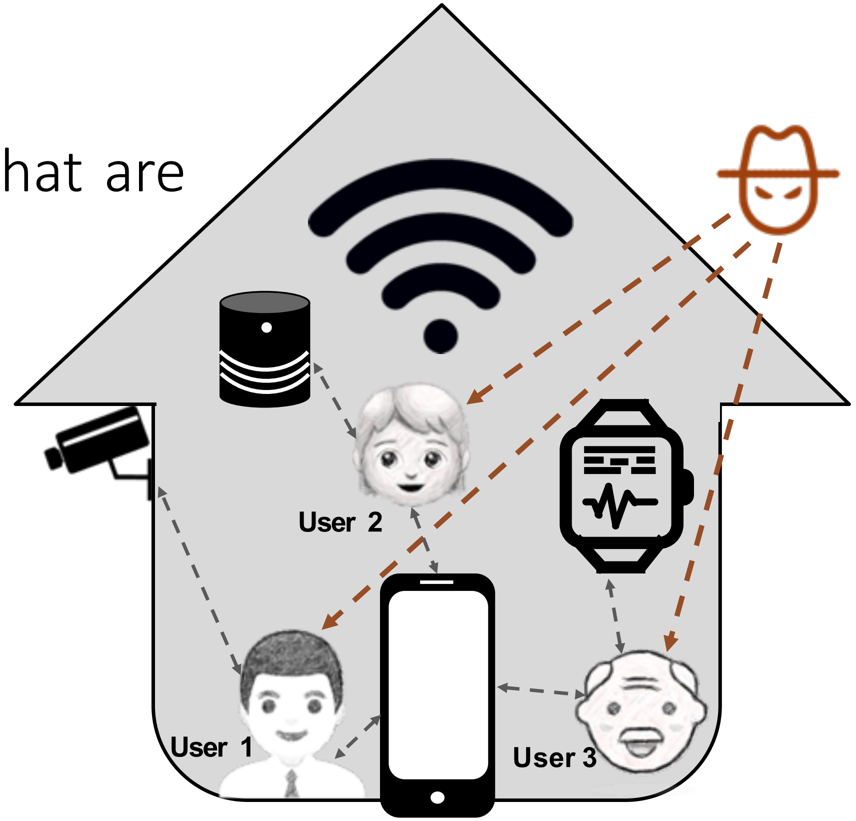


Figure 1 Illustration of the proposed model.

NORMAL-FORM GAME

- Let T_i and $\bar{T}_i$ respectively, be the events *User i* has got cybersecurity awareness training and *User i* has not got cybersecurity awareness training with $1 \leq i \leq 3$.

- Moreover, we consider the following *User i*'s costs: c_{mi} the monetary costs related to the event *T*, c_{ti} the time costs related to the event S, and $c_{t'i}$ the time costs related to the event $\bar{S}$.

- We consider

$$0 \leq c_{m1} \leq c_{m2} \leq c_{m3} \qquad (1)$$

$$0 \leq c_{t1} \leq c_{t2} \leq c_{t3} \qquad (2)$$

$$0 \leq c_{t' I} < c_{ti} \qquad (3)$$

TABLE I: PART OF THE NORMAL FORM GAME WHEN AN ATTACKER TARGETS USER 1 (“Adult”)

Attacker targets “Adult”			Senior citizen (User 3)		
			T		
			S		
			Child (User 2)		
			T		$\overline{T}$
			S	$\overline{S}$	
Adult (User 1)	T	S	$\phi - c_{m1} - c_{t1} + R$; $\phi - c_{m2} - c_{t2} + R$; $\phi - c_{m3} - c_{t3} + R$; 0	$\phi - c_{m1} - c_{t1} + R$; $\phi - c_{m2} - c_{t'2}$; $\phi - c_{m3} - c_{t3} + R$; 0	$\phi - c_{m1} - c_{t1} + R$; ϕ; $\phi - c_{m3} - c_{t3} + R$; 0
		$\overline{S}$	$\phi - c_{m1} - c_{t'1} - \theta P(A/T_1 \cap \overline{S}) - \delta - \lambda$; $\phi - c_{m2} - c_{t2} + R - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/T_1 \cap \overline{S}) + \delta + \lambda$;	$\phi - c_{m1} - c_{t'1} - \theta P(A/T_1 \cap \overline{S}) - \delta - \lambda$; $\phi - c_{m2} - c_{t'2} - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/T_1 \cap \overline{S}) + \delta + \lambda$;	$\phi - c_{m1} - c_{t'1} - \theta P(A/T_1 \cap \overline{S}) - \delta - \lambda$; $\phi - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/T_1 \cap \overline{S}) + \delta + \lambda$;
	$\overline{T}$		$\phi - \theta P(A/\overline{T_1}) - \delta - \lambda$; $\phi - c_{m2} - c_{t2} + R - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/\overline{T_1}) + \delta + \lambda$;	$\phi - \theta P(A/\overline{T_1}) - \delta - \lambda$; $\phi - c_{m2} - c_{t'2} - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/\overline{T_1}) + \delta + \lambda$;	$\phi - \theta P(A/\overline{T_1}) - \delta - \lambda$; $\phi - \delta$; $\phi - c_{m3} - c_{t3} + R - \delta$; $\theta P(A/\overline{T_1}) + \delta + \lambda$;

GAME ANALYSIS

❑ Pure Strategy Nash Equilibrium

- It refers to a game in which every player’s mixed strategy in a mixed strategy Nash equilibrium assigns probability 1 to a single action [6]. In pure strategy Nash equilibrium, a player plays his or her best strategy; the rational player would never change his or her strategy to get a lower payoff than that of the best strategy.

- Theorem 1. When every user observes every security measure learned, the proposed game admits a pure strategic Nash equilibrium related to the strategic profile (S, S, S, A).

Proof. The proposed game generates nine strategic profiles when users choose the same actions and 72 otherwise. We studied every strategic profile.

GAME ANALYSIS

❑ Pure Strategy Nash Equilibrium (Proof)

- Strategic profiles (Type 1): Users play the same actions.

✓ Case 1.1: Every user has not got cybersecurity awareness training.

$U_{att\ (User\ i)}(\bar{T}, \bar{T}, \bar{T}, A) = \theta P(A/\bar{T}_i) + \delta + \lambda$

From Equation (2), there is equality between the attacker's payoffs. The attacker cannot increase his or her payoff. However, *User i* can increase his or her payoff from $\phi - \theta P(A/\bar{T}_i) - \delta - \lambda$ to $\phi - c_{mi} - c_{ti} + R$ by choosing to play (S) instead of ($\bar{T}$). Therefore, the strategic profile ($\bar{T}$, $\bar{T}$, $\bar{T}$, A) is not a pure strategy Nash equilibrium.

✓ Case 1.2: Every user notices part of security countermeasures.

$U_{att(User\ i)}(\bar{S}, \bar{S}, \bar{S}, A) = \theta P(A/T_i \cap \bar{S}) + \delta + \lambda$

From Equation (5), there is equality between the attacker's payoffs. The attacker cannot increase his or her payoff. However, User i can increase his or her payoff from $\phi - c_{mi} - c_{t'i} - \theta P(A/T_i \cap \bar{S}) - \delta - \lambda$ to $\phi - c_{mi} - c_{ti} + R$ by choosing to play (S) instead of ($\bar{S}$). Therefore, the strategic profile ($\bar{S}$, $\bar{S}$, $\bar{S}$, A) is not a pure strategy Nash equilibrium.

✓ Case 1.3: Every user notices security countermeasures.

$U_{att(User\ i)}(S, S, S, A) = 0$

The attacker gets the same payoff whoever his or her target is. Furthermore, users get the maximum payoff (i.e., $\phi - c_{mi} - c_{ti} + R$) when they play S. Therefore, the strategic profile (S, S, S, A) is a pure strategy Nash equilibrium.

GAME ANALYSIS

❑ Pure Strategy Nash Equilibrium (Proof)

- Strategic profiles (Type 2): Every user does not play the same action.

✓ Case 2.1: One or two users notices security countermeasures.

The attacker’s payoff is zero when targeting a user who notices security countermeasures. The attacker can increase his or her payoff by targeting a user who notices part of security countermeasures. Therefore, the related strategic profiles, such as (S, $\bar{S}$, $\bar{T}$, A), (S, S, $\bar{T}$, A), and (S, S, $\bar{S}$, A), are not pure strategy Nash equilibria.

✓ Case 2.2: One or two users notices part of security countermeasures and the other user(s) has (have) not got cybersecurity awareness training.

The attacker’s payoff is $\theta P(A/T_i \cap \bar{S})+\delta+\lambda$ or $\theta P(A/\bar{T}_i)+\delta+\lambda$. From Inequality (5), $P(A/T_i \cap \bar{S}) < P(A/\bar{T}_i)$; then the attacker can increase his or her payoff by targeting a user who has not got cybersecurity awareness training. Therefore, the related strategic profiles, such as (S, $\bar{T}$, $\bar{T}$, A), (T , $\bar{T}$, $\bar{S}$, A), and (S, $\bar{S}$, $\bar{T}$, A), are not pure strategy Nash equilibria.

GAME ANALYSIS

❑ Mixed Strategy Nash Equilibrium

- It refers to a game in which every player plays a mixed strategy (i.e., a probability distribution over the pure strategies) and cannot improve his or her payoff under the mixed-strategy profile.

- Theorem 2 The proposed game admits many mixed strategy Nash equilibria, especially when $\lambda = 0$, User$_i$ chooses to randomize to play S and $\overline{S}$ with $c_{ti} - c_{t'i} > R$, or chooses to play S and $\overline{T}$ with $c_{mi} + c_{ti} > R$, or chooses to randomize to play $\overline{S}$ and $\overline{T}$.

- The strategy profile at mixed strategy Nash equilibrium

  $u_1u_{s1}S+u_1(1-u_{s1})\,\overline{S}+(1-u_1)\,\overline{T}$; $u_2u_{s2}S+u_2(1-u_{s2})\,\overline{S} + (1-u_2)\,\overline{T}$; $u_3u_{s3}S+u_3(1-u_{s3})\,\overline{S}+(1-u_3)\,\overline{T}$; $a_1A_1 + a_2A_2 + a_3A_3$

NUMERICAL RESULTS

❑ Pure Strategy Nash Equilibrium

- When users estimate that the comfort and benefit of living in a smart home are less considerable than security costs (money and time) to be invested,
  - ✓ User 1, User 2, and User 3 will be satisfied with taking security training and noticing security countermeasures only if the security rewards are extremely significant and greater than the security costs invested.
  - ✓ "Actual User 2" and "Actual User 3" could be satisfied with a very few security reward (R > 2) while "Actual User 1", will not be satisfied because his or her payoff remains negative.

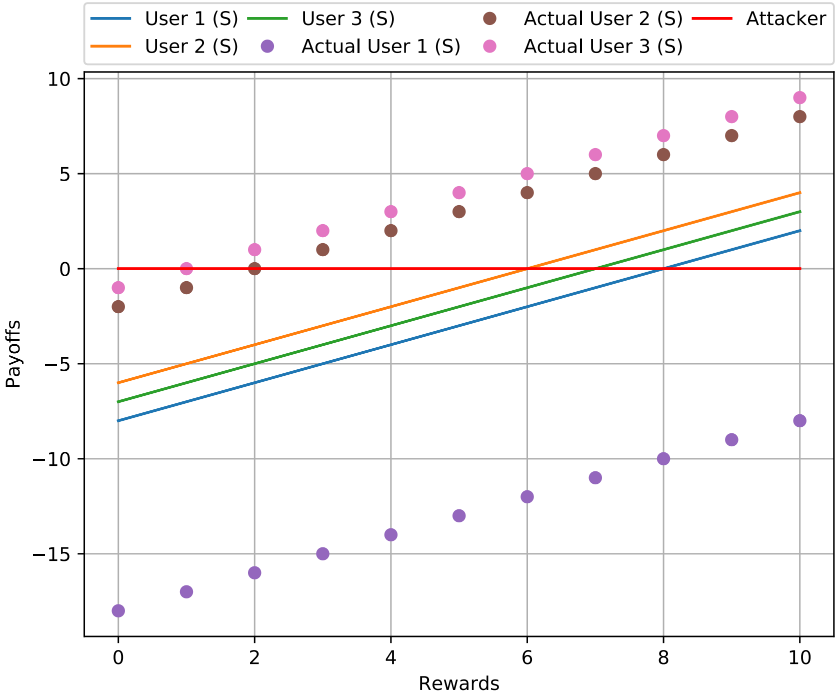


Figure 2. Players' payoffs based on users' rewards for noticing security countermeasures with ϕ < min($c_{m1}+c_{t1}, c_{m2}+c_{t2}, c_{m3}+c_{t3}$ (Scenario 1)

NUMERICAL RESULTS

❑ Pure Strategy Nash Equilibrium

- When users estimate that the comfort and benefit of living in a smart home are more significant than security costs (money and time) to be invested,
  - ✓ User 1, User 2, and User 3 are more likely to invest and notice security countermeasures.
  - ✓ "Actual User 2" and "Actual User 3" are keen to notice security countermeasures. However, "Actual User 1" will be satisfied only if the security rewards are extremely significant (R > 9).

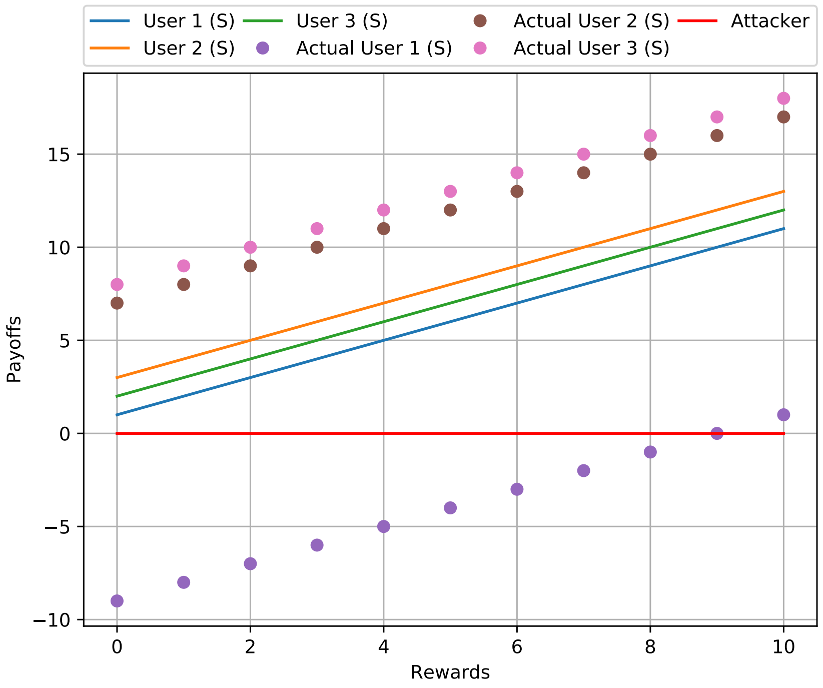
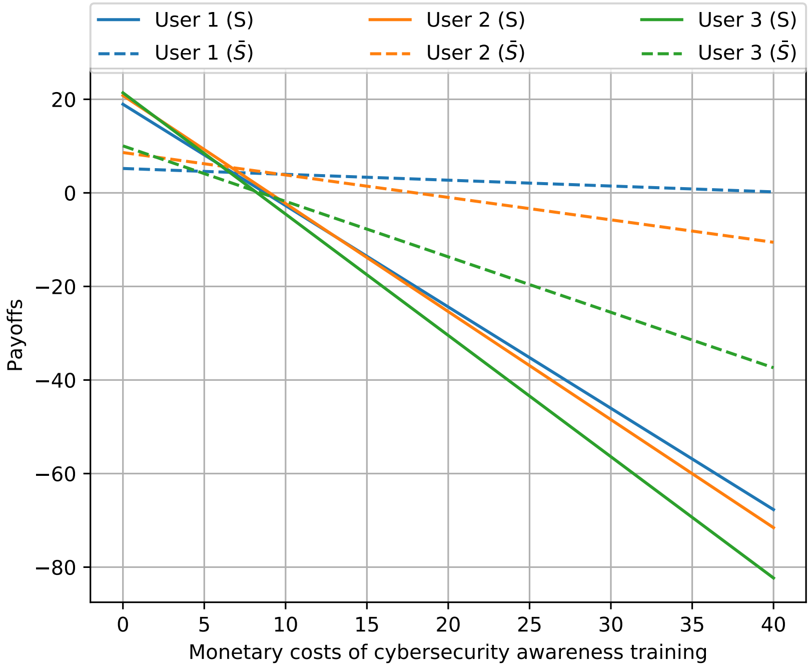


Figure 3. Players' payoffs based on users' rewards for noticing security countermeasures with ϕ > max($c_{m1}+c_{t1}$,$c_{m2}+c_{t2}$,$c_{m3}+c_{t3}$ (Scenario 2)

NUMERICAL RESULTS

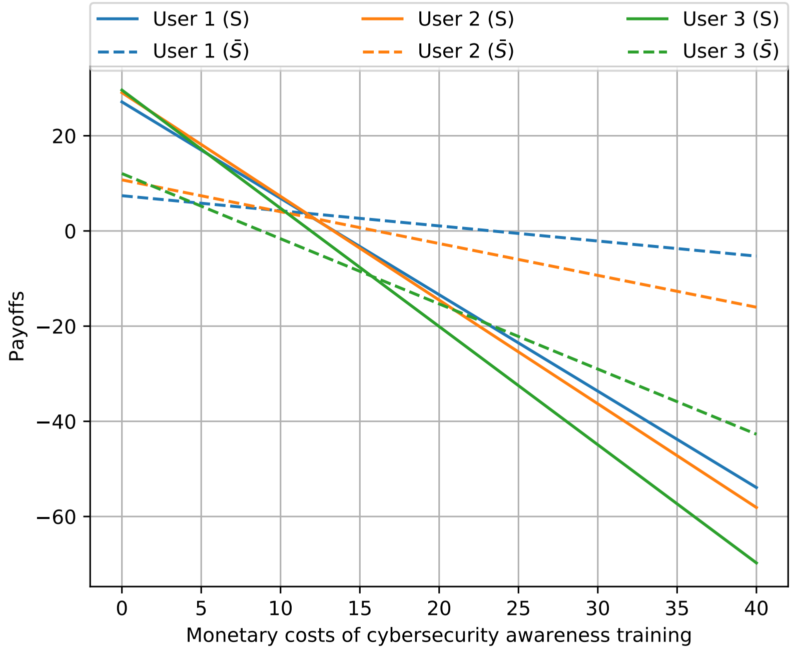
❑ Mixed Strategy Nash Equilibrium

We analyzed the maximin strategy (the best of a set of worst possible security investment strategies) of each mixed strategy scenario.



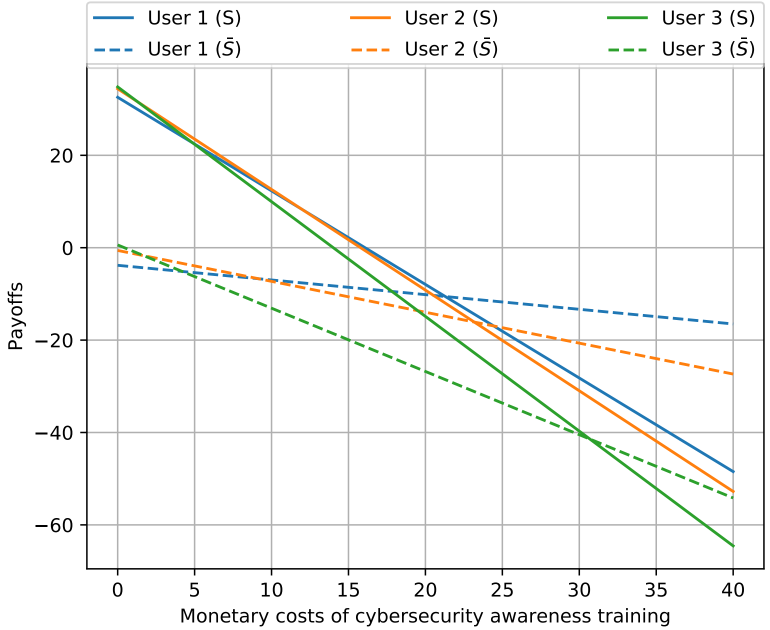
$\phi > (\theta+\delta) > R$

(Scenario 3)



$\phi > R > (\theta+\delta)$

(Scenario 4)



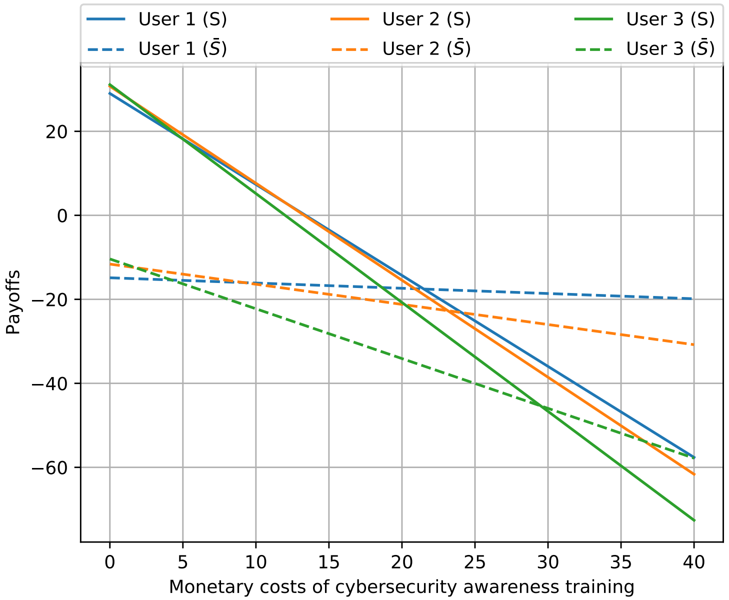
$R > \phi > (\theta+\delta)$

(Scenario 5)

NUMERICAL RESULTS

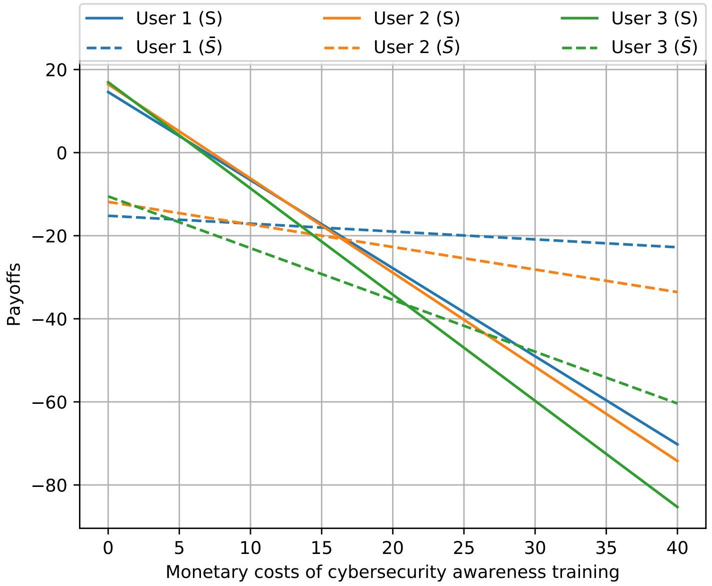
❑ Mixed Strategy Nash Equilibrium

- We found that Scenario 3 is the best option for households because users can minimize the security investment costs and get a positive payoff.



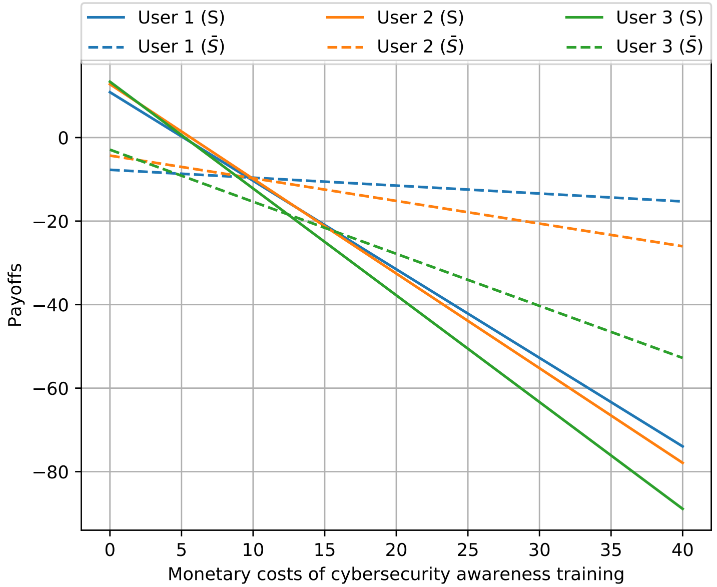
R > (θ + δ) > ϕ

(Scenario 6)



(θ + δ) > R > ϕ

(Scenario 7)



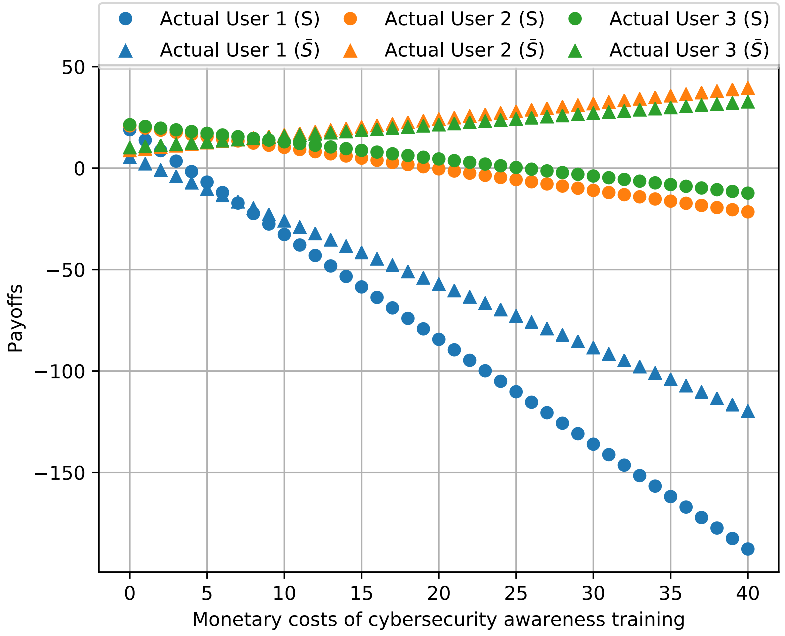
(θ + δ) > ϕ > R

(Scenario 8)

NUMERICAL RESULTS

❑ Mixed Strategy Nash Equilibrium

- However, the results of scenario 9 showed Scenario 3 may not suit actual users when only ``Actual User 1'' is accountable for the monetary costs. We can see that the maximin strategy of actual users is reached when ``Actual User 1'' plays $\bar{S}$ or S with c_{m1}= 6.71, and payoff = -15.80 < 0.



ϕ >(θ+δ)> R

(Scenario 9)

NUMERICAL RESULTS

❑ Mixed Strategy Nash Equilibrium

- Figure 11 showed that under the same conditions as Scenario 3, the payoffs of ``Actual User 1'' increased linearly from -19.16 to -13.28 when P($T_1$ ∩ S) = 1. The payoffs of ``Actual User 1'' remained negative. However, this payoff was positive when we considered the monetary cost c_{m1} = 0

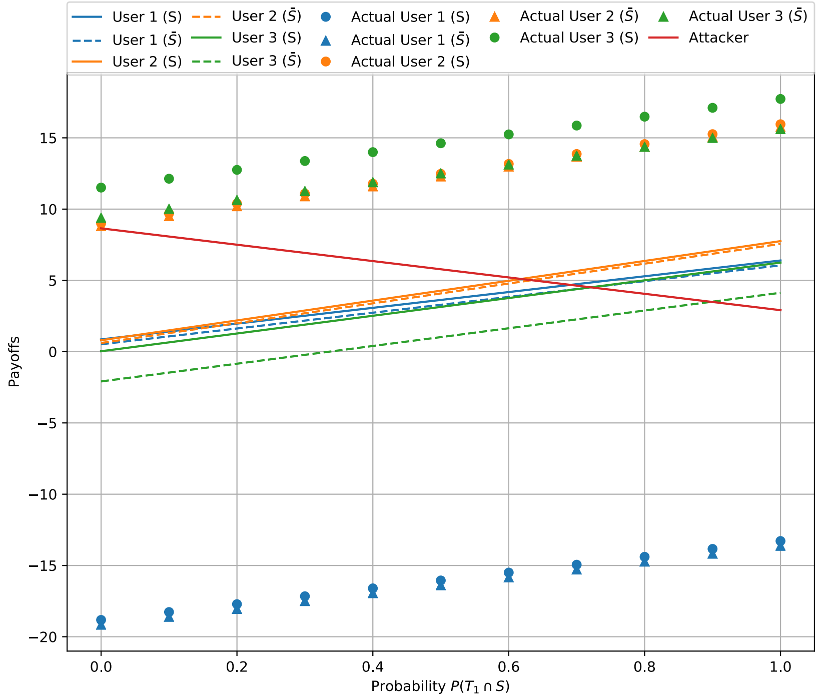


Figure 11. Players' payoffs based on P (T_1 ⋂ S) when ϕ > (θ + δ) > R and c_{m1} = 6.56. (Scenario 10)

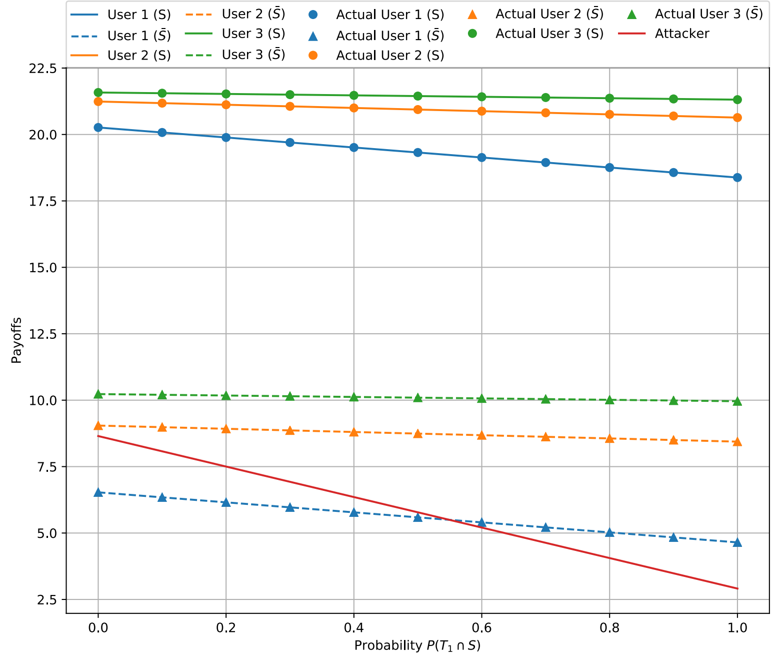


Figure 12. Players' payoffs based on P (T_1 ⋂ S) when ϕ > (θ + δ) > R and c_{m1} = 0. (Scenario 11)

CONCLUSION AND FUTURE WORK

Background

- Households lack cybersecurity education which could motivate attackers to compromise a smart home.

Problem

- Cybersecurity awareness education is expensive for individuals and is not design yet for the specificity of smart-home users.

Approach

- We proposed a game-theoretic model to analyze the security investment costs-benefits of households, including a senior citizen, an adult, and a child, given a cyberattack.

CONCLUSION AND FUTURE WORK

Actions

- We provided a normal-form game with four players: three home users, including a senior citizen, an adult, and a child, and one attacker.
- We determined the conditions to reach the pure and mixed Nash equilibria of the proposed game.
- We presented the numerical results of the proposed game model.

Findings

- The quality of services provided in a smart home, the security rewards of taking cybersecurity awareness training and noticing security countermeasures, and the potential impacts of cyberattacks may influence households' decisions of engaging in cybersecurity education.

Future work

- Proposing a dynamic model of the system based on evolutionary game theory.
- Analyzing thoroughly the impact of time costs.
- Investigating the design of security rewards.

REFERENCES

[1] Statista, "Smart Home Report 2021," 2021, retrieved: October, 2021.[Online]. Available: https://www.statista.com/study/42112/smart-home-report/

[2] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," in 2019 Cybersecurity and Cyberforensics Conference (CCC). IEEE, 2019, pp. 111–117

[3] J. Ricci, F. Breitinger, and I. Baggili, "Survey results on adults and cybersecurity education," Education and Information Technologies, vol. 24, no. 1, pp. 231–249, 2019.

[4] Z. Zuo, Y. Fang, L. Liu, F. Fang, and X. Hu, "Research on information security cost based on game-theory," in 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA). IEEE, 2013, pp. 1435– 1436.

[5] Z. J. Zhang, W. He, W. Li, and M. Abdous, "Cybersecurity awareness training programs: a cost–benefit analysis framework," Industrial Management & Data Systems, 2021.

[6] M. J. Osborne et al., An introduction to game theory. Oxford university press New York, 2004, vol. 3, no. 3.

NARA INSTITUTE OF
SCIENCE AND TECHNOLOGY
- Outgrow your limits -

IARIA

Thank you for your attention.

Comments? Questions?

Presenter’s email address: douha.nguessan_yves-roland.dn6@is.naist.jp

iplab
Laboratory for
Cyber Resilience