Cyber security: Influence of patching vulnerabilities on the decision-making of hackers and analysts

Zahid Maqbool[1], V.S. Chandrasekhar Pammi[2] and Varun Dutt[1]
[1]Applied Cognitive Science Laboratory
Indian Institute of Technology Mandi, India – 175005
[2]Centre of Behavioral and Cognitive Sciences
University of Allahabad, India – 211002

Introduction

- With the explosive growth of the Internet and its extensive use in all sectors, network security has become a challenge (Shiva et al., 2010).
- Organizations need to identify and fix these vulnerabilities as their presence pose a serious threat to the normal working of computer systems.
- This patching may be effective sometimes; however, patches may also lead to new vulnerabilities in computer systems.
- The primary objective of this research is to investigate how the effectiveness of the patching process influences the decisions of hackers and analysts.
- Recently, researchers have studied the patching process through a game theoretic framework called as Markov Security games (Alpcan 2006; Lye 2002; Lye 2005; Roy 2010).

Payoff and State Transition Matrices

Payoff matrices:

State nv

Analyst

Hacker	Defend (d)	Not Defend (nd)
Attack (a)	-5, 5	10, -10
Not Attack (na)	1, -1	0, 0

Nash proportions: p = 0.06, q = 0.62

State v

Analyst

Hacker	Defend (d)	Not Defend (nd)
Attack (a)	-3, 3	11, -11
Not Attack (na)	2, -2	0, 0

Nash proportions: p = 0.12, q = 0.68

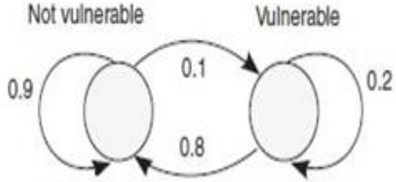
$$p = \frac{D(na,d)}{D(na,d)+D(a,d)+D(a,nd)} \quad (1)$$

$$q = \frac{A(a,nd)}{A(a,nd)+A(a,d)} \quad (2)$$

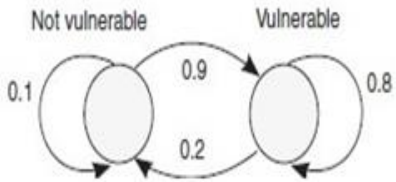
State transition matrices:

(i) Effective Patching

$M(d) = \begin{bmatrix} 0.9 & 0.8 \\ 0.1 & 0.2 \end{bmatrix}$; or

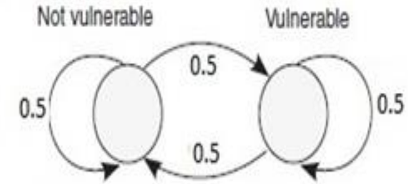


$M(nd) = \begin{bmatrix} 0.1 & 0.2 \\ 0.9 & 0.8 \end{bmatrix}$; or

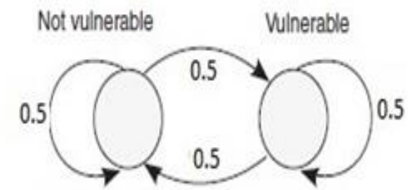


(ii) Less effective patching

$M(d) = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$; or



$M(nd) = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$; or



where p represents the proportion of attack (a) actions and q represents the proportion of defend (d) actions.

Literature and Expectations

- A stochastic security game was proposed and the Nash equilibrium was calculated using simulation (Lye 2002; Lye 2005).
- Current game-theoretic approaches have proposed mathematical solutions, disregarding role of humans with cognitive limitations.
- Across both matrices, the payoff for hackers and analysts are similar and these payoffs possess the same valance (positive or negative).
- Thus, we expect similar proportion of attack and defend actions across both the effective and less-effective patching conditions.
- Instance-based Learning Theory (IBLT) , a theory of decisions from experience in dynamic environments, has been shown to be successful in accounting for decisions of participants performing as hackers and analysts
- Furthermore, according to IBLT, overall, we expect human decisions to deviate from their Nash proportions. That is because human participants would possess cognitive limitations on memory and recall processes and human beings would tend to rely upon recency and frequency of outcomes to make their repeated decisions

Participants and Experimental design

Hundred participants were employed to play the game.

79% males, 74% Undergraduate, Age Min = 18 years, Max = 30years (average = 21.2 years), all participants from STEM Background

- Payment: INR 30 (for participation) + up to INR 20 earned for performance in the game (where 55 points = INR 1)

Mixed factorial design (2*50 design)

- Between-subjects factor:
  - Effective patching (N = 50)

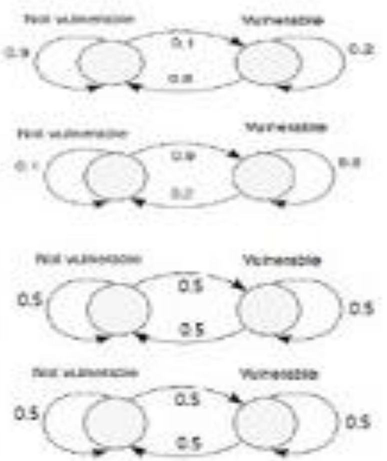
$$M(d) = \begin{bmatrix} 0.9 & 0.8 \\ 0.1 & 0.2 \end{bmatrix}, \text{ or}$$

$$M(nd) = \begin{bmatrix} 0.1 & 0.2 \\ 0.9 & 0.8 \end{bmatrix}, \text{ or}$$

  - Less-effective patching (N = 50)

$$M(d) = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$$

$$M(nd) = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$$



- Within subjects factor: Rounds = 50
  - Independent variable: Patching conditions (Effective patching, Less-effective patching).
- Dependent variable: Average proportion of actions.

Hackers and Analysts Screens

Hacker's feedback (previous trial):

You chose: **Attack** You obtained: **-5 pts**

Analyst Chose: **Defend** Analyst obtained: **5 pts**

Your total points won: **545 pts**

Trial: 2

Your are Hacker.

Your payoffs will be determined by the following matrix

		Analyst	
		Defend (d)	*Not Defend (nd)*
Hacker	*Attack(a)*	-5, 5	10, -10
	Not Attack(na)	1, -1	0, 0

Please choose between the following actions:

Attack Not Attack

Analyst's feedback (previous trial):

You chose: **Defend** You obtained: **5 pts**

Hacker Chose: **Attack** Hacker obtained: **-5 pts**

Your total points won: **555 pts**

Trial: 2

Your are Analyst.

Your payoffs will be determined by the following matrix

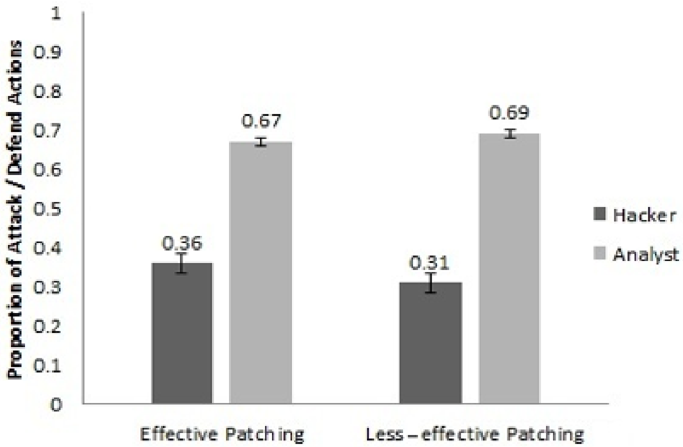
		Analyst	
		Defend (d)	*Not Defend (nd)*
Hacker	*Attack(a)*	-5, 5	10, -10
	Not Attack(na)	1, -1	0, 0

Please choose between the following actions:

Defend Not Defend

Results

Proportion of actions across patching conditions



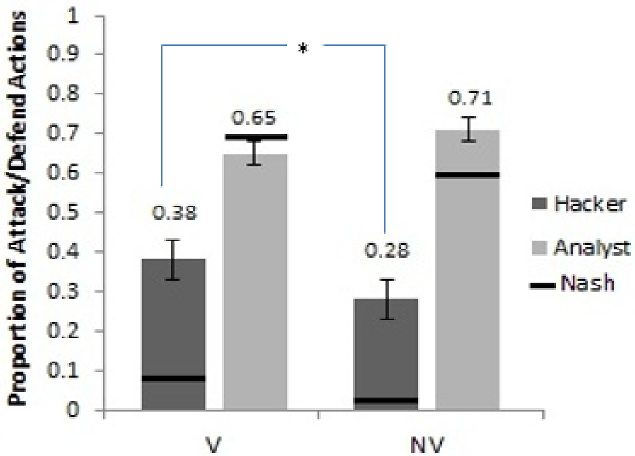
Hacker

$F(1{,}49) = .32, p = .57, n_p^2 = .007$

Analyst

$F(1{,}49) = .133, p = .71, n_p^2 = .003$

Proportion of actions across states



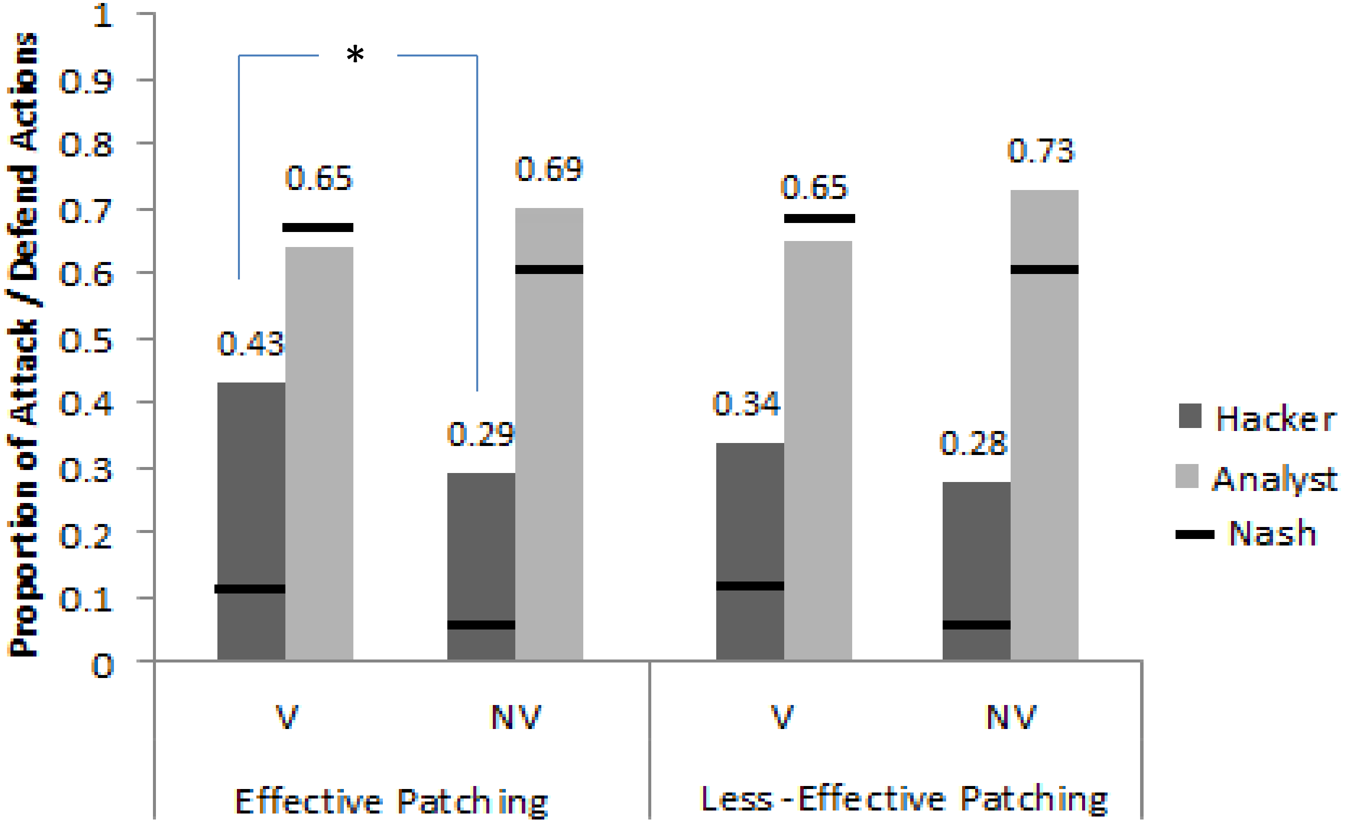
Hacker

$F(1, 98) = 5.70, p < .05, n_p^2 = .06$

Analyst

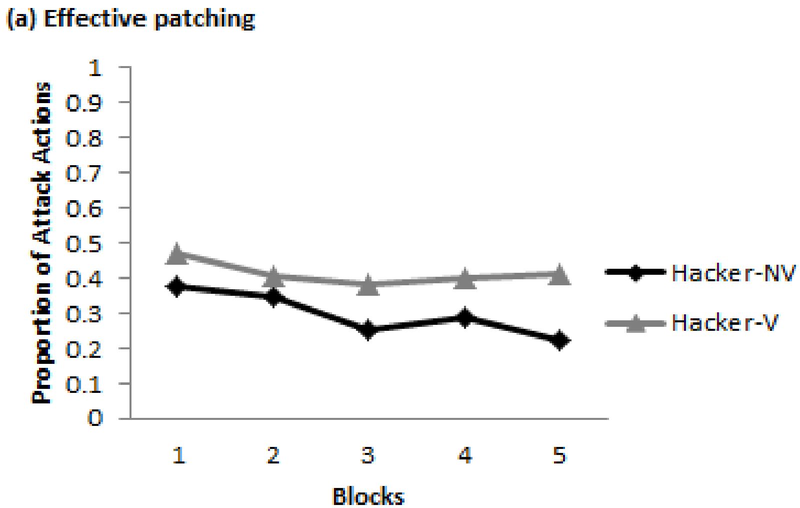
$F(1, 98) = .74, p = .39, n_p^2 = .002$

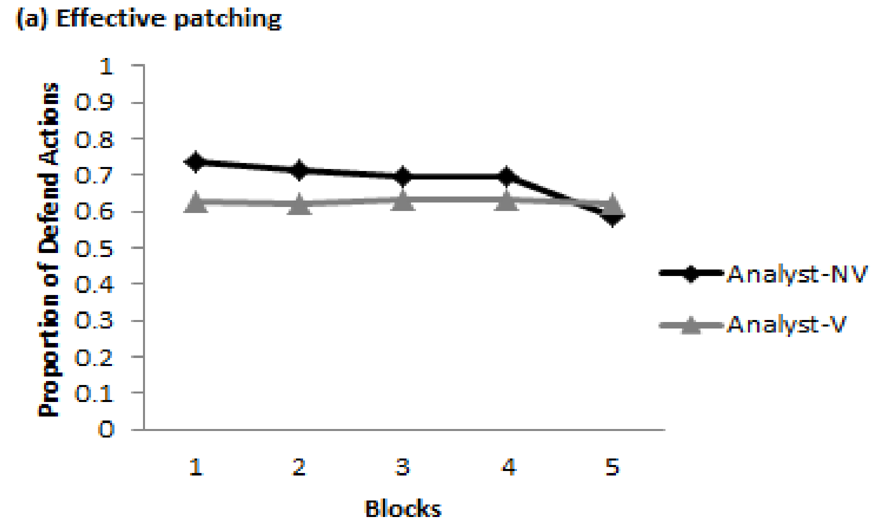
Proportion of actions across conditions and states

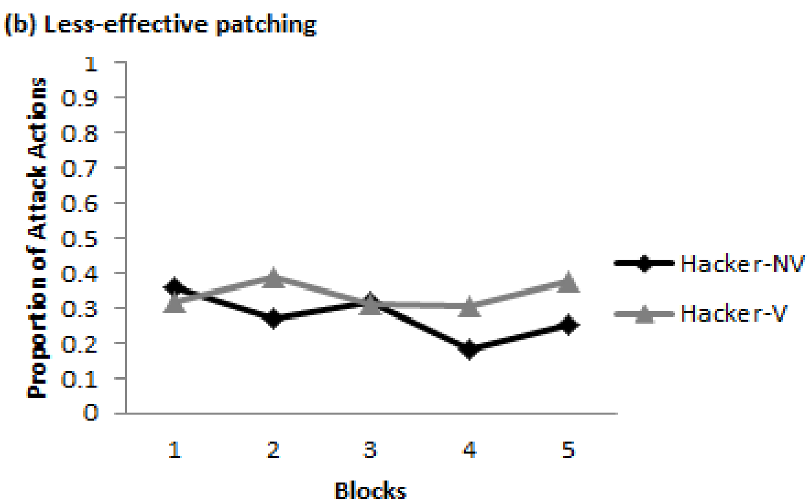


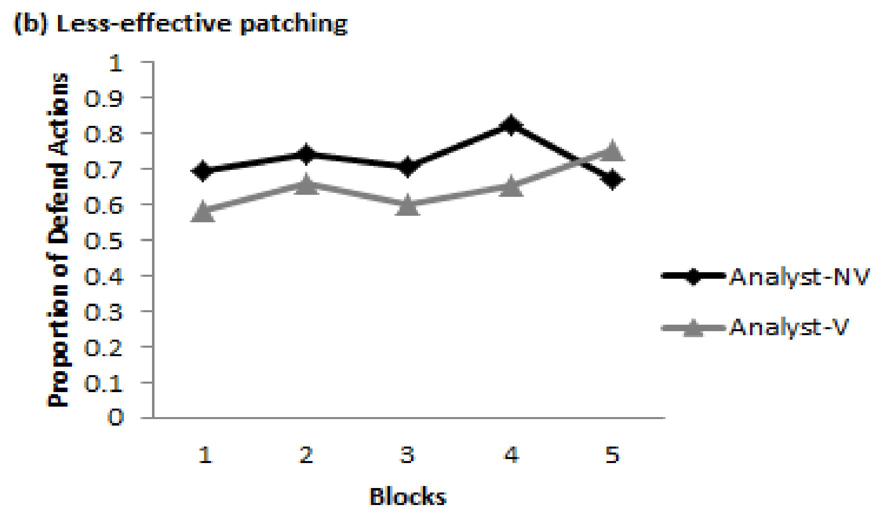
	Hacker	Analyst
Interaction :	$F(1,98) = .71$, $p = .39$, $n_p^2 = .007$	$F(1,98) = .69$, $p = .41$, $n_p^2 = .006$
State :	$F(1,98) = 5{,}75$, $p < .05$, $n_p^2 = .06$	$F(1,98) = 1.97$, $p = .20$, $n_p^2 = .02$

Proportion of attack/defend actions across blocks









	Hacker	**Analyst**
Effective:	$F(4, 192) = 0.19$, $p = .95$, $\eta_p^2 = .004$	$F(4, 192) = 0.59$, $p = .67$, $\eta_p^2 = .012$
Less-effective:	$F(4, 192) = 1.01$, $p = .40$, $\eta_p^2 = .020$	$F(4, 192) = 1.25$, $p = .29$, $\eta_p^2 = .024$

Discussion and conclusion

- Based upon our results, we expect that analysts would continue to excessively patch computer systems in the real-world irrespective of the optimality and the effectiveness of these patching decisions.

- It seems that hackers, while attacking networks, do not seem to worry about whether computer systems are patched effectively or not.

- However, hackers do worry about the vulnerability of computer systems to their attacks. Thus, this perception of vulnerability is likely to influence hacker’s cyber-attack decisions.

- As per Instance Based learning Theory (IBLT), when the network is in non vulnerable state, then the expectation for the rewarded action becomes higher than the expectation for other actions

Implications for Real World

- In the real-world, it may be important to showcase computer networks as less vulnerable to cyber-attacks. One could do so via a number of methods including social networks, newspapers, reports, and multimedia.

- Furthermore, in real world scenarios the hackers would generally have no or limited information on actions and payoffs of analysts.

- Similarly, analysts may have no or limited information on actions and payoffs of hackers or they could get to know hacker’s actions to certain extent via tools like Honeypots. Thus in real world attack and defend proportions may be lesser.

Thank you

References

1. Arora A, & Dutt V. (2013). Cyber Security: Evaluating the Effects of Attack Strategy and Base Rate through Instance-Based Learning, In *Proceedings of the 12th International Conference on Cognitive Modeling (p. xx), Carleton University Campus, Ottawa.*
2. Alpcan T., & T. Başar. (2011). Network Security: A Decision and Game Theoretic Approach. Cambridge University Press.
3. Alpcan, T., & Basar, T. (2006, July). An intrusion detection game with limited observations. In Proceedings of the 12th Int. Symp. on Dynamic Games and Applications.
4. Cui .X, Tan. X, Yong. Z, & Xi. Z. (2008). A Markov Game Theory-Based Risk Assessment Model for Network Information System. In proceeding of: International Conference on Computer Science and Software Engineering, CSSE 2008, Volume 3: Grid Computing / Distributed and Parallel Computing / Information Security, December 12-14, 2008, Wuhan, China.Source: DBLP
5. Dutt, V., Ahn, Y., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber attacks with Instance-Based Learning Theory. *Human Factors*, *55(3), 605-618.*
6. Maqbool, Z., Makhijani, N., Pammi, V. C., & Dutt, V. (2016). Effects of Motivation: Rewarding Hackers for Undetected Attacks Cause Analysts to Perform Poorly. *Human Factors*, 0018720816681888.
7. NIST. (2013, July). Creating a Patch and Vulnerability Management Program Retrieved from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
8. Kahneman, Daniel; Tversky, Amos (1979). "Prospect Theory: An Analysis of Decision under Risk" (PDF). *Econometrica* 47 (2): 263. doi:10.2307/1914185.ISSN 0012-9682
9. Shiva, S., Roy, S., Bedi, H., Dasgupta, D., & Wu, Q. (2010, April). A stochastic game model with imperfect information in cyber security. In The 5th International Conference on i-Warfare and Security (pp. 308-318).