## Title of project

Optimizing Access Control Policies Using Game Theory: A Nash Equilibrium Approach.

## Participants/authors

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Phone** | **Email** | **Study program** |
| Najem Aldeen Abu Hamdah | 0737600483 | [naab0016@student.hv.se](mailto:naab0016@student.hv.se) | Datateknik, högskoleingenjör - programmering och nätverksteknik |
| Yazan Almoued | 0723393370 | [yaal0010@student.hv.se](mailto:yaal0010@student.hv.se) | Datateknik, högskoleingenjör - programmering och nätverksteknik |

## Project background (including literature)

Access control policies like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are crucial in cybersecurity but are generally developed reactively, hence leaving the systems vulnerable to evolving threats. In the past, administrators applied policies based on best practices or past incidents, but not on strategic attacker behavior. Some recent research has explored static access models and qualitative risk analysis, but few accounted for the dynamic, adversarial nature of access control decisions. Game theory, specifically Nash and Stackelberg games, offers a formal model for defining these attacker-defender interactions. By computing costs, payoffs, and probabilities, the project aims to fill a fundamental gap by developing a proactive, strategy-based policy design using real-world breach data (e.g., Verizon DBIR) and threat tactics (e.g., MITRE ATT&CK).

## Problem formulation

Administrators have limited proactive mechanisms to anticipate attacker behavior and tune access control policy accordingly. Existing models do not capture strategic, game-theoretic interaction between attackers and defenders. This project investigates the use of Nash Equilibrium to determine an optimal mix of RBAC and ABAC policies to minimize security breaches while preserving usability.

The central research question is:

"How can Nash Equilibrium guide the selection of access control policies to minimize breaches while maintaining usability?"

## Limitations (if applicable)

* The model assumes rational attackers who have knowledge about system defenses, which may not cover all real-world scenarios, especially with opportunistic or non-strategic attackers.
* Payoff values and success rates are based on approximations of public datasets and might not generalize across all environments.
* It is focused on technical policy optimization, rather than social engineering outside the reach of access control system.

## Methodology

* Data Collection: Public datasets such as Verizon DBIR and MITRE ATT&CK will be used to estimate breach costs and success rates.
* Game Setup: We will construct a 2-player normal form game with defenders choosing between "Strict RBAC" and "Loose ABAC" policies, and attackers choosing between "Phishing" and "Token Theft". A payoff matrix will be derived from the data gathered.
* Equilibrium Analysis: Nash Equilibria will be computed using the nashpy Python library to find optimal mixed strategies for both players.

## Resource plan (if applicable)

Hardware & Software:

* Personal labtop or PC.
* Software tools: VSCode, Python, Nashpy (for equilibrium analysis), and GitHub (for version control and collaboration).

Data Sources:

* Verizon DBIR
* MITRE ATT&CK

## References

[1]Verizon. (2023). Data Breach Investigations Report (DBIR). Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>

[2] MITRE. (n.d.). ATT&CK Framework. Retrieved from <https://attack.mitre.org/>

[3] V. Knight, "Nashpy: A Python Library for the Computation of Nash Equilibria," 2024. [Online]. Available: <https://nashpy.readthedocs.io/en/stable/>

[4] Y. Xu, Y. Zhang, Y. Sun, and S. Zhu, “Game theory-based access control mechanism for cyberspace security,” International Journal of Information Security, vol. 23, no. 2, pp. 321–333, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1000936124002140>