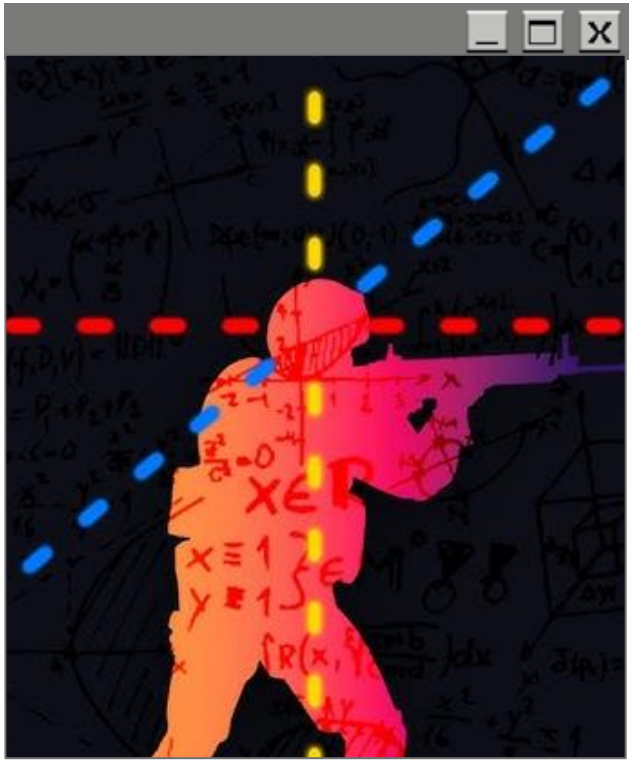
Detecting **Visual Aimbots** in MOGs via Honeytokens

Salman Shaikh, Tao Ni, Marc Dacier

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

THCON 2026
TOULOUSE HACKING CONVENTION

Table of Contents



What are Aimbots?

- Software that enhances the performance of a cheater.
- Automating the process of finding and shooting at the opponent [2,3].
- A prevalent problem that has been ongoing since the early days of shooter games.

[2] Anwar, M.S., Zuo, C., Yagemann, C., Lin, Z.: Extracting Threat Intelligence From Cheat Binaries For Anti-Cheating. In: 26th International Symposium on Research in Attacks, Intrusions and Defenses. p. 17–31. ACM (2023). https://doi.org/10.1145/3607199.3607211
[3] Karkallis, P., Blasco, J.: Vic: Evasive video game cheating via virtual machine introspection. https://arxiv.org/abs/2502.12322 (2025)

Types of Aimbots

- Memory-Based Aimbots [2,3]
  - Attaches to the game process and reads memory for enemy positions.
  - Calculates aim and injects input directly into the game.
  - Often paired with Triggerbots for automatic shooting.
    - ✓ Anti-Cheat Systems, shipped with the games (EAC, Vanguard, etc.) can detect such cheats. - To a certain extent..

- Visual Aimbots [4,5]
  - Utilize trained CV models that run alongside the game.
  - Analyzes live screen data instead of accessing game memory.
  - Being used in practice more and more, for commercial games.
    - × Anti-Cheat Systems cannot detect such cheats.

[2] Anwar, M.S., Zuo, C., Yagemann, C., Lin, Z.: Extracting Threat Intelligence From Cheat Binaries For Anti-Cheating. In: 26th International Symposium on Research in Attacks, Intrusions and Defenses. p. 17–31. ACM (2023). https://doi.org/10.1145/3607199.3607211
[3] Karkallis, P., Blasco, J.: Vic Evasive video game cheating via virtual machine introspection. https://arxiv.org/abs/2502.12322 (2025)
[4] Kelik Nugroho, A., Permadi, I., Habiballah, A.: Image detection in the aimbot program using yolov4tiny. Jurnal Teknik Informatika (Jutif) 4 (1), 109–115 (Feb 2023). https://doi.org/10.52436/1.jutif.2023.4.1.821
[5] Sun, C., Ye, K., Su, L., Zhang, J., Qian, C.: Invisibility Cloak: Proactive Defense Against Visual Game Cheating. In: 33rd USENIX Security Symposium. pp. 3045– 3061. USENIX Association (Aug 2024)

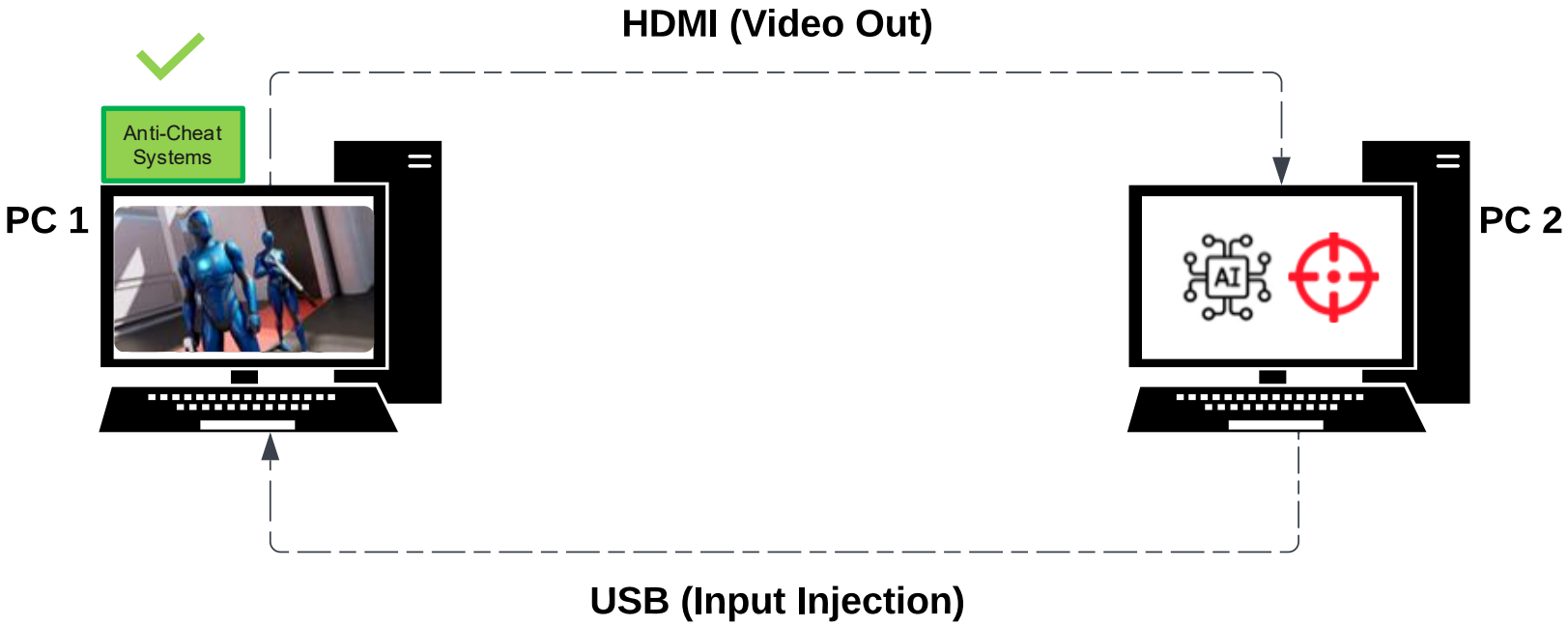

HDMI (Video Out)
Anti-Cheat Systems
PC 1
PC 2
AI
USB (Input Injection)

Table of Contents

PATCH: Proactive Adversarial Traps for Cheaters in MOGs

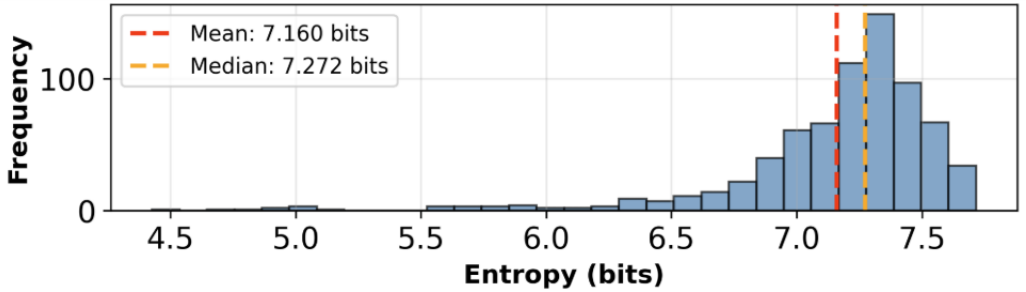
- Generate ***Adversarial Patches*** of different sizes, which serve as honeytokens.
- No typical disruption
- Focusing on deliberately triggering the attacker's visual aimbot.

Table of Contents

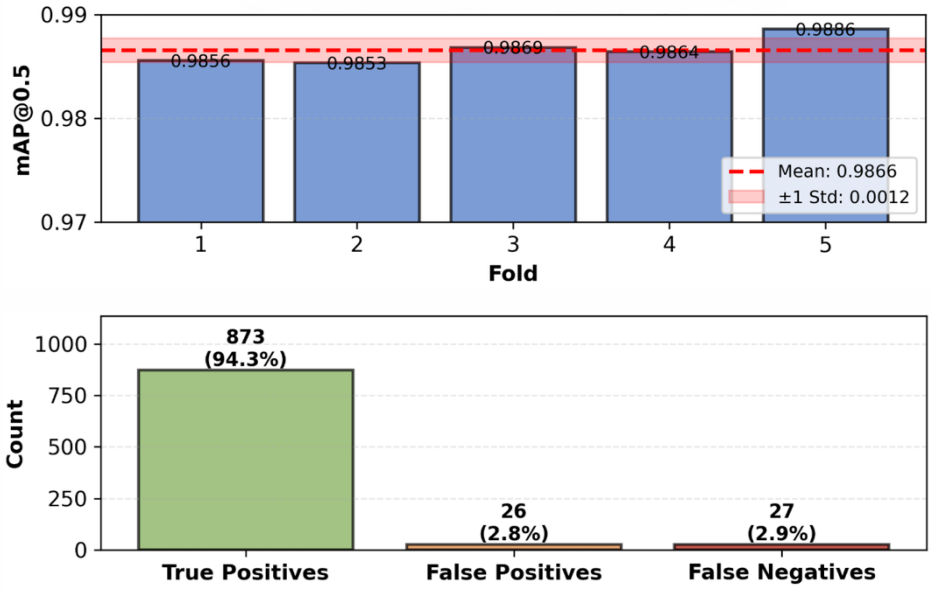

99:31
12
EMPTY
EMPTY

Generating a Visual Aimbot

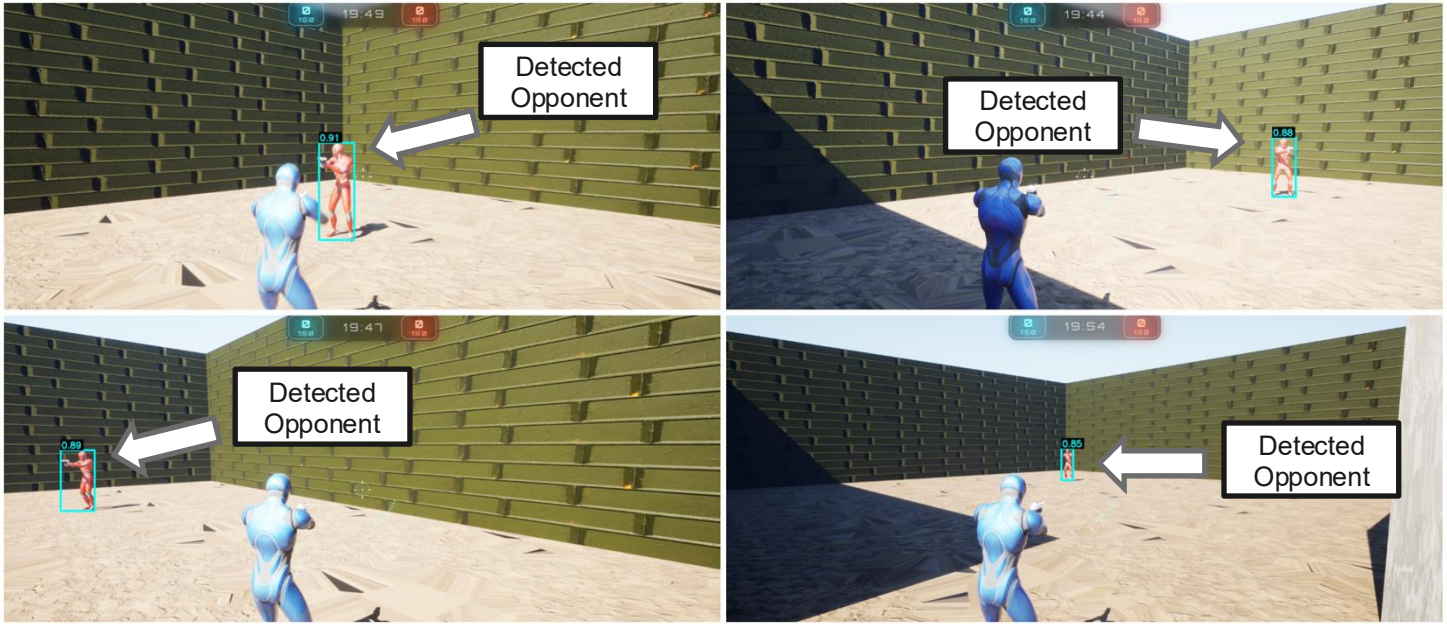
- Utilize pre-trained YOLO11m provided by Ultralytics
  - Most widely used in practice due to its accuracy and latency.
- Finetune to detect one class: 'player'.
- 5-fold cross validation on 900 diverse images.



Results – 1


0.99
0.98
0.97
mAP@0.5
0.9856
0.9853
0.9869
0.9864
0.9886
Mean: 0.9866
±1 Std: 0.0012
1
2
3
4
5
Fold
1000
750
500
250
0
Count
873
(94.3%)
26
(2.8%)
27
(2.9%)
True Positives
False Positives
False Negatives

Results – 2

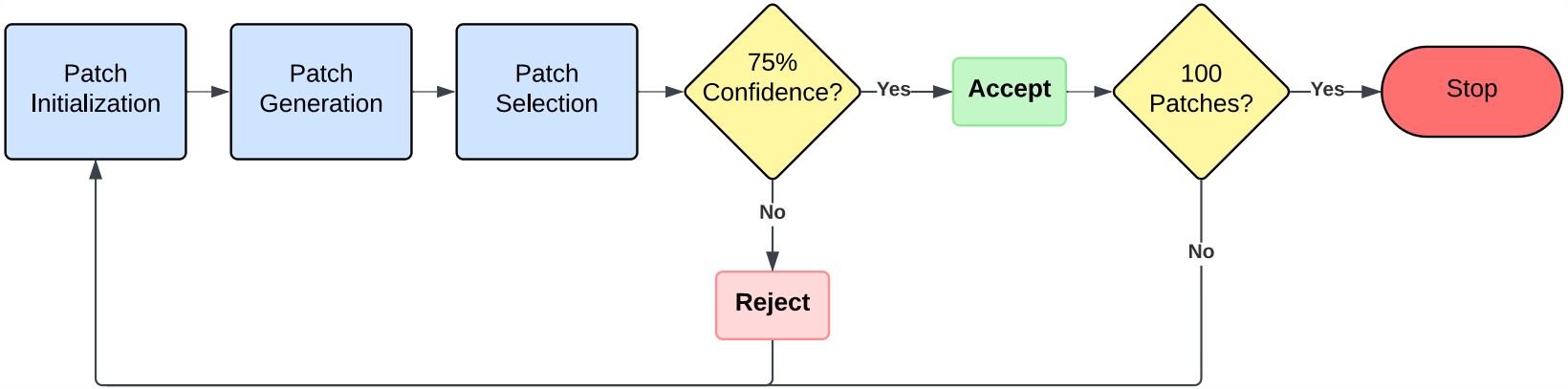

Detected Opponent
Detected Opponent
Detected Opponent
Detected Opponent

Generating Patches (Honeytokens)

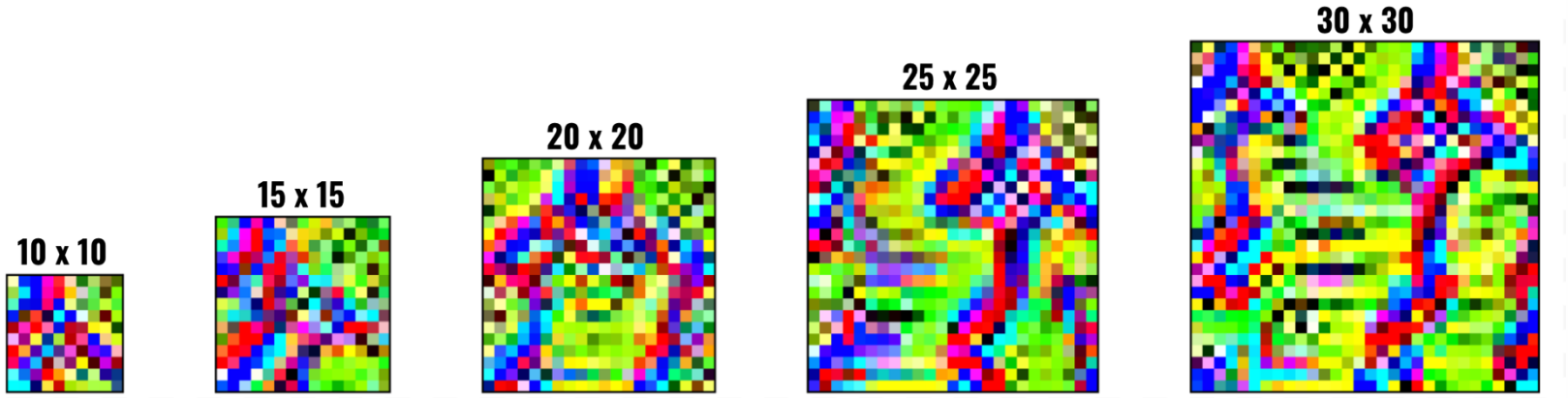
- **Our Approach:**
  - **White-Box: The defender can leverage the cheater's model to generate honeytokens designed to trigger it.**
  - **Replicates real-world scenarios.**

Black-Box: The defender will not know the attacker's model. Thus, uses a known surrogate model to generate honeytokens.

Generating Patches (Honeytokens): Pipeline



Results – 1



Results – 2

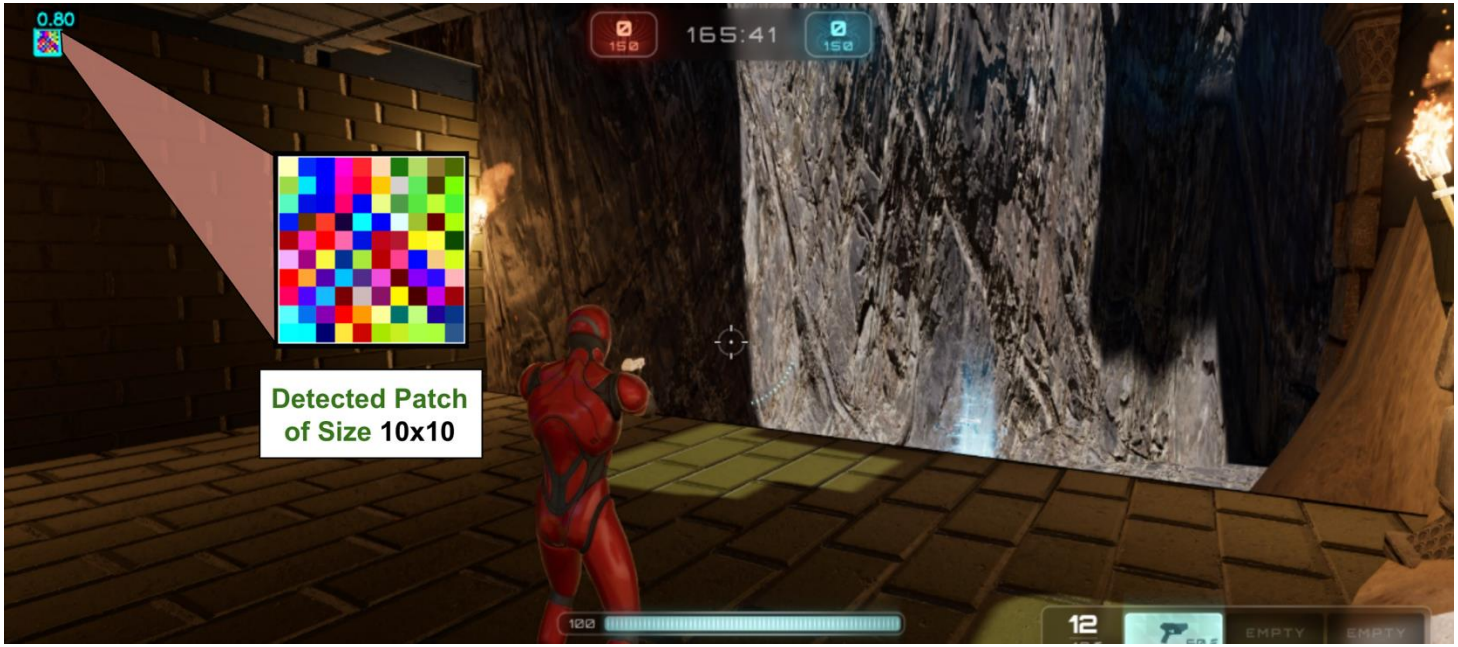
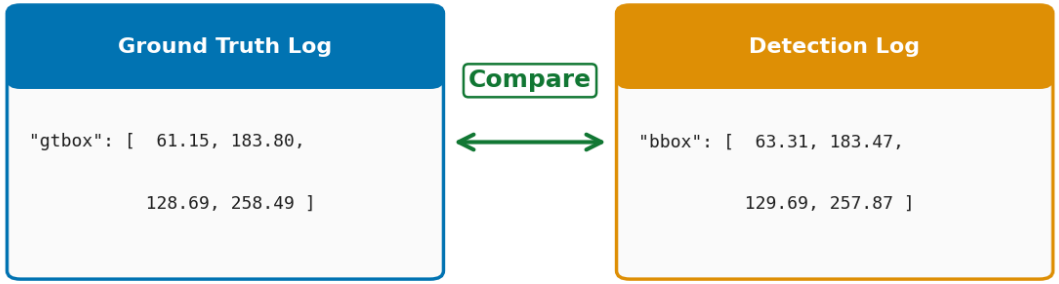


Table of Contents

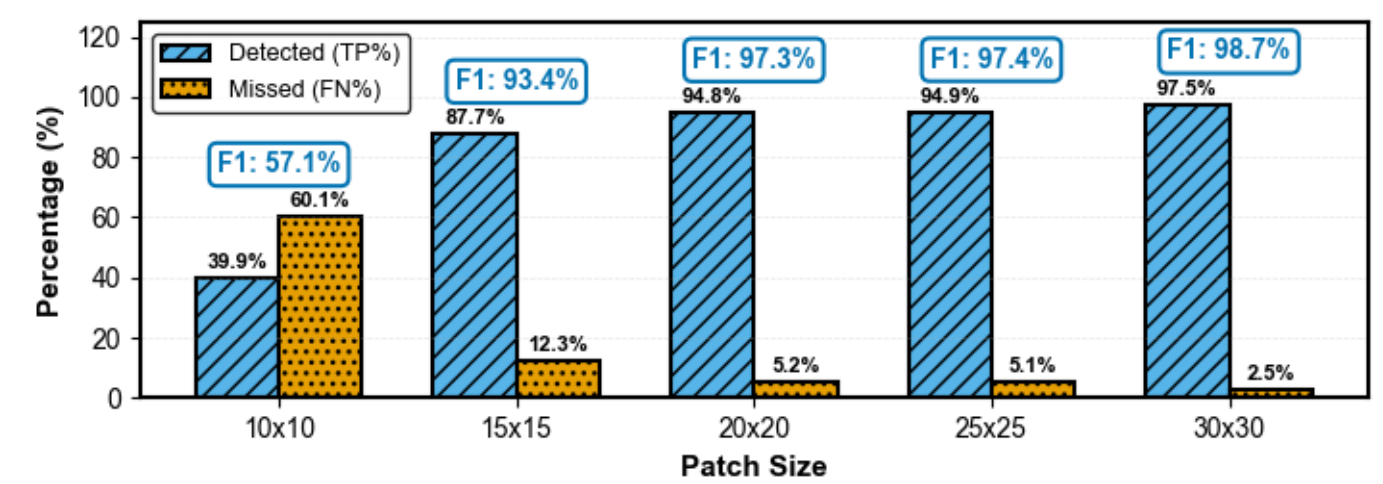
Evaluation Approach

- Patches deployed within the game for 100ms.
- Dual Logging System.



- All patch analysis experiments were conducted across multiple trials.

Evaluation Test – Whitebox



Evaluation Test – Fortnite [6]

[6] Sunone: Sunone boosty page. https://boosty.to/sunone (2026), accessed: 2026-04-03

Table of Contents

Conclusion

- Adversarial Patches as Honeytokens.
- Effective for all patch sizes.
- Limitations: Patch Effectiveness v/s Stealthiness
- Limitations: Cross-Model Transferability
- Future Work: Game-Based Patch Initialization
- Future Work: Adaptive Mitigation Techniques

References

1. SlidesGo Template.

2. Anwar, M.S., Zuo, C., Yagemann, C., Lin, Z.: Extracting Threat Intelligence From Cheat Binaries For Anti-Cheating. In: 26th International Symposium on Research in Attacks, Intrusions and Defenses. p. 17–31. ACM (2023). https://doi.org/10.1145/3607199.3607211

3. Karkallis, P., Blasco, J.: Vic: Evasive video game cheating via virtual machine introspection. https://arxiv.org/abs/2502.12322 (2025)

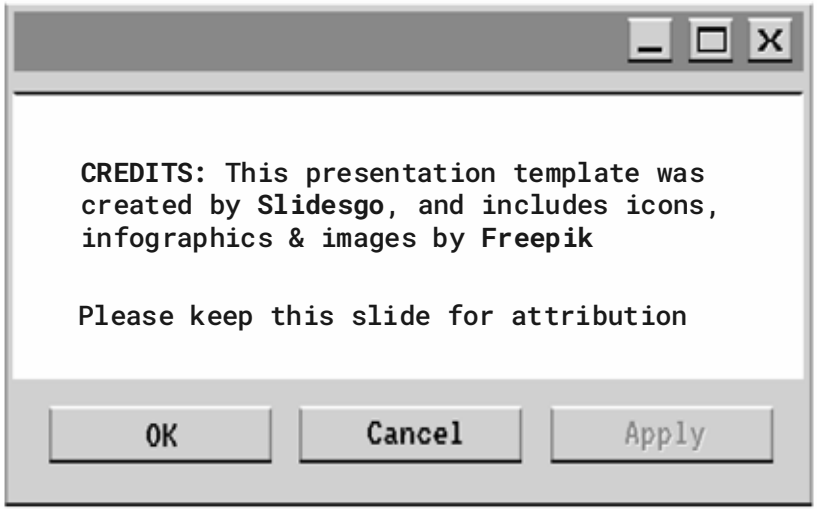
4. Kelik Nugroho, A., Permadi, I., Habiballah, A.: Image detection in the aimbot program using yolov4-tiny. Jurnal Teknik Informatika (Jutif) 4(1), 109–115 (Feb 2023). https://doi.org/10.52436/1.jutif.2023.4.1.821

5. Sun, C., Ye, K., Su, L., Zhang, J., Qian, C.: Invisibility Cloak: Proactive Defense Against Visual Game Cheating. In: 33rd USENIX Security Symposium. pp. 3045– 3061. USENIX Association (Aug 2024)

6. Sunone: Sunone boosty page. https://boosty.to/sunone (2026), accessed: 2026- 04-03

Thank You!

Questions?



salman.shaikh@kaust.edu.sa