

Understanding Human Behavior in Cyber Operations: A Methodical Approach

Georgel Savin (USNA), Ammar Asseri (USNA), Josiah Dykstra (NSA), Jonathan Goohs (CSA-63), Dr. Anthony Melaragno (USNA), Dr. William Casey (USNA)





Unmasking the Need for Full-Scale Attack Data

- How can we measure technical skills and enable learning to match the needs of cyberspace?
- Goal - Enhancing offense while also developing defensive models

The Game

- 2 teams of 4 individuals each
- *Cyber Mayhem* hosted by Hack The Box
- Secure own system whilst exploiting opposing team's systems
- Problem sets involved - web exploitation, reverse engineering, and penetration testing





Methodological Approach

1. Simulation of real-world cyber operations via Capture the Flag (CTF) games
2. Data collection off player's actions during CTF events
3. Measurable metrics - Keystroke accuracy, app logs, video capture
4. Automated data processing and labeling to industry standard Tactics, Techniques, and Procedures (TTPs)



Data Collection

time	user entered data			stats
date-time	raw	normalized	cmd	accuracy
2023-02-23 16:34:33 -0500	<Enter>	ssh	ssh	0.88
	ssh s<BckSp>	root@		
	root<LShft> @10.10.111.102	10.10.111.102		

Table 1: Example of data collected, keystroke normalization, and statistical measures are shown for an example entry.



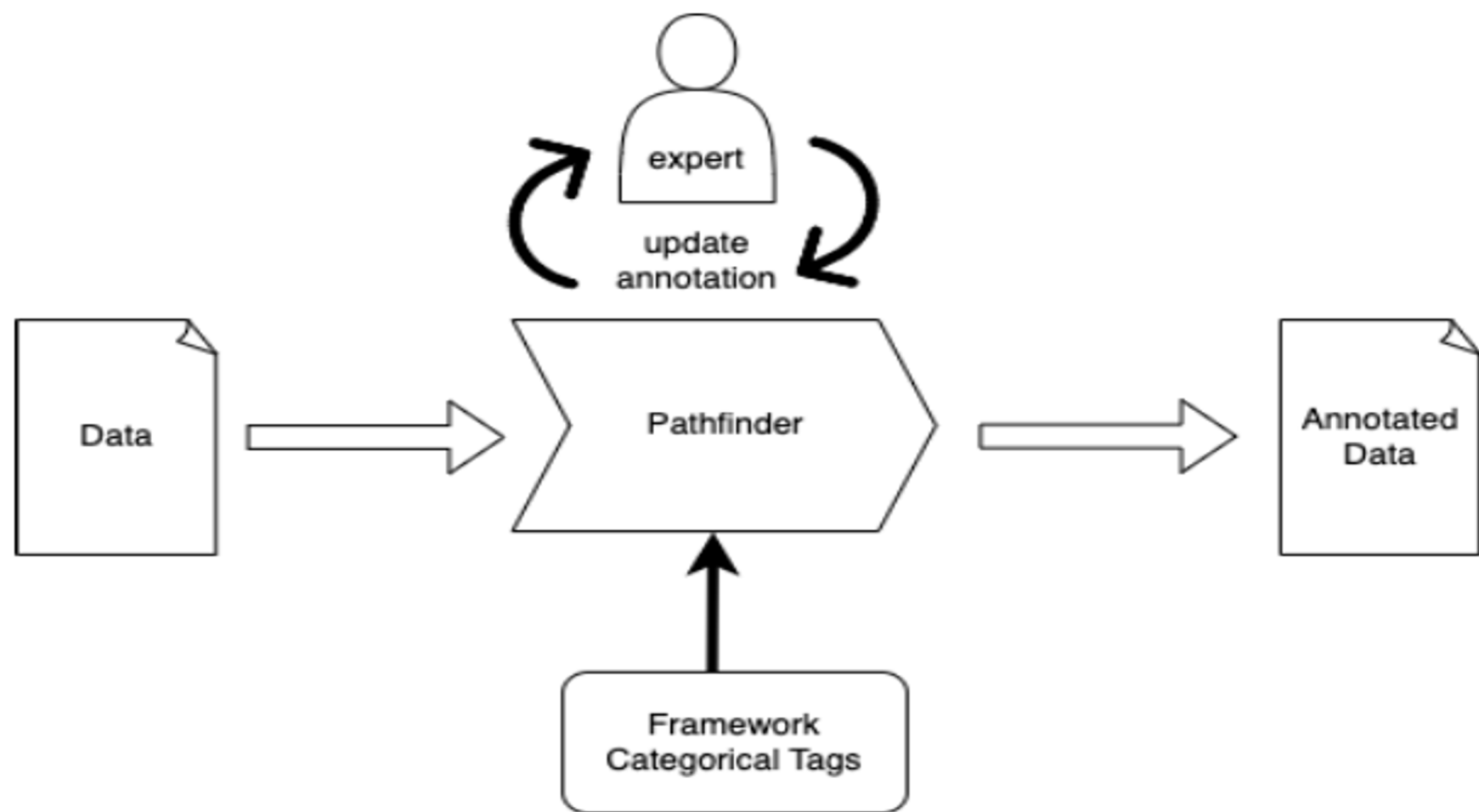
Keystroke Accuracy (KA)

- How accurately players execute actions during the CTF game
- Average KA of 69.1% game-wide
- Winning team used less commands, but actually had a lower KA by 4%

Frequency of Action Classification

- Actions performed by players were classified in line with the MITRE ATT&CK framework

<p>[Framework Category]</p> <p>Reconnaissance</p> <p>ResourceDevelopment</p> <p>>InitialAccess</p> <p>Execution</p> <p>Persistence</p> <p>PrivilegeEscalation</p> <p>DefenseEvasion</p> <p>CredentialAccess</p> <p>Discovery</p> <p>LateralMovement</p> <p>Collection</p> <p>CommandandControl</p> <p>Exfiltration</p> <p>Impact</p>	<p>[techniques]</p> <p>Drive-by Compromise</p> <p>Exploit Public-Facing Application</p> <p>External Remote Services</p> <p>Hardware Additions</p> <p>>Phishing</p> <p>Replication Through Removable Media</p> <p>Supply Chain Compromise</p> <p>Trusted Relationship</p> <p>Valid Accounts</p>	<p>[more]</p> <p>Spearphishing Attachment</p> <p>Spearphishing Link</p> <p>>Spearphishing via Service</p>
<p>[info]</p> <p>Category: The adversary is trying to get into your network.Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.</p> <p>technique: Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.</p> <p>more: Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.</p>		



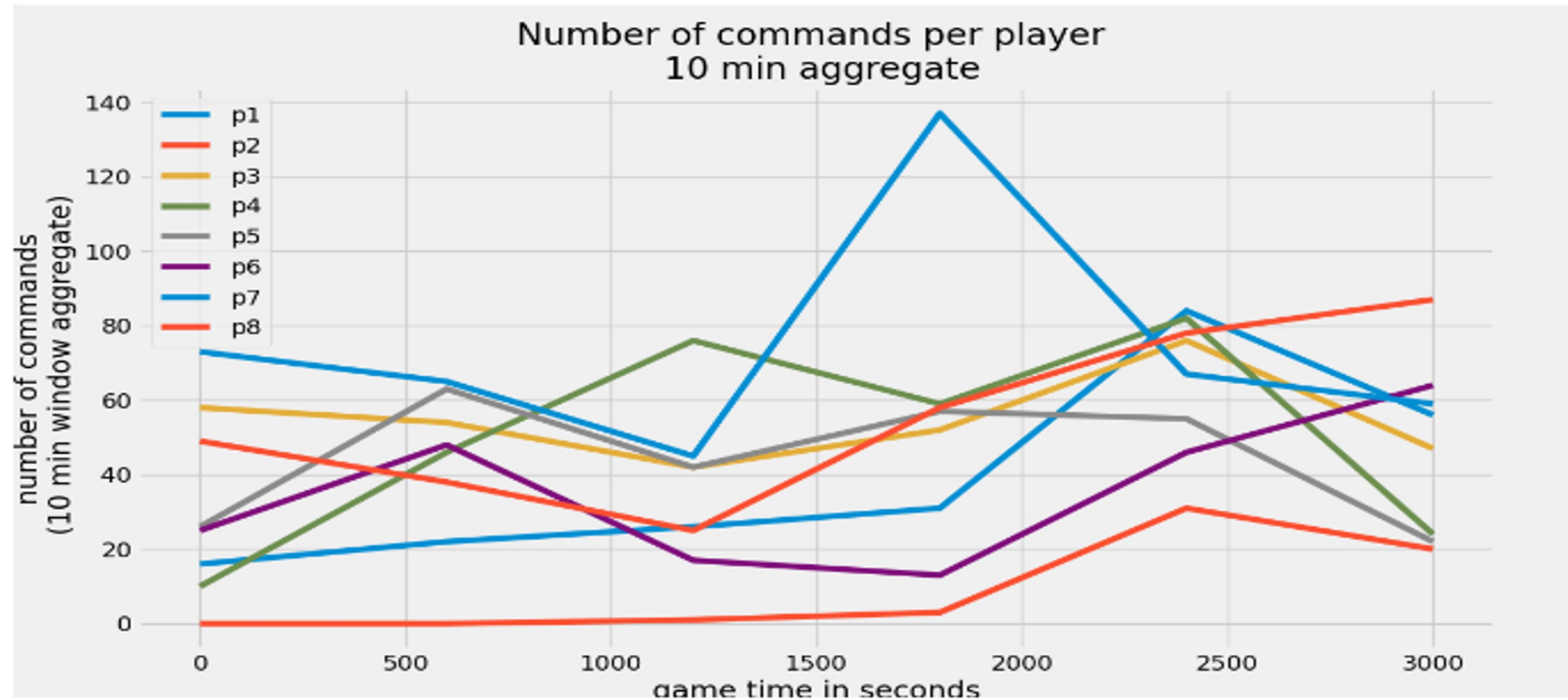


Figure 5: Command counts time series per player where counts are aggregated into 10 minute non-overlapping windows during a one-hour game.



Into the Future - Limitations, Implications and Extensions

- Lack of sample size for experiment
- Study enables organizations to identify areas for improvement in training, as well as defensive posture
- Application for training AI towards more realistic training simulations



Conclusion

- Use of realistic full-scale data and analysis of multiple parameters aids in characterizing human factors in offensive cyber operations
- Similar efforts supports efficient cyber defense strategies, which reduce organizational resource costs

Q&A/Contact Us!

POCs: Dr. William Casey (wcasey@usna.edu)

Dr. Anthony Melaragno (melaragn@usna.edu)

