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 s<BckSp> root<LShft> @10.10.111.102	ssh root@ 10.10.111.102	ssh	0.88

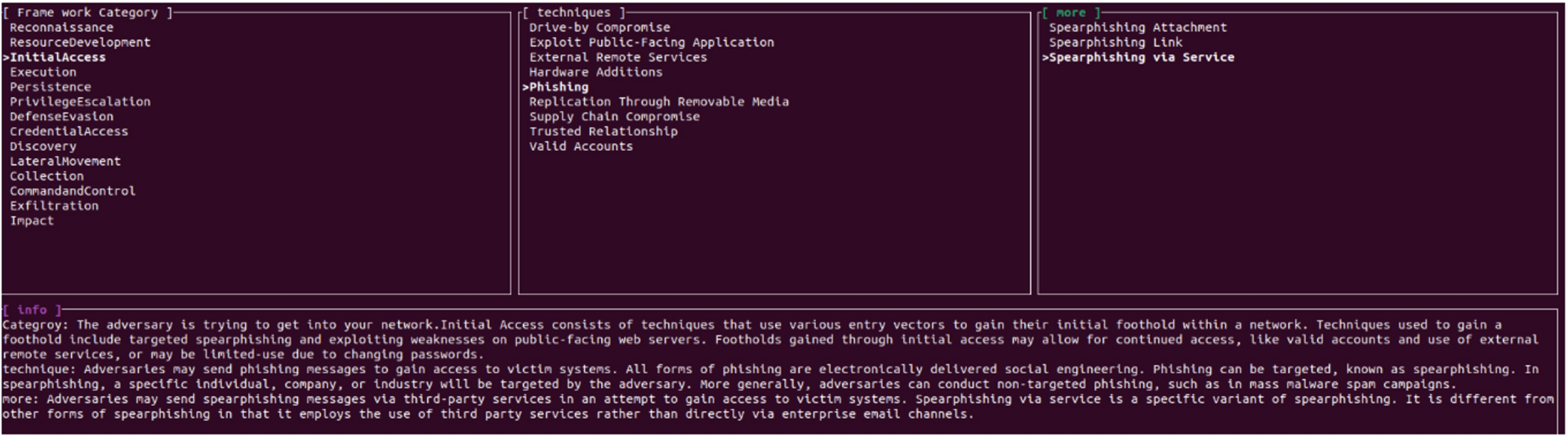
Table 1: Example of data collected, keystroke normalization, and statistical measures are shown for an example entry.

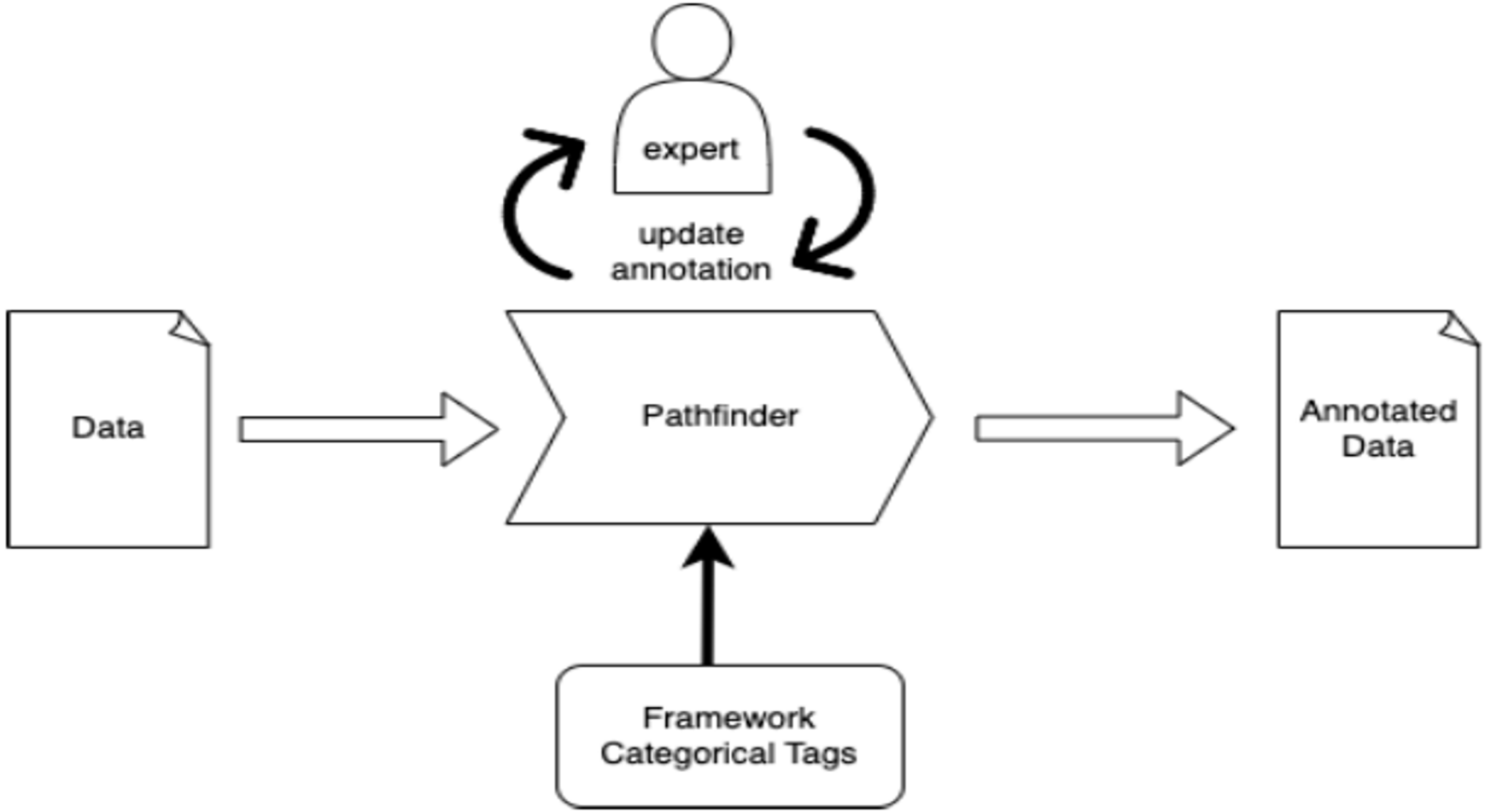
Keystroke Accuracy (KA)

- 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




expert
update
annotation
Data
Pathfinder
Annotated
Data
Framework
Categorical Tags

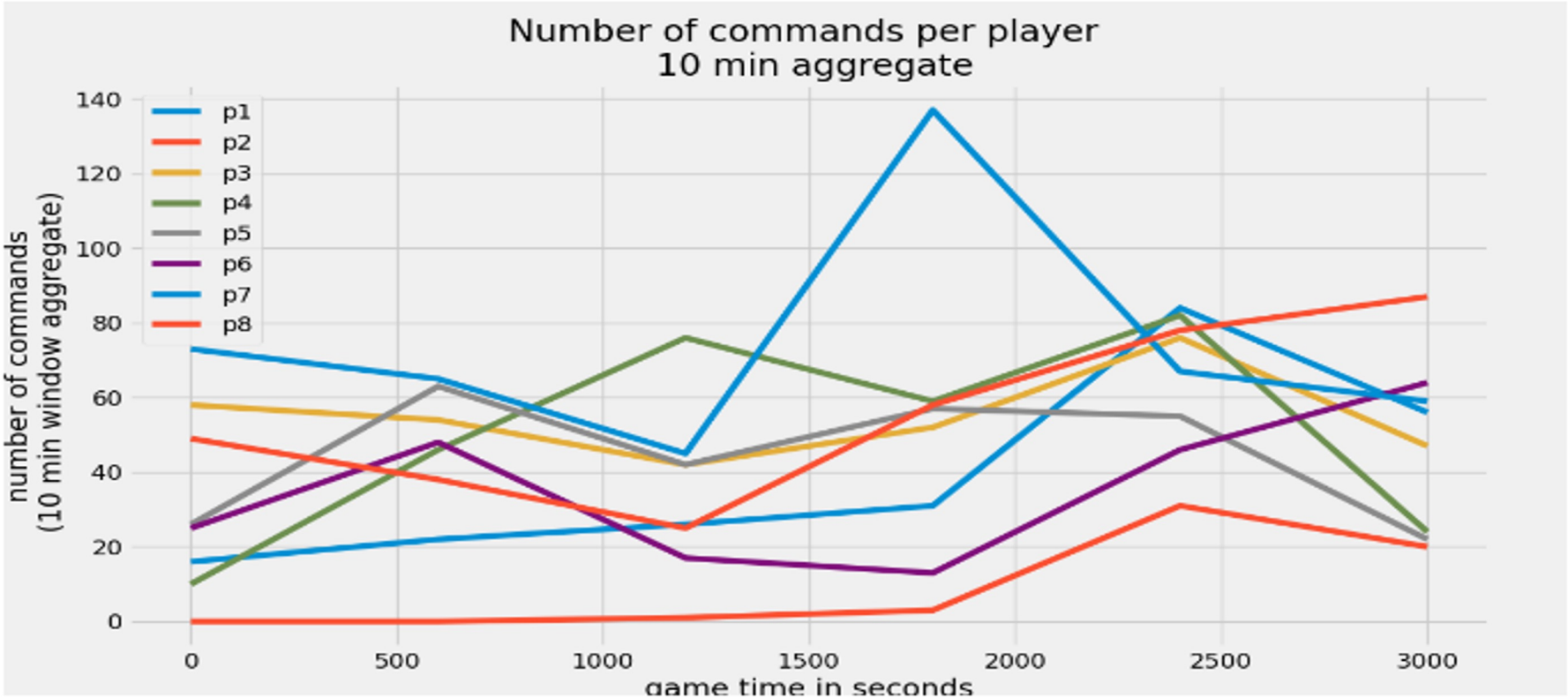


Figure 5: Command counts time series per player where counts are aggregated into 10 minute non-overlapping windows during a one-hour game.

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)