Predicting Behaviors of Advanced Persistent Threats Using Collaborative Filtering

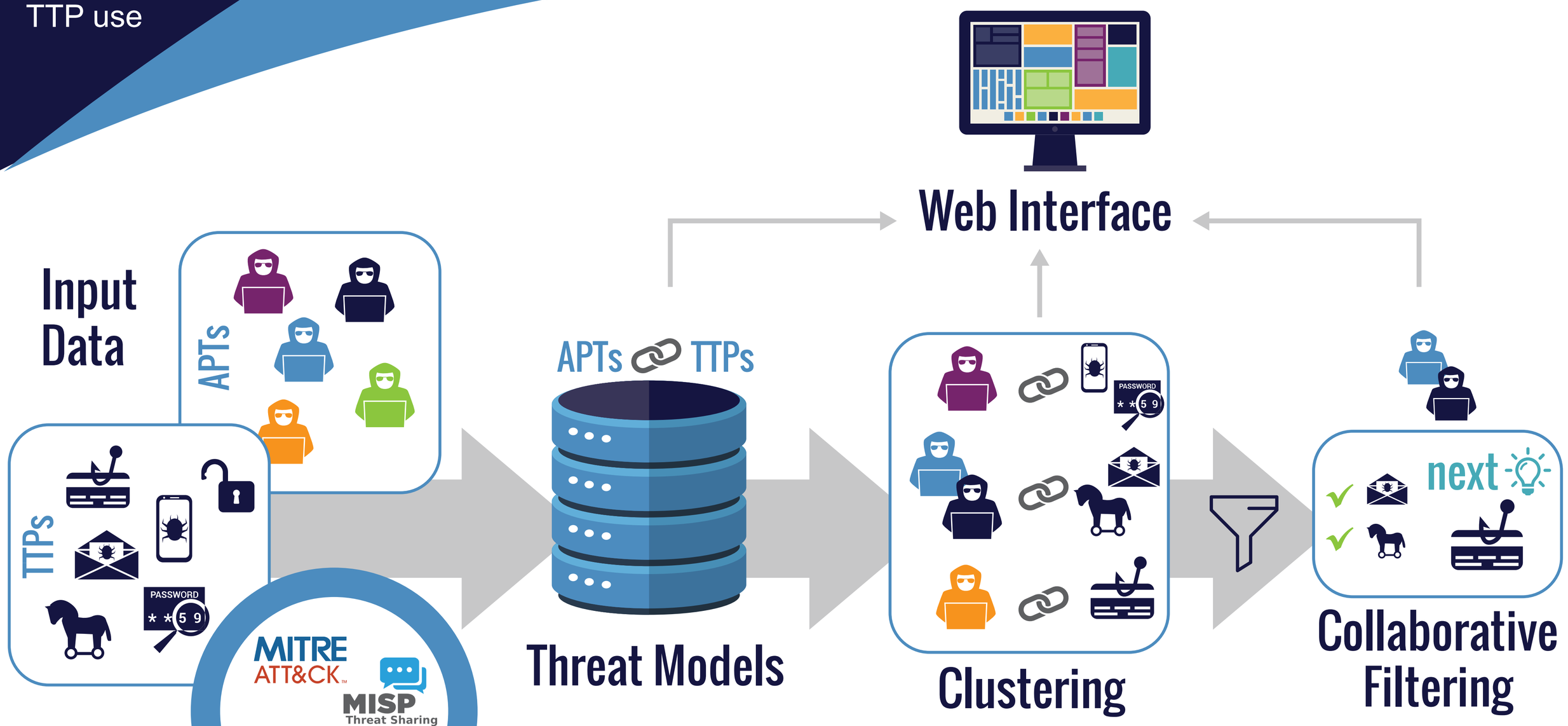
Guy Howard[1], Adrienne Decker[2], Adam Schwartz[1], Mary Anne DeHart[1]
[1]IntelliGenesis LLC, [2]University at Buffalo

APTs use a variety of methods to disrupt and destroy cyber operations of their targets

By examining their Tactics, Techniques, and Procedures (TTPs) we model APT behavior

Based on these models and models of similar actors, we can predict future TTP use

Rialto



Gamaredon Group is a suspected Russian sponsored APT that has been active and targeting Ukrainian government officials since 2013. Below are our predictions based on behavior by similar groups *(Rancor, FIN10, and others)*

	Gamaredon Group	Rancor	FIN10
Scripting	✓	✓	✓
Standard Application Layer Protocol	✓	✓	✗
Peripheral Device Discovery	✓	✗	✗
Remote File Copy	✓	✓	✓
System Owner/User Discovery	✓	✗	✓
Data from Removeable Media	✓	✗	✗
Scheduled Task	💡	✓	✓
Registry Run Keys/Startup Folder	💡	✗	✓

✓ *APT uses TTP* ✗ *APT does not use TTP*
💡 *PREDICTED*

Results

Gamaredon utilized previously unseen malware leveraging Scheduled Tasks and the Startup Folder to achieve persistence

* **Collaborative filtering predicted these TTPs based on publicly available data over a month before the attacks occurred**

Conclusion

Collaborative Filtering provides accurate, meaningful predictions

Clustering first results in more focused, narrow predictions (not always better)

Filters using multiple groupings all provide potentially valuable answers

APT behavior is affected by many things other than previous behavior, such as real world events

Next Steps: New Data Sources | Refine Predictions | Visualizations

University at Buffalo
IntelliGenesis LLC WHERE INTELLIGENCE BEGINS