Decision Analysis Applications in Threat Analysis Frameworks

Emily Shawgo

October 6, 2018

Agenda

- Background
- Framework
- Future directions
- Conclusion
- Questions

Background

Framework

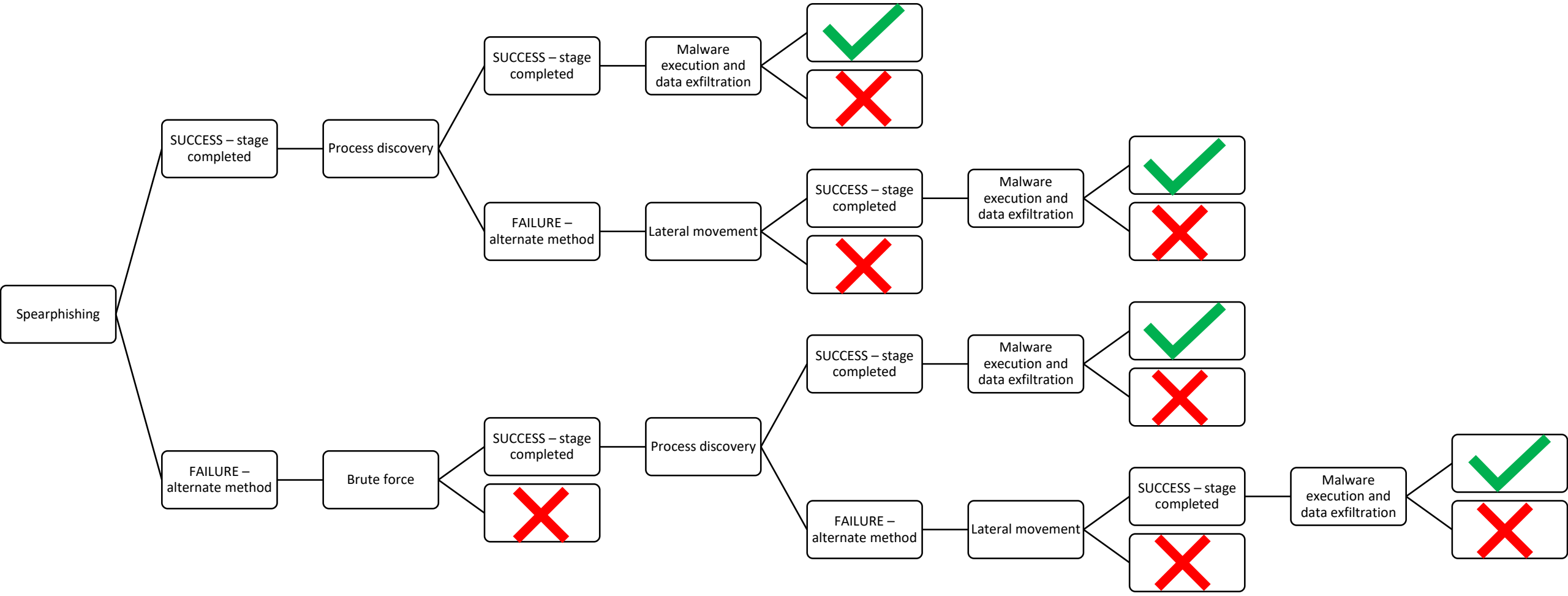
Identify top threats

Research attack methods of threats

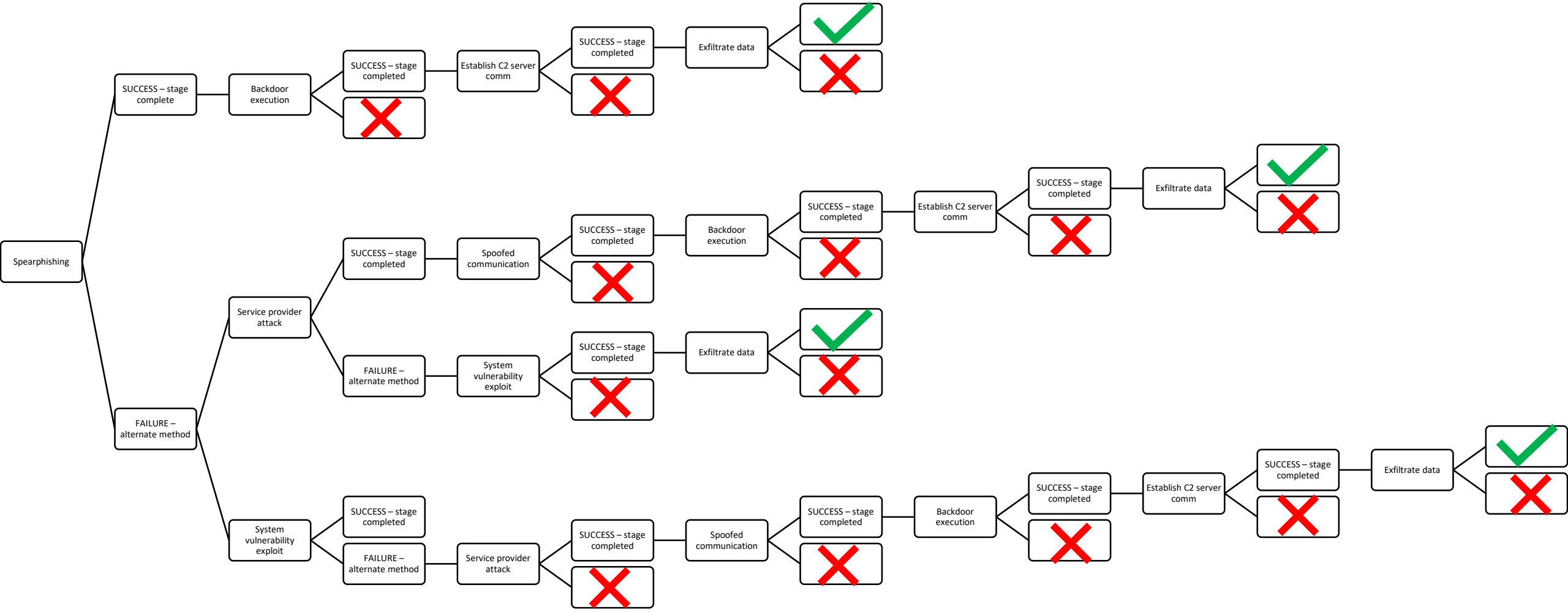
Form decision tree to understand primary and secondary attacks

Synthesize with organizational weaknesses

Turla


Spearphishing
SUCCESS – stage completed
Process discovery
SUCCESS – stage completed
Malware execution and data exfiltration
FAILURE – alternate method
Lateral movement
SUCCESS – stage completed
Malware execution and data exfiltration
FAILURE – alternate method
Brute force
SUCCESS – stage completed
Process discovery
SUCCESS – stage completed
Malware execution and data exfiltration
FAILURE – alternate method
Lateral movement
SUCCESS – stage completed
Malware execution and data exfiltration

APT10


Spearphishing
SUCCESS – stage complete
Backdoor execution
SUCCESS – stage completed
Establish C2 server comm
SUCCESS – stage completed
Exfiltrate data
FAILURE – alternate method
Service provider attack
SUCCESS – stage completed
Spoofed communication
SUCCESS – stage completed
Backdoor execution
SUCCESS – stage completed
Establish C2 server comm
SUCCESS – stage completed
Exfiltrate data
FAILURE – alternate method
System vulnerability exploit
SUCCESS – stage completed
Exfiltrate data
System vulnerability exploit
SUCCESS – stage completed
FAILURE – alternate method
Service provider attack
SUCCESS – stage completed
Spoofed communication
SUCCESS – stage completed
Backdoor execution
SUCCESS – stage completed
Establish C2 server comm
SUCCESS – stage completed
Exfiltrate data

Conclusion

- Framework can be used for prioritization of mitigations
- It can also allow for personalization of corporate policy
- It is not just for APTs!

Questions?

Twitter: @EmilyShawgo

LinkedIn: https://www.linkedin.com/in/emily-shawgo-00ab73100/

References

- (1)Binde, B.E., McRee, R., & O'Connor, T.J. (2017). Assessing outbound traffic to uncover Advanced Persistent Threat. SANS Technology Institute. Retrieved from https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor-slideswnote.pdf
- (2)FireEye Intelligence. (2017, April 06). APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. Retrieved from https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
- (3)ICS-CERT (n.d.). Cyber Threat Source Descriptions. Retrieved from https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
- (4)Lockheed Martin (n.d.). Gaining the advantage: Applying Cyber Kill Chain methodology to network defense. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- (5)MITRE. (n.d.). Group: Turla, Waterbug, WhiteBear. Retrieved from https://attack.mitre.org/wiki/Group/G0010
- (6)MITRE. (n.d). Group: menuPass, Stone Panda, … Retrieved from https://attack.mitre.org/wiki/Group/G0045
- (7)MITRE. (n.d.). Introduction and Overview. Retrieved from https://attack.mitre.org/wiki/Introduction_and_Overview
- (8)Neely, L. (2017). 2017 Threat Landscape Survey: Users on the Front Line. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
- (9)Rapid7. (2017, December 06). Top Threat Actors and Their Tactics, Techniques, Tools, and Targets. Retrieved from https://blog.rapid7.com/2017/05/16/top-threat-actors/
- (10)Rass, S., König, S., & Schauer, S. (2017). Defending Against Advanced Persistent Threats Using Game-Theory. *PLoS ONE*, *12*(1), e0168675. http://doi.org/10.1371/journal.pone.0168675
- (11)Recorded Future. (2017, February 04). Top 6 Sources for Identifying Threat Actor TTPs. Retrieved from https://www.recordedfuture.com/threat-actor-ttp-sources/