Increasing Security in a Resilient Energy Delivery Infrastructure through the Analysis of Vulnerability and Exploit Markets

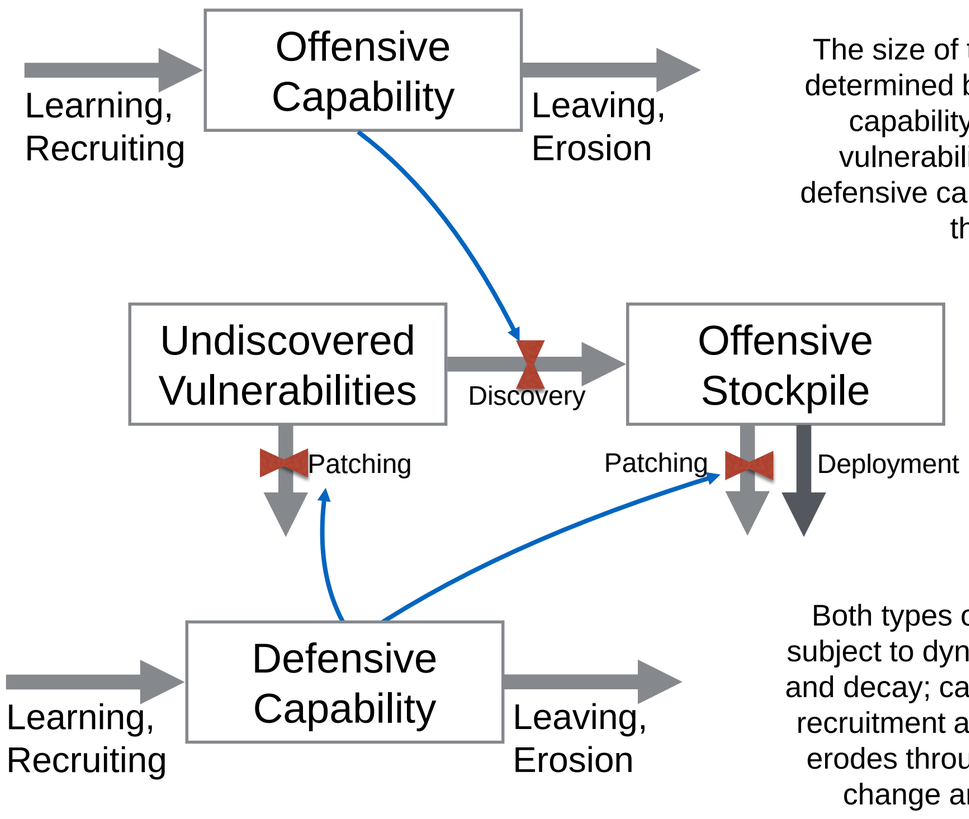
James Houghton and Michael Siegel

INTRODUCTION

- Providing a resilient energy delivery infrastructure requires analysis of the risk exposure, knowledge of the vulnerabilities in the IT and OT organizations, an understanding of the exploit capabilities of potential attackers, and the ability to respond to attacks.
- This work specifically examines the existence of zero-day vulnerabilities in the IT and OT ecosystem. We examine the discovery and stockpiling of these vulnerabilities, and the performance of the "hacker" workforce.
- A number of factors must be in place for a zero-day exploit to be successful. In this analysis, we focus on the prevalence of exploitable vulnerabilities.
- The initial results reveal an understanding of vulnerabilities gained through examination of "bug bounty" programs sponsored by software companies. The next phase of this work will extend those results to improve threat intelligence and reduce the vulnerability in energy delivery systems.

DEVELOPING A DYNAMIC MODEL

- The risk of a zero-day attack is dependent upon the stockpile of exploitable vulnerabilities held by offensive actors.

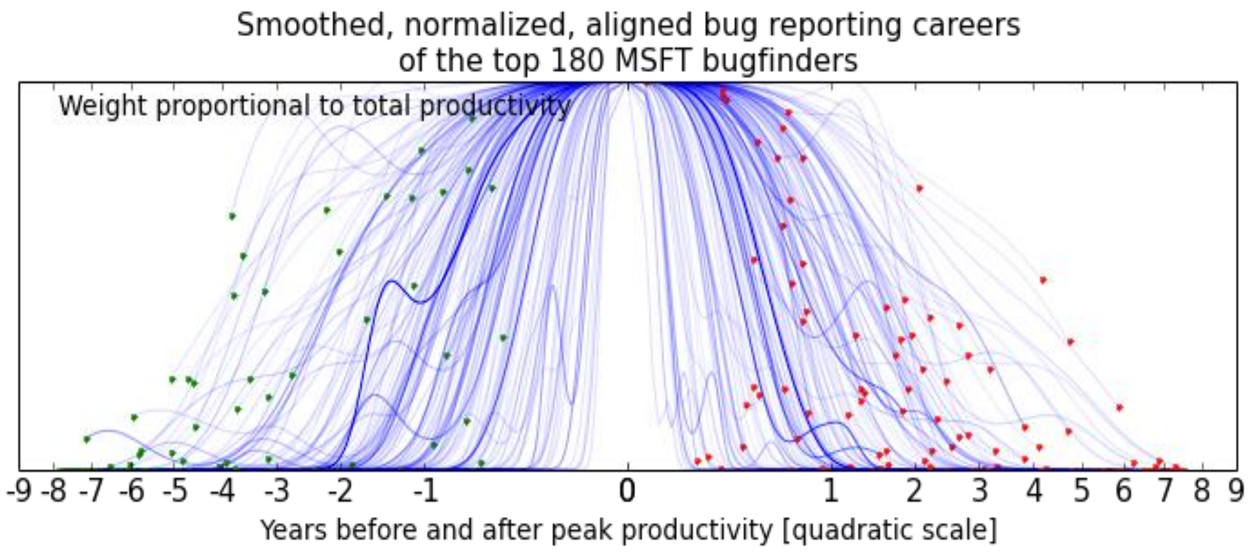


The size of the stockpile is determined by the offensive capability to discover vulnerabilities, and the defensive capability to patch them.

Both types of capacity are subject to dynamics of growth and decay; capacity is built by recruitment and study, and it erodes through technology change and turnover.

INITIAL FINDINGS

- In the archetypical career of a bug finder, he or she grows in productivity over the first 1 to 3 years while developing skills and application knowledge, reaches a peak in productivity, and then skills out or leaves the pool of researchers in just over a year following the peak.

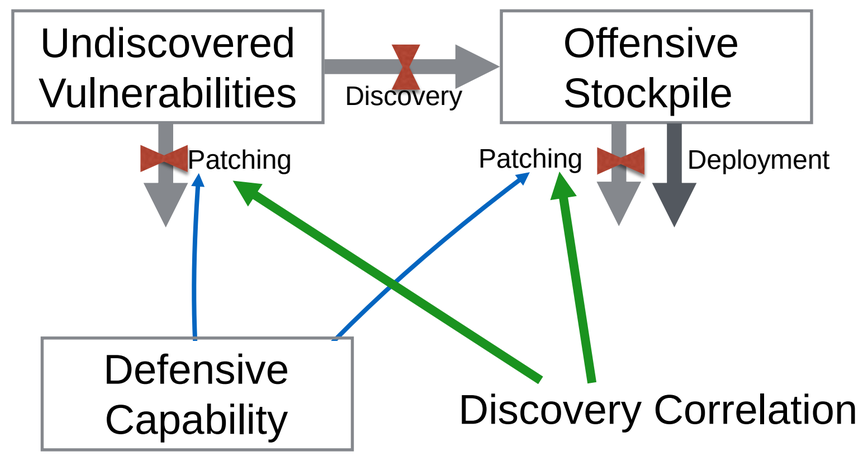


- Bug finders are freelance hackers or researchers who typically receive a monetary reward (or recognition) from the company that receives the vulnerability information.
- Policymakers can work to increase the turnover of offensive actors, or decrease their recruitment and skill development.
- Alternatively, they can focus on improving the capacity of defensive actors.

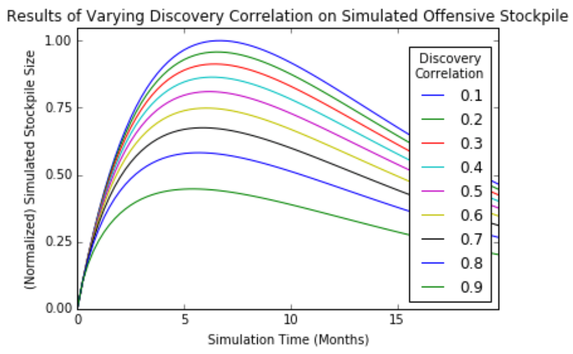
contact: msiegel@mit.edu

SIMULATION ANALYSIS

- An optimal strategy for influencing the system depends on factors such as the capabilities of the offensive and defensive workforce, and the correlation between discovery by defensive and offensive actors.



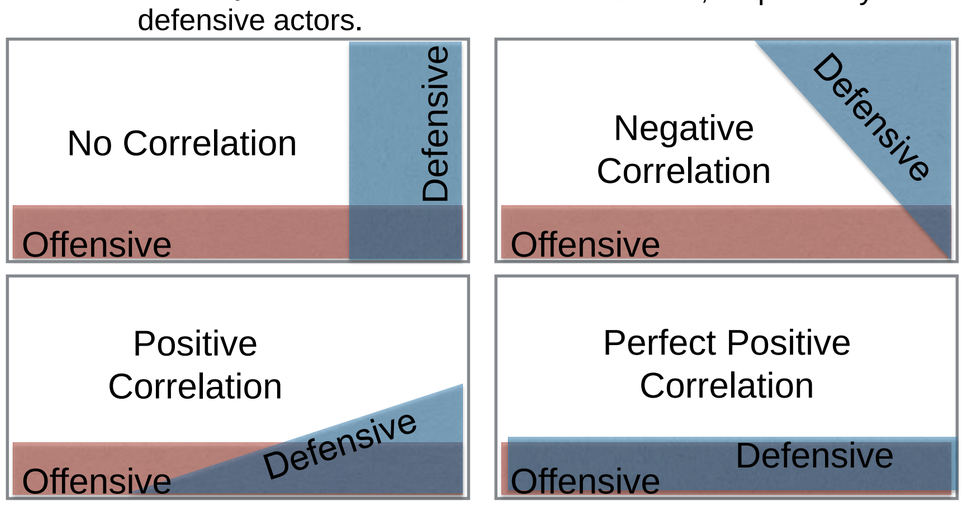
- A reduction in the offensive stockpile (simulation results below) is made possible by increasing the discovery correlation. One can think about this as learning the tools that are used by the offensive actors.



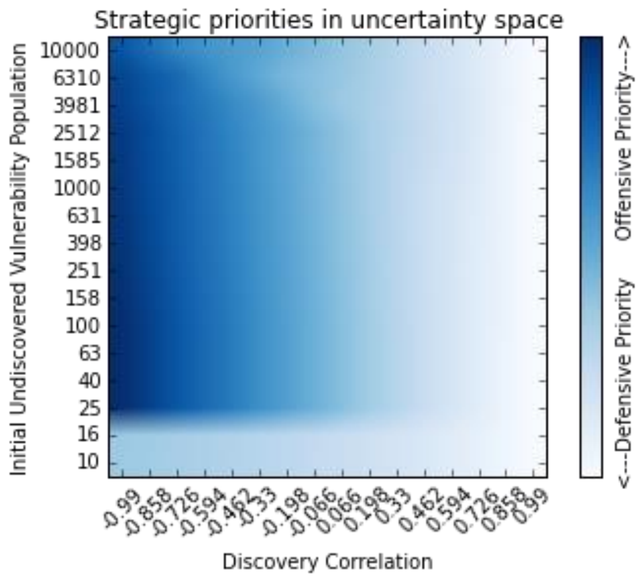
BROADER IMPACT

If exploitable vulnerabilities are discovered in a purely random fashion, we expect no correlation between the vulnerabilities discovered by offensive and defensive actors.

However, if the techniques used by the two groups are markedly similar or unexpectedly different, we expect positive or negative correlation, respectively.



- In the ideal scenario, defensive actors discover all of the exploitable vulnerabilities in the offensive stockpile, and spend no resources on vulnerabilities that remain unfound by offensive actors.
- We can get a rough sense of how the discovery correlation and the initial quantity of vulnerabilities influence our strategy by simulating how small (10%) changes to development of offensive or defensive capabilities influence the end-state number of vulnerabilities.
  - As the correlation between offensive and defensive capabilities declines, the offensive actors are able to increase their stockpile.
  - When there are very few vulnerabilities, the optimal strategy is to prevent them from being discovered by removing them from the initial pool.



FUTURE EFFORTS

- Continue analysis of the security research labor market.
- Examine vulnerability market for EDS.
- Provide implications for threat intelligence.
- Suggest approaches for reducing vulnerabilities in EDS.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY