Small Worlds for Cyber Security (SWCS)

Nicola Bates, supervised by
Konstantinos Markantonakis, Darren Hurley-Smith, Andrew Dwyer

Introduction

My work uses a 'small world' representation of a networked environment. This technique allows defender and attacker dynamics to be systematically changed many times permitting the relative impact on network defence to be observed.

Frameworks used

The attacker profile is modelled based on the Lockheed Martin Cyber Kill Chain comprising the three stages of intrusion and two stages of breach.

A defender profile is modelled on the NIST framework, using the stages of identify, protect, detect and respond.

Scenarios and findings

Five scenarios have been constructed, based on academic findings of the cyber security ecosystem, to demonstrate how the model can be used.

1. Common network set-up

What are impacts of different standard network set-ups?

- Use of defensive settings which observe the attacker for a period are more effective than instant ejection
- Attacks which penetrate through the three security layers instantly are more impactful for the *very high* defender

2. Defender spending:

What spending actions have most impact on defence?

- Tightening security and completing scans at lower levels of the network perimeter has the most benefit for defence
- There comes a point of diminishing returns, when increasing scans across multiple security layers gave little extra defence

3. Attacker resources

How does attacker resource affect outcomes for defenders?

- Increased attacker resource impacts a *low defender* most
- Incorporating machine learning into the attacker resource reallocation redeployed attacks from *low* to *higher defenders*

4. Shared vulnerabilities

Does security of one defender impact others in the network?

- When an attacker reuses a common vulnerability, the *higher defenders* are impacted more relative to the *lower defenders*
- Benefits of very high defence may thus not be fully achieved in a network of common vulnerabilities with low defenders

5. Knowledge sharing:

Are information sharing schemes beneficial to defence?

- Defenders sharing knowledge of detected vulnerabilities with other defenders improves collective security
- The more defenders share knowledge, the higher the security impact

Contact

nicola.bates.2018@live.rhul.ac.uk

Purpose

This approach is designed to improve decision-making by:

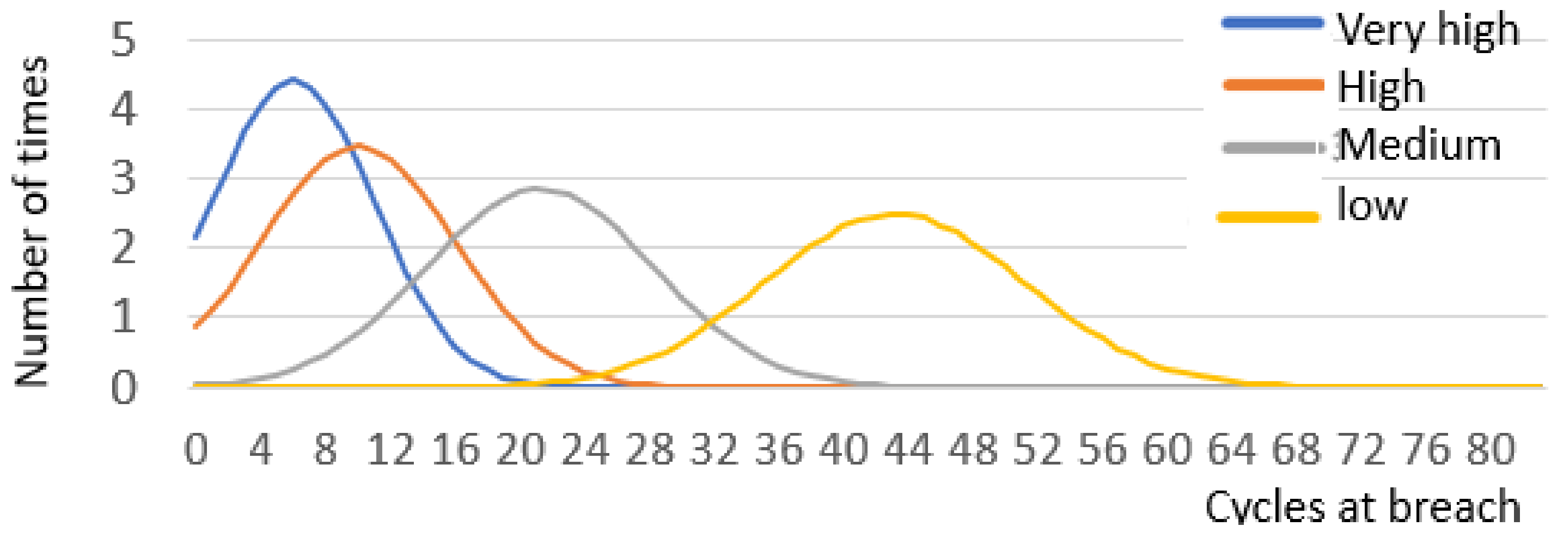
- demonstrating the relationship between defence actions and the impact on security
- providing a modelling method to assess defence investment decisions
- helping to identify how external networks effects can impact security

Model set-up

I have modelled four different levels of defender strength: *very high, high, medium* and *low*. These are differentiated by vulnerability (gap) numbers in their network and how frequently they scan for attacks. Attacker impact on these defenders is shown in graph 1 for the common network set up scenario.

Work has been validated through experts examining the model logic and mathematics and through interviews with cyber security professionals.

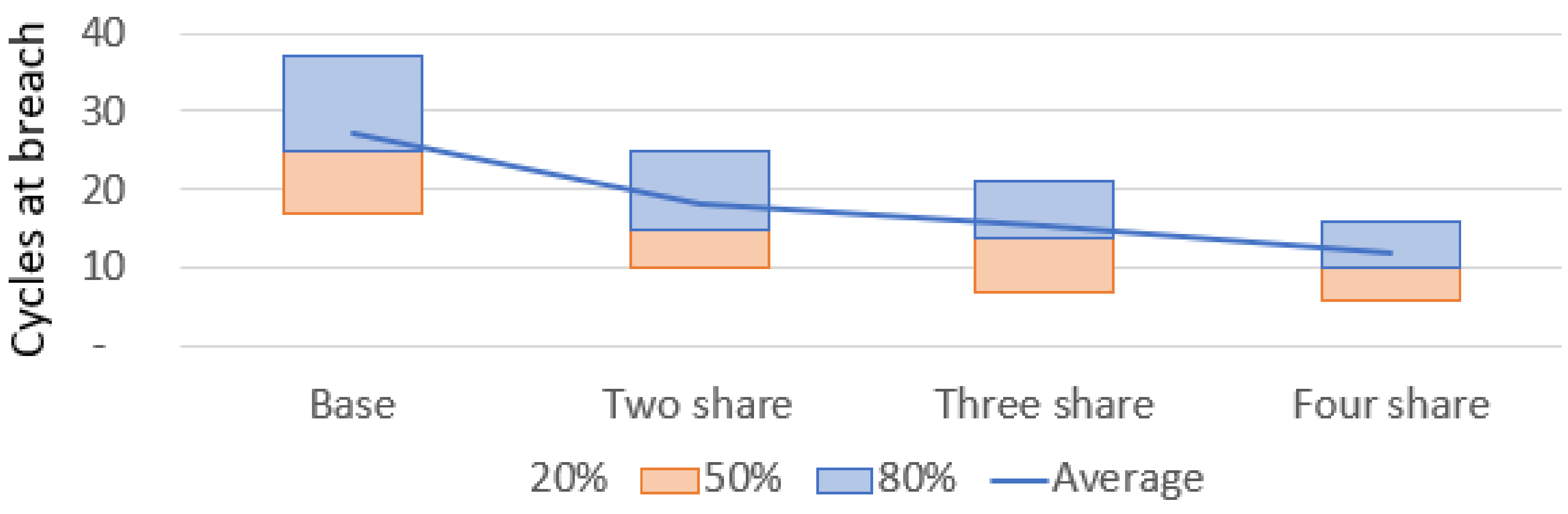
Graph 1: How long an attacker has been at breach in various defenders



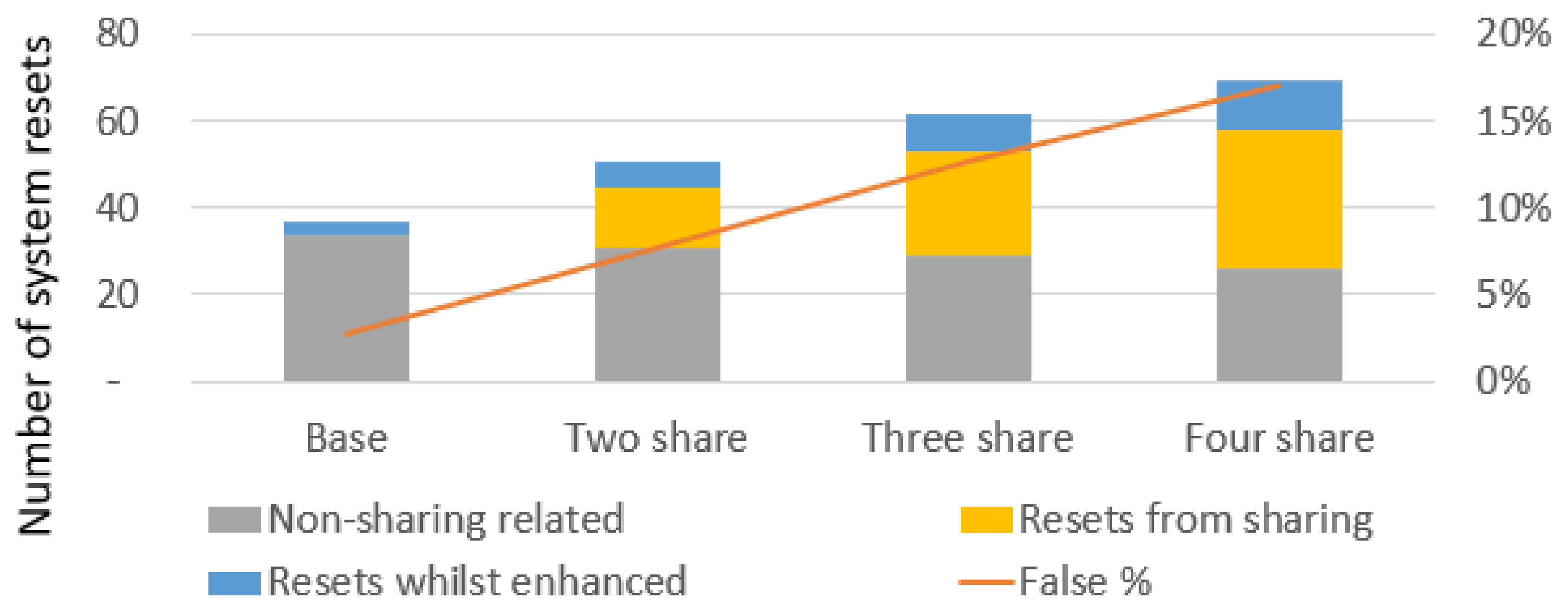
Knowledge sharing

As you increase the level of sharing, the likelihood of the attacker succeeding decreases, as shown in graph 2. The sharing of knowledge, however, also comes with the potential to reset unnecessarily as shown in graph 3.

Graph 2: Number of cycles the attacker has breached the network



Graph 3: Drivers of false alarms and positive resets



Conclusion

Using a small world modelling approach (SWCS) allows us to view a complete picture of a networked system. By adjusting various levers and observing the relative outcome of defenders and the attacker, an indication of these actions within real world situations can be examined quickly and cheaply.