ROYAL HOLLOWAY UNIVERSITY OF LONDON

Small Worlds for Cyber Security (SWCS)

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

The Smart Card and Internet of Things Security Centre

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.

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 the number of vulnerabilities (gaps) in their network and how frequently they scan for attacks.

Five scenarios have been constructed to demonstrate how the model can be used. Work has been validated through experts examining the model logic and mathematics and through interviews with cyber security professionals.

Contact

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

Scenario findings

1. Common network set-up

- 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

- 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 for when increasing scans across multiple security layers gave little extra defence

3. Attacker resources

- With increased attacker resource the *low defender* was most impacted
- Incorporating machine learning into the attacker resource reallocation redeployed attacks from *low* to *higher defenders*
- Higher defenders in a networked environment with lower defenders become more vulnerable through the attacker redeploying resources

4. Shared vulnerabilities

- When an attacker reuses a common vulnerability, the *higher defenders* are impacted more relative to the *lower defenders – the* impact on *higher defenders* is even more with attacker resource reallocation
- Benefits of very high defence may thus not be fully achieved if others in the network have low defences and share common vulnerabilities

5. Knowledge sharing

- Defenders sharing knowledge of detected vulnerabilities with other defenders improves collective security
- The more defenders share knowledge, the higher the security impact
- The increased security gained from knowledge sharing acts to reduce the ability of the attacker to increase resources for further attacks

Frameworks used

The attacker stages are based on the Lockheed Martin Cyber Kill Chain (figure 1), with defender alignment to the NIST framework (figure 2).

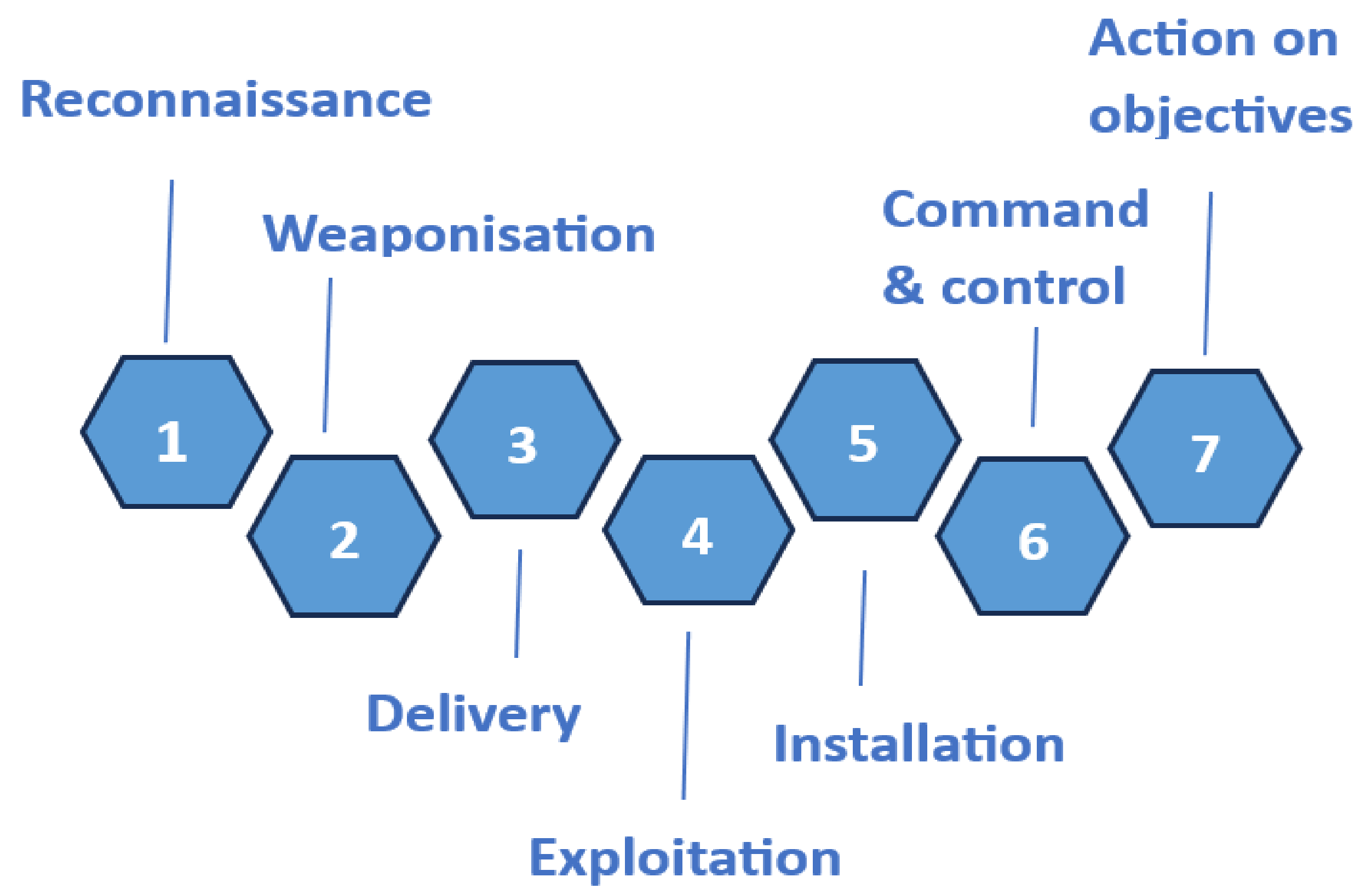

Figure 1: Cyber Kill Chain, source: www.lockheedmartin.com

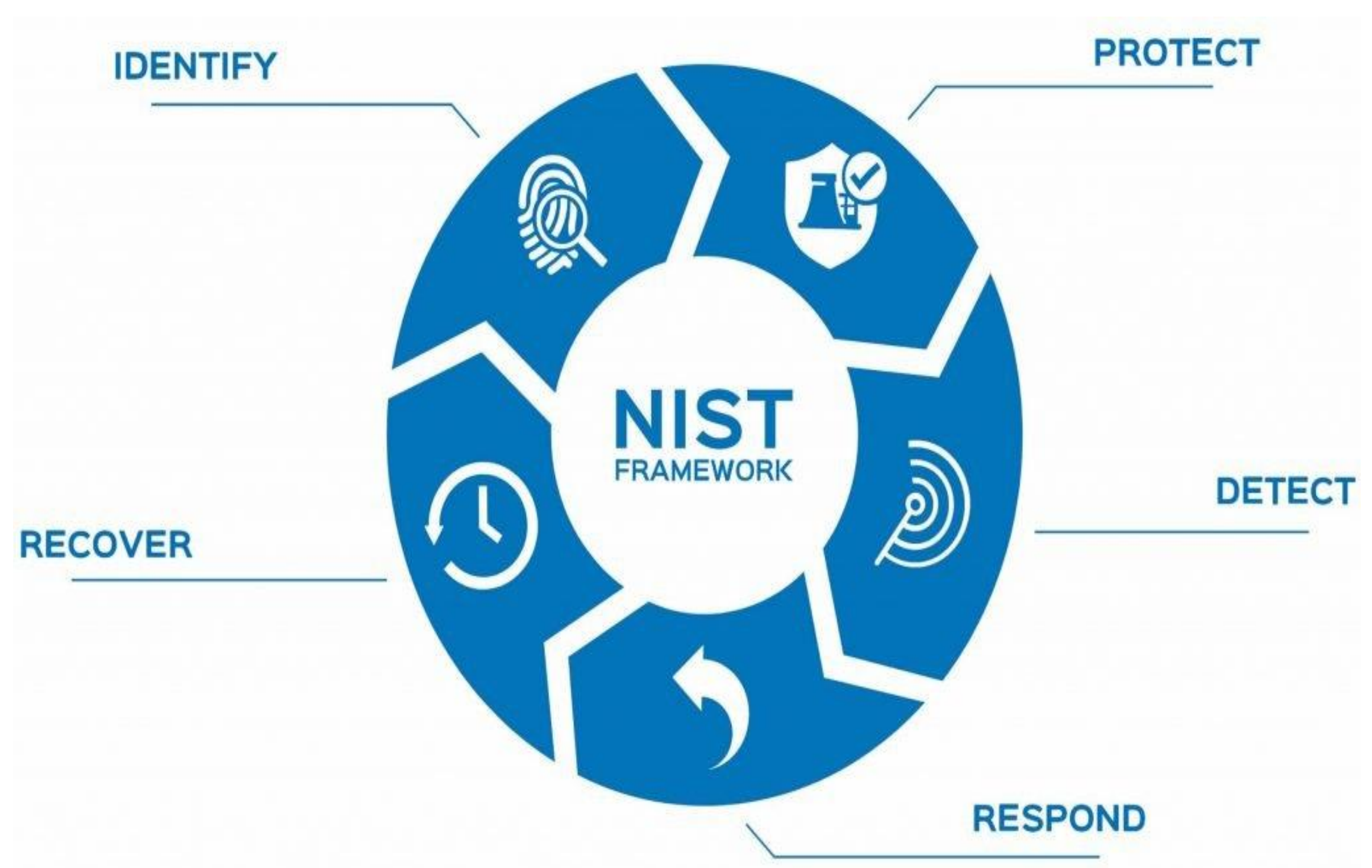

Figure 2: NIST cyber security framework, source: www.nist.gov

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.