Using decision science to model potential impacts of network effects in below threshold UK cyber deterrence

Nicola Bates – Supervised by Konstantinos Markantonakis
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objective

To determine how quantitative modelling can aid understanding of cumulative networked effects in the cyber domain in order to inform defence and deterrence decision making.

Introduction

Work focuses on situations in which attacks fall below thresholds of armed conflict but could in large numbers have strategic effects. Decision science is used to find the most appropriate way to solve this problem.

What is decision science?

Decision science is used for finding the best analytical method for understanding a system or solving a specific problem. It can be thought of as a series of steps, being:

- Break the system/problem down into subsystems to find how it works. What are the drivers, inputs, outputs, connections.
- Understand the drivers of the subsystems, the links between inputs and outputs.
- Understand the level of analysis needed to determine the most suitable method.
- Apply this method to model the system.
- Stress test the analytical model with various scenarios to determine reactions to alterations

Model

Modelling the attacker / defender interactions has been performed by converting these into a series of discrete steps to which probabilities of success can be applied.

The model is set up with an attacker having to penetrate three layers of network defences, each with a different number of vulnerabilities. The vulnerabilities in the model are generic and can represent ports or people.

Figures 1 and 2 represent a single attacker and a single defender model which run independently in a turn-based manner.

Approach

The attack landscape is being modelled using a probabilistic approach within a weak Markov Chain model. This is one where the next actions at each stage are influenced by limited historical knowledge. This permits rapid iteration and multiple scenarios to be run efficiently.

The numbers in the model are designed to allow probabilistic modelling to be carried out efficiently and multiple scenarios to be run to create a risk-based expectation value.

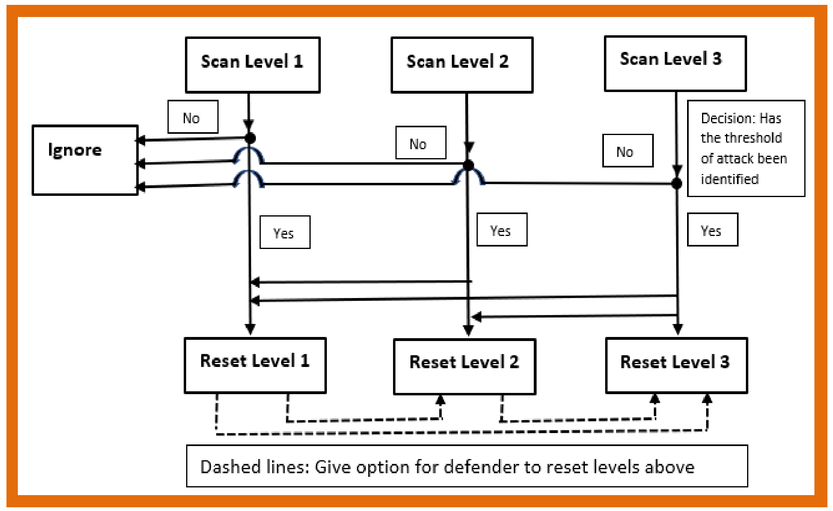

Figure 1: Defender Loop

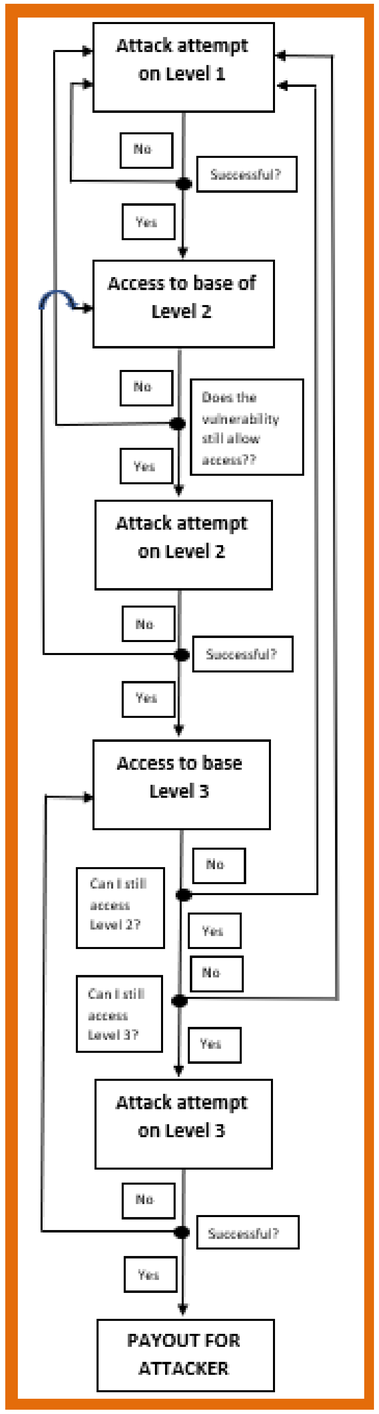

Figure 2: Attacker Loop

Attacker and Defender KPIs

To model impacts of an attack systems thinking has been applied to identify a set of Key Performance Indicators (KPI's) and the actions they will likely drive for both the attacker and defender. These will be tracked at the end of each attack cycle.

Defender KPI	Attacker KPI
Level of system penetrated (days)	Level of system penetrated (days)
Cost of network security	Number of attempts to access next level of systems
Times attacker caught	Times caught
Times attacker successful	Cost of being caught
Value of payload achieved	Value of payload expected
	Value of payload achieved
	Cost per attack cycle

Adding complexity

This single attacker / defender model will be built upon to incorporate further complexity, for example, network effects such as shared vulnerabilities across targets and sharing of attack information between targets.

Through running multiple scenarios this will identify how factors such as defenders sharing of attack information will impact KPIs.

Final model outputs will form the basis of discursive analysis on relative impact different strategies can have on mitigating attacks.

Contact

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