Using systems thinking to model cyber defence strategies within the UK

Nicola Bates, Information Security Group, Supervised by:
Konstantinos Markantonakis, Darren Hurley-Smith, Andrew Dwyer

The Smart Card and Internet of Things Security Centre

Objective

This work uses systems thinking to model cyber defence within networks. Different approaches within cyber defence are simulated to provide insight into how different choices affect network defence.

What is systems thinking?

"Systems thinking is a framework for seeing the interconnection in a system and a discipline for seeing and understanding the relevant aspects of the whole system – the 'structures' that underlie complex situations.", see figure 1.

For modelling steps completed are:

- System/goal broken down into subsystems to find how it works.
- Drivers of the subsystems understood.
- Level of analysis needed determined.
- Analysis method used to model the system.
- Analytical model stress tested with various scenarios to find reactions to alterations

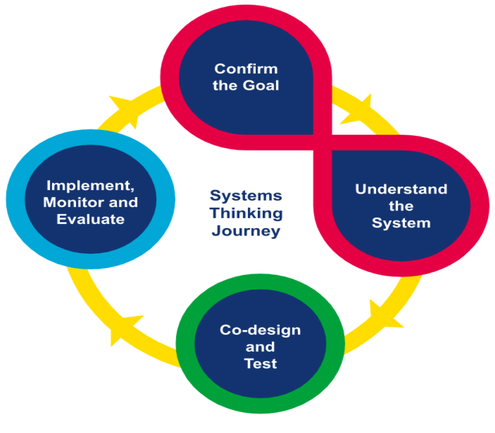

Figure 1:Systems thinking stages for complex problems
Source: Introduction to systems thinking for civil servants. Jan 2023

The model

Attacker and defender interactions are modelled by converting these into a series of discrete steps. An attacker is modelled as having to penetrate three layers of network defences containing vulnerabilities with a defenders able to run network scans and implement honey pots and traps. Attacker and defender stages run independently in a turn-based manner.

The model covers the intrusion and active breach stage of the cyber kill chain (a framework explaining how attackers move through a network, see figure 2) but not attacker preparation.

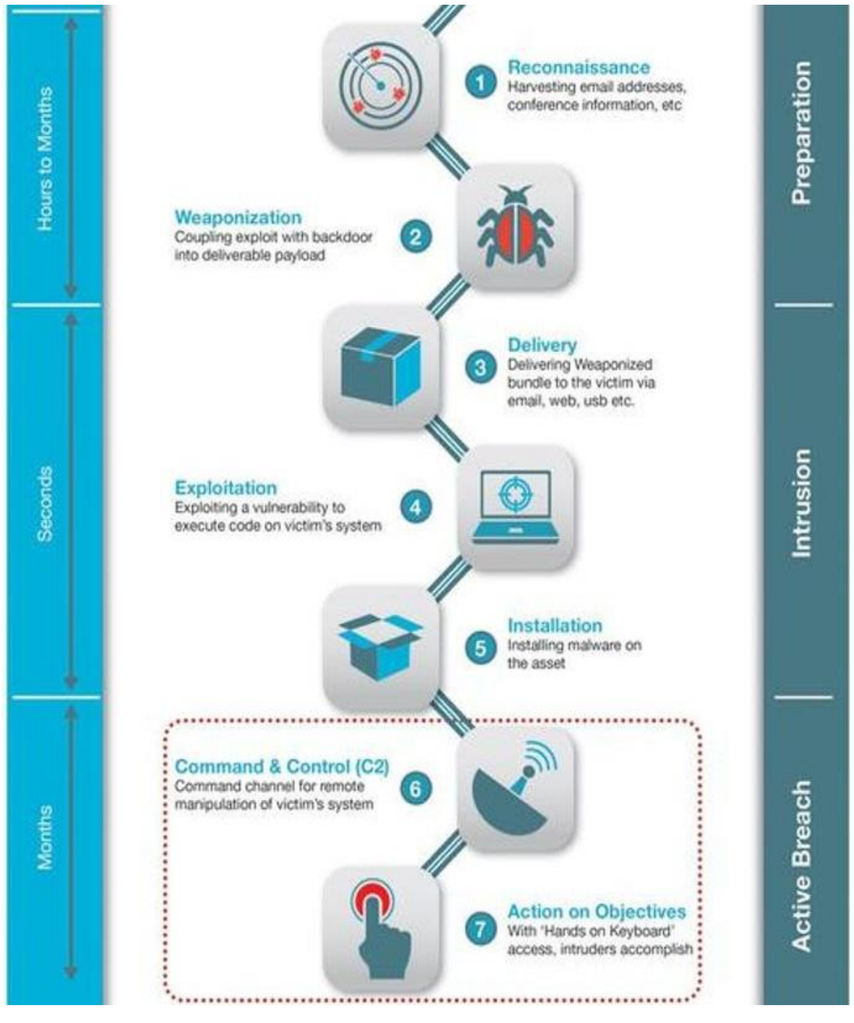

Figure 2 Stages of the cyber kill chain
Source: Lightcyber, now part of Palo Alto Networks

Key Results

1. Quantitative model for cyber defence completed using systems thinking methods.
2. Model linkages and assumptions validated through expert input into processes used.
3. Model outcomes presented to decision makers for discussion in scenario format.

Modelling approach

The attack landscape is modelled within excel using a probabilistic approach. A Markov Chain model is implemented, where the next actions at each stage is 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.

Scenarios

To aid decision maker understanding four scenarios have been created. Story telling narratives makes data derived from modelling clearer and more relatable. Scenarios used are:

1. Defender spending changes
2. Knowledge sharing amongst defenders
3. Use of honey traps and penalty traps
4. Defender links through spending variability

Contact

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