CASE STUDY

DECAAS: CYBER DECEPTION AS A SERVICE

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

PROJECT SNAPSHOT

This project uses cutting-edge machine learning (ML) algorithms and artificial intelligence (AI) to detect and trap intruders and data thieves.

WHO'S INVOLVED

This project is a collaboration between the Cyber Security CRC, CSIRO's Data61 and Penten. The research lead for the DecaaS project is Kristen Moore.

WHAT'S THE ISSUE?

Individuals and organisations make significant investments in cyber security to protect their businesses, but many still fall victim to cyber attacks, breaches and data theft.

Most existing cyber defence solutions are reactive and unable to deal with sophisticated attacks. They generate many alerts, often far more than can be investigated. Since the prioritisation and classification of alerts remains a challenge, this can lead to breaches being missed due to 'alert fatigue' among workers.

Cyber deception presents a novel way to mitigate some of these issues by providing an intrusion detection approach with an inherently low false alarm rate. It works by setting up decoys to trap attackers. The decoys are deceptive versions of IT assets that mimic the real objects. Since a legitimate employee of an organisation has no use for the fake content, any interaction with the deceptive environment is a strong signal of a breach.

The uptake of cyber deception has been previously impeded by the difficulty of generating realistic deceptive content. As cyber threats increase in volume and sophistication, ML and AI offer an opportunity to assist overwhelmed human cyber defenders and speed up decision making and response. Recent advances in ML mean it is now possible to simulate many IT assets, providing an opportunity for the development of new cyber deception technology.

WHAT WERE THE OBJECTIVES?

Develop cyber deception technology to automate the creation of realistic decoys which involves ML approaches including:

- generating rich and believable deceptions,
- simulating the behaviour of people and their interactions within the system
- developing metrics to measure how enticing and realistic the generated deceptive content is to attackers.
- create technology that will speed up decision making and responses for defenders

TECHNOLOGY DESCRIPTION

Deception technology is an emerging category of cyber security defence. It can detect, analyse and defend against zero-day and advanced attacks, often in real time.

Traps (decoys) can be IT assets that either use real operating system software or are emulations of these devices.

Upon penetrating a network, attackers seek to establish a 'backdoor' and then use this to identify and exfiltrate data and intellectual property. They begin moving through the network and ideally come across one of the traps. Interacting with one of the decoys will trigger an alert.

APPLICATION

The DecaaS project team is developing a suite of technologies that can generate a variety of deceptive artefacts including source codes, documents, database schema, and network communications such as email and WiFi. Parts of this technology have been made open source, such as HoneyCode, while the deceptive communication technology is being patented.

Outside of deception, our researchers have discovered additional uses for generated content and behaviours. Specifically, these technologies are increasingly used in a host of simulation activities. For example, cyber range environments rely on content generation to make each environment distinct and convincing. Cyber ranges have some important applications, including capability development, and security research, testing and education.