UNSW
Institute for
Cyber Security

Deception for Advanced Cyber Defence

Cyber Deception technologies are an increasingly valuable tool for network defenders, but they are still in their infancy in terms of what they could potentially offer.

Manoeuvring to take back control

Cyber deception is an active way to defend a network by rendering it a hostile environment to an attacker. Deception techniques operate once the attacker has bypassed the perimeter defences and gained access to a network, endpoint, operating system, or application. Once inside, deception technology attempts to mislead, confuse, and expose the attacker by causing them to unwittingly reveal sufficient information about their methods so they can be efficiently purged, or by causing fear and uncertainty such that they abandon their attack.

When perimeter defences fail - and they will - effective deception systems mean that attackers cannot distinguish true data from decoy data and unwittingly trigger alerts. This allows network defenders to gather information about the attackers' tools, tactics, and procedures.

There are difficulties though in deploying cyber deception technologies - such as knowing where best to place them on a network or how to develop a playbook of deception strategies and campaigns. One way our research aims to help work through these issues is to start from the original premise of deception as a human activity that aims to cause 'erroneous sensemaking' so that an attacker changes their behaviour allowing the defender to gain an advantage (Henderson, 2011).

An inflatable decoy tank.

Emerging research indicates that cyber attackers are, like all of us, vulnerable to decision-making biases (Gutzwiller et al., 2019) and yet in the majority of cyber deception research the attackers' decisionmaking processes are often missing or, at best, the attacker is assumed to be a rational actor. In contrast, research into human decision-making across multiple domains frequently emphasises the tendency for people to make so-called 'irrational' decisions, particularly when they are under pressure. The field of Behavioural Economics holds that these quick decisions, although technically suboptimal, are often an efficient trade-off between accuracy and speed, and are therefore measurable and predictable (Gutzwiller, Ferguson-Walter, &Fugate, 2019).

This is a perfectly flat floor tiled to look as if it is undulating to ensure that people walk rather than run.

Fusing Behavioural Science with Deception

By taking human behaviour and decision-making as the starting point for our research we can broaden the scope of cyber deception to encompass the space from the defender's cognitive processes through to the attacker's cognitive processes. We aim to better understand erroneous sensemaking, quick thinking shortcuts, and decision-making biases that, like all humans, will be operating in the mind of the attacker. Once understood, these cognitive vulnerabilities could be leveraged by deception techniques to encourage the attacker to make mistakes, act quickly without considering all angles, reveal their methods, and question their situational awareness in the network.

From Indiana Jones to Network Defence

One way to ideate novel applications of cyber deception technology is to use culturally salient examples of deception as a metaphor to plan a cyber deception campaign. For example, many people are familiar with the narrative from the classic film Indiana Jones and The Last Crusade, in which Indiana Jones must deal with a series of protective booby traps to find the Holy Grail. The true Grail is hidden amongst hundreds of other potential grails, all of which fatally poison the person who drinks from it. This idea of multiple potential grails is the equivalent of the cyber deception technique of hay-stacking (for example, hiding real database entries amongst vast numbers of fake entries).

It is also similar to honeypots and honey tokens, which attempt to lure attackers by mimicking the appearance of valuable content (such as a database of clear-text passwords). When accessed, these honeypots alert the security team to the presence of the attacker.

What does this research mean?

This research will produce evidence based decision support tools in the form of a planning process for use in Defence Security Operating Centres (SOCs). This tool will give SOCs a road map for how to best integrate deception technologies into their networks and how to feedback the resultant attack data to the SOC team. This will expand into a validated technology toolkit for delivering behavioural science informed cyber detection on a network as part of an active defence strategy. Future work will produce a proof-of-concept demonstrator for how AI/ML can contribute.

Key References

Ashenden, D., Black, R., Reid, I., & Henderson, S. (2021, January). Design Thinking for Cyber Deception. In Proceedings of the 54th Hawaii International Conference on System Sciences (p.1958).

Gutzwiller, R. S., Ferguson-Walter, K. J., & Fugate, S. J. (2019). Are Cyber Attackers Thinking Fast and Slow? Exploratory Analysis Reveals Evidence of Decision- Making Biases in Red Teamers. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 427-431. doi:10.1177/1071181319631096

Henderson, S. (2011). Deceptive Thinking Workshop. Paper presented at the 1st MilDec Military Deception Symposium, Defence Academy of the United Kingdom, Shrivenham.

Further enquiries

Professor Debi Ashenden
UNSW IFCYBER Director

ifcyber@unsw.edu.au
ifcyber.unsw.edu.au

UNSW

CRICOS 00098G | 4180486